Role of policy maker and Regulator in Internet and IPv6 Security

ITU Asia-Pacific CoE Training on "Internet and IPv6 Infrastructure Security"
23-27 May, 2016
Bangkok, Thailand

,
ITU Regional Office for Asia and the Pacific

ITU: A Brief Overview

Founded in 1865

A specialized agency of the UN with focus on Telecommunication / ICTs

193 Member States
567 Sector Members
159 Associates
104 Academia

Headquartered in Geneva,
4 Regional Offices
7 Area Offices.

ITU-R: ITU's Radio-communication Sector globally manages radio-frequency spectrum and satellite orbits that ensure safety of life on land, at sea and in the skies.

ITU-T: ITU's Telecommunication Standardization Sector enables global communications by ensuring that countries' ICT networks and devices are speaking the same language.

ITU-D: ITU's Development Sector fosters international cooperation and solidarity in the delivery of technical assistance and in the creation, development and improvement of telecommunication/ICT equipment and networks in developing countries.

ICT Services Uptake

Global, 2014

Mobile cellular subscriptions:
- Almost 7 billion

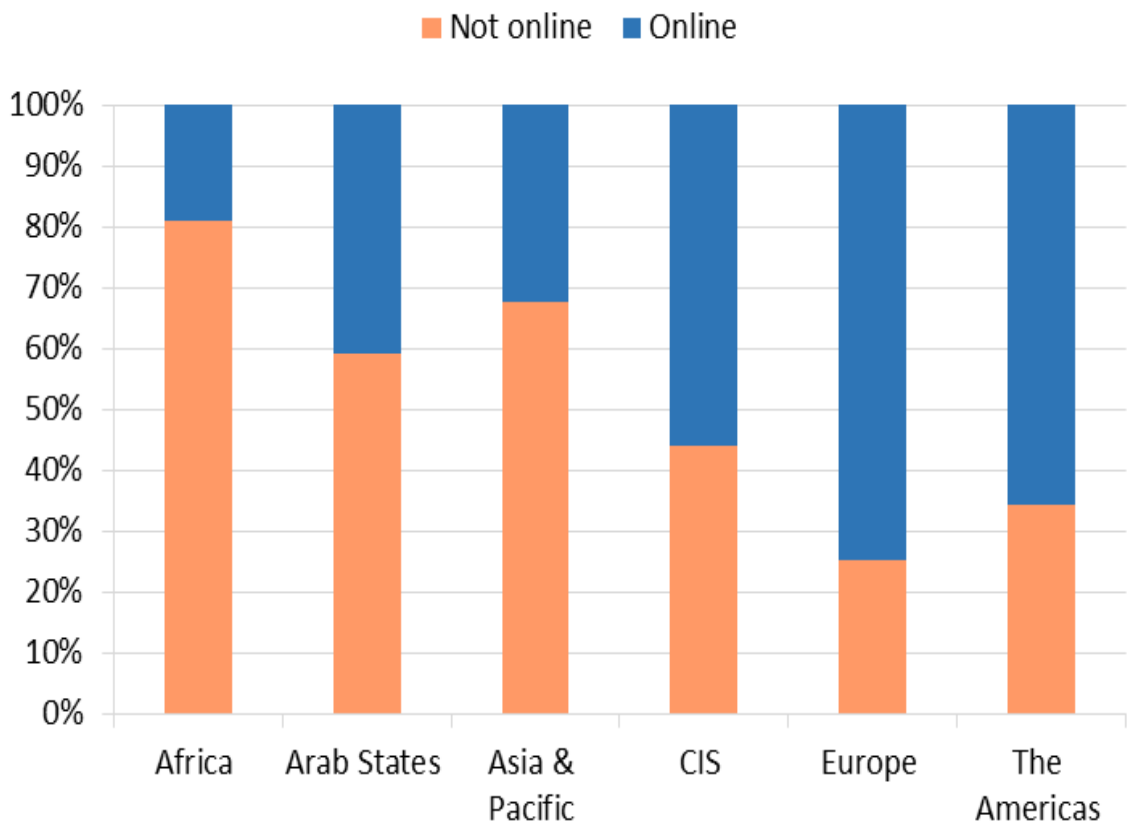
Mobile broadband penetration:
- 84% developed countries
- 21% developing countries

Fixed broadband penetration:
- 27.5 % developed countries
- 6 % developing countries

- Almost 3 billion people online (individuals using the Internet)

Who's online?

By region, 2014



Source: ITU World Telecommunication/ICT Indicators database

Agreed Global Telecommunication/ICT Targets - 2020

Goal 1 Growth : Enable and foster access to and increased use of telecommunications/ICTs

55%
of households should have access to the Internet

60%
of individuals should be using the Internet

40%
Telecommunications/ICTs should be **40%** more affordable

GROWTH

Goal 2 Inclusiveness – Bridge the digital divide and provide broadband for all

50%
of households should have access to the Internet in the developing world; **15%** in the least developed countries

50%
of individuals should be using the Internet in the developing world; **20%** in the least developed countries

40%
affordability gap between developed and developing countries should be reduced by **40%**

5%
Broadband services should cost no more than **5%** of average monthly income in the developing countries

INCLUSION

90%
of the rural population should be covered by broadband services

Gender equality among Internet users should be reached

Enabling environments ensuring accessible ICTs for persons with disabilities should be established in all countries

Goal 3 Sustainability – Manage challenges resulting from the telecommunication/ICT development

40%
improvement in cybersecurity readiness

50%
reduction in volume of redundant e-waste

30%
decrease in Green House Gas emissions per device generated by the telecommunication/ICT sector

SUSTAINABILITY

Goal 4 Innovation and partnership – Lead, improve and adapt to the changing telecommunication/ICT environment

Telecommunication/ICT environment conducive to innovation

Effective partnerships of stakeholders in telecommunication/ICT environment

INNOVATION

A multi-tier SSC ICT architecture from communication view
(physical perspective)

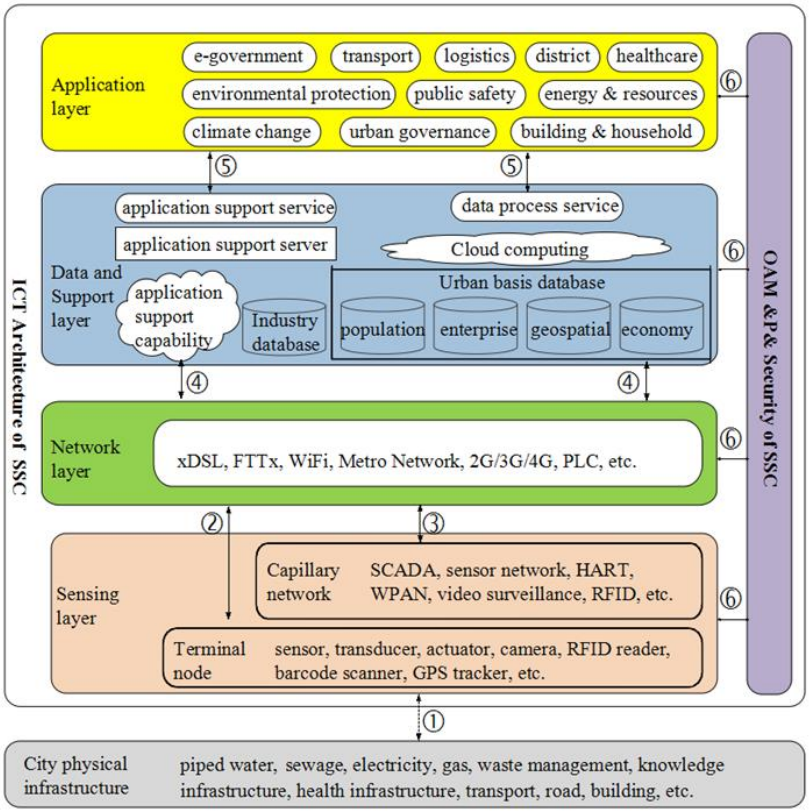
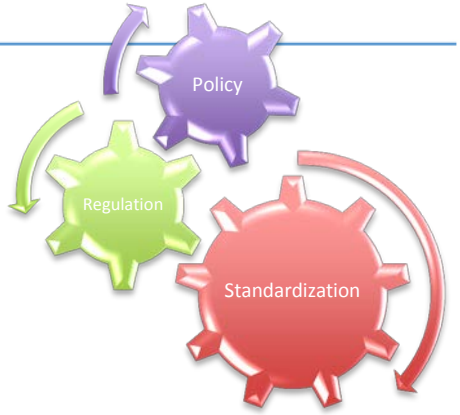


Figure source: ITU-T Focus Group on Smart Sustainable Cities: *Overview of smart sustainable cities infrastructure*

Telecom/ ICT Sector Issues (examples)



- Cross-Sector Collaboration
- Competition
- Investment
- Licensing
- Spectrum
- HetNets
- Broadband
- Cloud
- IoT / M2M
- Interoperability
- QoS/QoE
- Numbering & Addressing
- Big Data & Open Data
- Security
- Privacy
- Right of Way
- Green ICTs
- Infrastructure Sharing
- Data Centres
- e-Waste
- Emergency Telecommunications

Different Services, Different Requirements - Examples

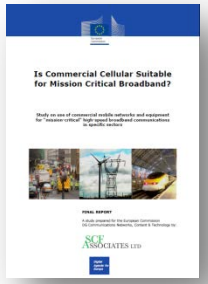
PPDR services

- **Constant availability** –
- **Ubiquitous coverage** – not just outdoors, but inside buildings (including large ferroconcrete structures such as shopping malls) and in tunnels (including subways).
- **Regionally harmonised spectrum** –
- **Differentiated priority classes** .
- **Support for dynamic talkgroups,**
- **Automatic identification with authentication.**
- **Automatic location discovery and tracking**
- **The ability to maintain connectivity**
- **Fast call setup** (<200ms) and immediate access on demand: the **Push-to-talk** (PTT)function and **all-calls** (internal broadcasts).
- **Relay capabilities**
- **Support for Air-Ground-Air (AGA) communication** when and where needed.
- **Adequate quality of service**
- **The ability to roam onto commercial networks**
- **Interworking between various PPDR services,** and increasingly, across borders.

Utility industry :

- **Teleprotection** – safeguarding infrastructure and isolating sections of the network during fault conditions whilst maintaining service in unaffected parts of the network.
- **Data monitoring** via SCADA (Supervisory, Control And Data Acquisition) systems.
- **Automation** – systems to autonomously restore service after an interruption or an unplanned situation.
- **Security** – systems to ensure the safety and security of plant.
- **Voice services** –.
- **Metering** – collecting data from smart meters and communicating with them for various reasons, such as demand management and to implement tariff changes.
- **Connectivity** – telecommunication networks to interconnect the above services in a reliable and resilient manner under all conditions.
- Other operational requirements include:
- **Coverage of all populated areas with points of presence throughout the service territory**
- **Costs must be low**
- **Continuity of service is vital,** and price stability
- **Utilities want network separation,**

Intelligent Transport Services… *and more*



What type of network is required to deliver these services?

- Private networks
- Public networks

What preparations are required to make best use of commercial networks to deliver smart services (some of them such as Emergency Telecommunication, Utilities, Transportation critical in character)?

- Technical (e.g. coverage, resilience, quality, spectrum, interoperability)
- Commercial (e.g. availability, long term pricing, SLAs
- Policy & Regulatory (e.g. critical services as priority, quality of service, long term tariffs, security, privacy, USO, infrastructure sharing, licensing)

Key Cybersecurity Challenges

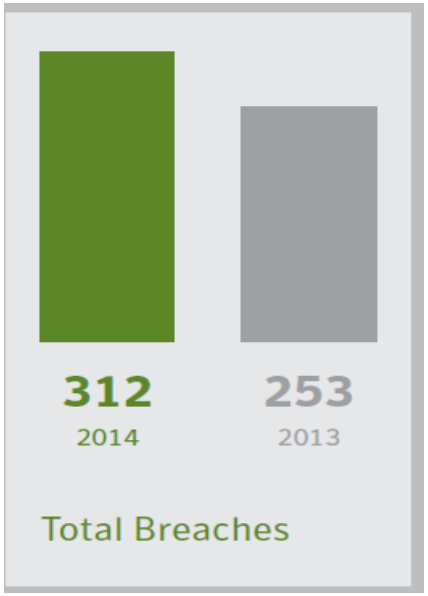
- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software for ICT-based applications
- Lack of appropriate national and global organizational structures to deal with cyber incidents
- Lack of information security professionals and skills within governments; lack of basic awareness among users
- Lack of international cooperation between industry experts, law enforcements, regulators, academia & international organizations, etc. to address a global challenge
- Complexity of ICTs imply a need for the ability to respond, not just protect, as cybersecurity incidents will happen even if protective measures are deployed.

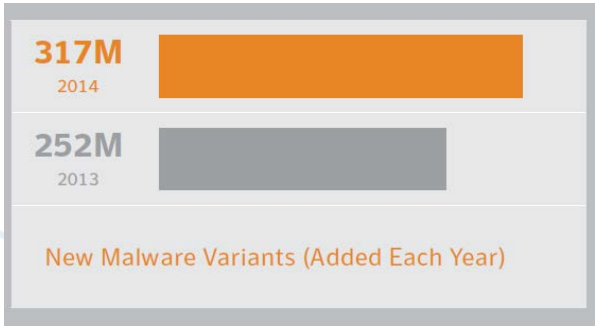
Cybersecurity not seen yet as a cross-sector, multi-dimensional concern.

Still seen as a technical/technology problem.

Importance of Cybersecurity

- From industrial age to information societies
  - Increasing dependence on the availability of ICTs
  - Number of Internet users growing constantly (now 40% of world's population)
- Statistics and reports show that cyber-threats are on the rise
  - The likely annual cost to the global economy from Cybercrime is estimated at more than $455 billion *(Source: McAfee Report on Economic Impact of Cybercrime, 2013).*
- Developing countries most at risk as they adopt broader use of ICTs
  - E.g. Africa leading in Mobile-broadband penetration: almost 20% in 2014 - up from less than 2% in 2010 *(Source: ITU ICT Statistics)*
- Need for building cybersecurity capacity
  - Protection is crucial for the socio-economic wellbeing of a country in the adoption of new technologies

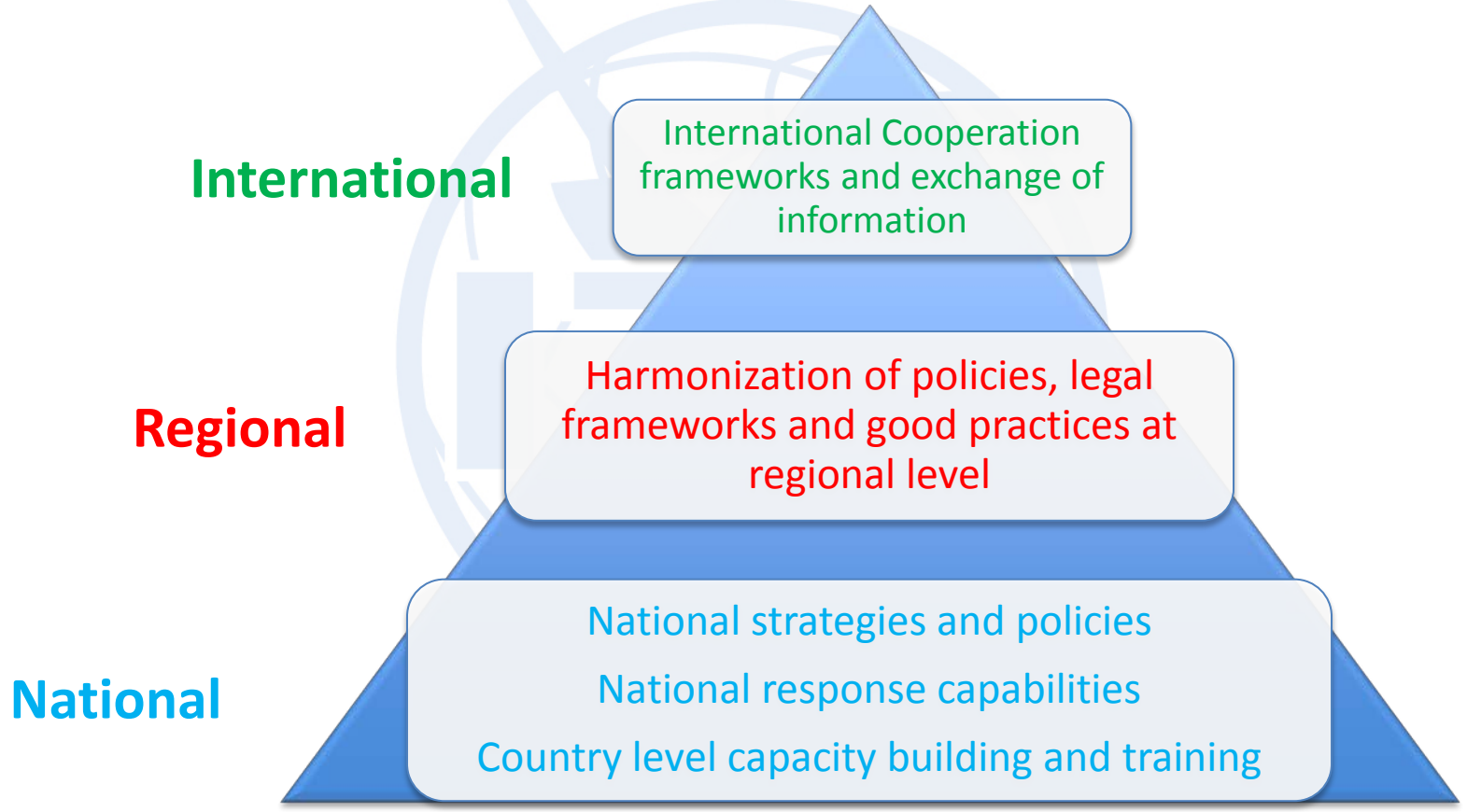




Source: Symantec 2015 Internet Security Threat Report

Coordinated Response

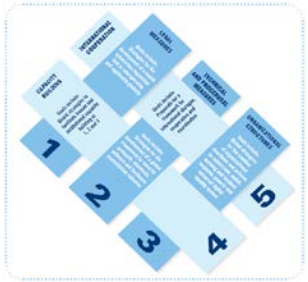
Need for a multi-level response to the cybersecurity challenges



ITU Mandate on Cybersecurity

2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action Line C5 - "**Building Confidence and Security in the use of ICTs**"

world summit on the information society
Geneva 2003 - Tunis 2005



2007
Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General
GCA is a **framework for international cooperation in cybersecurity**

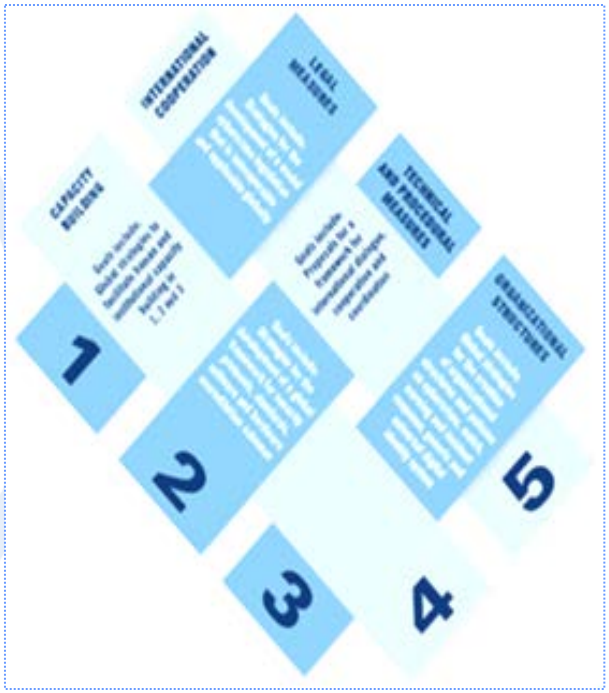
2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

GCA GLOBAL CYBERSECURITY AGENDA

Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, from legal to policy, to technical and organization measures.

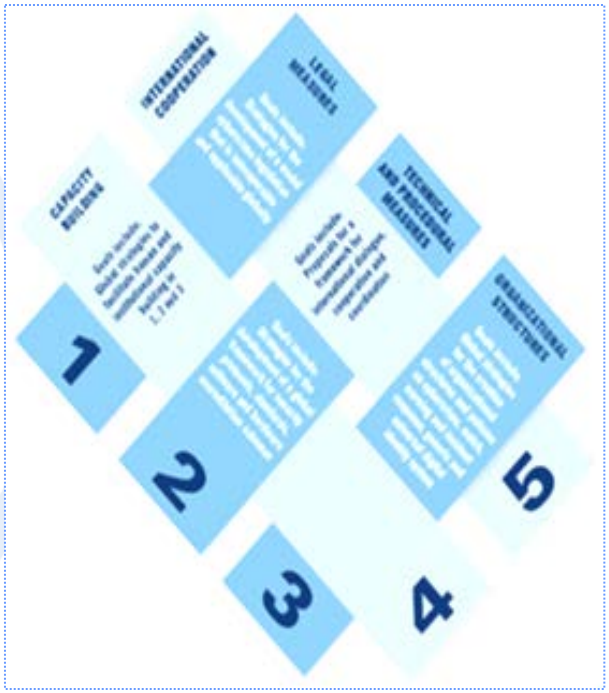
Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
    1. Legal Measures
    2. Technical and Procedural Measures
    3. Organizational Structure
    4. Capacity Building
    5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.



Global Cybersecurity Agenda (GCA)

- GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.
- GCA builds upon five pillars:
    1. Legal Measures
    2. Technical and Procedural Measures
    3. Organizational Structure
    4. Capacity Building
    5. International Cooperation
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.



Global Cybersecurity Index

Objective

The Global Cybersecurity Index (GCI) aims to measure the level of commitment of each nation in cybersecurity in five main areas:

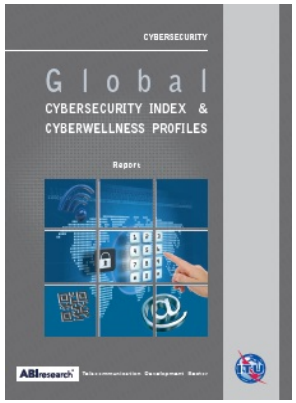
- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

104 countries have responded

Final Global and Regional Results 2014 are on ITU Website

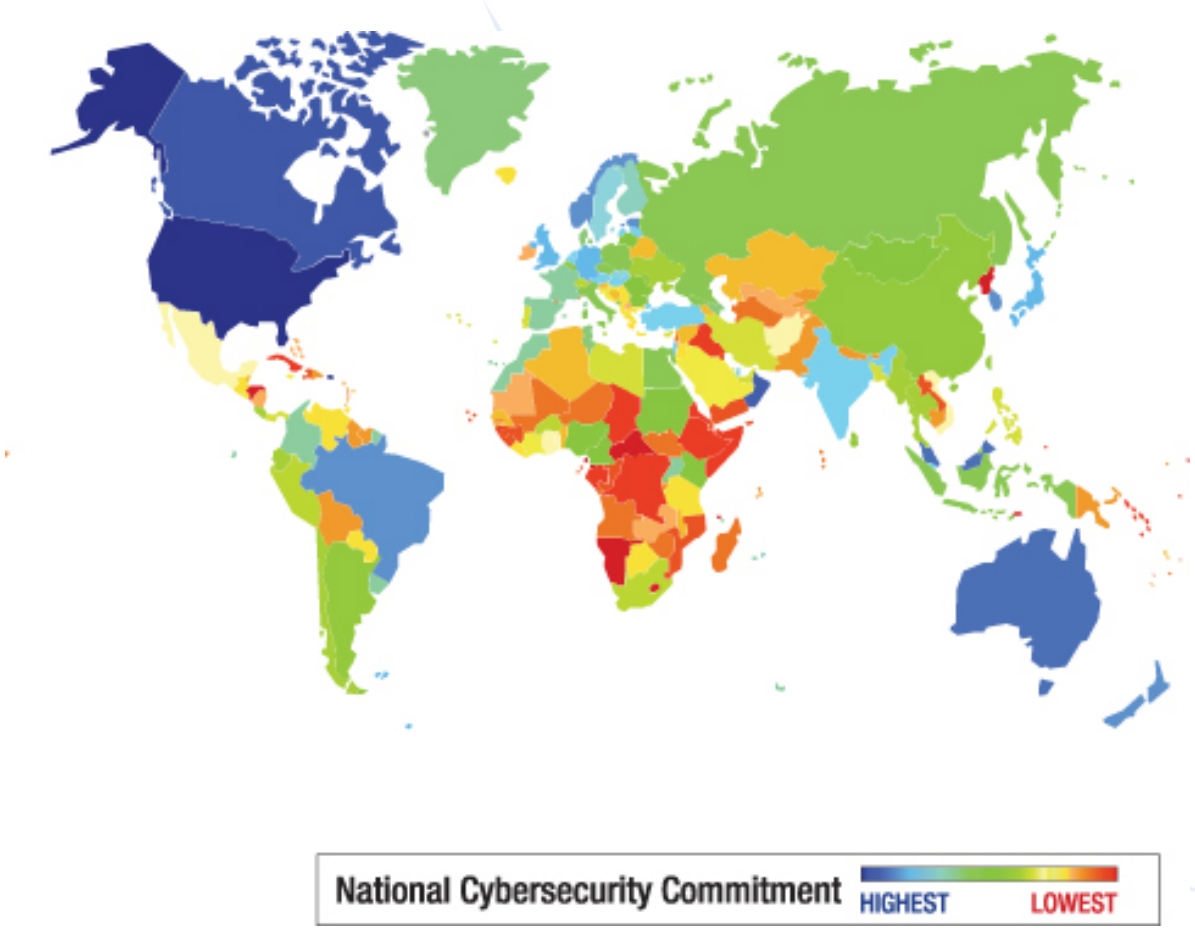
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

Next iteration in progress



ABIresearch | Global Cybersecurity Index

ABIresearch | Global Cybersecurity Index



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

Global Ranking 2014 - Top 5

Many countries share the same ranking which indicates that they have the same level of readiness.
The index has a low level of granularity since it aims at capturing the cybersecurity commitment/preparedness of a country and
NOT its detailed capabilities or possible vulnerabilities.

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

Top Performers in Asia-Pacific

Asia Pacific	Index	Regional Rank
Malaysia	0.7353	1
Australia*	0.6765	2
New Zealand*	0.6765	2
India*	0.6471	4
Singapore	0.6471	4
Japan*	0.5588	6
Republic of Korea*	0.4706	7
Indonesia*	0.4412	8
Brunei Darussalam	0.3824	9
China*	0.3824	9
Sri Lanka	0.3824	9
Myanmar	0.3529	12
Thailand*	0.3529	12
Bangladesh	0.2941	14
Iran (Islamic Republic of)*	0.2941	14
Philippines*	0.2941	14
Afghanistan	0.2647	17
Viet Nam*	0.2647	17
Vanuatu	0.1471	19

Cyberwellness Country Profiles

Factual information on cybersecurity achievements on each country **based on the GCA pillars**

Over 196 profiles to date

Live documents –
Invite countries to assist us in maintaining updated information
cybersecurity@itu.int

1. Legal Measures
A. Criminal Legislation
B. Regulation & Compliance.

2. Technical Measures
A. CERT/CIRT/CSIRT
B. Standards
C. Certification

3. Organizational Measures
A. Policy
B. Roadmap for Governance
C. Responsible Agency
D. National Benchmarking

4. Capacity building
A. Standardization Development
B. Manpower Development
C. Professional Certification
D. Agency Certification

5. Cooperation
A. Intra-state Cooperation
B. Intra-agency Cooperation
C. Public-Private Partnerships
D. International Cooperation

Cyberwellness Profile example - USA

CYBERWELLNESS PROFILE
UNITED STATES

BACKGROUND

Total Population: 315 791 00 (data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 84.20% (data source: ITU Statistics, December 2013)

1.CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- 15 USC Chapter 103 - Controlling the Assault of Non-solicited Pornography and Marketing
- 18 USC, Chapter 47, § 1029 - Fraud and related activity in connection with access devices
- 18 USC, Chapter 47, § 1030 - Fraud and related activity in connection with computers
- 18 USC, Chapter 47, § 1037 - Fraud and related activity in connection with electronic mail
- 18 USC Chapter 119 - Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC Chapter 121 - Stored Wire and Electronic Communications and Transactional Record Access

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- 44 USC Chapter 35, Subchapter III
- Information Security (§3541)
- Uniform Electronic Transactions Act
- Electronic Signatures in Global and National Commerce Act
- Homeland Security Act
- Cyber Security Research and Development Act
- Protecting Children in the 21st Century Act
- Children's Internet Protection Act
- Adam Walsh Child Protection and Safety Act
- Keeping the Internet Devoid of Sexual Predators Act
- Freedom of Information Act (5 USC § 552)
- Privacy Act (5 U.S.C. § 552a)
- Federal Information Security Management Act of 2002.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

United States has an officially recognized national CIRT (US CERT) and an industrial control systems CERT (ICS-CERT).

1.2.2 STANDARDS

United States has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

-National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.0

-Federal Information Security Management Act of 2002

-NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems"

-The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200.

-National Institute of Standards and Technology Special publication 800-12 provides a broad overview of computer security and control areas.

1.2.3 CERTIFICATION

The National Initiative for Cybersecurity Education (NICCS) offers a cybersecurity framework for the certification and accreditation of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

United States has officially recognized International Strategy for Cyberspace. There is also an executive order in order to improve critical infrastructure cybersecurity. A Critical Infrastructure Protection Program has been in place since 1996.

1.3.2 ROADMAP FOR GOVERNANCE

The NIST Roadmap for Improving Critical Infrastructure Cybersecurity, the Cross-Sector Roadmap for Cybersecurity of Control Systems and the Roadmap to achieve energy delivery systems cybersecurity provide the national governance roadmap for cybersecurity in the United States.

1.3.3 RESPONSIBLE AGENCY

The White House has an appointed US Cybersecurity Coordinator at the level of Special Assistant to the President to guide Executive branch efforts. The Department of Homeland Security (DHS) and the Department of Defense (DoD) are the primary cybersecurity actors in order to monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provides detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

The Department of Defense (DOD) established the Defense Industrial Base (DIB) Cybersecurity/Information Assurance (CS/IA) Program that aims to provide cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector. The National Institute of Standards and Technology (NIST) leads also in developing a Cybersecurity Framework of standards and best practices for protecting critical infrastructures.

The Cybersecurity Division (CSD) provides information resources—standards, frameworks, tools, and technologies to enable seamless and secure interactions among homeland security stakeholders and leads the government's charge in funding cybersecurity research and development (R&D).

Also the IT Security Essential Body of Knowledge (EBK) establishes a national baseline of the essential knowledge and skills that IT security practitioners in the public and private sector should have to perform specific roles and responsibilities.

1.4.2 MANPOWER DEVELOPMENT

United States has the following various types of awareness programs, industry talk, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees:

- National Cybersecurity Awareness Month
- Stop.Think.Connect. Campaign
- Cyber-Physical Systems Public Working Group Workshop
- National Initiative for Cybersecurity Education

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

Cyberwellness Profile example - USA

- National Cybersecurity Education Council (NCEC)
- Cybersecurity Education and Training Assistance Program (CETAP)
- National Cybersecurity Workforce Framework - NICCS
- National Centers of Academic Excellence (CAEs) that provide students valuable technical skills in various disciplines of Information Assurance.
- The Federal Cybersecurity Training Events (FedCTE) that delivers training, labs, and competitions for Federal cybersecurity and IT professionals.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information regarding the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information regarding any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, United States has officially recognized partnerships with the following organizations:

- DHS and Canada Public Safety Plan to Strengthen Cybersecurity Cooperation

- FIRST

- US CERT

- United States and Estonia: Partners in Cyber Security and Internet Freedom

1.5.2 INTRA-AGENCY COOPERATION

United States has officially recognized the following national or sector-specific programs for sharing cybersecurity assets within the public sector through the Department of Homeland Security (DHS) created by the Homeland Security Act of 2002.

- The National Infrastructure Protection Plan (NIPP)

- The Department of Homeland Security and the Department of Defense (DOD) signed a landmark memorandum of agreement in 2010 to protect against threats to critical civilian and military computer systems and networks.

- The Department of Homeland Security, the Department of Defense, and the Financial Services Information Sharing and Analysis Center launched a pilot initiative designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information.

- The Cybersecurity Partners Local Access Plan.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Administration provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through a Cybersecurity Framework, a guide developed collaboratively with the private sector for private industry to enhance their cybersecurity, in 2014.

The National Cybersecurity Center of Excellence (NCCoE) provides businesses with real-world cybersecurity solutions—based on commercially available technologies. Finally the Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks.

1.5.4 INTERNATIONAL COOPERATION

United States is signatory to Council of Europe Convention on Cybercrime and there is an EU-US cooperation on cybersecurity and cyberspace.

2 CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION AND STRATEGY

Specific legislation on child online protection has been enacted through the following instruments:

- Section 15 of the US Code, Chapter 91, §§ 6501-6506, included in the US Code by the Children's Online Privacy Protection Act, 1998.

- Section 47 of the US Code, Chapter 5, §§ 254(h)(6).

- Section 18 of the US Code, Chapter 110, §§ 2251-2260A, amended by H.R. 1981, May 2011.

- Section 20 of the US Code, Chapter 72, §§ 9134 (f), included in the US Code by the Children's Internet Protection Act, 2000.

- Adam Walsh Child Protection and Safety Act, July 2006.

- Securing Adolescents from Exploitation Online Act, February 2007.

- Protect our Children Act, October 2008.

- Keeping the Internet Devoid of Sexual Predators, October 2008.

The International Strategy for Cyberspace does not outline child online protection.

2.2 UN CONVENTION AND PROTOCOL

United States has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. United States has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

The following supports provide information on internet safety for parents, children and educators:

-Branch created within the Department of Justice: Internet Crime against Children Task Force.

-The Federal Trade Commission runs the OnGuardOnline website, the federal government website dedicated to bringing information on internet safety.

-Branch created within the US Department of Health and Public Service: Administration for Children and Families.

-Organization authorized to work in partnership with the US Department of Justice: National Center for Missing and Exploited Children.

-The United State Computer Emergency Response Team (US-CERT) does not provide specific information on child online protection but hosts a series of links redirecting to it.

2.4 REPORTING MECHANISM

Complaints can be filed through the OnGuardOnline website. Cyber Tipline of the National Centre for Missing and Exploited Children has a dedicated space to report incidents which include computer incidents related to child online protection.

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

Cyberwellness Profile example – MALAYSIA

CYBERWELLNESS PROFILE
MALAYSIA

BACKGROUND

Total Population: 29.82 million (data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 66.97% (data source: ITU Statistics, December 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:

- Communications and Multimedia Act 1998 [Act 588]
- Computer Crime Act 1997 [Act 563]
- Personal Data Protection Act 2010 [Act 709]
- Penal Code [Act 574]
- Copyright Act 1987
- Digital Signature Act 1997[Act 562]
- Financial Services Act 2013
- Electronic Commerce Act 2006 [Act 658].

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- Communications and Multimedia Act 1998
- Financial Services Act 2013
- Digital Signature Act 1997.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Malaysia has an officially recognized national CIRT (MyCERT) operated by the office of Cybersecurity Malaysia. Malaysia has also a Government CERT (GCERT) which coordinates knowledge sharing and exchanges programs between MyCERT, Internet Service Providers and enforcement agencies.

1.2.2 STANDARDS

Malaysia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the following instruments:

- National Cybersecurity Policy (NCSP)
- National Security Council directive No. 24 "Arahan 24"
- The Cabinet's Decision in 2010
- Arahan Keselamatan under Chief Government Security Office (CGSO).

1.2.3 CERTIFICATION

The Policy Thrust 3 Cybersecurity Technology Framework from the National Cybersecurity policy (NCSP) offers a cybersecurity framework for the certifications and accreditations of national agencies and public sector professionals.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Malaysia has an officially recognized National Cybersecurity Policy (NCSP) which was initiated by the Ministry of Science Technology and Innovation, to harness national effort to enhance the security of Malaysia's Critical National Information Infrastructure (CNII).The Policy was formulated based on a National Cybersecurity Framework that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

1.3.2 ROADMAP FOR GOVERNANCE

The Policy Thrust 1 "Effective Governance" from the National Cybersecurity Policy (NCSP) provides a national governance roadmap for cybersecurity in Malaysia.

1.3.3 RESPONSIBLE AGENCY

The Ministry of Communications and Multimedia (KKMM) and the Ministry of Science, Technology and Innovation (MOSTI) monitor and coordinate the implementation of a national cybersecurity strategy, policy and roadmap by respective agencies.

1.3.4 NATIONAL BENCHMARKING

Malaysia has officially recognized national benchmarking for the national cyber crisis management plan. Malaysia conducted on 2007 by Cybersecurity Malaysia a Malaysian Incident Handling Drill. Cybersecurity Malaysia coordinated the first National Cyber Crisis Exercise Cyber Drill codenamed X-Maya in collaboration with the National Security Council in 2008.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Standards Malaysia is the national standards Body and the national accreditation body, providing confidence to various stakeholders, through credible standardization and accreditation services for global competitiveness and has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

Malaysian Communications and Multimedia Commission provides various types of awareness programs, industry talks, conferences, training programs and workshops on cybersecurity, for the general public as well as for public and private sector employees. CyberSAFE, short for Cybersecurity Awareness for Everyone, is Cybersecurity Malaysia's initiative to educate and enhance the awareness for the general public on the technological and social issues facing internet users, particularly on the dangers of getting online.

1.4.3 PROFESSIONAL CERTIFICATION

Malaysia does not have the exact number of public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

Malaysia does not have any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Malaysian Communications and Multimedia Commission has officially recognized partnerships with the following organizations:

- ASEAN – Japan Partnership
- APT Cybersecurity
- ASEAN Cyber Drill.

1.5.2 INTRA-AGENCY COOPERATION

Malaysia has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector through the national X-MAYA and the National Security Council directive No. 24 named Arahan 24.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Policy Thrust 7 "Cybersecurity Emergency Readiness" from the National Cybersecurity Policy (NCSP) provides officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

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

Cyberwellness Profile example – MALAYSIA

1.5.4 INTERNATIONAL COOPERATION

Malaysia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Malaysia participated in the International Cyber Shield Exercise 2014 in Turkey (ICSE 2014).

Malaysia participated in the following cybersecurity activities:

- ASEAN JAPAN Information Security
- APT Cybersecurity Forum
- Meridian Conference
- Octopus Conference (Cooperation against cybercrime)
- JTC 1/SC 27 Meeting

MyCERT is a member of FIRST.

2. CHILD ONLINE PROTECTION

2.2 NATIONAL LEGISLATION

Specific legislation on child online protection has been enacted through the following instruments:

- Child Act 2001 (Act 611)
- Section 293, Penal Code (Act 574)
- Sections 211 and 233, Communications and Multimedia Act 1998.

2.3 UN CONVENTION AND PROTOCOL

Malaysia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child. Malaysia has acceded, with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.4 INSTITUTIONAL SUPPORT

Ministry of Women, Family and Community Development (MWFCD), Malaysian Communications and Multimedia Commission (MCMC) and the Ministry of Education (MOE) provide information on internet safety for parents, children and educators.

2.5 REPORTING MECHANISM

Online illegal content can be reported on the Child line 15999. NUR Alert is responsible for spreading information as fast as possible to help trace missing children (below 12 years of age) who could be victims of crime or abuse. NUR Alert comes under the National Child Protection Policy and Action Plan.

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

National Strategies Repository

YOU ARE HERE HOME > ITU-D > CYBERSECURITY > NATIONAL STRATEGIES REPOSITORY

SHARE

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

This Repository includes the National Cybersecurity Strategies, be it in a form of a single or multiple documents or as an integral part of a broader ICT or national security strategies.

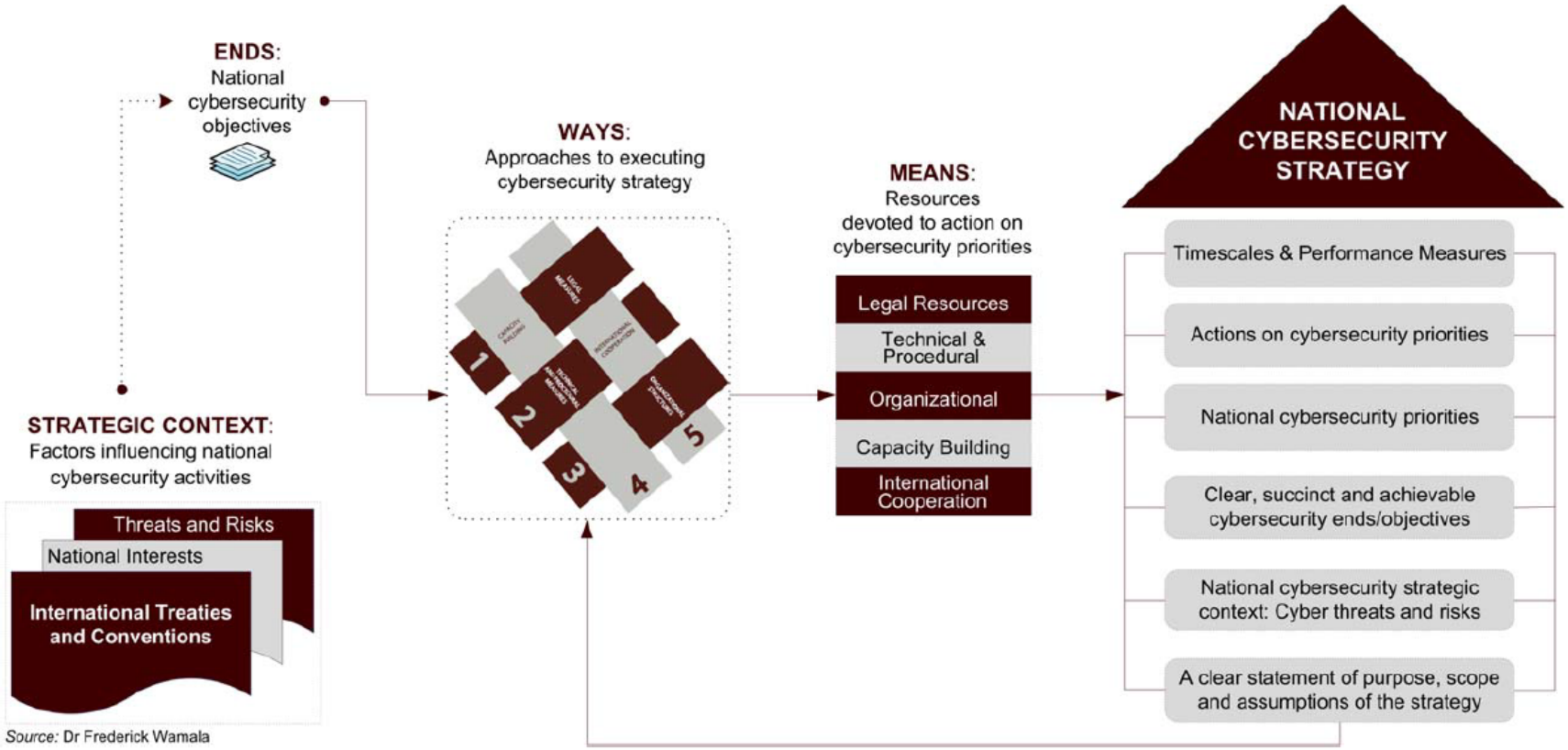
** Please note that not all of the documents are available in English.*

72 *out of 193 ITU Member States currently have a publicly available National Cybersecurity Strategy.*

A-J	K-Q	R-Z
Afghanistan	Kenya	Romania
Albania	Korea (Republic of)	Russian Federation (1, 2)
Australia	Latvia	Rwanda
Austria	Lithualia	Saudi Arabia
Azerbaijan	Luxembourg	Serbia
Bangladesh	Malawi	Singapore
Belgium (1, 2)	Malaysia	Slovakia
Bosnia and Herzegovina *(Draft)*	Malta	South Africa
Brazil (1, 2, 3, 4, 5)	Mauritania	Spain
Brunei Darrussalam	Mauritius	Sweden
Canada	Micronesia	Switzerland
China	Moldova	Trinidad and Tobago
Colombia	Montenegro	Turkey
Croatia	Morocco	Uganda
Cyprus	Netherlands (1, 2)	United Kingdom
Czech Republic	New Zealand	United States of America (1, 2, 3)

Source: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

Cybersecurity Strategy Model



Source: Dr Frederick Wamala

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

National Cyber Security Strategy ITU Cyber Security Toolkit:

The aim – create a toolkit to help states to create or improve cyber security strategies

Examples of Topics To Be Addressed

- The role, objectives and scope of a National Cyber Security Strategy in a line with the UN SDGs
- The definition/publication/review process: the Governance Model
- National and International Standards and government compliance program
- Critical Infrastructure Protection and integration with other national security/emergency programs
- National Risk Management program
- National Incident Response/CERT - integration/alignment with Military/Intelligence
- Implementation strategies for the Government
- Implementation strategies for Private Sector
- The definition/publication/review process: the Awareness Programme
- Aspects not typically covered by public strategies that should be considered and addressed

Components of Toolkit

Reference Guide

- A **single resource** for any country to gain a clear understanding of National Cyber Security Strategy in terms of:
  - the **purpose and content**
  - how to go about **developing a strategy,** including **strategic areas and capabilities**
  - the relevant **models and resources** available
  - the **assistance available** from various organisations and their contact details
- FORMAT: 15-20 page Word / PDF

Evaluation Tool

- A **simple tool** that allows national governments and stakeholders to:
  - Evaluate their **current status in each of the strategic areas** identified in the reference guide
  - Evaluate their **current status in cyber security lifecycle management**
  - Easily **identify key areas** for improvement
  - Provide a means for **measuring improvements** over time
- FORMAT: Excel or web-based worksheet

Cybersecurity in Asia-Pacific region

- National Cybersecurity Strategy & Cybersecurity Awareness : Nepal (2016-2015)
- Readiness Assessment to Establish a National CIRT for Fiji (2014-2015)
- Workshop on Cybersecuirty and Cybercrime Legislation & Cybersecurity Incident Simulation Bangkok 23 March 2015
- INTERPOL-ITU Cybercrime Investigation Seminar,19-21 Feb 2014, Malaysia
- First Pacific Islands Capacity Building Workshop on Child Online Protection and Commonwealth National Cybersecurity Framework Regional Workshop, 22-24 September 2014, Vanuatu
- Establishment of Pac CIRT, Fiji
- Readiness assessment National Cybersecurity Strategy, Bangladesh (2013)
- ITU Cyber Security Forum & Cyber Drill, 9-11 Dec 2013, Vientiane, Lao P.D.R
- Enhancement of cybersecurity capabilities (CIRT) Bhutan (2013)
- CIRT Capacity Building for Afghanistan (2014 and 2015)

ITU/EC ICB4PAC : Model Cybersecurity Strategies &COP

Regulatory Harmonization Cycle

7 Priority Areas
National ICT Policy
Interconnection Cost Modeling
International Roaming
Cyber-security
Licensing
Universal Service
Numbering

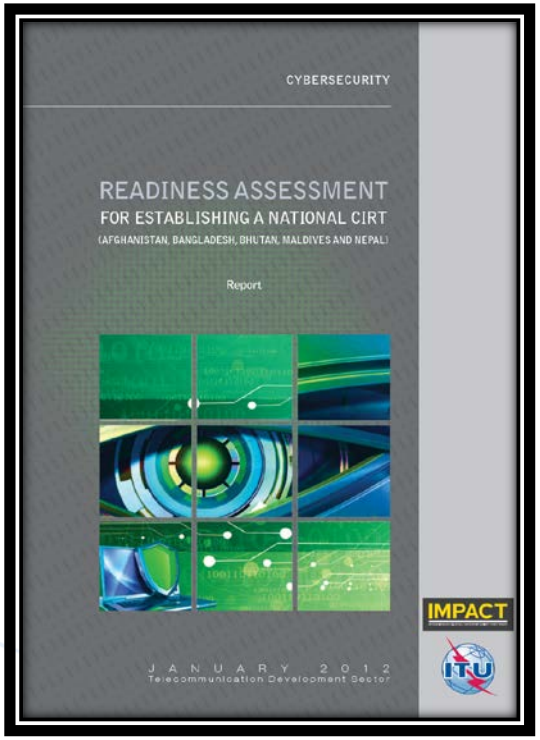
Country
Cook Islands
Fiji
Micronesia
Kiribati
Marshall Islands
Nauru
Niue

Country
Palau
PNG
Samoa
Solomon Islands
Tonga
Tuvalu
Vanuatu

CIRT Assessment in ABBMN Countries

ITU carried our CIRT assessment as a part of Afghanistan Bangladesh Bhutan Maldives Nepal (ABBMN) Ministerial Forum in 2012 in five South Asian Countries with following objectives

1. Assist in study of the readiness assessment of current cybersecurity needs in each country
2. Study and suggest institutional and organizational requirements and arrangements for CIRT in each country
3. Develop areas of proactive and reactive response measures in each country
4. Develop Membership Policies for CIRT in each country
5. Develop Policies to coordinate with internal agencies as well as international CIRTs taking into account policies for ITU IMPACT initiative on CIRT in each country
6. Design specifications for hardware and software for CIRT for each country



The Ministerial Declaration along with the CIRT Assessment was published in January 2012 and is available at :

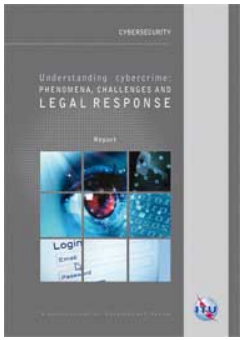
http://www.itu.int/ITU-D/asp/CMS/Docs/CIRT_ABBMN_Assessment.pdf

Cyber Drills in Asia-Pacific

- Two Cyber Drills carried out in the region by ITU in 2011 and 2012
- A Forum was also organized inviting CERT representatives who shared their experiences, issues, challenges and initiatives.
- Industry leaders shared their thoughts on cybersecurity-related technologies and solutions.
- Buit networking among participating CERTs. For example, during the 2011 Forum, CERTs agreed to collaborate and coordinate among each other even after the Froum
- Bilateral actions/cooperation such as mission exchange were done by themselves and only informing/updating ITU
- In the case of the 2013 drill, we invited telcos, academia and other government agencies to observe the drill

✓2011 : http://www.itu.int/ITU-D/asp/CMS/Events/2011/CIRTWkshp/index.asp)
✓ 2013 : http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2013/12_Vientiane_Lao_PDR/CDrill.aspx).

Building a global partnership



INTERPOL

Capacity building initiatives, joint consultations and more.

UNODC
United Nations Office on Drugs and Crime

Best practices in cybercrime legislations, joint technical assistance to member states, information sharing

Symantec. TREND MICRO

Tap on expertise of globally recognized industry players and accelerate info sharing with ITU member states

ABIresearch
technology market intelligence

Collaboration with ABI Research – **The Global Cybersecurity Index (GCI)**

FIRST
Improving Security Together

Collaboration with FIRST – To share best practices on computer incident response, engage in joint events, facilitate affiliation of national CIRTS of member states

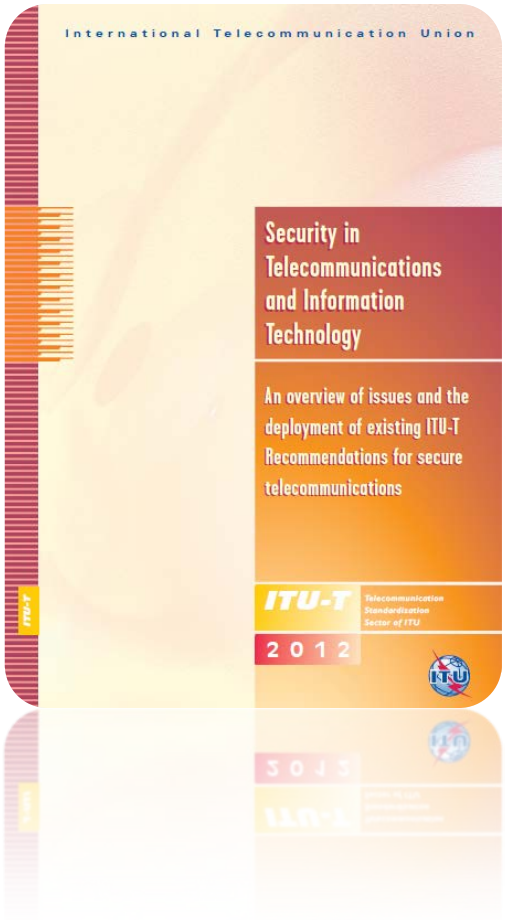
e.oman

NCC
NIGERIAN COMMUNICATIONS COMMISSION

Collaboration with Member States – Regional Cybersecurity Centres

ITU

General security objectives for ICT networks



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.

Global Cybersecurity Index

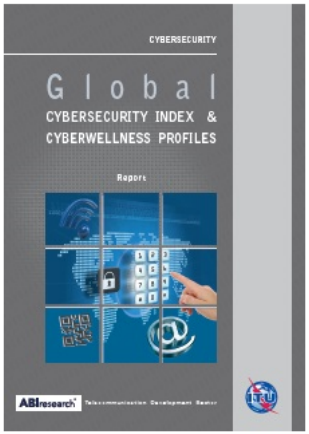
YOU ARE HERE HOME > ITU-D > CYBERSECURITY > GLOBAL CYBERSECURITY INDEX

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

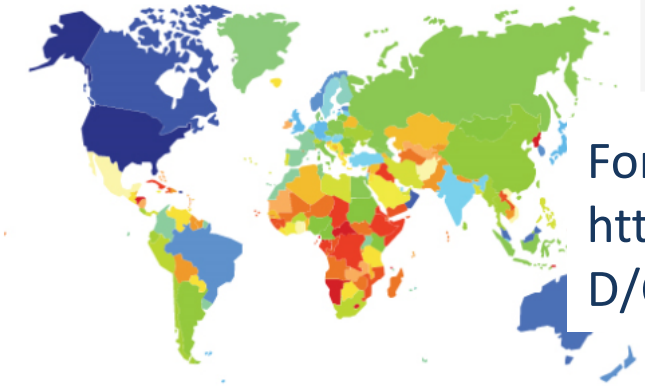
Global Cybersecurity Index Conceptual Framework: English, French, Spanish

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

Conclusions

- While it will never be possible to completely remove all risks, drawing together an effective policies and practices, infrastructure & technology, awareness and communication can do a great deal to help.
- The international cooperation, based on a multi-stakeholder approach and the belief that every organization – whether online or mobile, educator or legislator, technical expert or industry body – has something to contribute.
- Human and institutional capacity building critical to understand and take reactive / proactive response to cyberthreats
- By working together with ITU and its partners critical international collaboration can be achieved to make the Internet a safe and secure not for us but for our children as well!

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

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

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

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

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);

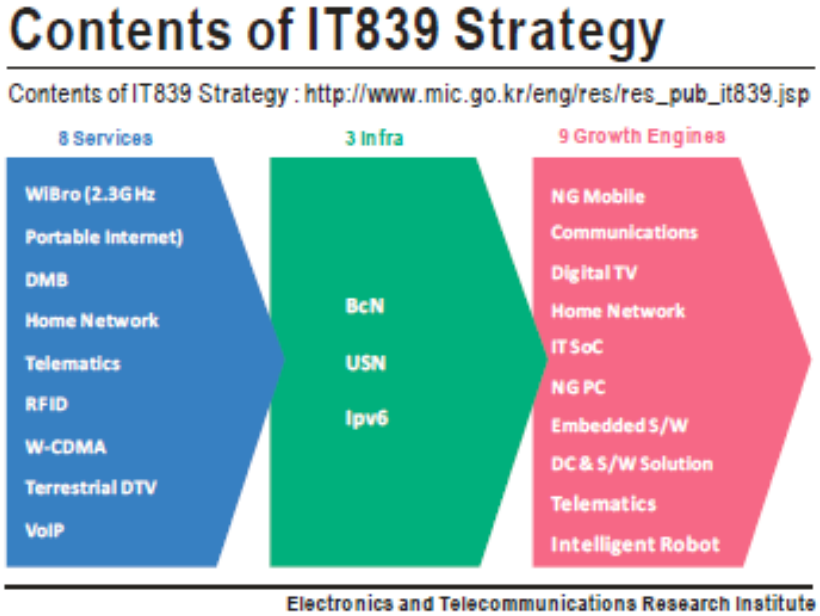
- Establishing national “roadmaps” with benchmarks and timetables for IPv6 deployment;

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

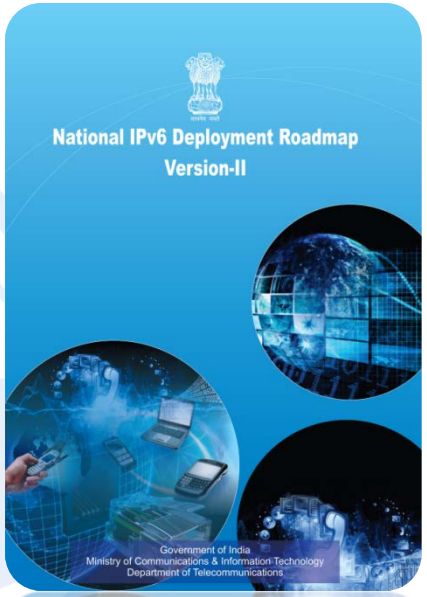
- Promoting the use of IPv6 in government-funded educational, science and research networks; and

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

Governments promoting IPv6 deployment (examples)



LAOS



MONGOLIA

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;

IPv6 Infrastructure Security (ITU-T X.1037)

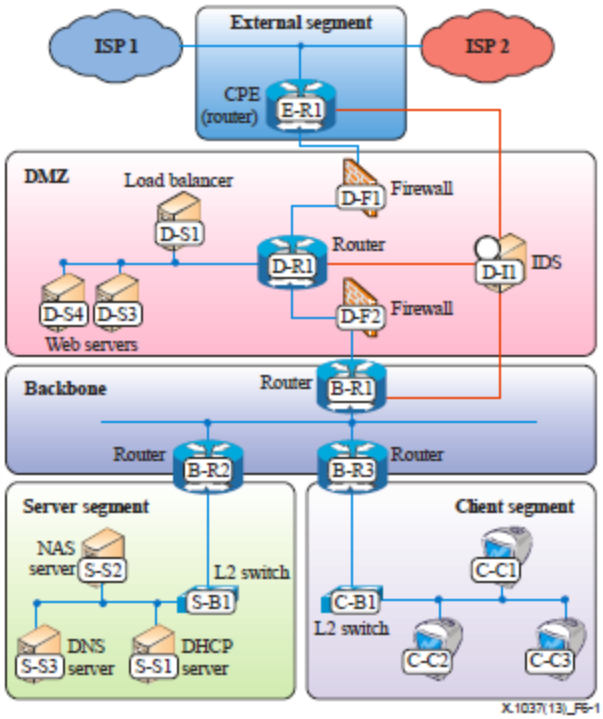


Figure 6-1 – Example topology of an IPv6 enterprise network

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

ITU : I Thank U