
Role of ITU in Building Security & Trust in Cyberspace

Odessa, Ukraine, 15-17 June 2016

Sameer Sharma

Senior Advisor, ITU Regional Office, Bangkok



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

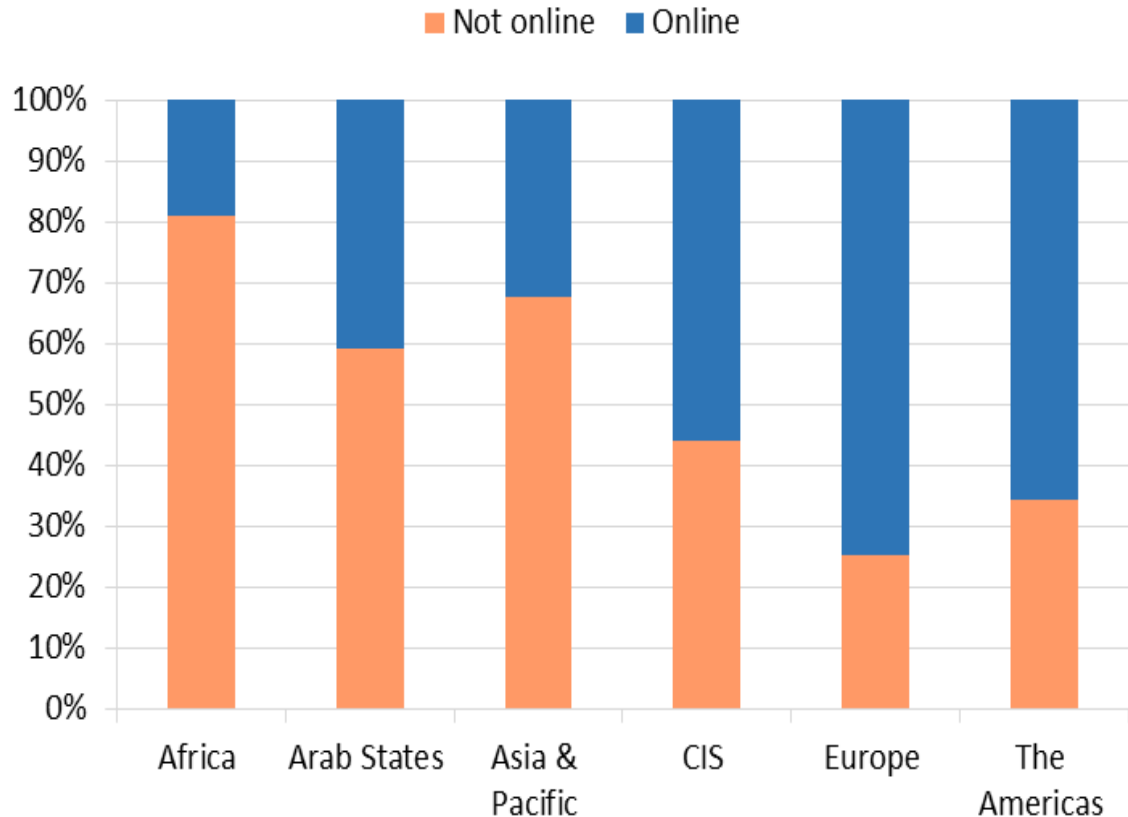
Mobile broadband penetration:
- 84% developed countries
- 21% developing countries

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

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.



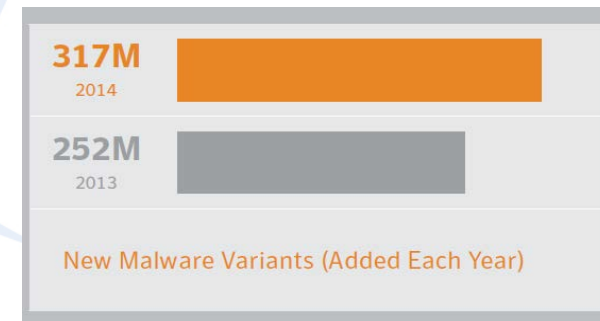
Cybersecurity not seen yet as a cross-sector, multi-dimensional concern.

Still seen as a technical/technology problem.



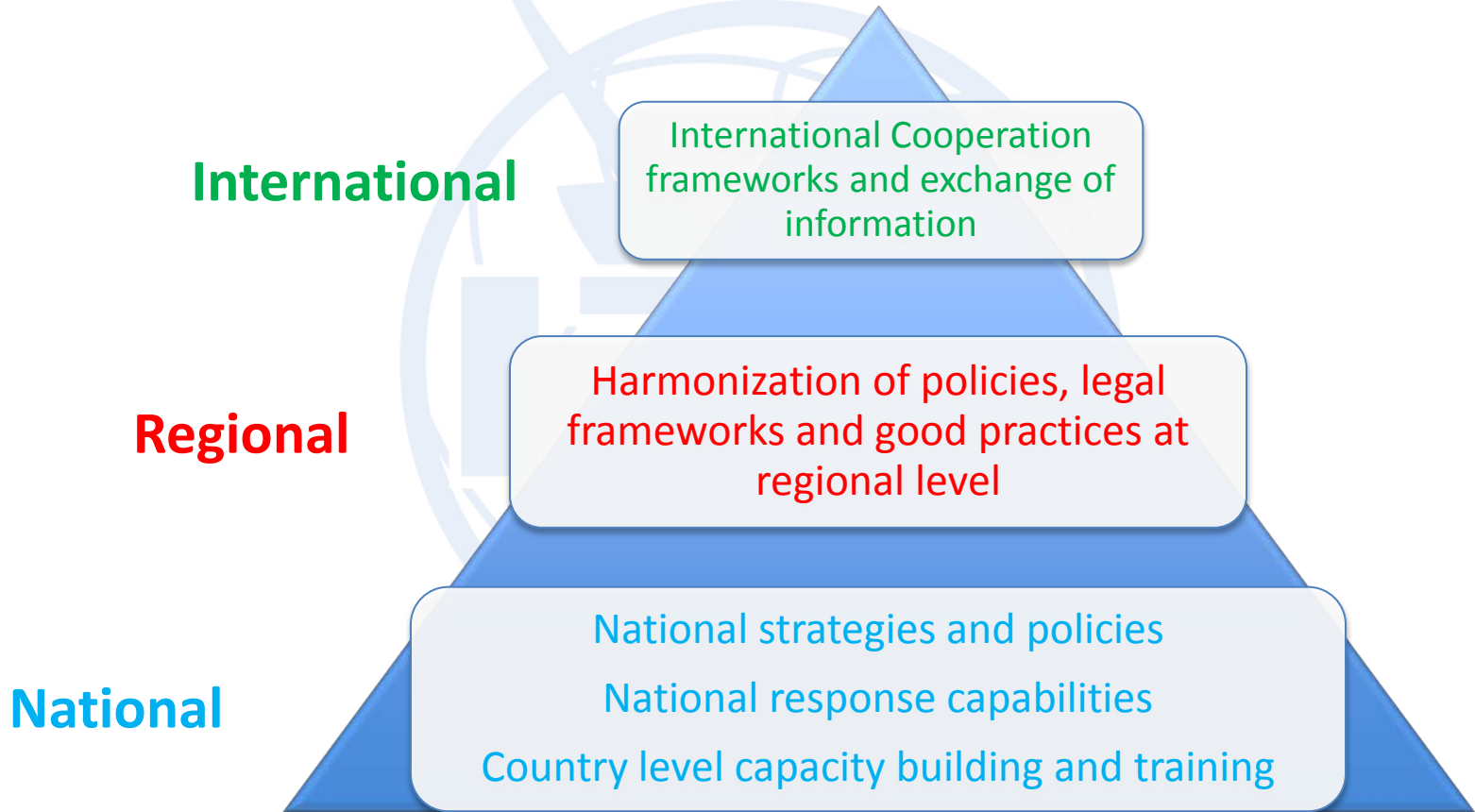
Importance of Cybersecurity

- 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



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**”



2007

Global Cybersecurity Agenda (GCA) was launched by ITU
Secretary General

GCA is a **framework for international cooperation in cybersecurity**

2008 to date

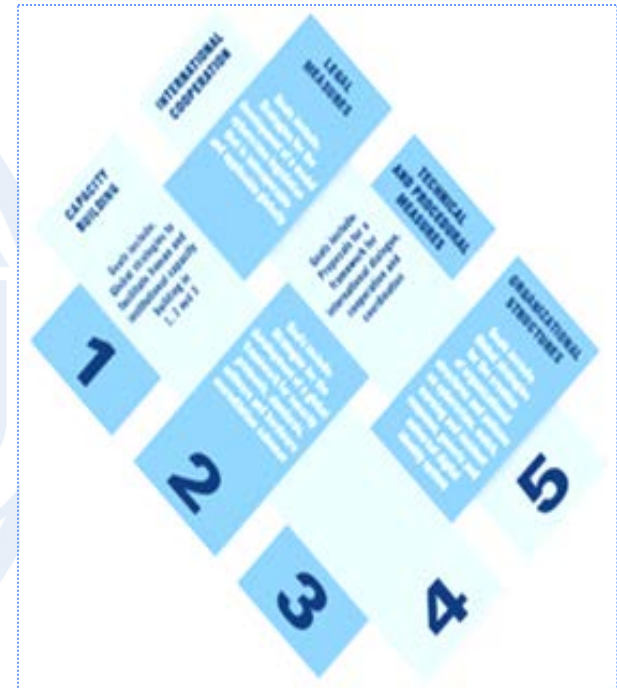
ITU Membership endorsed the GCA as the ITU-wide
strategy on international cooperation.



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 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**

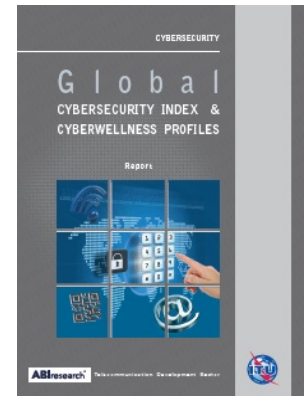
<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>

Next iteration in progress

ABIresearch®



Global
Cybersecurity
Index



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

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



CYBERWELLNESS PROFILE UKRAINE



BACKGROUND

Total Population: 44 940 000

(data source: [United Nations Statistics Division](#), December 2012)

Internet users, percentage of population: 41.80%

(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:

- The Penal Code Act
- The Computer Misuse Act.

1.1.2 REGULATION AND COMPLIANCE

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

- NITA-U Act
- Access to information Act
- Electronic Signatures Act
- Electronic Transactions Act
- The Electronic Transactions Regulations.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Ukraine has an officially recognized national CIRT known as [CERT-UA](#).

1.2.2 STANDARDS

There is no officially approved national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards in Ukraine.

1.2.3 CERTIFICATION

There is no cybersecurity framework for the certification and accreditation of national agencies and public sector professionals in Ukraine.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Ukraine has an officially recognized National Security Strategy.

1.3.2 ROADMAP FOR GOVERNANCE

There is no national or sector-specific governance roadmap for cybersecurity in Ukraine.

1.3.3 RESPONSIBLE AGENCY

The function of overseeing cybersecurity is shared between: The Security Service of Ukraine ([SSU](#)), the [State Special Communication Service](#), and [the Ministry of Internal Affairs](#).

1.3.4 NATIONAL BENCHMARKING

Ukraine has no officially recognized national benchmarking and referential to measure cybersecurity development.

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

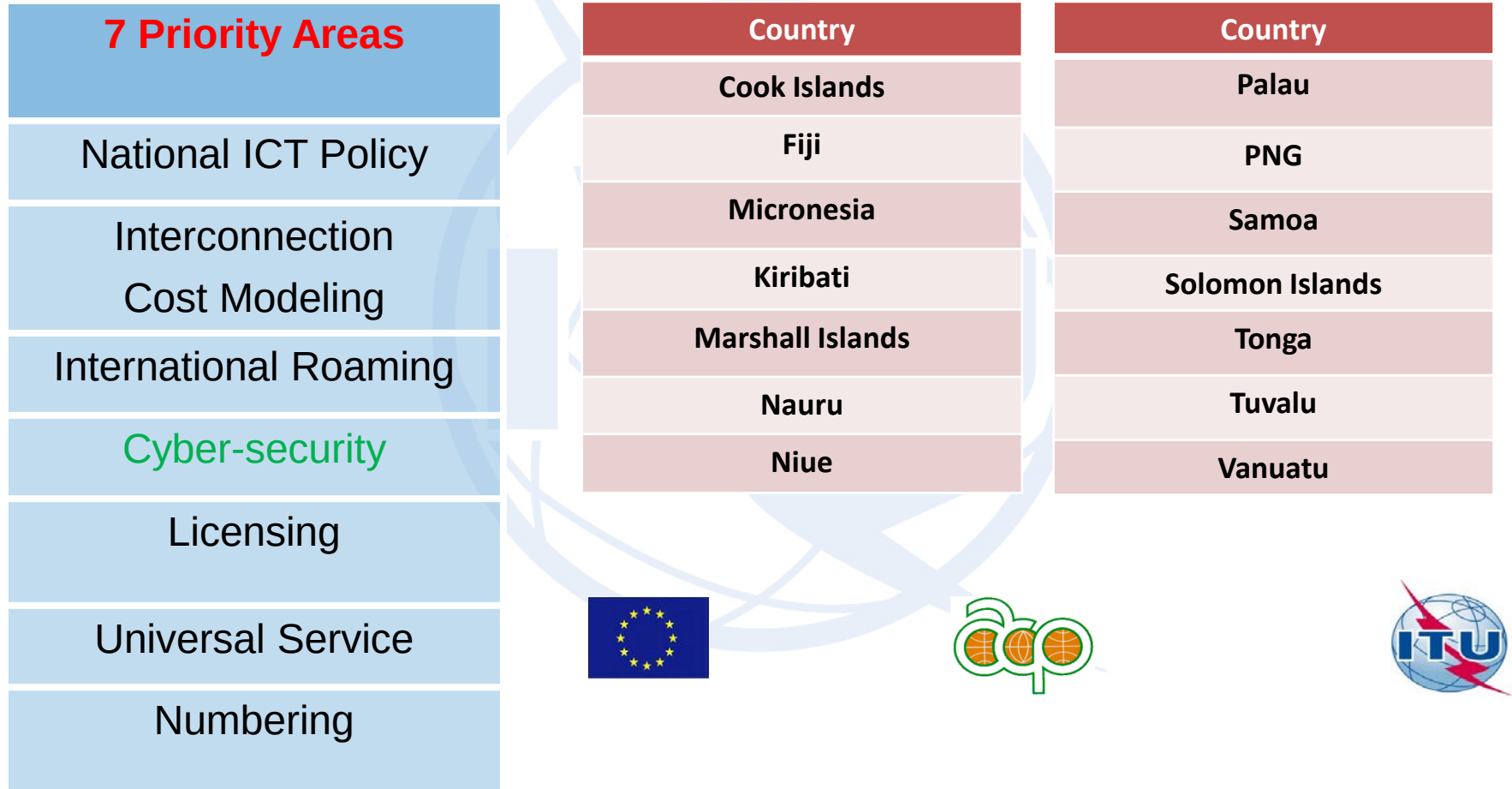
Evaluation Tool

- 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 Cybersecurity 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)

Regulatory Harmonization Cycle



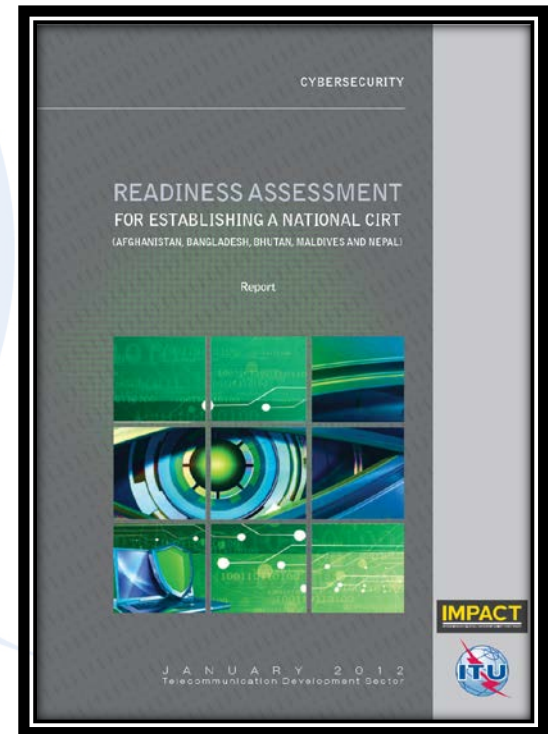
CIRT Assessment in ABBMN Countries

ITU carried out 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.
- Built networking among participating CERTs. For example, during the 2011 Forum, CERTs agreed to collaborate and coordinate among each other even after the Forum
- 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

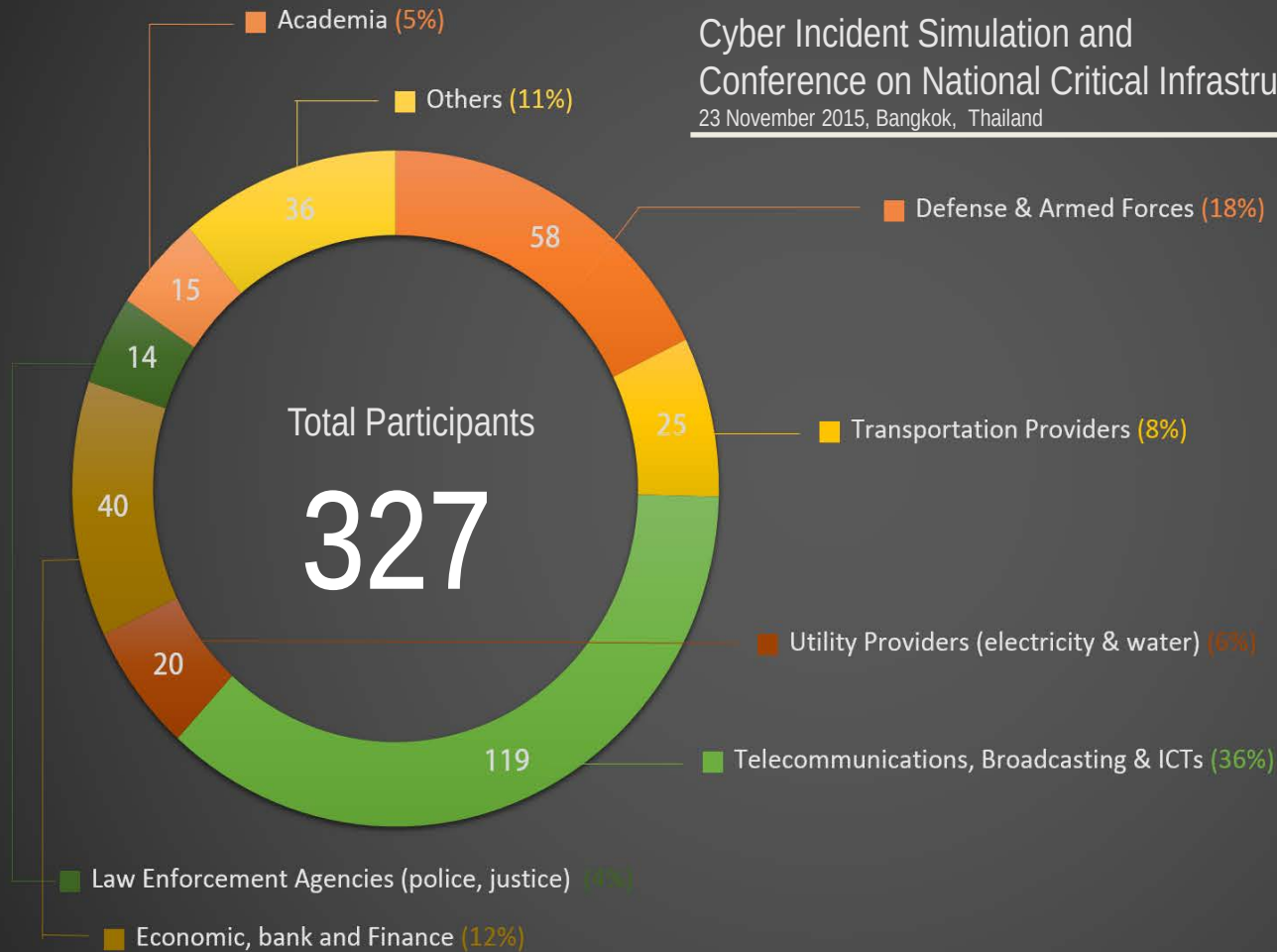
✓2011 : <http://www.itu.int/ITU-D/asp/CMS/Events/2011/CIRTWkshp/index.asp>)

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

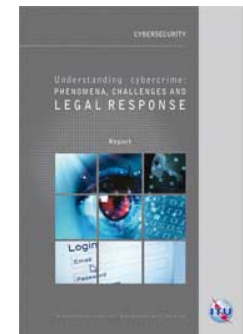


Critical Infrastructure Protection Conference

Cyber Incident Simulation and
Conference on National Critical Infrastructure Protection
23 November 2015, Bangkok, Thailand



Building a global partnership



Capacity building initiatives, joint consultations and more.



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



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



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



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



Collaboration with Member States – Regional Cybersecurity Centres



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 : I Thank U