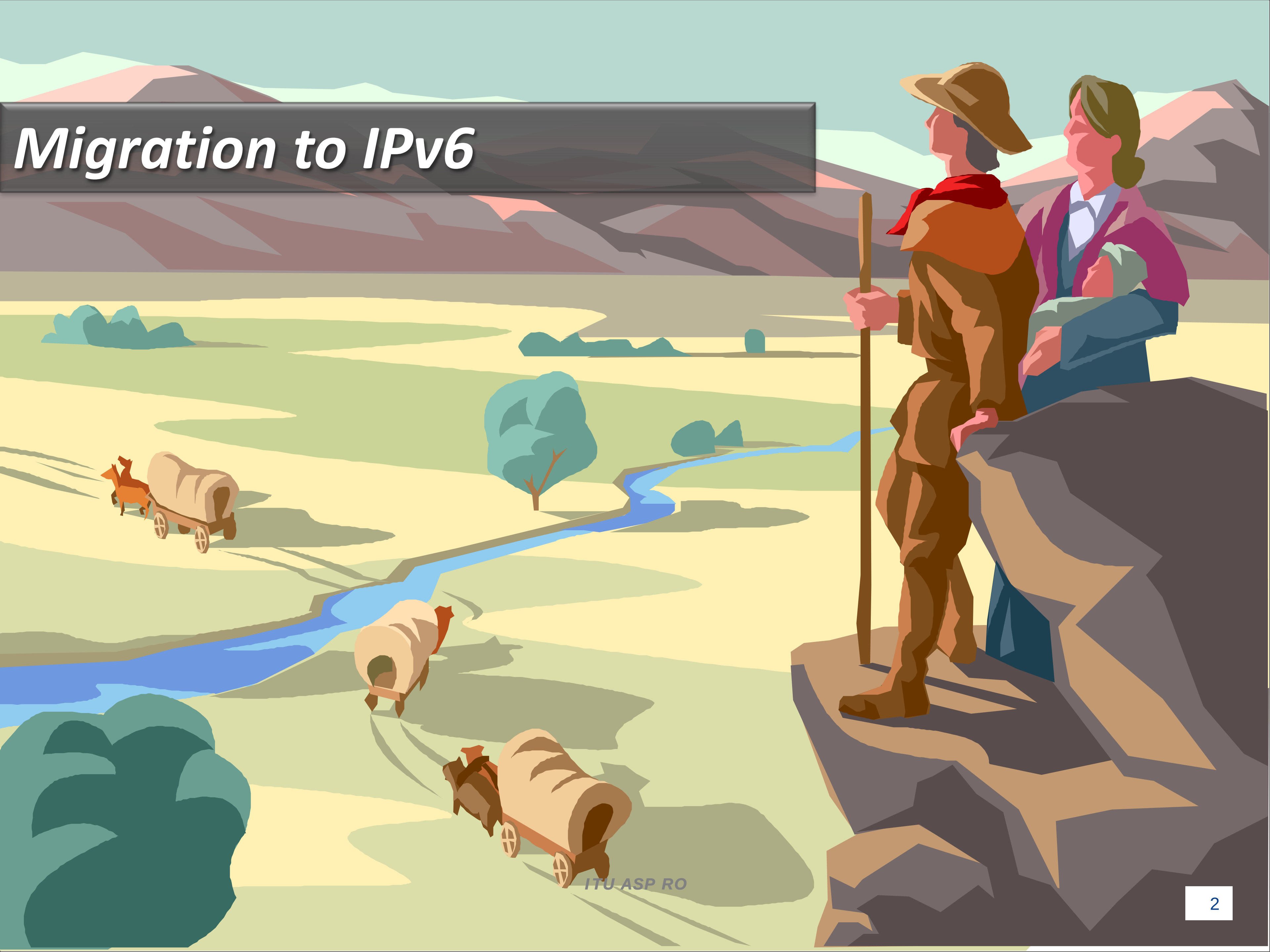
Role of Policy maker and Regulator in IPv6 Migration

ITU Asia-Pacific CoE Training on “IPv6 Infrastructure Security”
22-26 June, 2015
Bangkok, Thailand

Ashish Narayan, Programme Coordinator,
ITU Regional Office for Asia and the Pacific

Migration to IPv6



OSI MODEL	PROTOCOLS	IDENTIFYING ADDRESS
Application	HTTP, SMTP etc.	Port Address and IP Address (or Domain name)
Presentation		
Session		
Transport	TCP or UDP	IP Address or Domain name
Network	IP	
Data Link	Ethernet	MAC Address
Physical		

Understanding Naming and Addressing

	Name (Source – Destination independent)	**Address** (Source independent – Destination dependent)
 Fixed Telephone	**E.164 Number**	**Q.708 ISPC**
 Mobile Telephone	**E.164 Number**	**E.212 IMSI**
 Internet	**Domain Name**	**IP Address**

Promoting Efficiency in Allocation of IP Addresses

32 bit address space allocated

- 256 Networks, 16 Million Hosts each

Network Class Based Architecture

- Class A (128 Networks, 16 Million Hosts each)
- Class B (16384 Networks, 65,535 Hosts each)
- Class C (4 Million Networks, 255 Hosts each)

Classless Inter-Domain Routing

- Variable length network portion in the address

Use of Restrictive Policy by RIR for allocation

Taking into account: -

- Scarcity of IPv4 Addresses
- Need to Maximize Aggregation
- Limit Routing Table Growth

Migration from IPv4 to IPv6

- 128 Bits,
- 3.4 X 10 ^38 Addresses

ITU and IPv6…………

ITU and IPv6

RESOLUTION 101 (REV. BUSAN, 2014)
Internet Protocol-based networks

RESOLUTION 180 (REV. BUSAN, 2014)
Facilitating the transition from IPv4 to IPv6

PP14
BUSAN
KOREA

RESOLUTION 63 (Rev. Dubai, 2014)
IP address allocation and facilitating the transition to IPv6 in the developing countries
ASIA-PACIFIC REGIONAL INITIATIVE 3
Harnessing the benefits of new technologies

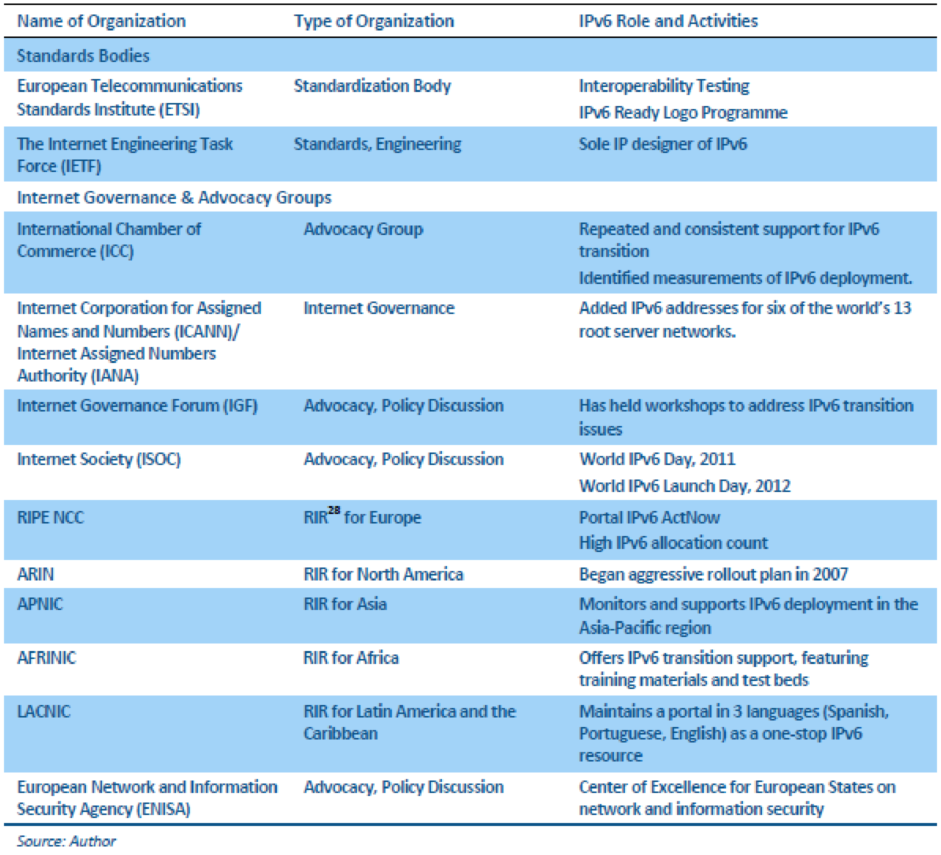
RESOLUTION 64 (REV. DUBAI, 2012)
IP address allocation and facilitating the transition to and deployment of IPv6

WTSA2012
Dubai, UAE
World Telecommunication Standardization Assembly
20-29 NOVEMBER 2012

ITU COUNCIL

ITU-T and ITU-D STUDY GROUPS

CAPACITY BUILDING AND MEMBER ASSISTANCES



Name of Organization	Type of Organization	IPv6 Role and Activities
Standards Bodies		
European Telecommunications Standards Institute (ETSI)	Standardization Body	Interoperability Testing IPv6 Ready Logo Programme
The Internet Engineering Task Force (IETF)	Standards, Engineering	Sole IP designer of IPv6
Internet Governance & Advocacy Groups		
International Chamber of Commerce (ICC)	Advocacy Group	Repeated and consistent support for IPv6 transition Identified measurements of IPv6 deployment.
Internet Corporation for Assigned Names and Numbers (ICANN)/ Internet Assigned Numbers Authority (IANA)	Internet Governance	Added IPv6 addresses for six of the world's 13 root server networks.
Internet Governance Forum (IGF)	Advocacy, Policy Discussion	Has held workshops to address IPv6 transition issues
Internet Society (ISOC)	Advocacy, Policy Discussion	World IPv6 Day, 2011 World IPv6 Launch Day, 2012
RIPE NCC	RIR[28] for Europe	Portal IPv6 ActNow High IPv6 allocation count
ARIN	RIR for North America	Began aggressive rollout plan in 2007
APNIC	RIR for Asia	Monitors and supports IPv6 deployment in the Asia-Pacific region
AFRINIC	RIR for Africa	Offers IPv6 transition support, featuring training materials and test beds
LACNIC	RIR for Latin America and the Caribbean	Maintains a portal in 3 languages (Spanish, Portuguese, English) as a one-stop IPv6 resource
European Network and Information Security Agency (ENISA)	Advocacy, Policy Discussion	Center of Excellence for European States on network and information security

Source: Author

- ***Collaboration between ITU and relevant Organisations***
- ***Raising awareness and human capacity building***

- e.g. ITU , APNIC, MICT Thailand, Others

- ***Assist Member States with existing IPv6 management and allocation policies***

-e.g. ITU APNIC assistance in Asia-Pacific

- ***Undertake detailed studies of IP address allocation…, both for IPv4 and IPv6***
- ***Technical Standards***

ITU-T Study Groups and IPv6

Study Group 2

Operational aspects of service provision and telecommunications management

Study Group 3

Tariff and accounting principles including related telecommunication economic and policy issues

Study Group 13

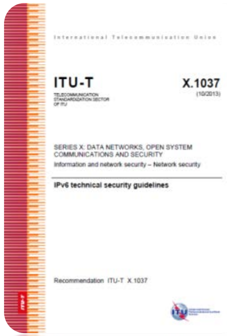
Future networks including mobile and NGN

Study Group 16

Multimedia coding, systems and applications

Study Group 17

IPv6 Security



International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1037

(10/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

IPv6 technical security guidelines

Recommendation ITU-T X.1037

Source: http://www.itu.int/net/ITU-T/ipv6/itudocs.aspx

IPv6 Related ITU-T Recommendations

Rec. ITU-T Y.2051 - General overview of IPv6-based NGN
Rec. ITU-T Y.2052 - Framework of multi-homing in IPv6-based NGN
Rec. ITU-T Y.2053 - Functional requirements for IPv6 migration in NGN
Rec. ITU-T Y.2054 - Framework to support signaling for IPv6-based NGN
Rec. ITU-T X.1037 - IPv6 technical security guidelines

International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

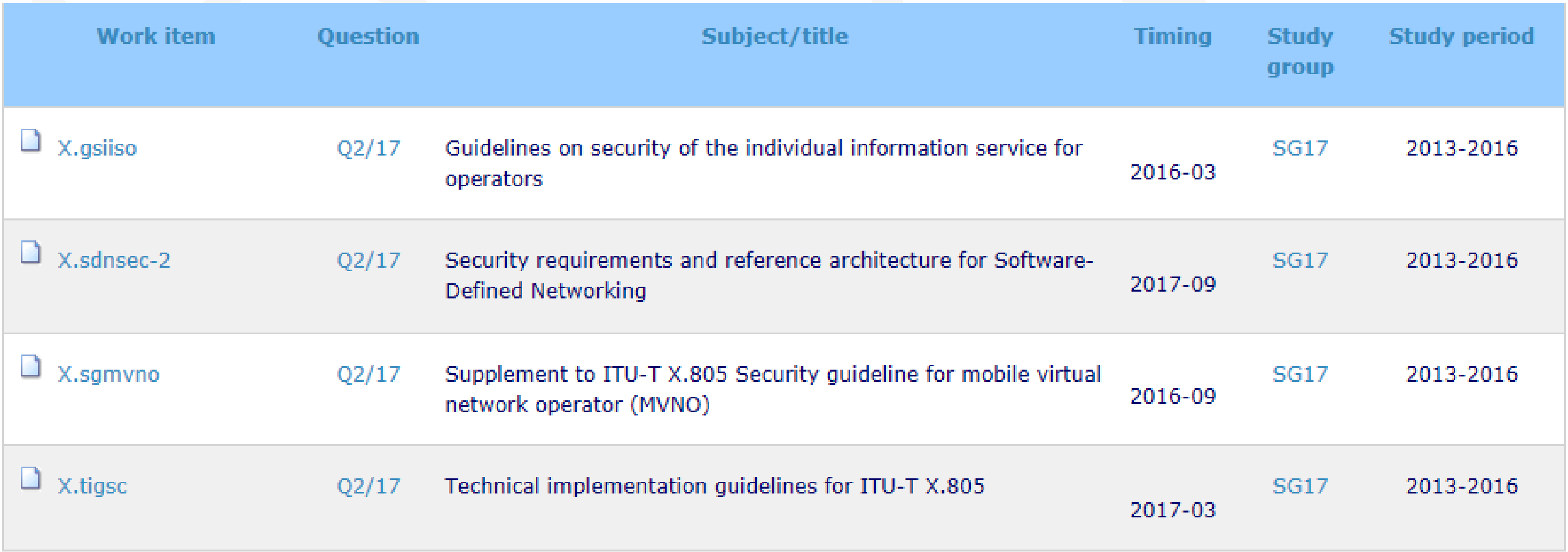
X.1037
(10/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Information and network security – Network security

IPv6 technical security guidelines

Recommendation ITU-T X.1037

ITU-T related work on IPv6 Security (ongoing)



Work item	Question	Subject/title	Timing	Study group	Study period
X.gsiiso	Q2/17	Guidelines on security of the individual information service for operators	2016-03	SG17	2013-2016
X.sdnsec-2	Q2/17	Security requirements and reference architecture for Software-Defined Networking	2017-09	SG17	2013-2016
X.sgmvno	Q2/17	Supplement to ITU-T X.805 Security guideline for mobile virtual network operator (MVNO)	2016-09	SG17	2013-2016
X.tigsc	Q2/17	Technical implementation guidelines for ITU-T X.805	2017-03	SG17	2013-2016

Source: http://www.itu.int/net/ITU-T/ipv6/itudocs.aspx

Migration to IPv6: Building Roadmaps, Action Plans

General Approach

- Policy Announcements
- Creation of IPv6 Task Force
- Encouraging IPv6 deployment in government
- Standards, Pilot tests, Interoperability etc.
- Awareness and Capacity Building
- Measuring Deployments and Tracking Progress

Key elements of government action

Key elements of governmental action have included:

- Establishing or supporting national IPv6 transition task forces (often in conjunction with multistakeholder groups or RIRs);

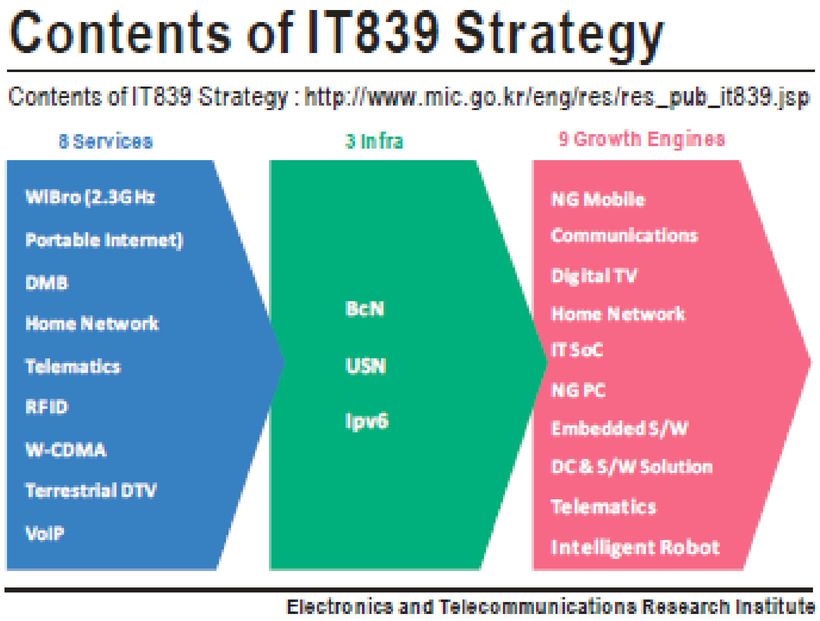
- Establishing national “roadmaps” with benchmarks and timetables for IPv6 deployment;

- Mandating that government agencies adopt IPv6 technology for their networks, websites or services;

- Promoting the use of IPv6 in government-funded educational, science and research networks; and

- Promoting overall awareness of the transition through setting up websites, hosting workshops or forums, and setting up training programmes.

Governments promoting IPv6 deployment (examples)

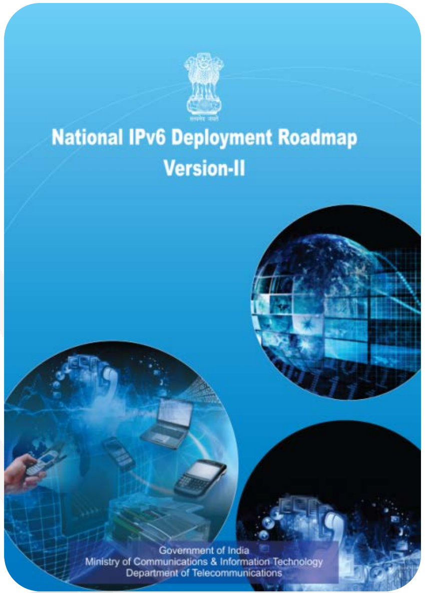


Contents of IT839 Strategy

Contents of IT839 Strategy : http://www.mic.go.kr/eng/res/res_pub_it839.jsp

8 Services	3 Infra	9 Growth Engines
WiBro (2.3GHz Portable Internet) DMB Home Network Telematics RFID W-CDMA Terrestrial DTV VoIP	BcN USN Ipv6	NG Mobile Communications Digital TV Home Network IT SoC NG PC Embedded S/W DC & S/W Solution Telematics Intelligent Robot

Electronics and Telecommunications Research Institute



National IPv6 Deployment Roadmap
Version-II

Government of India
Ministry of Communications & Information Technology
Department of Telecommunications

Taiwan, Republic of China, has announced a USD 1 billion budget for its "eTaiwan" programme, which entails a concerted joint effort between government and industry. The goal is to reach 6 million broadband users of IPv6 technology.

Governments promoting IPv6 deployment (examples)

Spain – the GEN6 programme is developing pilot projects to integrate IPv6 into government operations and cross-border services to address emergency response or EU citizens' migration issues.

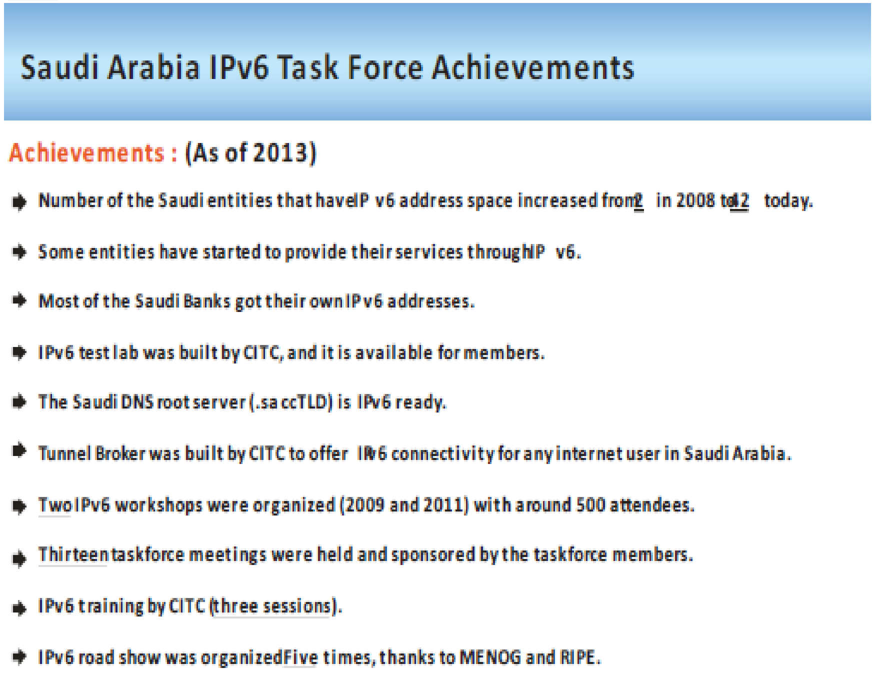
- **Luxembourg** – the Luxembourg IPv6 Council has defined a roadmap; the main telecom operator has followed through with offering IPv6 over fibre and published practical steps on implementation for other operators.
- **Germany** – the government has obtained a sizable IPv6 prefix from the RIR to completely enable its online citizen services infrastructure with IPv6.

The United Arab Emirates has formulated an IPv6 roadmap, and in March 2013 it held two workshops to prepare the UAE and its Internet stakeholders for looming IPv4 depletion;

- The Egyptian Ministry of Communications and Information Technology formed a national IPv6 task force;
- The Moroccan regulator ANRT has commissioned an IPv6 study to define a roadmap and is discussing a calendar for IPv6 deployment with the country's main telecom operators;

Governments promoting IPv6 deployment (examples)

Australian Government Information Management Office (AGIMO) has announced a transition strategy for the whole Australian government with a target completion date of 2015. AGIMO’s role in the government’s implementation of IPv6 includes developing the IPv6 Transition Strategy and Work Plan documents, monitoring and reporting on agencies’ progress, knowledge sharing, and monitoring international trends. There are 110 agencies, as named in Australia’s Financial Management and Accountability Act (FMA Act), rolling out IPv6 capabilities, including most of the major departments (Defence, Foreign Affairs and Trade, Human Services, Finance and Deregulation, etc.).



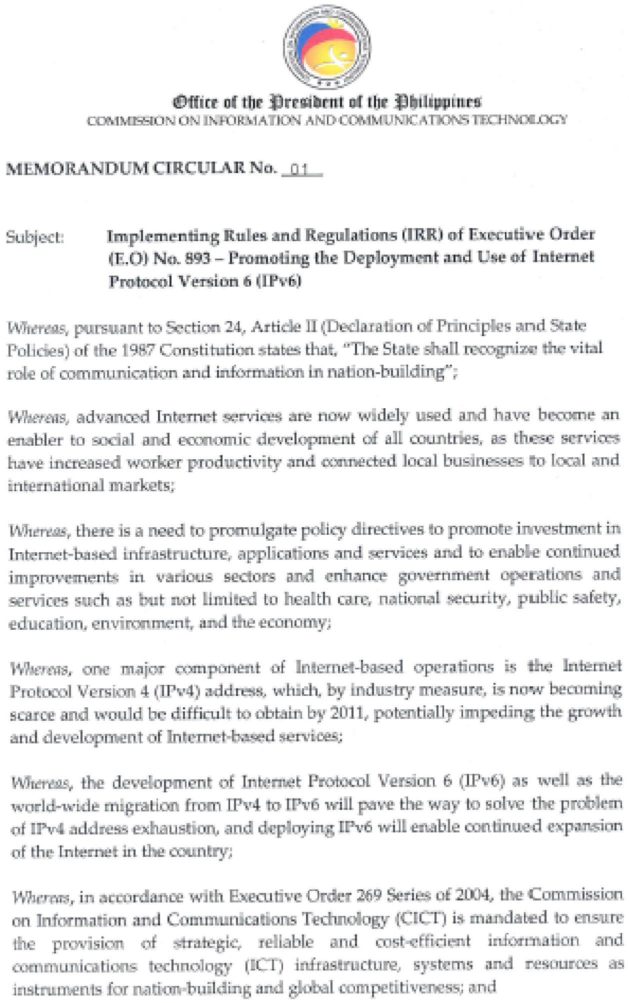
Saudi Arabia IPv6 Task Force Achievements

Achievements : (As of 2013)

- Number of the Saudi entities that haveIP v6 address space increased from2 in 2008 to42 today.
- Some entities have started to provide their services throughIP v6.
- Most of the Saudi Banks got their own IPv6 addresses.
- IPv6 test lab was built by CITC, and it is available for members.
- The Saudi DNS root server (.sa ccTLD) is IPv6 ready.
- Tunnel Broker was built by CITC to offer IPv6 connectivity for any internet user in Saudi Arabia.
- Two IPv6 workshops were organized (2009 and 2011) with around 500 attendees.
- Thirteen taskforce meetings were held and sponsored by the taskforce members.
- IPv6 training by CITC (three sessions).
- IPv6 road show was organizedFive times, thanks to MENOG and RIPE.

Source: Saudi Arabia IPv6 Task Force

Governments promoting IPv6 deployment (examples)



Office of the President of the Philippines
COMMISSION ON INFORMATION AND COMMUNICATIONS TECHNOLOGY

MEMORANDUM CIRCULAR No. 01

Subject: **Implementing Rules and Regulations (IRR) of Executive Order (E.O) No. 893 – Promoting the Deployment and Use of Internet Protocol Version 6 (IPv6)**

Whereas, pursuant to Section 24, Article II (Declaration of Principles and State Policies) of the 1987 Constitution states that, "The State shall recognize the vital role of communication and information in nation-building";

Whereas, advanced Internet services are now widely used and have become an enabler to social and economic development of all countries, as these services have increased worker productivity and connected local businesses to local and international markets;

Whereas, there is a need to promulgate policy directives to promote investment in Internet-based infrastructure, applications and services and to enable continued improvements in various sectors and enhance government operations and services such as but not limited to health care, national security, public safety, education, environment, and the economy;

Whereas, one major component of Internet-based operations is the Internet Protocol Version 4 (IPv4) address, which, by industry measure, is now becoming scarce and would be difficult to obtain by 2011, potentially impeding the growth and development of Internet-based services;

Whereas, the development of Internet Protocol Version 6 (IPv6) as well as the world-wide migration from IPv4 to IPv6 will pave the way to solve the problem of IPv4 address exhaustion, and deploying IPv6 will enable continued expansion of the Internet in the country;

Whereas, in accordance with Executive Order 269 Series of 2004, the Commission on Information and Communications Technology (CICT) is mandated to ensure the provision of strategic, reliable and cost-efficient information and communications technology (ICT) infrastructure, systems and resources as instruments for nation-building and global competitiveness; and

Promotion of IPv6

IPv6 deployment and use

Interagency Task Force

Funding

Singapore: IPv6 Transition Programme

The IPv6 Transition Programme is a national effort spearheaded by IDA in its role as the national planner for Infocomm development, to address the issue of IPv4 (Internet Protocol version 4) exhaustion and to facilitate the smooth transition of the Singapore Infocomm ecosystem to IPv6 (Internet Protocol version 6).

Developed by the Singapore IPv6 Task Force, it involves a two-pronged approach to drive IPv6 adoption in the nation as well as encourage the efficient use of the remaining pool of IPv4 addresses to minimise the risks of depletion

- *Developing reference specifications and transition guides*
- *Engaging stakeholders*
- *Developing IPv6 capabilities*
- *Establishing an IPv6 Marketplace*
- *Setting up IPv6 industry exemplars*
- *Others*

Source: http://www.ida.gov.sg/Technology/20110414104645.aspx

Singapore: IPv6 Adoption Guide Report - I

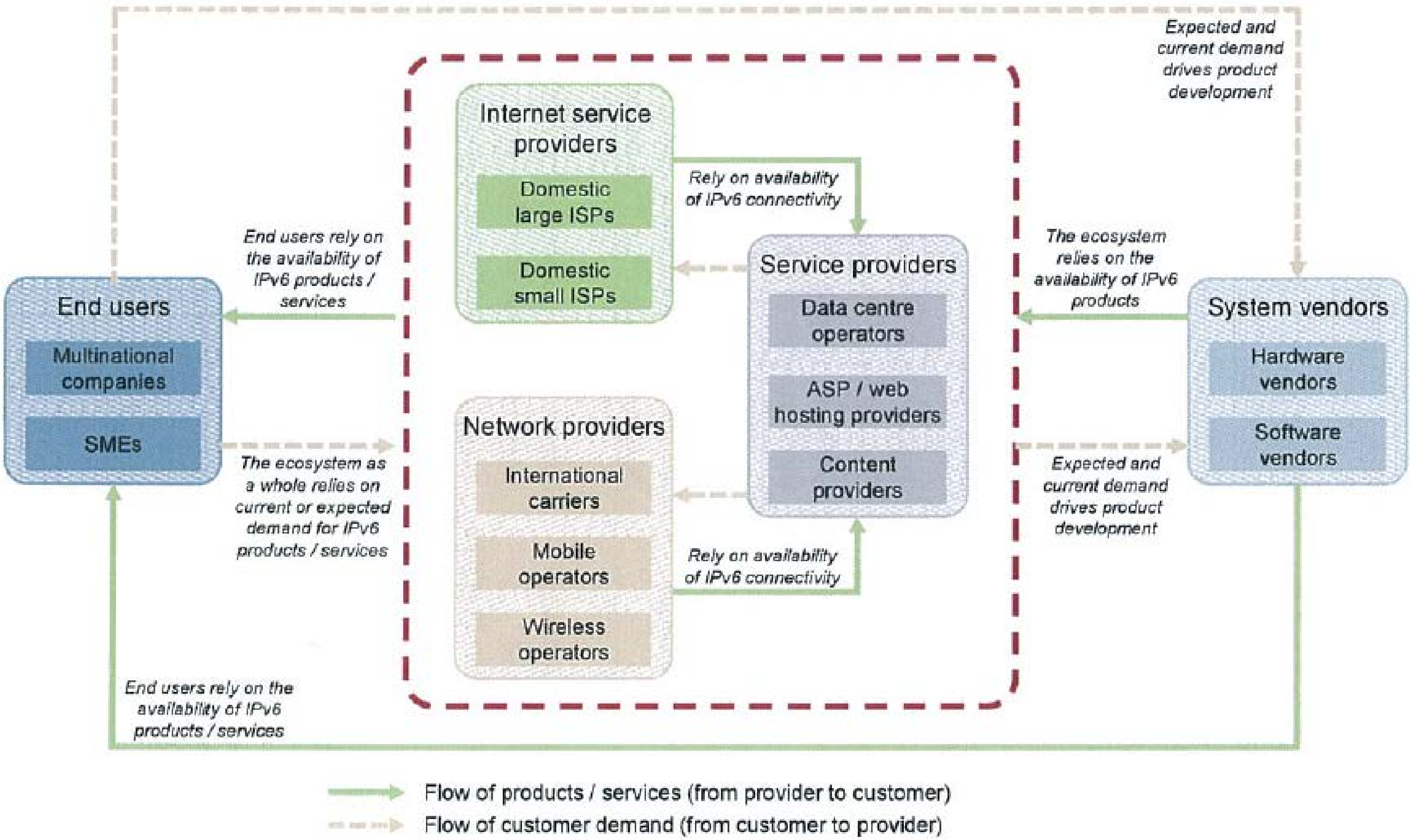

Expected and current demand drives product development
Internet service providers
Domestic large ISPs
Domestic small ISPs
Rely on availability of IPv6 connectivity
End users rely on the availability of IPv6 products / services
Service providers
Data centre operators
ASP / web hosting providers
Content providers
The ecosystem relies on the availability of IPv6 products
End users
Multinational companies
SMEs
System vendors
Hardware vendors
Software vendors
Network providers
International carriers
Mobile operators
Wireless operators
The ecosystem as a whole relies on current or expected demand for IPv6 products / services
Expected and current demand drives product development
Rely on availability of IPv6 connectivity
End users rely on the availability of IPv6 products / services
Flow of products / services (from provider to customer)
Flow of customer demand (from customer to provider)

Figure 3.1: Summary of IPv6 dependencies between stakeholder categories [Source: Analysys Mason]

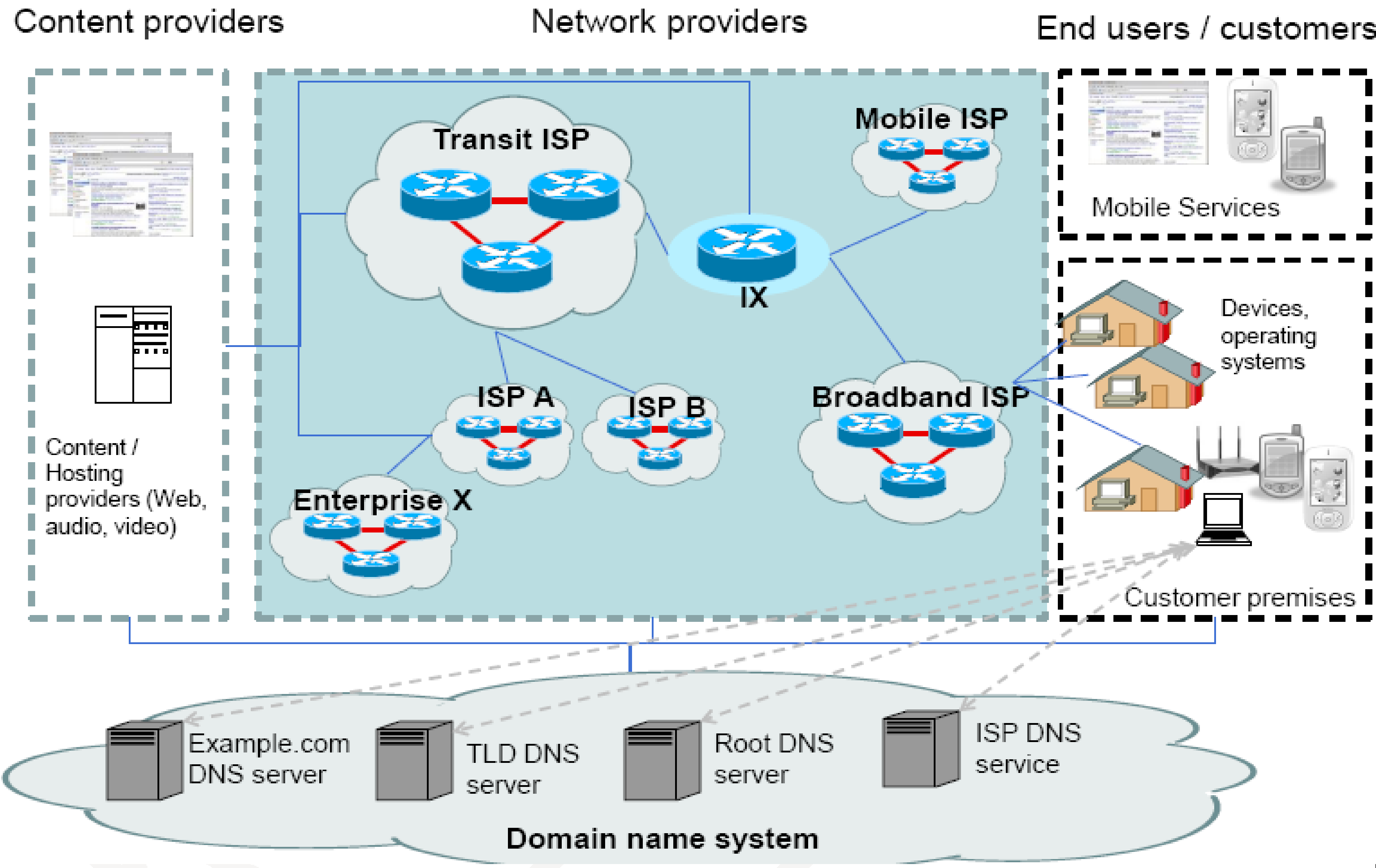
Report prepared by analysys mason and Tech Mahindra for IDA Singapore available at http://www.ida.gov.sg/images/content/Technology/Technology_Level1/ipv6/download/IPv6AdoptionGuideforSingapore.pdf

Singapore: IPv6 Adoption Guide Report - II

Focus areas identified in the report

- ***Planning***
- ***Network***
- ***Applications***
- ***Skills***
- ***Services / products***

Zoom on **network providers**



Source: OECD Presentation; Measuring Deployment of IPv6, Karine Perset

India: NTP 2012 and IPv6

Preamble

NTP-2012 recognises futuristic roles of Internet Protocol Version 6 (IPv6) and its applications in different sectors of Indian economy.

Objectives

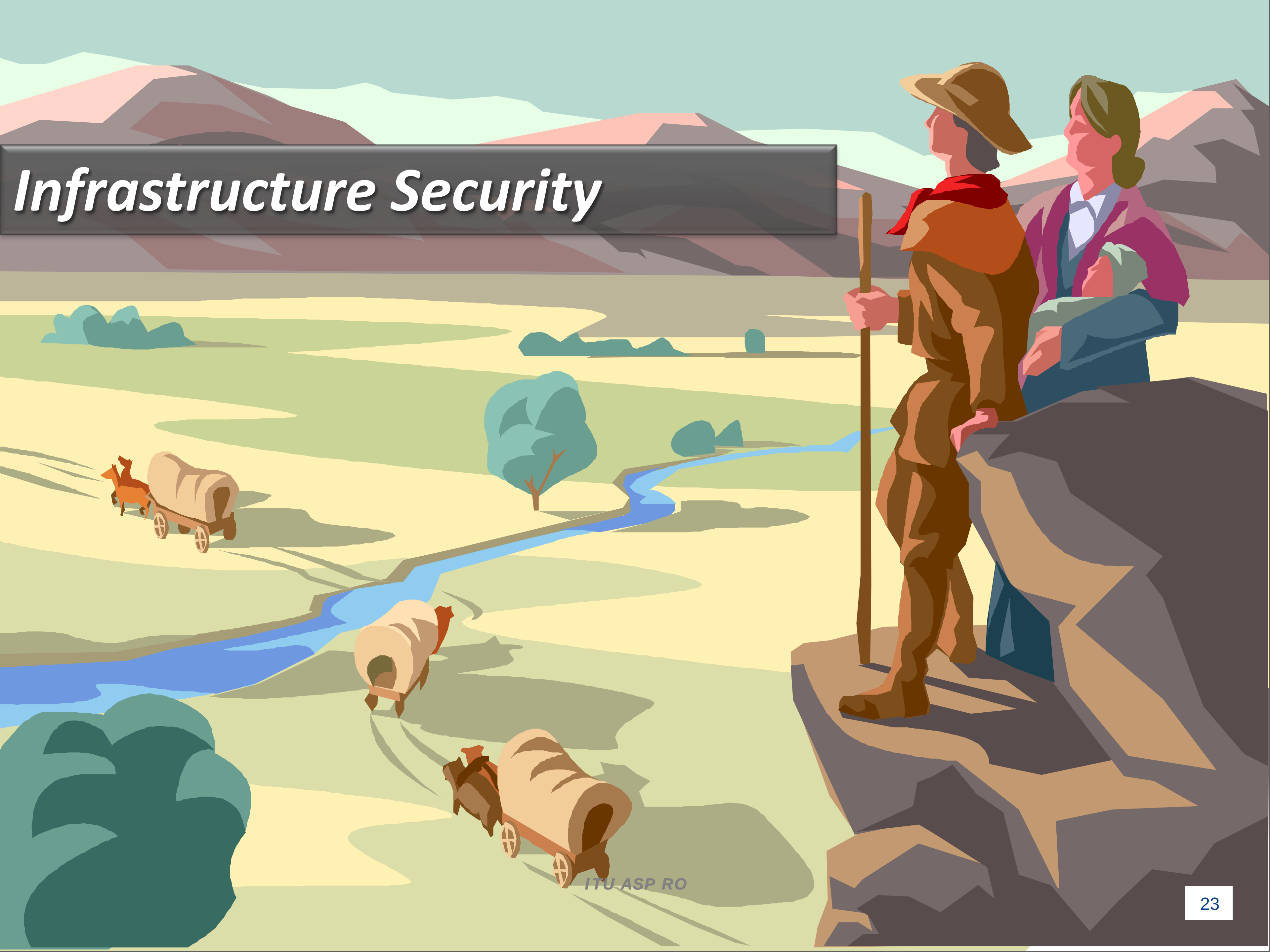
Achieve substantial transition to new Internet Protocol (IPv6) in the country in a phased and time bound manner by 2020 and encourage an ecosystem for provision of a significantly large bouquet of services on IP platform.

Telecom Enterprise Data Services, IPv6 Compliant Networks and Future Technologies

To recognize the importance of the new Internet Protocol IPv6 to start offering new IP based services on the new protocol and to encourage new and innovative IPv6 based applications in different sectors of the economy by enabling participatory approach of all stake holders.

To establish a dedicated centre of innovation to engage in R & D, specialized training, development of various applications in the field of IPv6. This will also be responsible for support to various policies and standards development processes in close coordination with different international bodies.

Infrastructure Security



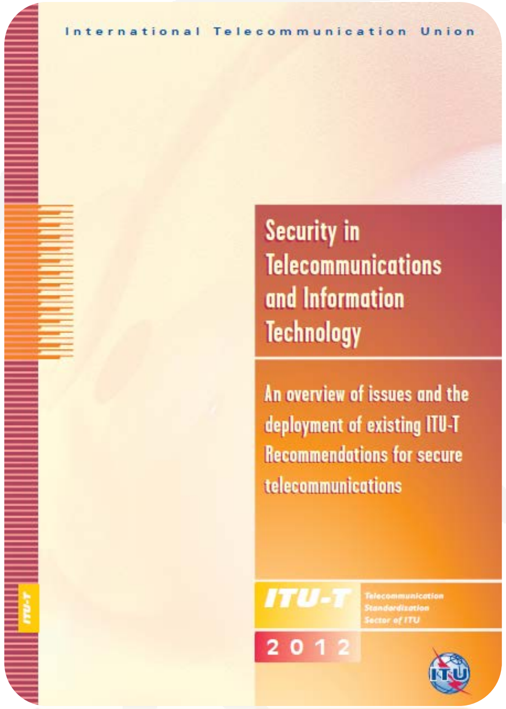
ITU Global Cybersecurity Agenda

"Building confidence and security in the use of ICTs"

In 2007, ITU Secretary-General launched the Global Cybersecurity Agenda, an international framework for collaboration on Cybersecurity matters that addresses five main areas:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structure
4. Capacity Building
5. International Cooperation

General security objectives for ICT networks



International Telecommunication Union

Security in Telecommunications and Information Technology

An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

ITU-T Telecommunication Standardization Sector of ITU

2012

a) Access to, and use of networks and services should be restricted to authorized users;

b) Authorized users should be able to access and operate on assets they are authorized to access;

c) Networks should support confidentiality to the level prescribed in the network security policies;

d) All network entities should be held accountable for their own, but only their own, actions;

e) Networks should be protected against unsolicited access or operations;

f) Security-related information should be available via the network, but only to authorized users;

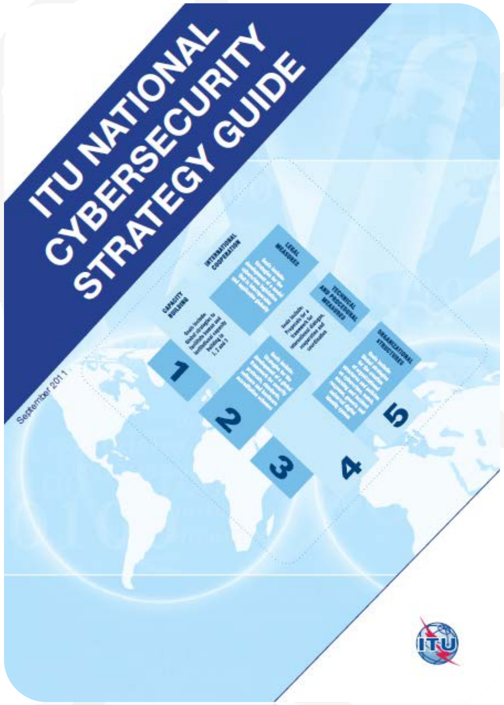
g) Plans should be in place to address how security incidents are to be handled;

h) Procedures should be in place to restore normal operation following detection of a security breach;

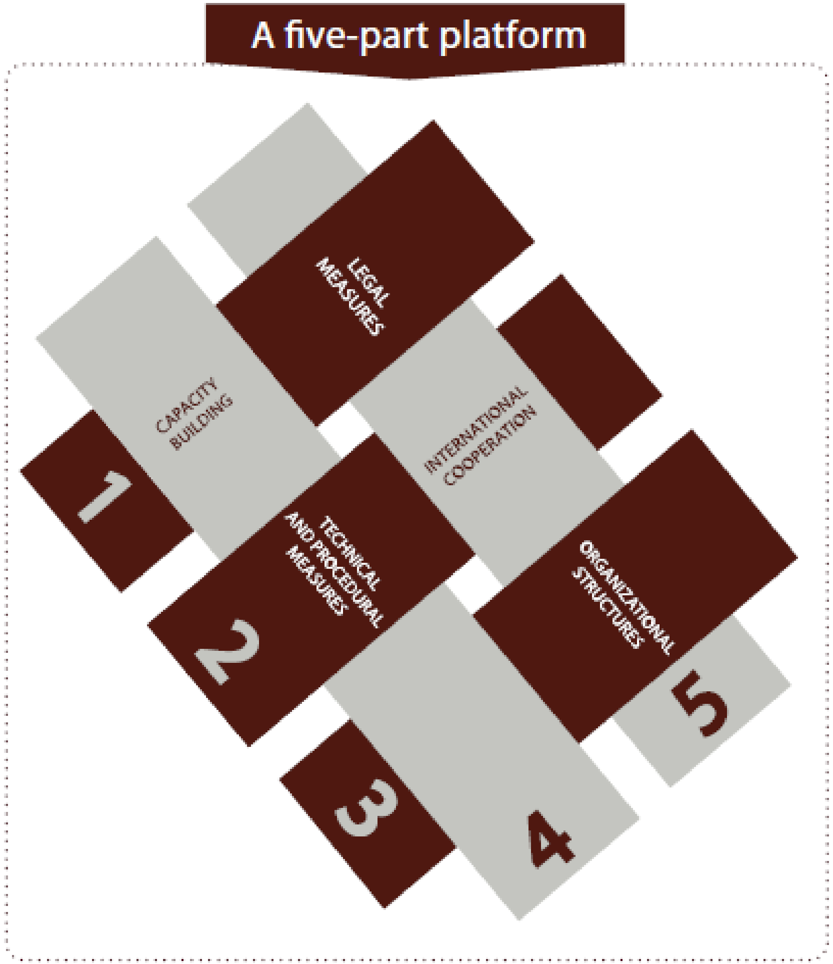
and

i) The network architecture should be able to support different security policies and security mechanisms of different strengths.

Five Pillars of Global Cybersecurity Agenda


ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

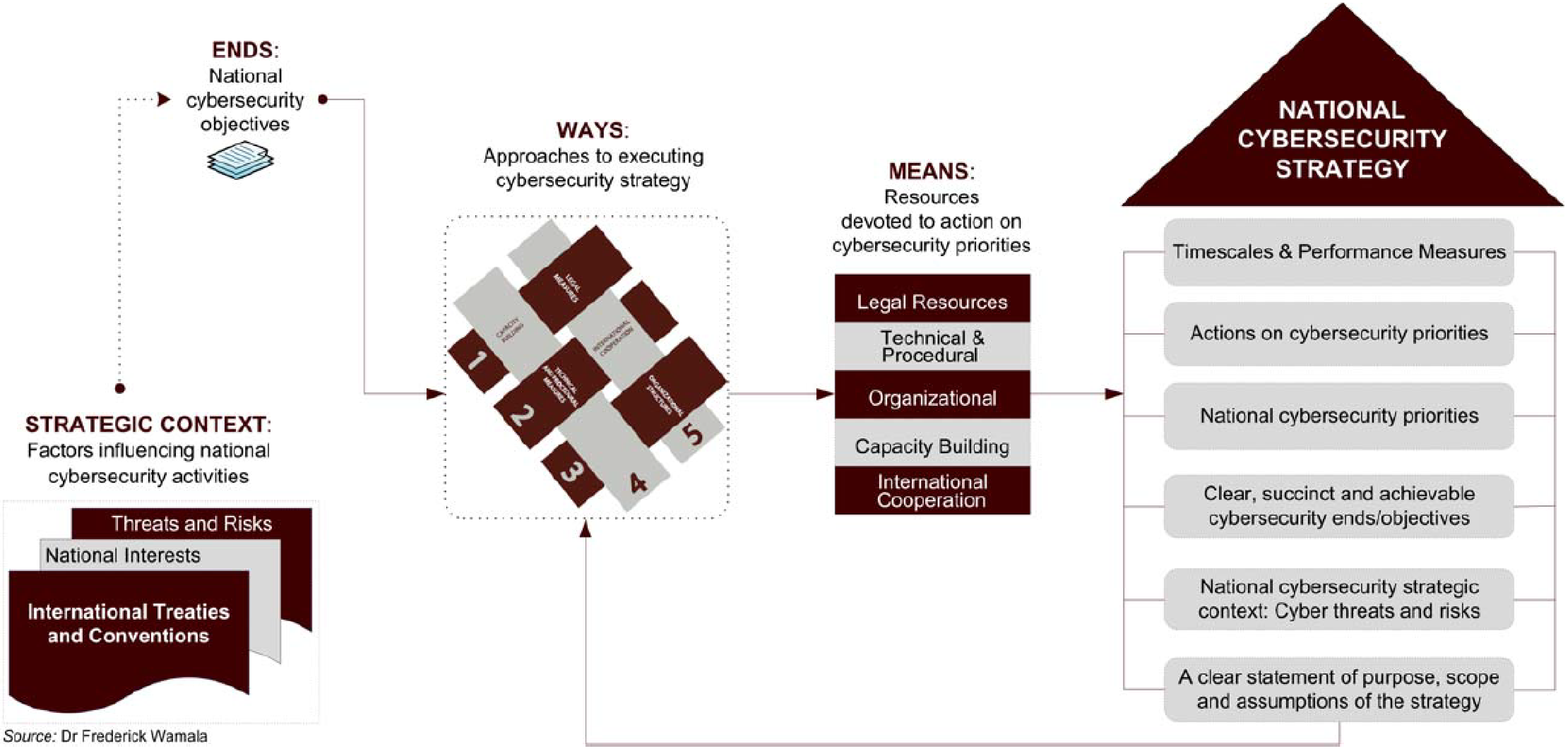
September 2011


A five-part platform

LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

Source: http://www.ida.gov.sg/Technology/20110414104645.aspx

Cybersecurity Strategy Model

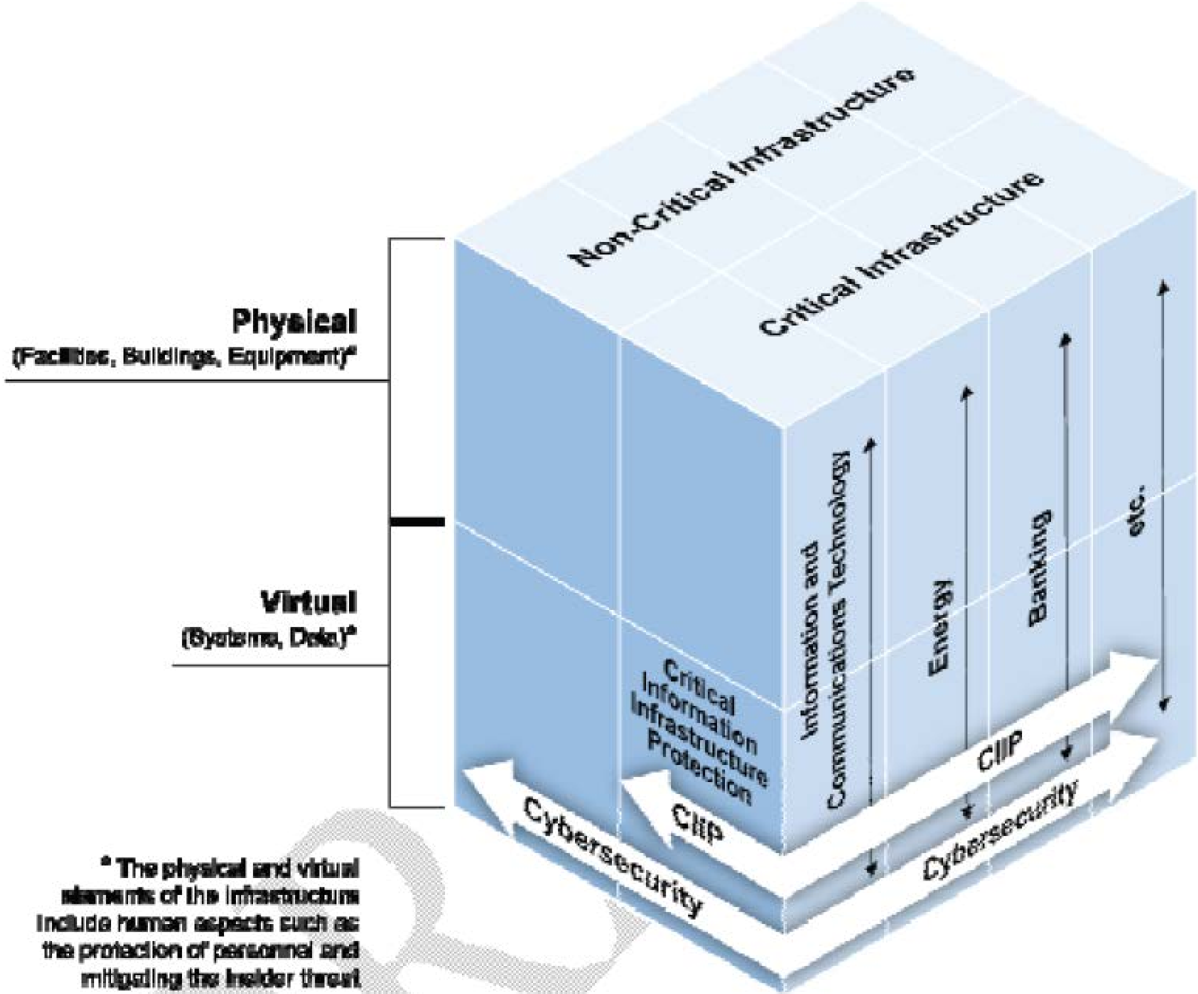


ENDS:
National cybersecurity objectives
WAYS:
Approaches to executing cybersecurity strategy
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5
MEANS:
Resources devoted to action on cybersecurity priorities
Legal Resources
Technical & Procedural
Organizational
Capacity Building
International Cooperation
NATIONAL CYBERSECURITY STRATEGY
Timescales & Performance Measures
Actions on cybersecurity priorities
National cybersecurity priorities
Clear, succinct and achievable cybersecurity ends/objectives
National cybersecurity strategic context: Cyber threats and risks
A clear statement of purpose, scope and assumptions of the strategy
STRATEGIC CONTEXT:
Factors influencing national cybersecurity activities
Threats and Risks
National Interests
International Treaties and Conventions

Source: Dr Frederick Wamala

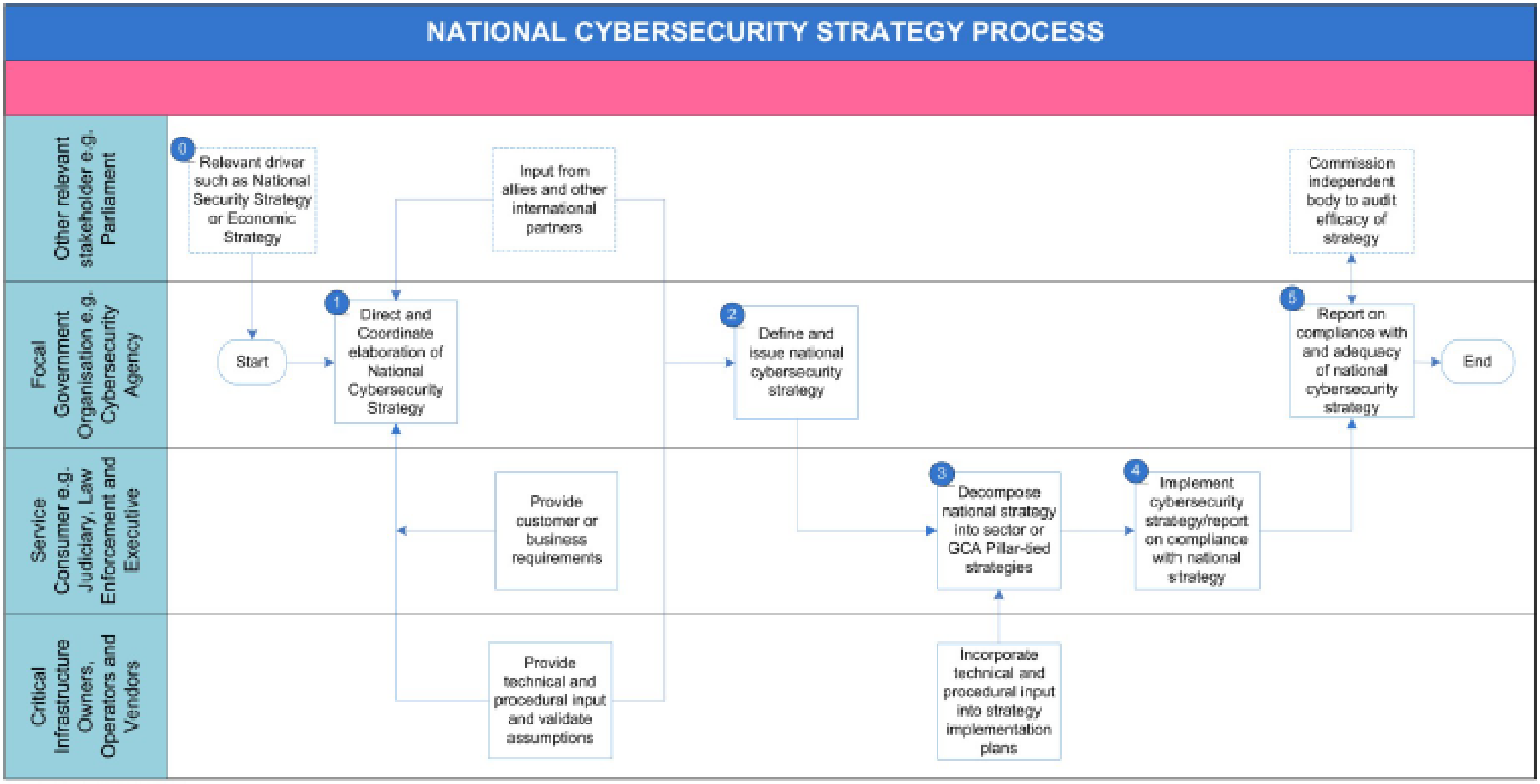
Source: http://www.ida.gov.sg/Technology/20110414104645.aspx

Critical Infrastructure


Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
Non-Critical Infrastructure
Critical Infrastructure
Critical Information Infrastructure Protection
Information and Communications Technology
Energy
Banking
etc.
CIIP
CIIP
Cybersecurity
Cybersecurity
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat

Source: ITU-D Study Group 1

National Cybersecurity Strategy Process



NATIONAL CYBERSECURITY STRATEGY PROCESS

Other relevant stakeholder e.g. Parliament

Focal Government Organisation e.g. Cybersecurity Agency

Service Consumer e.g. Judiciary, Law Enforcement and Executive

Critical Infrastructure Owners, Operators and Vendors

0 Relevant driver such as National Security Strategy or Economic Strategy

Input from allies and other international partners

Commission independent body to audit efficacy of strategy

Start

1 Direct and Coordinate elaboration of National Cybersecurity Strategy

2 Define and issue national cybersecurity strategy

5 Report on compliance with and adequacy of national cybersecurity strategy

End

Provide customer or business requirements

3 Decompose national strategy into sector or GCA Pillar-tied strategies

4 Implement cybersecurity strategy/report on compliance with national strategy

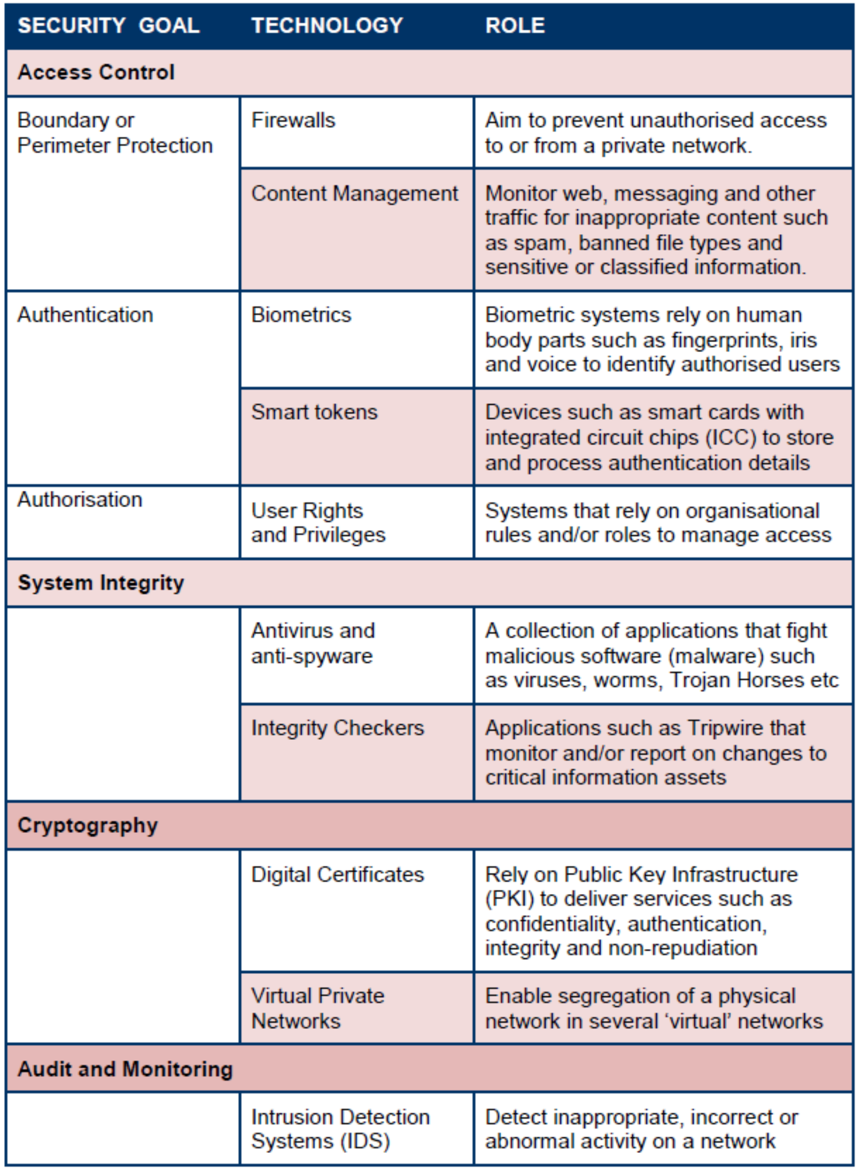
Provide technical and procedural input and validate assumptions

Incorporate technical and procedural input into strategy implementation plans

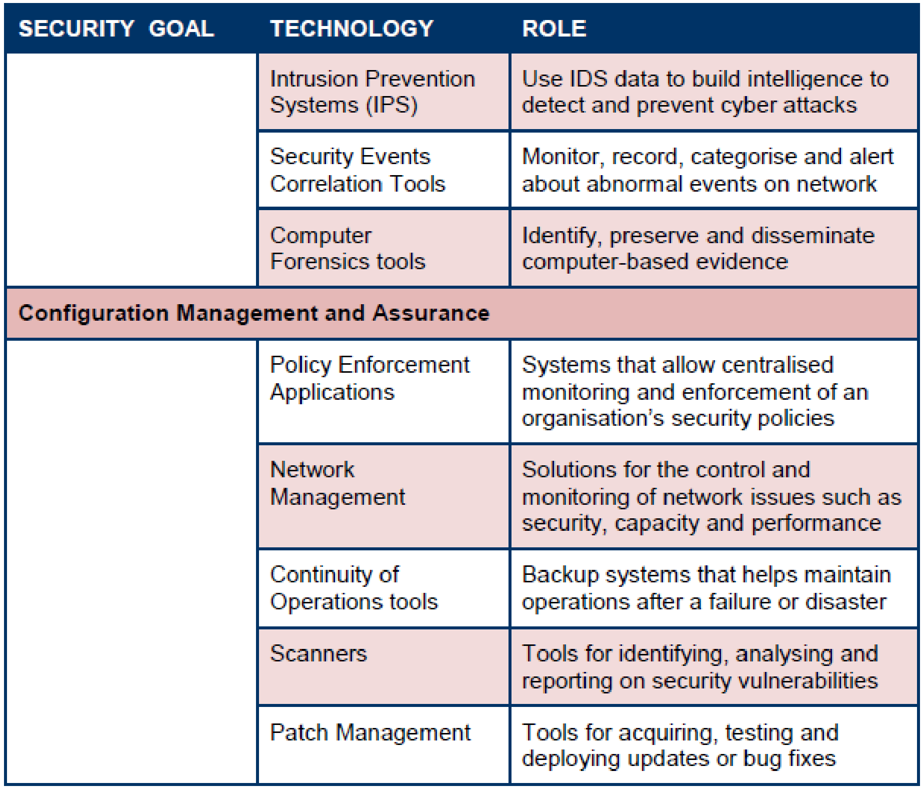
Source: Dr Frederick Wamala

Source: ITU National Cybersecurity Strategy Guide

Technical Solutions

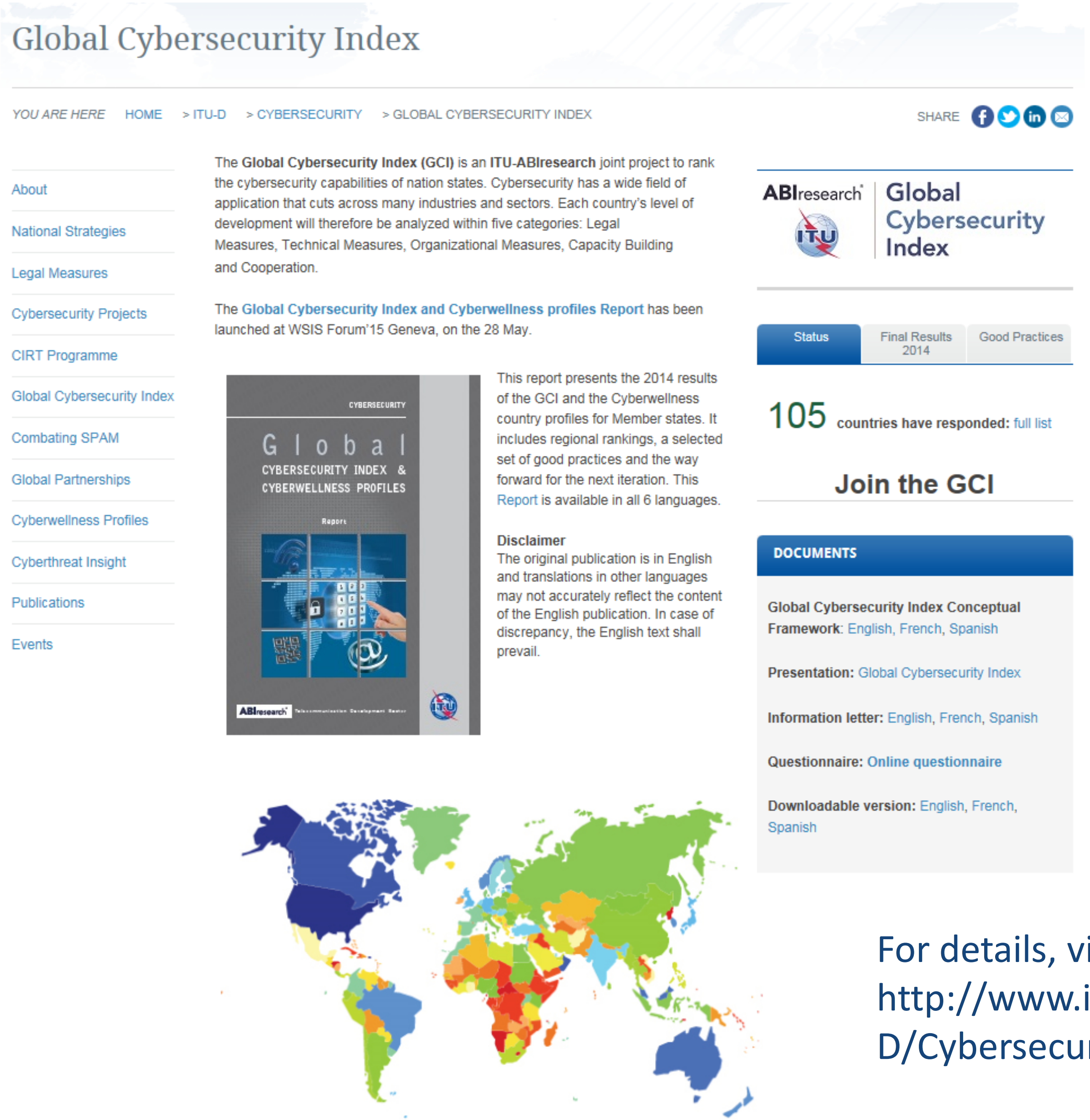


SECURITY GOAL	TECHNOLOGY	ROLE
Access Control		
Boundary or Perimeter Protection	Firewalls	Aim to prevent unauthorised access to or from a private network.
	Content Management	Monitor web, messaging and other traffic for inappropriate content such as spam, banned file types and sensitive or classified information.
Authentication	Biometrics	Biometric systems rely on human body parts such as fingerprints, iris and voice to identify authorised users
	Smart tokens	Devices such as smart cards with integrated circuit chips (ICC) to store and process authentication details
Authorisation	User Rights and Privileges	Systems that rely on organisational rules and/or roles to manage access
System Integrity		
	Antivirus and anti-spyware	A collection of applications that fight malicious software (malware) such as viruses, worms, Trojan Horses etc
	Integrity Checkers	Applications such as Tripwire that monitor and/or report on changes to critical information assets
Cryptography		
	Digital Certificates	Rely on Public Key Infrastructure (PKI) to deliver services such as confidentiality, authentication, integrity and non-repudiation
	Virtual Private Networks	Enable segregation of a physical network in several 'virtual' networks
Audit and Monitoring		
	Intrusion Detection Systems (IDS)	Detect inappropriate, incorrect or abnormal activity on a network



SECURITY GOAL	TECHNOLOGY	ROLE
	Intrusion Prevention Systems (IPS)	Use IDS data to build intelligence to detect and prevent cyber attacks
	Security Events Correlation Tools	Monitor, record, categorise and alert about abnormal events on network
	Computer Forensics tools	Identify, preserve and disseminate computer-based evidence
Configuration Management and Assurance		
	Policy Enforcement Applications	Systems that allow centralised monitoring and enforcement of an organisation's security policies
	Network Management	Solutions for the control and monitoring of network issues such as security, capacity and performance
	Continuity of Operations tools	Backup systems that helps maintain operations after a failure or disaster
	Scanners	Tools for identifying, analysing and reporting on security vulnerabilities
	Patch Management	Tools for acquiring, testing and deploying updates or bug fixes

Source: ITU National Cybersecurity Strategy Guide



Global Cybersecurity Index

YOU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX

SHARE

- About
- National Strategies
- Legal Measures
- Cybersecurity Projects
- CIRT Programme
- Global Cybersecurity Index
- Combating SPAM
- Global Partnerships
- Cyberwellness Profiles
- Cyberthreat Insight
- Publications
- Events

The **Global Cybersecurity Index (GCI)** is an **ITU-ABIresearch** joint project to rank the cybersecurity capabilities of nation states. Cybersecurity has a wide field of application that cuts across many industries and sectors. Each country's level of development will therefore be analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

The **Global Cybersecurity Index and Cyberwellness profiles Report** has been launched at WSIS Forum'15 Geneva, on the 28 May.

This report presents the 2014 results of the GCI and the Cyberwellness country profiles for Member states. It includes regional rankings, a selected set of good practices and the way forward for the next iteration. This Report is available in all 6 languages.

Disclaimer
The original publication is in English and translations in other languages may not accurately reflect the content of the English publication. In case of discrepancy, the English text shall prevail.

ABIresearch | Global Cybersecurity Index

Status | Final Results 2014 | Good Practices

105 **countries have responded:** full list

Join the GCI

DOCUMENTS

Global Cybersecurity Index Conceptual Framework: English, French, Spanish

Presentation: Global Cybersecurity Index

Information letter: English, French, Spanish

Questionnaire: **Online questionnaire**

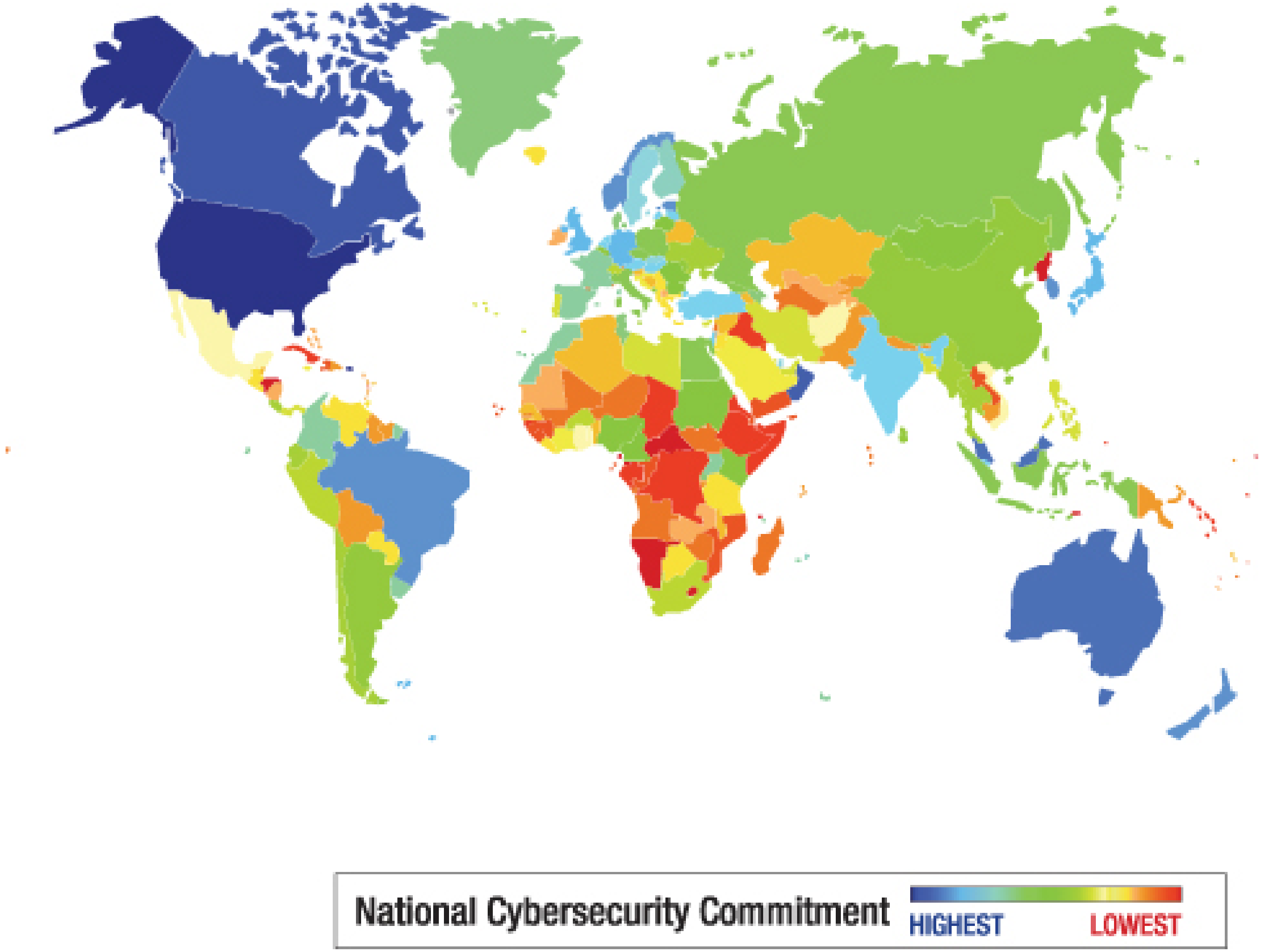
Downloadable version: English, French, Spanish

For details, visit http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

ABIresearch

ITU

Global Cybersecurity Index



Source: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Global Ranking

ABIresearch | Global Cybersecurity Index

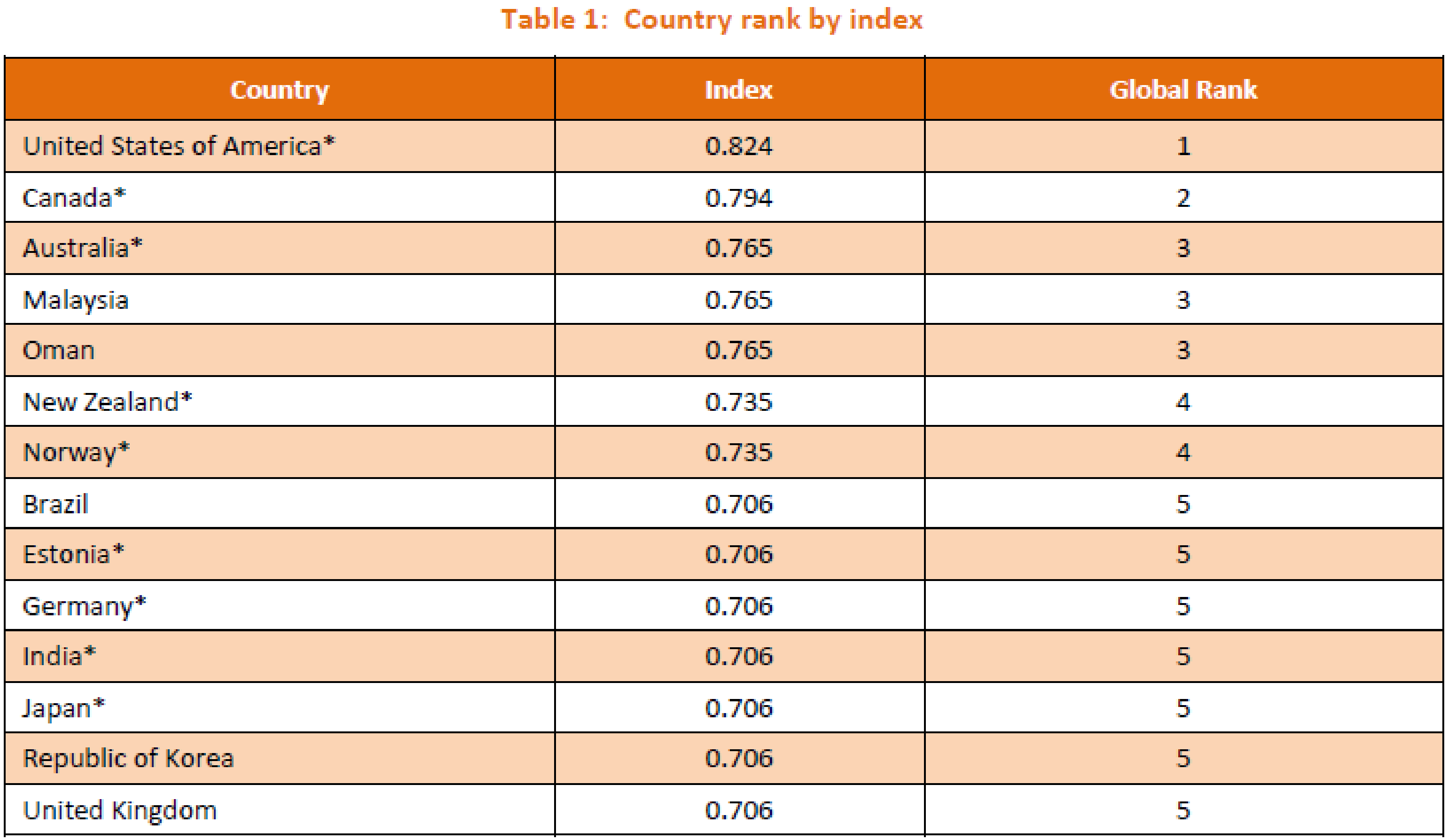


Table 1: Country rank by index

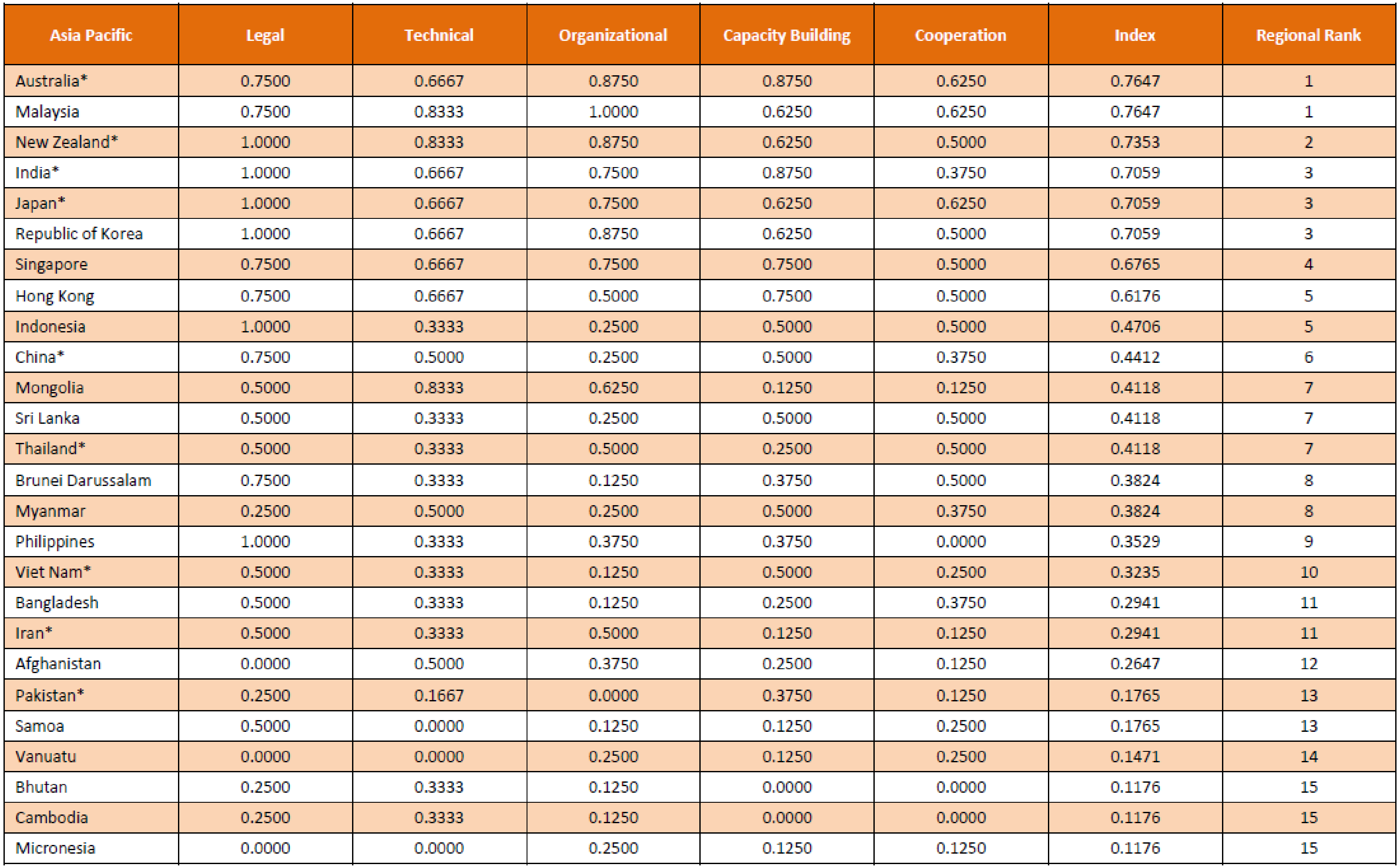
Country	Index	Global Rank
United States of America*	0.824	1
Canada*	0.794	2
Australia*	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand*	0.735	4
Norway*	0.735	4
Brazil	0.706	5
Estonia*	0.706	5
Germany*	0.706	5
India*	0.706	5
Japan*	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5

Source: GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES REPORT 2015

Regional Ranking (Asia-Pacific 2015)

ABIresearch ITU | Global Cybersecurity Index

Table 5: Asia Pacific region ranking by index



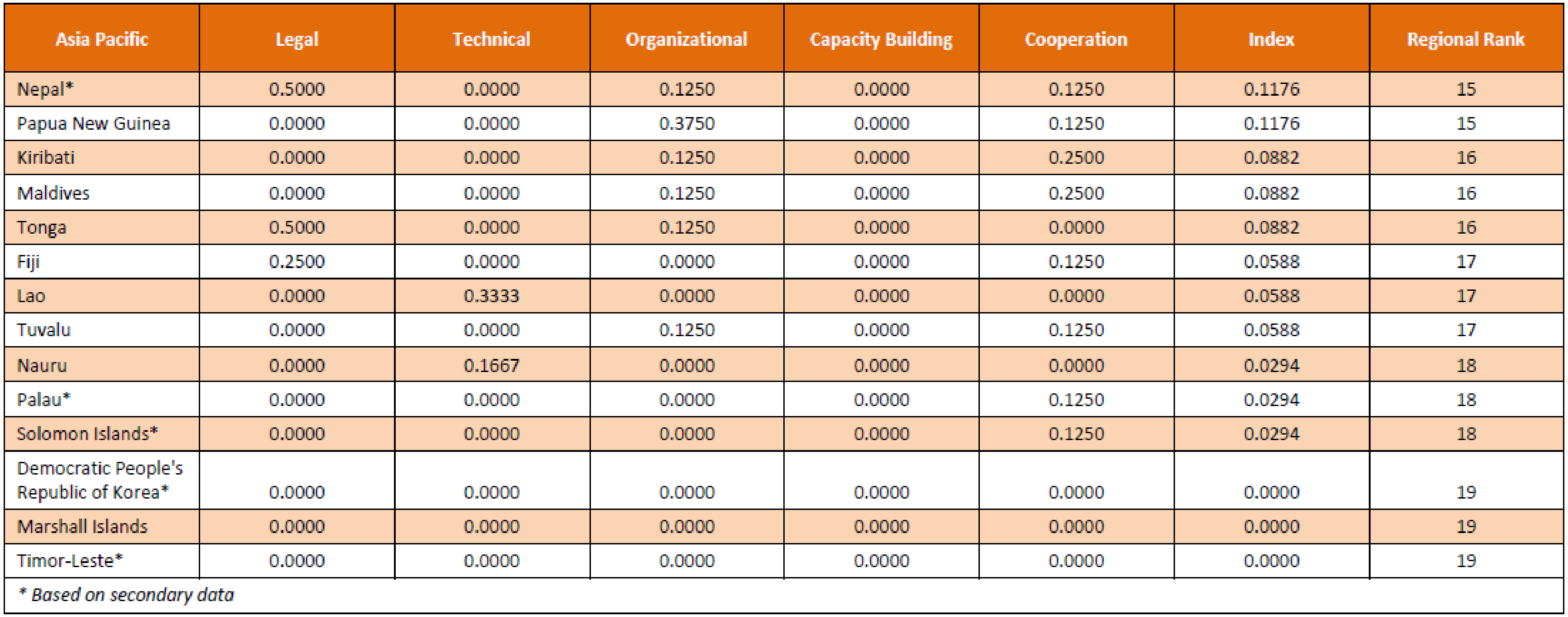
Asia Pacific	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Australia*	0.7500	0.6667	0.8750	0.8750	0.6250	0.7647	1
Malaysia	0.7500	0.8333	1.0000	0.6250	0.6250	0.7647	1
New Zealand*	1.0000	0.8333	0.8750	0.6250	0.5000	0.7353	2
India*	1.0000	0.6667	0.7500	0.8750	0.3750	0.7059	3
Japan*	1.0000	0.6667	0.7500	0.6250	0.6250	0.7059	3
Republic of Korea	1.0000	0.6667	0.8750	0.6250	0.5000	0.7059	3
Singapore	0.7500	0.6667	0.7500	0.7500	0.5000	0.6765	4
Hong Kong	0.7500	0.6667	0.5000	0.7500	0.5000	0.6176	5
Indonesia	1.0000	0.3333	0.2500	0.5000	0.5000	0.4706	5
China*	0.7500	0.5000	0.2500	0.5000	0.3750	0.4412	6
Mongolia	0.5000	0.8333	0.6250	0.1250	0.1250	0.4118	7
Sri Lanka	0.5000	0.3333	0.2500	0.5000	0.5000	0.4118	7
Thailand*	0.5000	0.3333	0.5000	0.2500	0.5000	0.4118	7
Brunei Darussalam	0.7500	0.3333	0.1250	0.3750	0.5000	0.3824	8
Myanmar	0.2500	0.5000	0.2500	0.5000	0.3750	0.3824	8
Philippines	1.0000	0.3333	0.3750	0.3750	0.0000	0.3529	9
Viet Nam*	0.5000	0.3333	0.1250	0.5000	0.2500	0.3235	10
Bangladesh	0.5000	0.3333	0.1250	0.2500	0.3750	0.2941	11
Iran*	0.5000	0.3333	0.5000	0.1250	0.1250	0.2941	11
Afghanistan	0.0000	0.5000	0.3750	0.2500	0.1250	0.2647	12
Pakistan*	0.2500	0.1667	0.0000	0.3750	0.1250	0.1765	13
Samoa	0.5000	0.0000	0.1250	0.1250	0.2500	0.1765	13
Vanuatu	0.0000	0.0000	0.2500	0.1250	0.2500	0.1471	14
Bhutan	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15
Cambodia	0.2500	0.3333	0.1250	0.0000	0.0000	0.1176	15
Micronesia	0.0000	0.0000	0.2500	0.1250	0.1250	0.1176	15

Source: GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES REPORT 2015

Regional Ranking (Asia-Pacific 2015)

ABIresearch | Global Cybersecurity Index

ITU



Asia Pacific	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Nepal*	0.5000	0.0000	0.1250	0.0000	0.1250	0.1176	15
Papua New Guinea	0.0000	0.0000	0.3750	0.0000	0.1250	0.1176	15
Kiribati	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
Maldives	0.0000	0.0000	0.1250	0.0000	0.2500	0.0882	16
Tonga	0.5000	0.0000	0.1250	0.0000	0.0000	0.0882	16
Fiji	0.2500	0.0000	0.0000	0.0000	0.1250	0.0588	17
Lao	0.0000	0.3333	0.0000	0.0000	0.0000	0.0588	17
Tuvalu	0.0000	0.0000	0.1250	0.0000	0.1250	0.0588	17
Nauru	0.0000	0.1667	0.0000	0.0000	0.0000	0.0294	18
Palau*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
Solomon Islands*	0.0000	0.0000	0.0000	0.0000	0.1250	0.0294	18
Democratic People's Republic of Korea*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
Marshall Islands	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19
Timor-Leste*	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	19

** Based on secondary data*

Source: GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS PROFILES REPORT 2015

IPv6 Infrastructure Security (ITU-T X.1037)

International Telecommunication Union

ITU-T
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.1037
(10/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
Information and network security – Network security

IPv6 technical security guidelines

Recommendation ITU-T X.1037

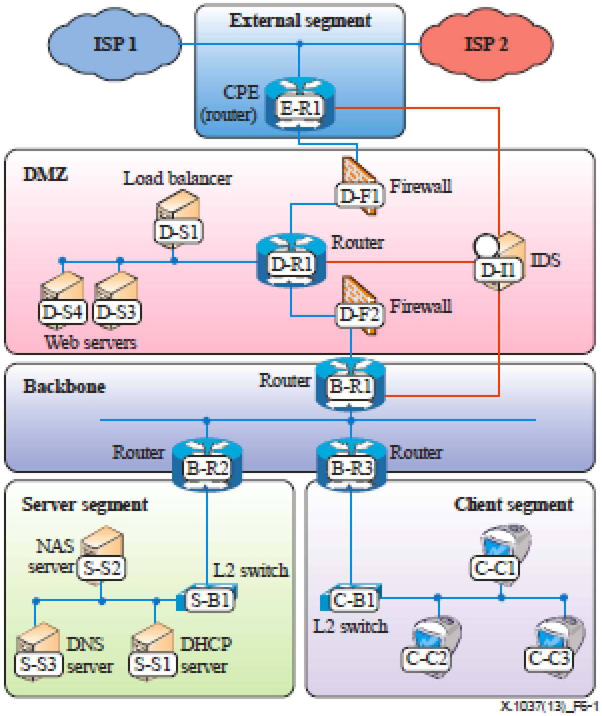


Figure 6-1 – Example topology of an IPv6 enterprise network

Network Devices

(Router, Switch, NAT device)

Security devices such as firewalls and IDS Devices

(Intrusion Detection System, Firewall)

Clients, servers, and other end devices

(End Nodes, DHCP, DNS)

Thank You