



Cyber Security @ ITU

By Tomas Lamanauskas, ITU

ITU Overview

- Founded in 1865
- UN Specialized Agency for ICTs
- HQs in Switzerland

- 4 Regional Offices & 7 Area Offices
- 193 Member States; 750 Sector Members and Associates
- 66 Academia Members

ITU-D

Promoting the availability and application of ICTs for socio-economic development

ITU-T

Developing international ICT standards

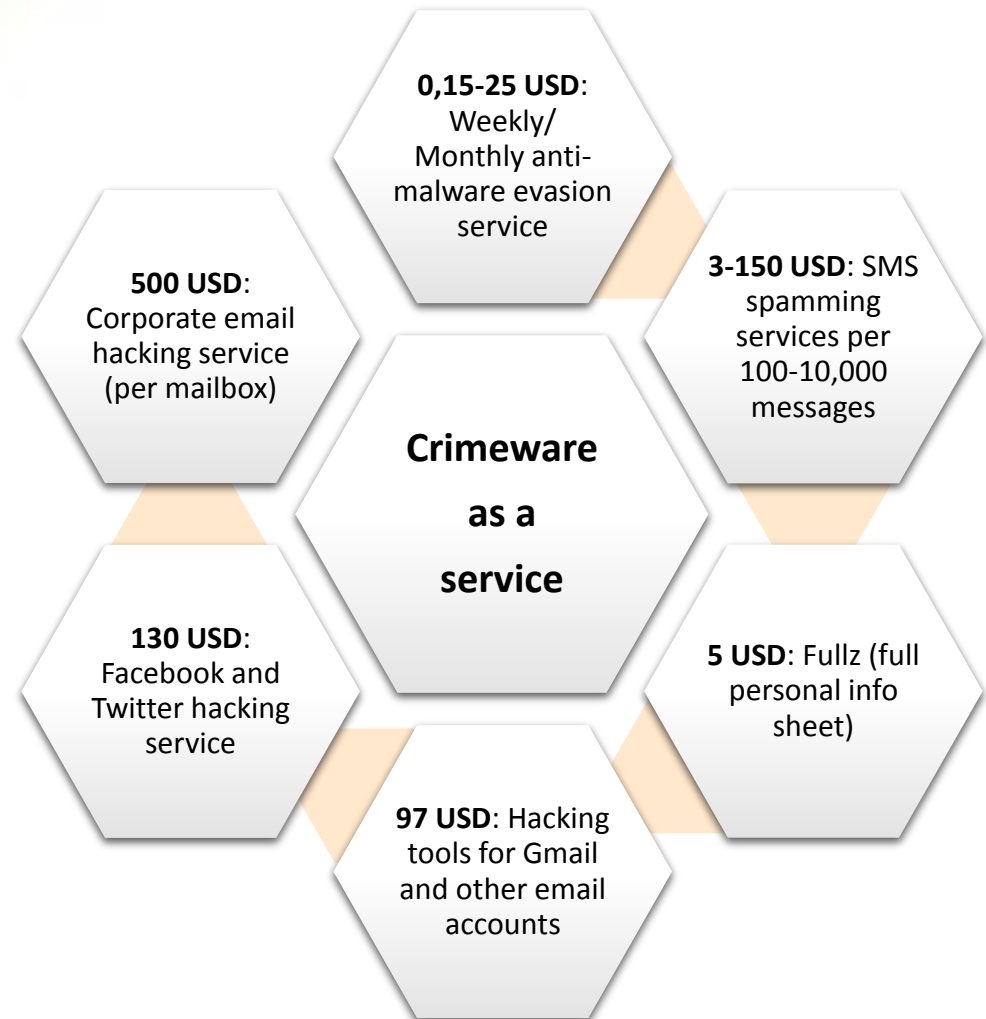


ITU-R

Managing the international radio-frequency spectrum and satellite orbit resources

CYBERSECURITY: A GLOBAL ISSUE

- Global losses due to cybercrime ≈ **500 billion USD** annually
(Source: McAfee, CSIS)
- **Hundreds of millions** of people directly affected every year
- Cybercriminals becoming **more skilled** – both at penetrating organizations and at **avoiding detection**
- Cybercrime tools and services available to **anyone** at low rates



Source: Trend Micro Ltd.

ITU & CYBERSECURITY

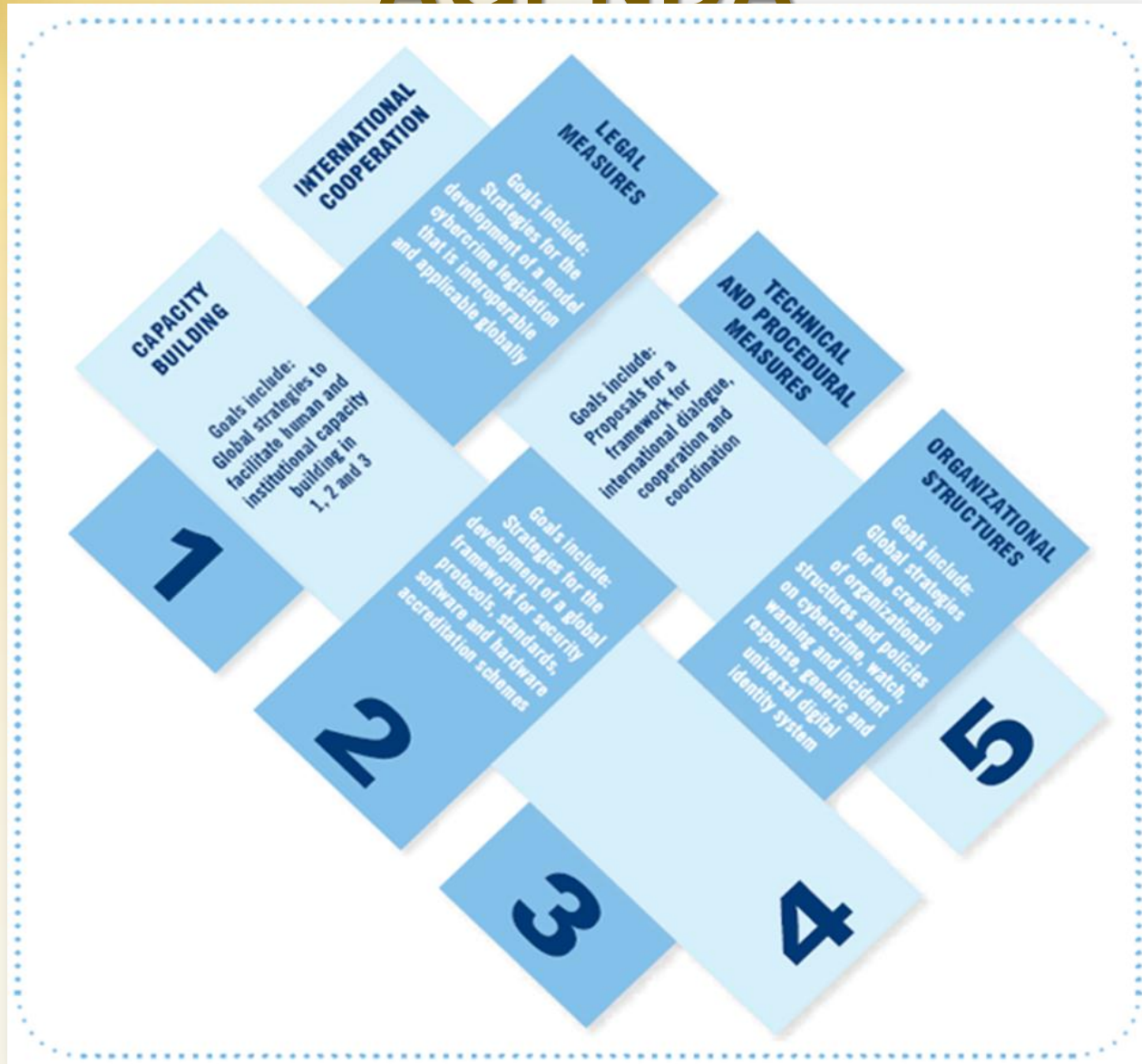
2005

- WSIS named ITU as sole facilitator for WSIS Action Line C5: “Building Confidence and Security in the use of ICTs”

2007

- ITU Secretary-General launched the Global Cybersecurity Agenda (GCA): A framework for international cooperation in cybersecurity

GLOBAL CYBERSECURITY AGENDA





147

PARTICIPATING MEMBERS

5+

CIRT IMPLEMENTATIONS

55+

CYBER DRILL PARTICIPATING COUNTIES

50+

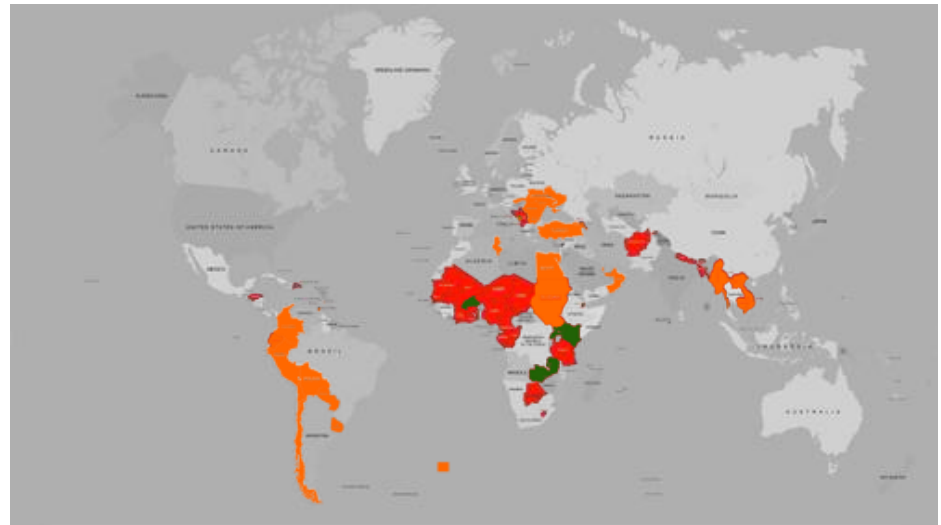
CYBERSECURITY ASSESSMENT

2000+

CYBERSECURITY PRACTITIONERS TRAINED

300+

CERTIFIED PROFESSIONALS



Source: IMPACT



REGIONAL AND SPECIAL SUPPORT

- **ITU-IMPACT Arab Regional Cyber Security and Innovation Centre** hosted by Oman CERT covering some 22 Arab countries
- Memorandum of Understanding (MoU) with the **Nigerian Communication Commission** to set up a Regional Cybersecurity Centre in Nigeria (July 2013)
- ITU project for “**Enhancing Cybersecurity in Least Developed Countries (LDCs)**” following 3 main pillars:
 - Policy-level assistance
 - Capacity building efforts
 - Equipment and software distribution



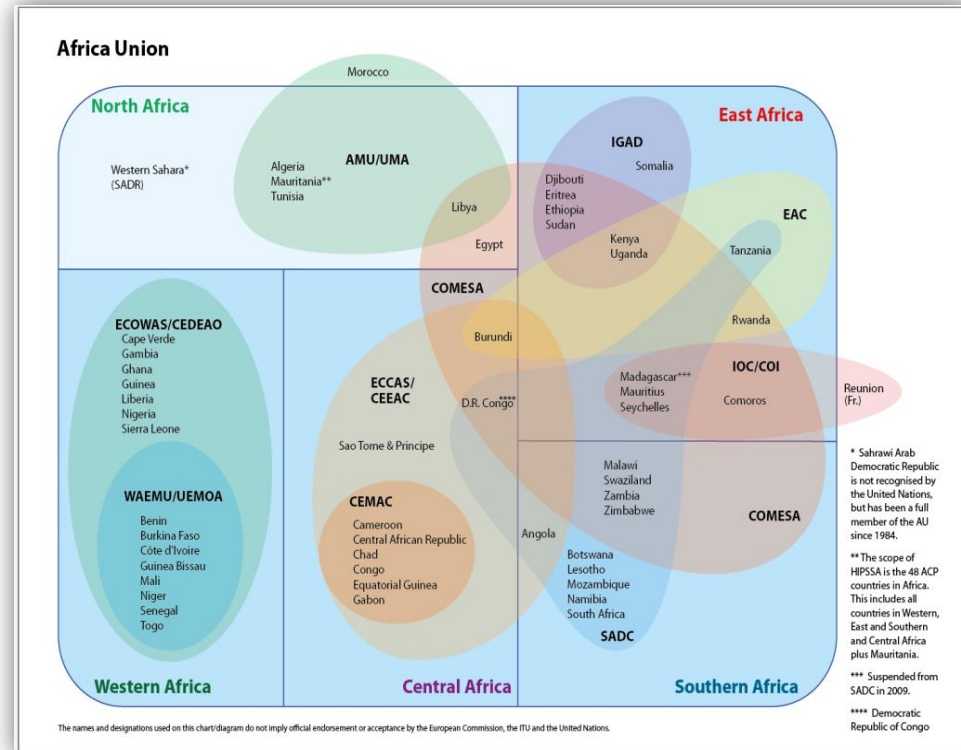
HIPSSA PROJECT



- Harmonization of the ICT Policies in Sub-Saharan Africa
- Sub-regional programs:
 - 1) East Africa
 - 2) Central Africa
 - 3) Southern Africa
 - 4) West Africa

Regional Outcomes on Cybersecurity

- ECOWAS cybersecurity guidelines
- ECCAS Model Law / CEMAC Directives on Cybersecurity
- SADC model law on data protection/ e-transactions/cybercrime
- In-Country Technical Assistance



HIPCAR PROJECT



- In collaboration with:
 - Caribbean Community (CARICOM) Secretariat
 - Caribbean Telecommunication union (CTU)
- **Key Achievements - Regional Model Policies and Regulations**
 - ICT legislative framework covering information society issues:
 - e.g. Model Policy Guidelines & Legislation texts on cybercrime and cybersecurity, privacy and data protection etc.
 - Telecommunication Acts
- In-Country Technical Assistance



ICB4PAC PROJECT



Pacific Region

Key Achievements

- Regional Knowledge-based Reports (e.g. on Cybercrime)
- In-Country Technical Assistance



Global Cybersecurity Index

Objective

The Global Cybersecurity Index (GCI) aims to measure and rank each nation state's level of cybersecurity development in five main areas:

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

Goals

Promote cybersecurity strategies at a national level

Drive implementation efforts across industries and sectors

Integrate security into the core of technological progress

Foster a global culture of cybersecurity

Expected delivery of the
full index - Q4 2014

ABIresearch®






**Global
Cybersecurity
Index**



Global Cybersecurity Index

Results: Arab States

A total of 22 countries were analyzed in the regional index for the Arab States

<i>Rank</i>		<i>Country</i>	<i>Index</i>
1 st		Oman	0.765
2 nd		Morocco	0.559
3 rd		Egypt & Tunisia	0.500

Source: **ABI**research®



Child Online Protection Initiative (COP)

ITU launched the Child Online Protection (COP) Initiative in 2008 within the GCA framework 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
- Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives



COP Guidelines



- Developed in cooperation with COP partners, is the first set of guidelines addressing different stakeholders. [Available in the six UN languages](#)
- ITU-UNICEF Consultation open until **20 December 2013**: <http://www.business-humanrights.org/Documents/itu-unicef-ict-guidelines-consultation>

ITU-T Study Group 17 - Security

- Coordinates security-related work across all ITU-T Study Groups
- Over **70 standards** (ITU-T Recommendations) focusing on security
- Deals with a broad range of standardization issues
- Key areas of current work
 - Cybersecurity
 - Child Online Protection
 - Security architectures and frameworks
 - Countering spam
 - Identity management
 - Security of applications and services for the Internet of Things, web services, social networks, cloud computing and Big Data

WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS (WCIT- 12)

- WCIT-12 set the ground for international cooperation on cybersecurity matters
- **Article 6, ITRs:** Security and robustness of networks
- **Article 7, ITRs:** Unsolicited bulk electronic communications



Collaborations

UNODC

- ITU and the United Nations Office on Drugs and Crime (UNODC) working together under an MoU, since May 2011, in assisting Member States to mitigate the risks posed by cybercrime.
- **Seoul (2011)** Coorganized Asia-Pacific Regional Workshop on Fighting Cybercrime
- **Panama, Kenya (2012)**: Worked together to revise cybersecurity policies and strategies as well as assessing capacity building needs

INTERPOL

- Cooperation agreement with IMPACT signed in November 2012.
- Exchange of information and expertise, as well as enhancement of both organizations knowledge base in the field of cybersecurity.
- Working together in performing cybersecurity assessments

Collaborations

CTO

- ITU partnership with the Commonwealth Telecommunication Organization (CTO) to facilitate the establishment of COP National Frameworks for 6 countries - **Nigeria, Ghana, Sierra Leone, Gambia, Mauritius and Cameroon**

AFRICAN UNION

- ITU has contributed to the draft of the African Union Convention on Cybersecurity

Collaborations

WORLD BANK

- Working with ITU under an MoU.
- **ITU-World Bank:** Assisting Bhutan in the implementation of a Computer Incidence Response Team (CIRT) in Bhutan.
- **ITU-World Bank- World Economic Forum-Interpol:** Worked closely for the support of the conference “Global Cybersecurity Cooperation: Challenges and Visions” in Azerbaijan (Baku, 2-3 December 2013)

PRIVATE SECTOR

- Partnerships with the private sector (including ITU Sector Members): Symantec, Kaspersky Labs, (ISC)², ABI Research, Trend Micro etc.

UN-Wide Framework on Cybersecurity & Cybercrime

- Developed by ITU and UNODC along with 33 UN Agencies
- Focuses **on the external efforts of UN entities** concerning Member States
- **Endorsed by the United Nations System Chief Executives Board for Coordination (CEB)** at its Second Regular Session meeting on 25 November 2013

UN-Wide Framework on Cybersecurity & Cybercrime

Purpose

Enhanced UN
agency
coordination

More efficient
and effective
response
mechanisms

Specialized
policy
development
based on a set
of principles

Principles

Principle 1:

- Deal with Cyber incidents in a holistic manner taking into account the various facets, including the technical and international cooperation aspects

Principle 2:

- Respond to needs within the agencies' respective mandates and collaborate/complement as necessary

Principle 3:

- Respect the principles of the rule of law and human rights

Principle 4:

- Focus on assisting Member States to take evidence-based action

Principles

Principle 5:

- Foster a “whole-of-government” response

Principle 6:

- Aim to strengthen relevant formal and informal mechanisms for international cooperation

Principle 7:

- Strengthen cooperation between government institutions and private sector enterprises

Coordinated Response

Need for a multilevel response to the cybersecurity challenges



Potential for Collaboration

Awareness

Frameworks

Standards

Capacity Building
and Knowledge
Sharing

THANK YOU

Tomas Lamanuskas
Head, Corporate Strategy Division (CSD)
Strategic Planning and Membership
Department (SPM)
e-mail : Tomas.Lamanuskas@itu.int

