ITU Global Cybersecurity Agenda and Child Online Protection (COP)

United Nations Cybercrime Study Workshop
7-8 April 2012, Bangkok, Thailand

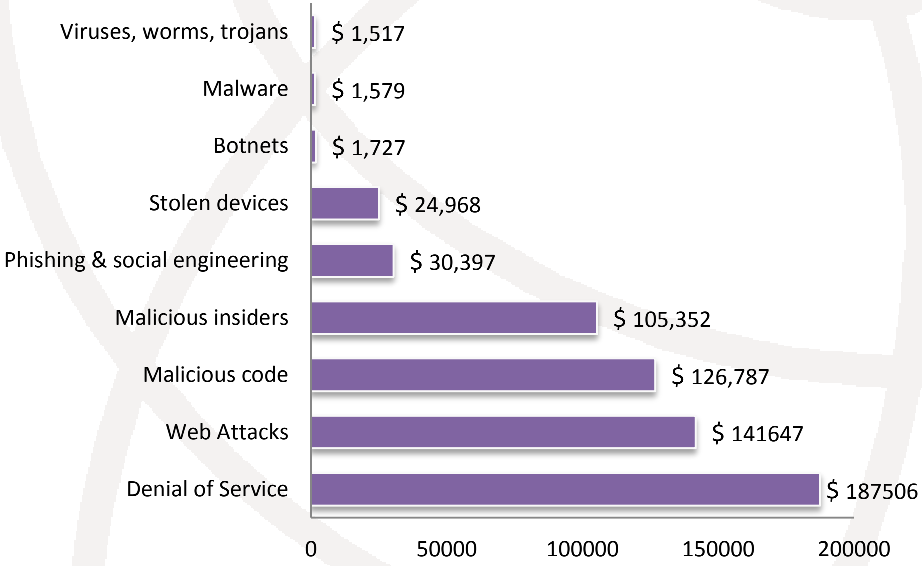
Sameer Sharma
(sameer.sharma@itu.int)
Senior Advisor, ITU Regional Office for Asia and the Pacific

Some Major Attacks in 2011-2012

March 2011	• Hackers penetrate French government computer network • South Korea Defense Network penetrated • RSA Secure ID compromised • Attacks at EU's Commission and External Action Service
June 2011	• Attacks at Sony. Millions of logins leaked • Attacks and NATO internal network • Attacks at International Monetary Fund (IMF) • Hackers disrupt 51 Malaysian government websites • UK Treasury under sustained cyberattack
October 2011	• Cyber-attacks on UK at disturbing levels • Japan under Heavy Cyber Attack
November 2011	• Hackers destroyed a pump used by a US water utility • Duqu computer virus Detected by Iran civil defense organization • More than 100 Pakistani Government Sites Under Malware attack • Thousands of United Nation (UNDP) logins leaked • Cyber attacks hit Fujitsu local government system in Japan • Largest DDOS attack hit Chinese company
January 2012	• Hackers attack Brazil's largest private bank, shut down online banking • European Parliament says its website taken offline by attackers • Investigations Involving the Internet and Computer Networks • DDoS against Polish government websites • Hackers manipulated railway computers • 103 Government of Kenya websites hacked overnight

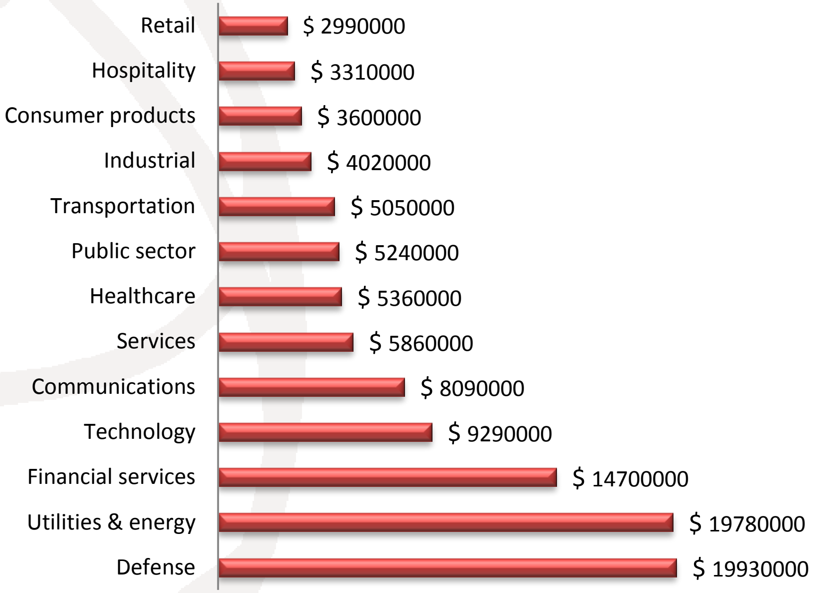
Financial impact

- It is estimated that overall cost of cybercrime is as much as $1 trillion on a global basis.
- The estimated average cost to an individual US organization was $3.8 million per year in 2010.
- In 2011 the estimated average cost to an individual US organization is $5.9 million per year, with a range from $1.5 million to $36.5 million per organization.
- The most costly cyber crimes are those caused by malicious code, denial of service, stolen or hijacked devices and malicious insiders.
- Cyber Crime costs British Economy £27 Billion a year.



Average annualized cyber crime cost weighted by the frequency of attack incidents

Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf



Average annualized cost by sector for sample of 50 US organizations for 2011

Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

Key Cybersecurity Challenges

- Lack of adequate and interoperable national or regional legal frameworks
- Lack of secure software and 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

Cybersecurity not seen yet as a cross-sector, multi-dimensional concern. Still seen as a technical/technology problem.

Global Cybersecurity Cooperation

Cyber threats/vulnerabilities are global challenges that cannot be solved by any single entity alone!

The world is faced with the challenging task of developing harmonized and comprehensive strategies at the global level and implementing these with the various relevant national, regional, and international stakeholders in the countries

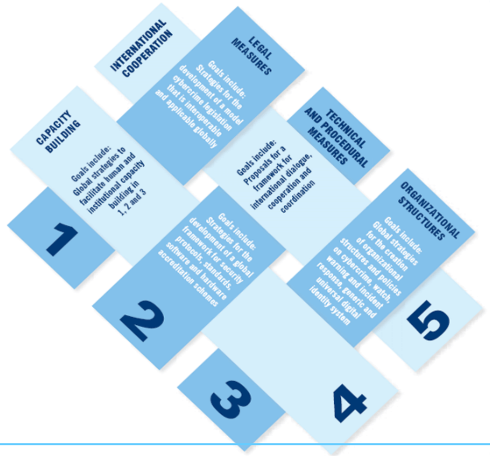
ITU and Cybersecurity

world summit
on the information society
Geneva 2003 - Tunis 2005

2003 – 2005

WSIS entrusted ITU as sole facilitator for WSIS Action Line C5

“Building Confidence and Security in the use of ICTs”



1 CAPACITY BUILDING
Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3

INTERNATIONAL COOPERATION

LEGAL MEASURES
Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally

2
Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes

TECHNICAL AND PROCEDURAL MEASURES

3

4
Goals include: Proposals for a framework for international dialogue, cooperation and coordination

ORGANIZATIONAL STRUCTURES
Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

5

2007

ITU Secretary-General launched the Global Cybersecurity Agenda (GCA)

A framework for international cooperation in cybersecurity

G C A GLOBAL CYBERSECURITY AGENDA

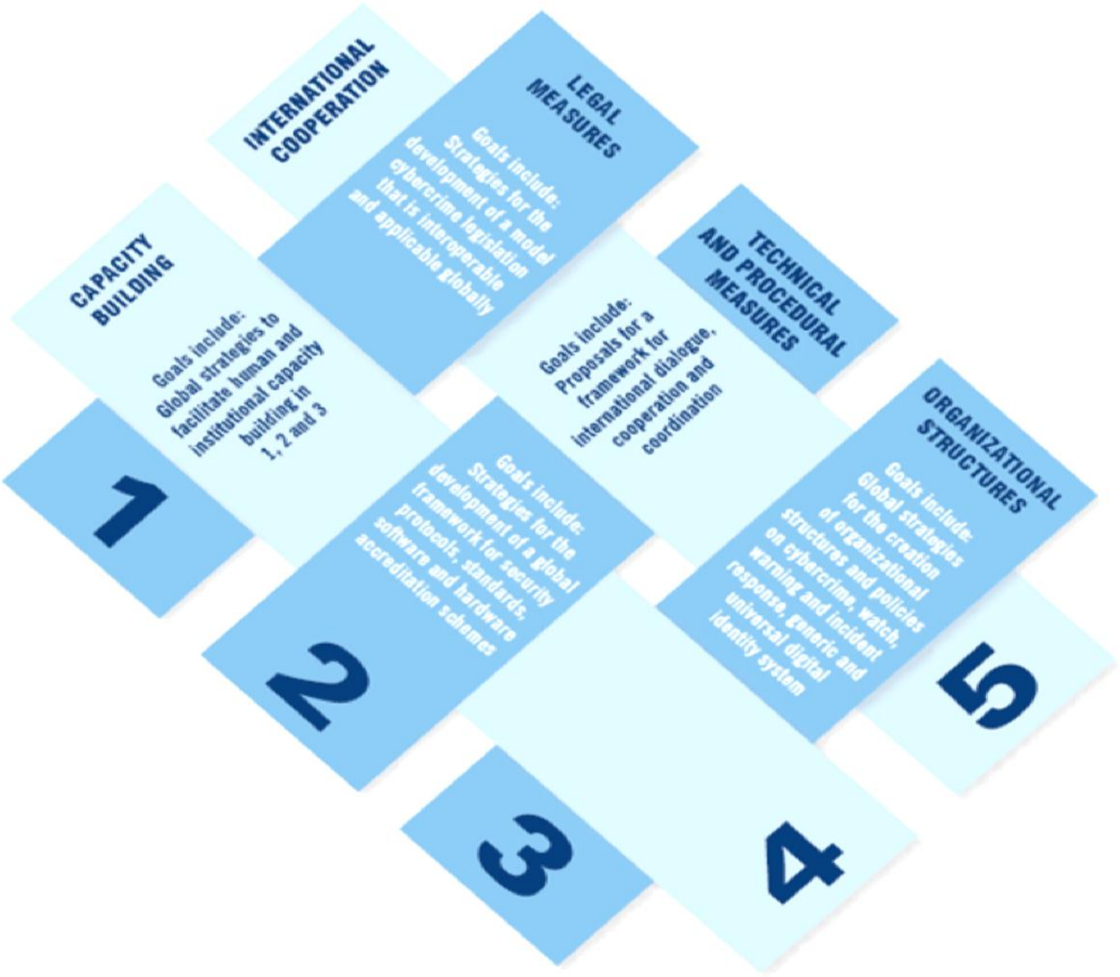
IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

Child Online Protection

2008 - 2010

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

Global Cybersecurity Agenda (GCA)



LEGAL MEASURES

Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally

1

TECHNICAL AND PROCEDURAL MEASURES

Goals include: Strategies for the development of a global framework for security protocols, standards, software and hardware accreditation schemes

2

ORGANIZATIONAL STRUCTURES

Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

3

CAPACITY BUILDING

Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3

4

INTERNATIONAL COOPERATION

Goals include: Proposals for a framework for international dialogue, cooperation and coordination

5

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: From Strategy to Action

Global Cybersecurity Agenda (GCA)

1. Legal Measures

ITU Toolkit for Cybercrime Legislation

ITU Publication on Understanding Cybercrime: A Guide for Developing Countries

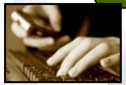
2. Technical and Procedural Measures

ITU Standardization Work
ICT Security Standards Roadmap
ITU-R Security Activities
ITU-T Study Group 17
ITU-T Study Group 2

3. Organizational Structures

CIRT assessments and deployment
ITU work on CIRTs cooperation
ITU Cybersecurity Information Exchange Network (CYBEX)

4. Capacity Building



ITU National Cybersecurity Strategy Guide
ITU Botnet Mitigation Toolkit and pilot projects

Regional Cybersecurity Seminars
Cybersecurity Assessment and Self assessment

5. International Cooperation

ITU High-Level Expert Group (HLEG)
ITU-IMPACT Collaboration
ITU Cybersecurity Gateway

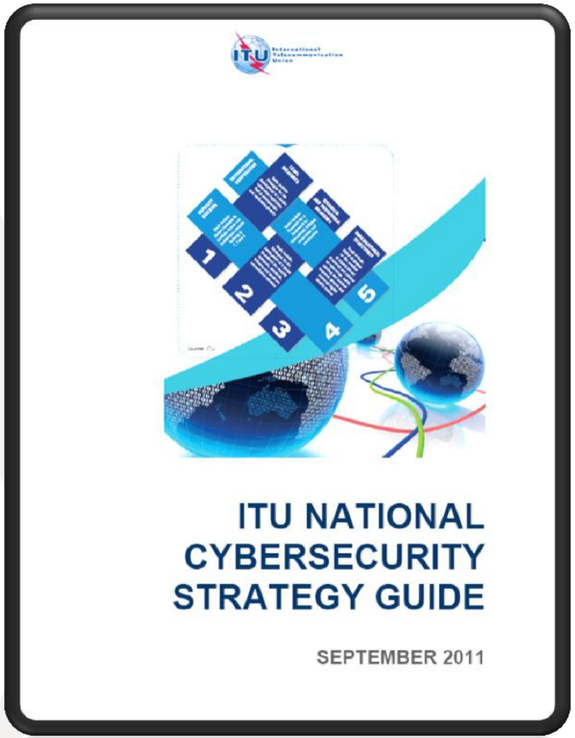
ITU's Child Online Protection (COP)

Collaboration with UNICEF, UNODC, UNICRI, UNICITRAL and UNDIR

Examples of Recent Initiatives

ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

The Guide focuses on the issues that countries should consider when elaborating or reviewing national Cybersecurity strategies.



ITU NATIONAL CYBERSECURITY STRATEGY GUIDE

SEPTEMBER 2011

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Collaboration towards A Global Strategy

The world's foremost cybersecurity alliance!

- Within GCA, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) are pioneering the deployment of solutions and services to address cyberthreats on a global scale.
- ITU-IMPACT's endeavor is the first truly global multi-stakeholder and public-private alliance against cyber threats, staging its state-of-the-art facilities in Cyberjaya, Malaysia.
- As executing arm of ITU on cybersecurity, IMPACT supports 193 Member States and others with the expertise, facilities and resources to effectively enhance the global community's capability and capacity to prevent, defend against and respond to cyber threats.

ITU IMPACT

Services for Member States

As of today, 140 countries joined ITU-IMPACT

- Region A – Americas – *23 Countries*
  - Antigua and Barbuda, Barbados, Belize, Brazil, Costa Rica, Cuba, Dominican Republic, Ecuador, Grenada, Guatemala, Guyana, Haiti, Honduras, Panama, Paraguay, Peru, Saint Lucia, Saint Vincent and Grenadines, Saint Kitts and Nevis, Suriname, Trinidad and Tobago, Uruguay, Venezuela
- Region B – Western Europe – *14 Countries*
  - Andorra, Austria, Bosnia & Herzegovina, Croatia, Cyprus, Italy, Lithuania, Malta, Monaco (Principality) Spain, Switzerland, Turkey, Vatican City, San Marino (Republic of)
- Region C – Eastern Europe – *13 Countries*
  - Albania, Armenia, Azerbaijani Republic, Bulgaria, Georgia, Kyrgyz Republic, Moldova, Montenegro, Poland, Romania, Serbia, Slovenia, Ukraine
- Region D – Africa – *50 Countries*
  - Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Chad, Cote d'Ivoire, Comoros, Democratic Republic of Congo, Republic of Congo, Djibouti (Republic of) Egypt, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Republic of Guinea, Republic of Guinea – Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, Sudan, Swaziland, Tanzania, Togo, Tunisia, Uganda, Zambia, Zimbabwe
- Region E – Asia & Australasia – *40 Countries*
  - Afghanistan, Bangladesh, Bhutan, Brunei Darussalam, China, Fiji, India, Indonesia, Iran,Iraq, Israel, Jordan, Lao PDR, Lebanon, Micronesia, Malaysia, Maldives, Marshall Islands, Mongolia, Myanmar, Nauru, Nepal, Oman, Pakistan, Philippines, Papa New Guinea, Qatar, SamoaSaudi Arabia, Sri Lanka, Syria, Solomon Islands, Timor Leste, Thailand, Tonga, Tuvalu, United Arab Emirates, Vanuatu, Vietnam, Yemen

ITU – UNODC MoU: Areas of Cooperation

- *Legal Measures*
- *Capacity Building and Technical Assistance (National and Regional)*
- *Intergovernmental and expert meetings*
- *Joint Study*
- *Sharing knowledge and information*

ITU COP Initiatives

Online Threats to Children

Cybergrooming

Child abuse materials

Pornography

Sexual solicitation

Disclosure private information

Child pornography

Threats & Risks

Violence

Cyberstalking

Racism

Online Fraud

Phishing attacks

Spam

Cyber Bullying

Youth-to-youth cybercrimes

Online Gaming & Addiction

Anorexia, self-harm or suicide

ITU’s Role in Child Online Protection

- At the ITU PP in 2010, ITU Member States adopted a new Resolution concerning ITU’s Role in Child Online Protection (Res. 179, Guadalajara 2010).
- This new resolution encourages ITU to continue its COP initiative as a platform to raise awareness and educate stakeholders on this important issue.

Instructs the [ITU] Secretary-General,

- *to deploy greater efforts to ascertain the activities carried out by other United Nations organizations in this domain, and to coordinate with them appropriately, with the objective of establishing partnerships to maximize and synergize efforts in this important area;*
- *to coordinate ITU activities also with other similar initiatives being undertaken at the national, regional and international levels, in order to eliminate possible overlaps;*
- *to bring this resolution to the attention of other COP members and of the United Nations Secretary-General, with the aim of increasing the engagement of the United Nations system in child online protection;*
- *to submit a progress report on the results of implementation of this resolution to the next plenipotentiary conference,*

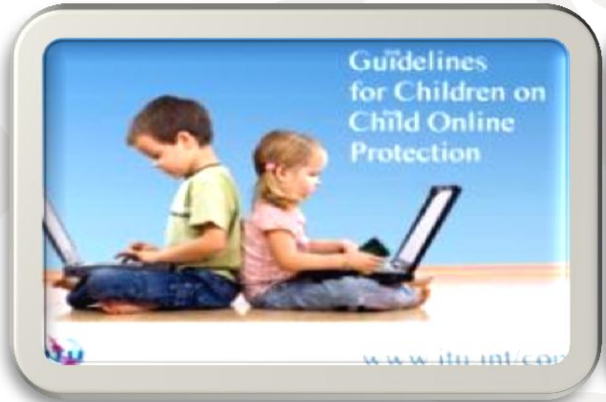
ITU Child Online Protection (COP)

- ITU launched the Child Online Protection (COP) Initiative in 2008 within the framework of the Global Cybersecurity Agenda (GCA), aimed at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

- **Key Objectives of COP**
  - Identify risks and vulnerabilities to children in cyberspace;
  - Create awareness of the risks and issues through multiple channels;
  - Develop practical tools to help governments, organizations and educators minimize risk; and
  - Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives

COP Guidelines

ITU has worked with some COP partners to develop the first set of guidelines for different stakeholders: Available in the six UN languages (+ more)



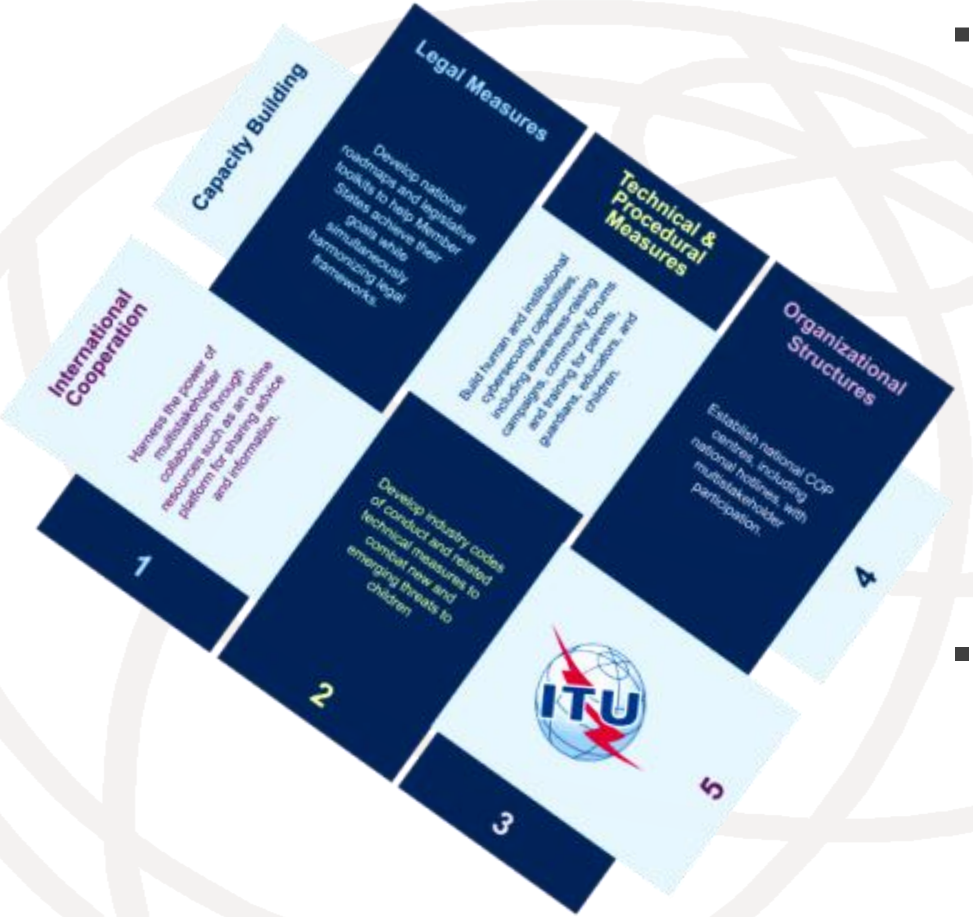
Guidelines for Children on Child Online Protection

Guidelines for Parents, Guardians and Educators on Child Online Protection

Guidelines for Industry on Child Online Protection

Guidelines for Policy Makers on Child Online Protection

COP Five Strategic Pillars



Legal Measures

Develop national roadmaps and legislative toolkits to help Member States achieve their goals while simultaneously harmonizing legal frameworks.

Technical & Procedural Measures

Build human and institutional cybersecurity capabilities, including awareness-raising campaigns, community forums and training for parents, guardians, educators, and children.

Organizational Structures

Establish national COP centres, including national hotlines, with multistakeholder participation.

Capacity Building

Develop industry codes of conduct and related technical measures to combat new and emerging threats to children

International Cooperation

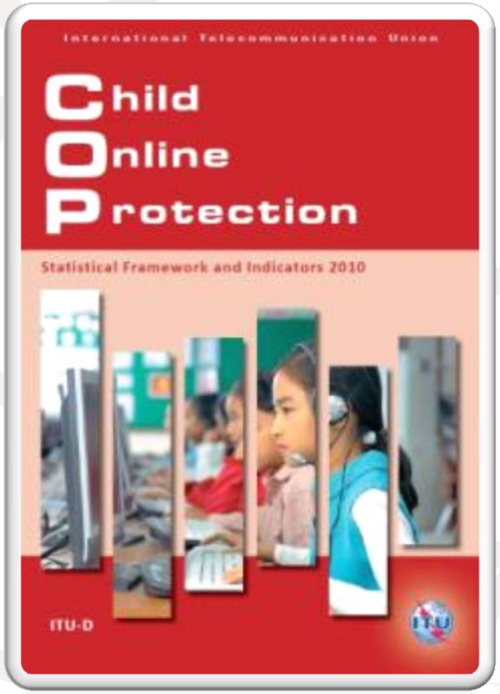
Harness the power of multistakeholder collaboration through resources such as an online platform for sharing advice and information.

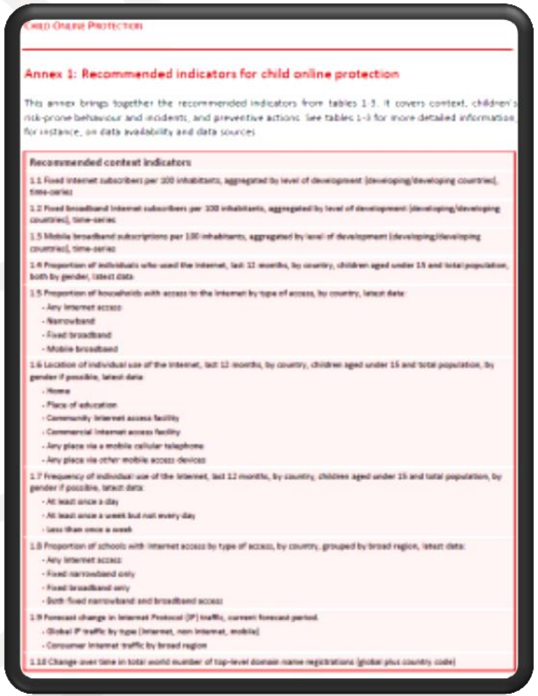
- COP high-level deliverables across the five strategic pillars are designed to be achieved by ITU and COP members in collaboration.
  - Legal Measures
  - Technical & Procedural Measures
  - Organizational Structures
  - Capacity Building
  - International Cooperation
- It is designed to transform the COP Guidelines into concrete activities by leveraging the active support provided by COP partners.

COP Statistical Framework

- ITU “Child Online Protection Statistical Framework and Indicators”

  The world’s first attempt to provide the overall statistical framework related to the measurement of child online protection with a particular emphasis on measures that are suitable for international comparison.


International Telecommunication Union
Child
Online
Protection
Statistical Framework and Indicators 2010
ITU-D
ITU



CHILD ONLINE PROTECTION

Annex 1: Recommended indicators for child online protection

This annex brings together the recommended indicators from tables 1-3. It covers context, children's risk-prone behaviour and incidents, and preventive actions. See tables 1-3 for more detailed information, for instance, on data availability and data sources.

Recommended context indicators

1.1 Fixed Internet subscribers per 100 inhabitants, aggregated by level of development (developed/developing countries), time-series

1.2 Fixed broadband Internet subscribers per 100 inhabitants, aggregated by level of development (developed/developing countries), time-series

1.3 Mobile broadband subscriptions per 100 inhabitants, aggregated by level of development (developed/developing countries), time-series

1.4 Proportion of individuals who used the Internet, last 12 months, by country, children aged under 15 and total population, both by gender, latest data

1.5 Proportion of households with access to the Internet by type of access, by country, latest data:
- Any Internet access
- Narrowband
- Fixed broadband
- Mobile broadband

1.6 Location of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data
- Home
- Place of education
- Community Internet access facility
- Commercial Internet access facility
- Any place via a mobile cellular telephone
- Any place via other mobile access devices

1.7 Frequency of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data
- At least once a day
- At least once a week but not every day
- Less than once a week

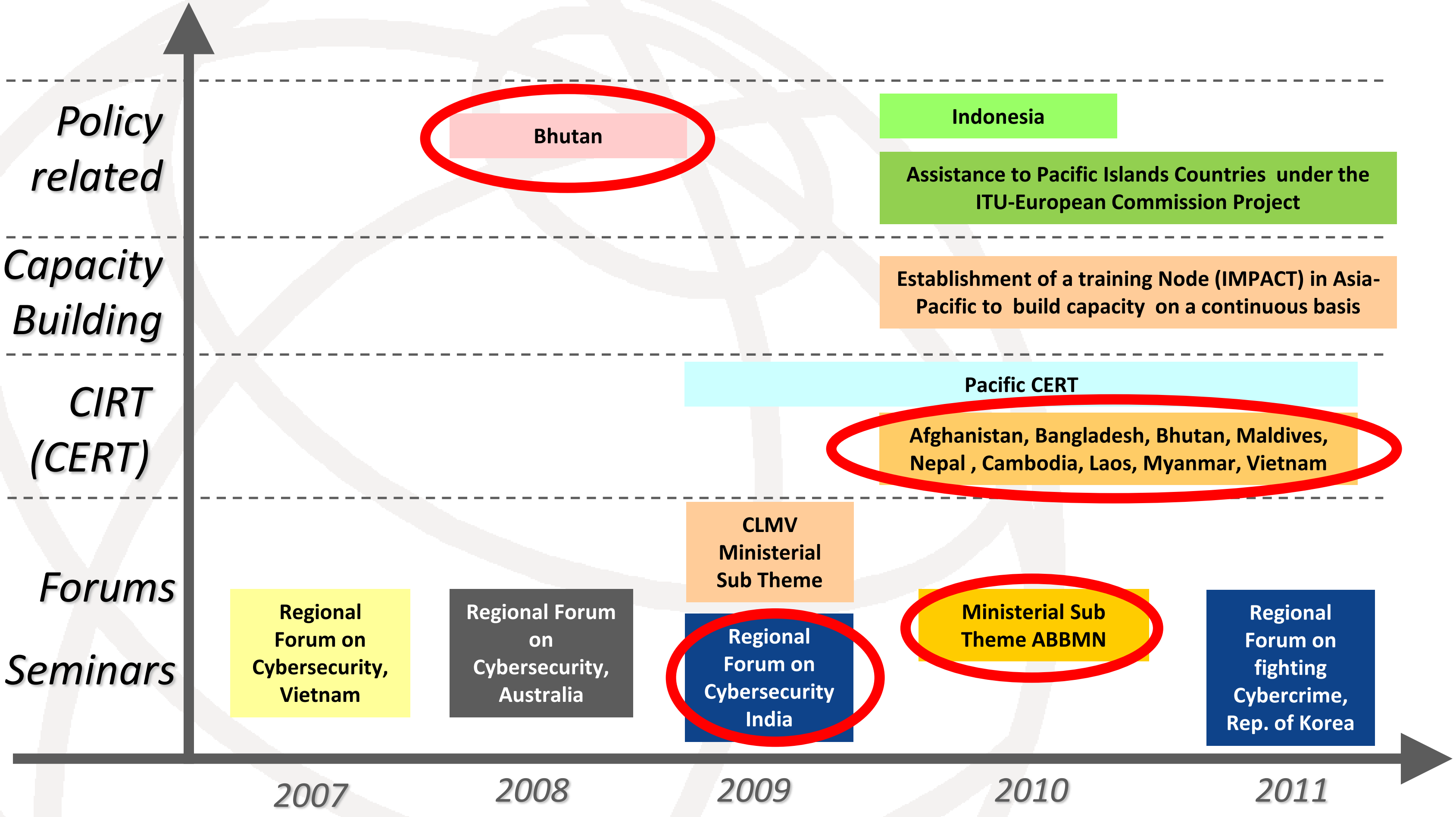
1.8 Proportion of schools with Internet access by type of access, by country, grouped by broad region, latest data:
- Any Internet access
- Fixed narrowband only
- Fixed broadband only
- Both fixed narrowband and broadband access

1.9 Forecast change in Internet Protocol (IP) traffic, current forecast period
- Global IP traffic by type (Internet, non Internet, mobile)
- Consumer Internet traffic by broad region

1.10 Change over time in total world number of top-level domain name registrations (global plus country code)

ITU Cybersecurity Activities in Asia-Pacific

ITU Cybersecurity Initiatives in Asia-Pacific



Policy related

Bhutan

Indonesia

Assistance to Pacific Islands Countries under the ITU-European Commission Project

Capacity Building

Establishment of a training Node (IMPACT) in Asia-Pacific to build capacity on a continuous basis

CIRT (CERT)

Pacific CERT

Afghanistan, Bangladesh, Bhutan, Maldives, Nepal , Cambodia, Laos, Myanmar, Vietnam

Forums Seminars

Regional Forum on Cybersecurity, Vietnam

Regional Forum on Cybersecurity, Australia

CLMV Ministerial Sub Theme

Regional Forum on Cybersecurity India

Ministerial Sub Theme ABBMN

Regional Forum on fighting Cybercrime, Rep. of Korea

2007

2008

2009

2010

2011

CIRT/CSIRT/CERT Subregional Workshop for Cambodia, Lao PDR, Myanmar and VietNam (CLMV)

- Held on 29 Nov-1 Dec 2011 in Yangon, Myanmar
- 45 participants from CLMV, other ASEAN countries, dialogue partners and other organizations, e.g. IMPACT
- Outcome statement issued. Some action steps/recommendations from the workshop include:
  - ✓ Closer Collaboration among CLMV National CIRTs e.g. creation of a CLMV CIRT 24x7 Points of Contact, CIRT Exchange programmes within CLMV, celebration of CLMV Cybersecurity Week to promote and strengthen their collaboration
  - ✓ ITU and ASEAN requested to continue providing a platform where the very important exchange of experiences, best practices and operational updates in CIRT operations, capacity building can be facilitated
- One day first ever Subregional Cyber drill conducted simulating several incident scenarios
- Country CERT Assessments also done for CLMV

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

Cross Regional Seminar on Current Methods for Combating Cybercrime in Europe, ASP and the CIS Region

- Held on **March 28-30, 2012** in Odessa, Ukraine,
- Targeted ministries, regulators, law enforcement agencies, operators, banks, universities and other organizations in Europe, ASP and the CIS Region.
- Focused on:
  - strategic aspects of cybersecurity and cybercrime;
  - legal regulation of issues cybercrime;
  - technical, organizational and procedural aspects of detection and prevention of cybercrime;
  - capacity building cybersecurity;
  - aspects of international collaboration on cybercrime; and,
  - integrated aspects of children protection over the Internet.

For more information, please visit:

http://seminar.onat.edu.ua/change_language/english

ITU-UNODC Cooperation in Asia-Pacific

- **Asia-Pacific Regional Workshop on Fighting Cybercrime 21-23 September 2011 in Seoul, Republic of Korea**

Partners: Supreme Prosecutors' Office (SPO), Korea Internet and Security Agency (KISA) and Korean Institute of Criminology (KIC)

Meeting Outcome Statement was adopted by the participants on assessment of cybersecurity and cybercrime at national level, capacity building, establishing legal framework, building cooperation mechanisms, building capacity, increasing public awareness, building consensus, adopting multi-disciplinary approach at national level amongst others.

Details available at http://www.itu.int/ITU-D/asp/CMS/Events/2011/CyberCrime/Meeting_Outcomes_FINAL.pdf

- **ITU and UNODC are coordinating to organise a mock court exercise on Cybersecurity in Indonesia in September 2012**

Human Capacity Building

IMPACT hosts ITU Asia-Pacific Centres of Excellence Node on Cybersecurity to provide continued capacity building opportunities

- ❖ **In 2011, ITU ASP COE Training Workshop was organised on Securing Networks with support from DBCDE (Australia) in Cyberjaya, Malaysia**

- ❖ **In 2012, ITU ASP COE Training Workshop on “Security Core” is scheduled from 27-30 August in Cyberjaya, Malaysia**

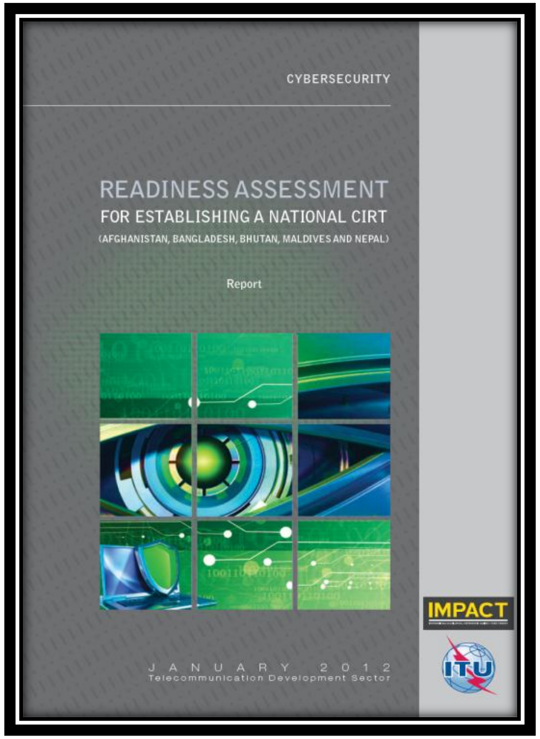
ICB4PAC – Overview of Cyber-security

- Assessment of the present situation has been done and approved by the recipient countries
- Workshop to finalize assessment was held in Vanuatu 2-4 March 2011
- Drafting skeleton cyber legislation and policy was held in Samoa 25-28 August 2011
- In-country support started Sept 2011
- Samoa’s cybercrime Chapter has passed the second reading in Parliament

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



CYBERSECURITY

READINESS ASSESSMENT
FOR ESTABLISHING A NATIONAL CIRT
(AFGHANISTAN, BANGLADESH, BHUTAN, MALDIVES AND NEPAL)

Report

JANUARY 2012
Telecommunication Development Sector

IMPACT

ITU

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

Conclusions

- While it will never be possible to completely remove all risks, drawing together an effective package of policies and practices, infrastructure and 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.
- Moreover, the online world respects neither boundaries nor borders, so creating a safe cyber-environment requires cooperation.
- By working together with ITU, all interested stakeholders and countries, can achieve this critical international collaboration, confronting child online threats with a dynamic and unified coalition.

I

Thank

U

ITU : http://www.itu.int
ITU Asia Pacific : http://www.itu.int/ITU-D/asp/CMS/index.asp