CYBERCRIME: Global Phenomenon and its Challenges

Fostering international cooperation on cybersecurity
A global response to a global challenge

Carla Licciardello
International Telecommunication Union (ITU)

Carla.licciardello@itu.int

I. Current Situation: challenges and tentative responses

Growing Cybersecurity Threats

1. ICTs have become an integral part of everyday life for many people of the world.
2. ICT networks are regarded as indispensable national infrastructure
3. ICTs are also exposing our societies to the threat of cyberattacks.
4. Vulnerability of national infrastructures increases as the use of ICTs take root.
5. Nations will be susceptible to attacks of an unprecedented and limitless variety.
6. Cyber attacks on ICTs are borderless and can be launched from virtually anywhere.
7. As global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructures through cyberspace.

Major attacks 2010 - 2011

	2010	2011
January	•Attack on google to gain access to gmail accounts and google password management system •Attack on Intel •Attack on Morgan Stanley. Email leaked out	•Major cyber intrusion in Defense Research and Development Canada. Finance Department and the Treasury Board forced to disconnect from the Internet.
February		
March	•Attack on NATO and European Union networks •200 attempts to hack into the networks of the legal defense team to gain inside information on the trial defense strategy	•Hackers penetrate French government computer networks •South Korea defense network penetrated •RSA SecurID Compromised
April	•Indian Defense Ministry and Indian embassies compromised	
May	•Canadian Security and Intelligence Service Memo leaked	
June		•Sony • NATO • International Monetary Fund (IMF) •Turkish Government Website •EU's Commission and External Action Service •Operation Malaysia
October	•Stuxnet •Zeus Malwares steals over 12million$ from 5 banks in US, UK	
December	•British Foreign Ministry, a defense contractor and other British interests attacked traced back to white house.	

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.

National Responses

Developing National Computer Incident Response Teams (CIRTs)

Enhancing public-private partnerships to enhance expertise, knowledge, skills, resources & experience

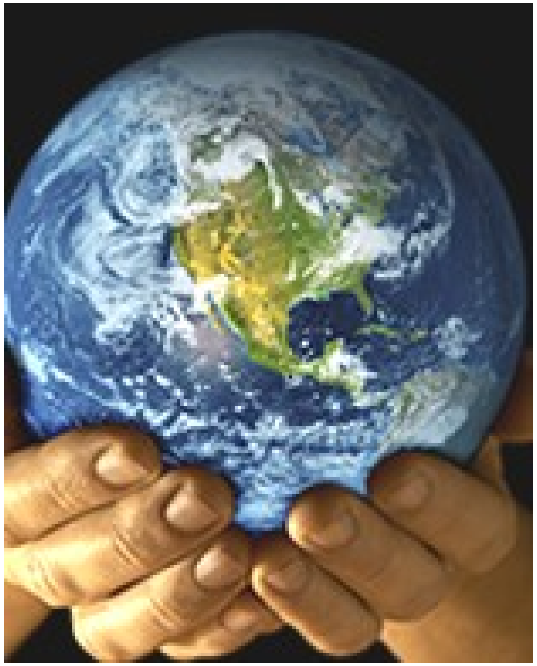
Enhancing International Cooperation

Also, many governments are preparing themselves for “Cyber-defense” as well as “Cyber-offense”: *Cyberwarfare*

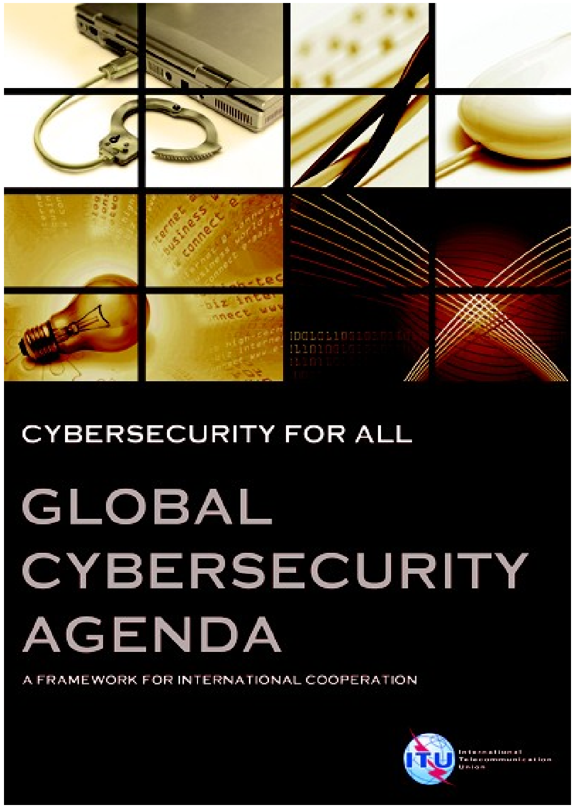
- Network-based attack and/or defense
- Building cyber capabilities as a part of conventional warfare, including cyber military outfits
- Cultivating cyber tactics as a national resource
- Educating citizens and raising awareness of cybersecurity problems

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



CYBERSECURITY FOR ALL

GLOBAL CYBERSECURITY AGENDA

A FRAMEWORK FOR INTERNATIONAL COOPERATION

International Telecommunication Union

II. ITU and Cybersecurity: Global Cybersecurity Agenda (GCA)

ITU Overview

- Founded in 1865
- Leading UN Special Agency for ICTs
- HQs in Switzerland

- Three sectors (ITU-T, ITU-D, and ITU-R)
- 4 Regional Offices & 7 Area Offices
- 193 Member States and 750 Sector Members

ITU-D

Established to help spread equitable, sustainable and affordable access to ICT.

ITU-T

ITU's standards-making efforts are its best-known – and oldest – activity.

ITU-R

Managing the international radio-frequency spectrum and satellite orbit resources

ITU TELECOM

Brings together the top names from across the ICT industry & ministers and regulators for a major exhibition, a high-level forum & a host of other opportunities

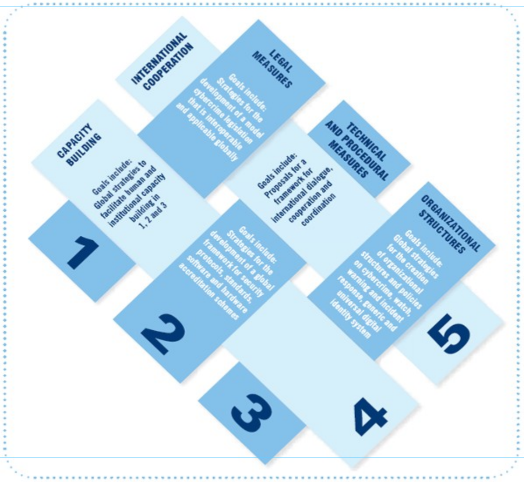
ITU and Cybersecurity

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”


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

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

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

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

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

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

2007

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

A framework for international cooperation in cybersecurity

GCA GLOBAL CYBERSECURITY AGENDA

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

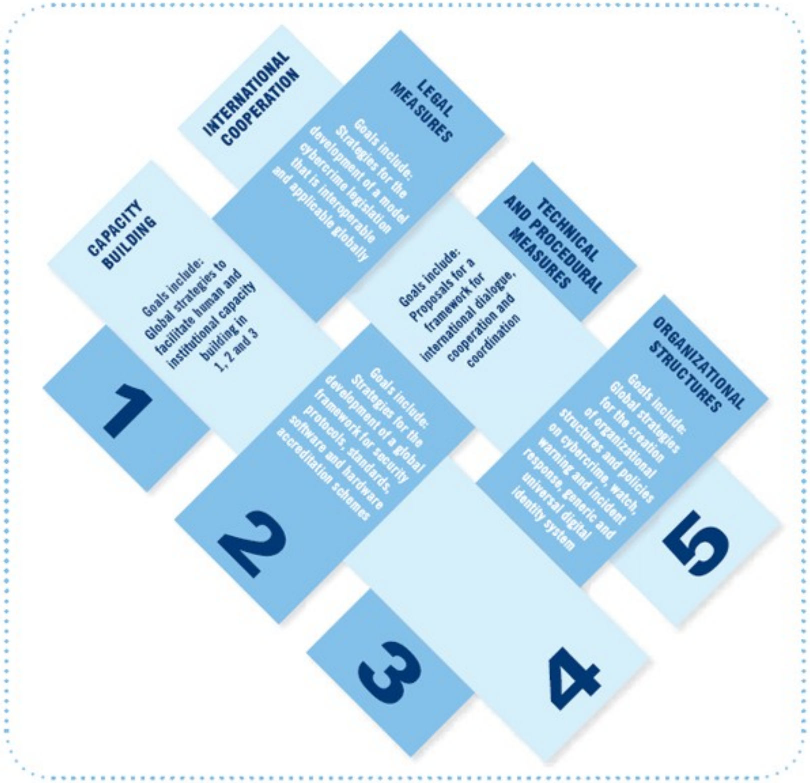
Child Online Protection

2008 - 2010

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

Global Cybersecurity Agenda (GCA)

GCA is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners, and building on existing initiatives to avoid duplicating efforts.


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

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

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

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

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

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

GCA builds upon five pillars:

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

GCA: From Strategy to Action

1. Legal Measures

ITU Toolkit for Cybercrime Legislation

ITU Publication on Understanding Cybercrime: A Guide for Developing Countries

2. Technical and Procedural Measures

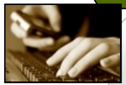
ITU Standardization Work
ICT Security Standards Roadmap
ITU-R Security Activities
ITU-T Study Group 17
ITU-T Study Group 2

3. Organizational Structures

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

Global Cybersecurity Agenda (GCA)

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

III. ITU and Cybersecurity: The Child Online Protection Initiative (COP)

COP Global Initiative

For a safer and more secure online experience for children

Current Status

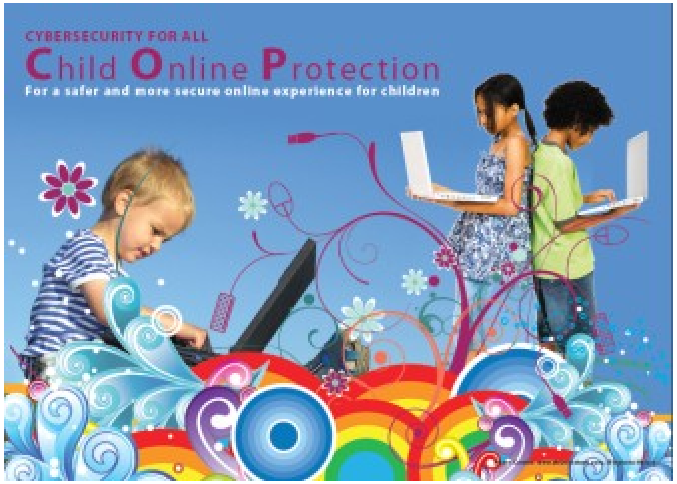
- As use of the Internet grows, so do the risks it presents to children.
- Children already spend large amounts of time in an online environment as active participants.
- Children are often more vulnerable when it comes to Internet safety as they are still developing and learning.
- This has consequences for their capacity to identify and manage potential risks on the Internet.
- With the arrival of new methods of communication on the Internet and mobile technologies, children are more and more exposed to complex and multi-faceted emerging threats.

ITU Child Online Protection (COP)

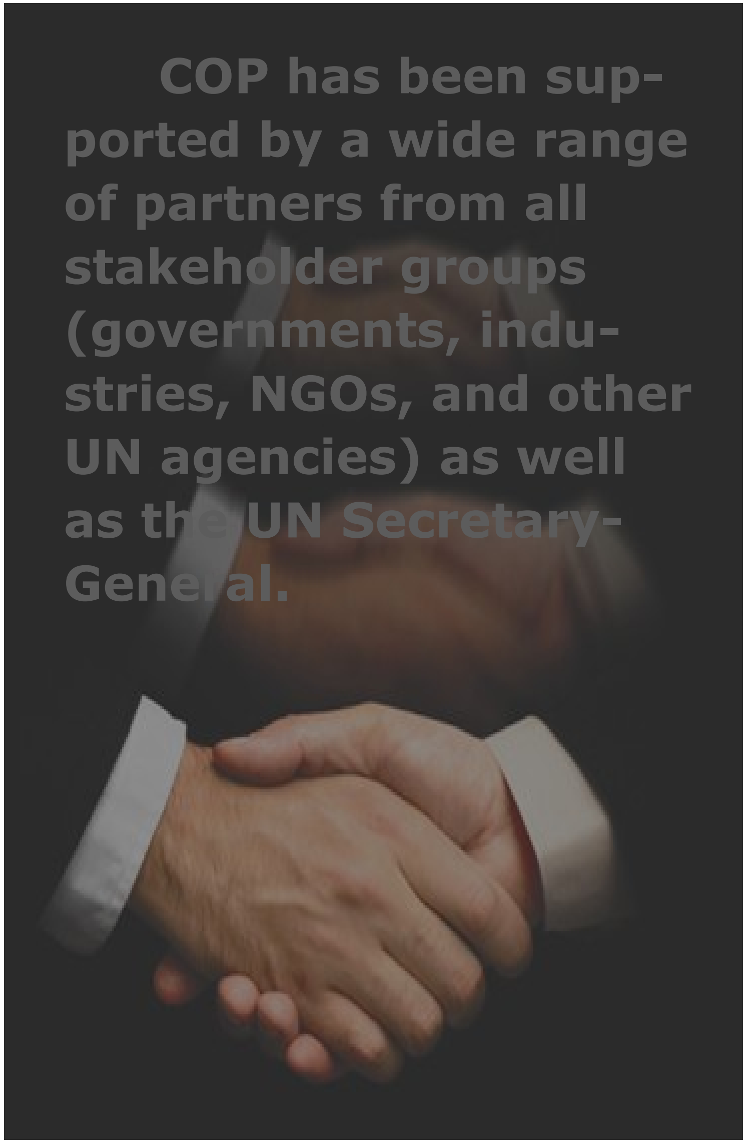
ITU launched the Child Online Protection (COP) Initiative in 2008 within the GCA framework aimed at bringing together partners from all sectors of the global community **to ensure a safe and secure online experience for children everywhere.**

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; and
- Share knowledge and experience while facilitating international strategic partnership to define and implement concrete initiatives



Working together....



COP has been supported by a wide range of partners from all stakeholder groups (governments, industries, NGOs, and other UN agencies) as well as the UN Secretary-General.

- Advanced Development for Africa (ADA)
- Child Helpline International (CHI)
- Children's Charities' Coalition on Internet Safety
- Cyber Peace Initiative
- ECPAT International
- European Broadcasting Union (EBU)
- European Commission - Safer Internet Programme
- European Network and Information Security Agency (ENISA)
- European NGO Alliance for Child Safety Online (eNASCO)
- eWWG
- Family Online Safety Institute (FOSI)
- Girl Scouts of America
- Government of Poland (UKE)
- GSM Association
- iKeepSafe
- International Criminal Police Organization (Interpol)
- International Multilateral Partnership Against Cyber Threats (IMPACT)
- International Centre for Missing & Exploited Children
- Microsoft
- Optenet
- Save the Children
- Telecom Italia
- Telefónica
- United Nations Children’s Fund (UNICEF)
- United Nations Institute for Disarmament Research (UNIDIR)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
- United Nations Office on Drugs and Crime (UNODC)
- Vodafone Group

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

www.itu.int/cop

Guidelines for
Parents, Guardians
and Educators on
Child Online
Protection

www.itu.int/cop

Guidelines
for Industry on
Child Online
Protection

www.itu.int/cop

Guidelines for
Policy Makers on
Child Online
Protection

www.itu.int/cop

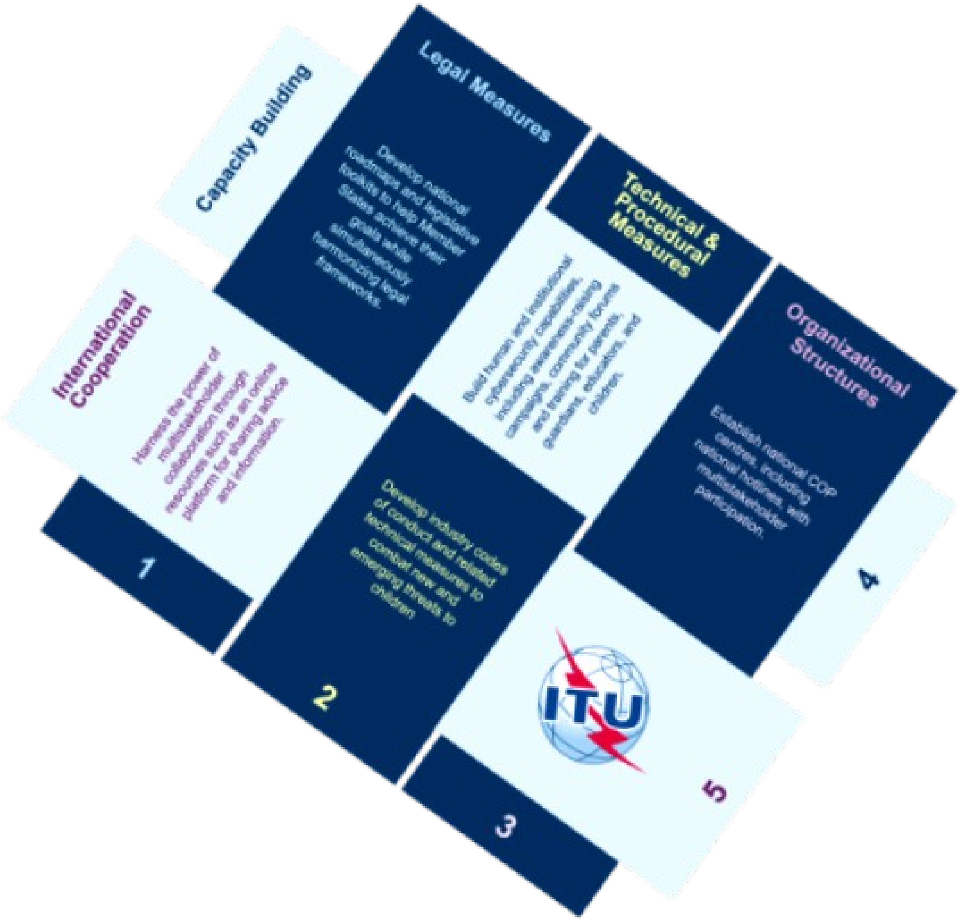
New COP Global Initiative

" Individual rights without the fulfillment of duties causes cracks in society. Democracy without responsibility undermines freedom."

H.E. Laura Chinchilla, President of Costa Rica became a Patron of Child Online Protection (COP) in 2010.

In November 2010, ITU Secretary-General, together with H.E. President Chinchilla, announced the launch of a new Global Initiative with high-level deliverables.

The COP Five Strategic Pillars



Capacity Building

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.

International Cooperation

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

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

- 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.

IV. ITU and Cybersecurity: ITU - IMPACT Collaboration

ITU-IMPACT
Enter
ITU
IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

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.

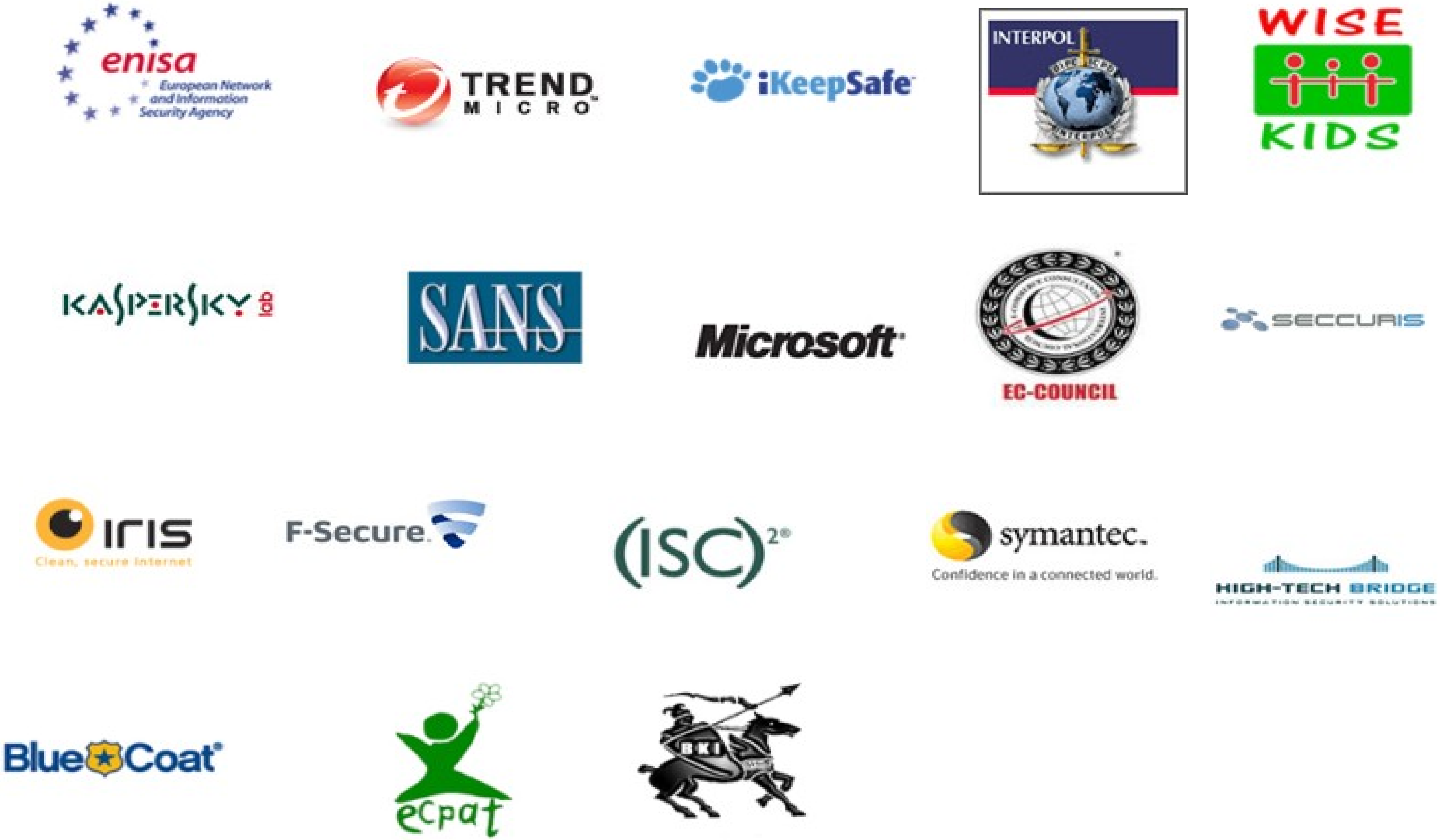
International Telecommunication Union
Committed to Connecting the World
ITU

IMPACT

A Global Coalition

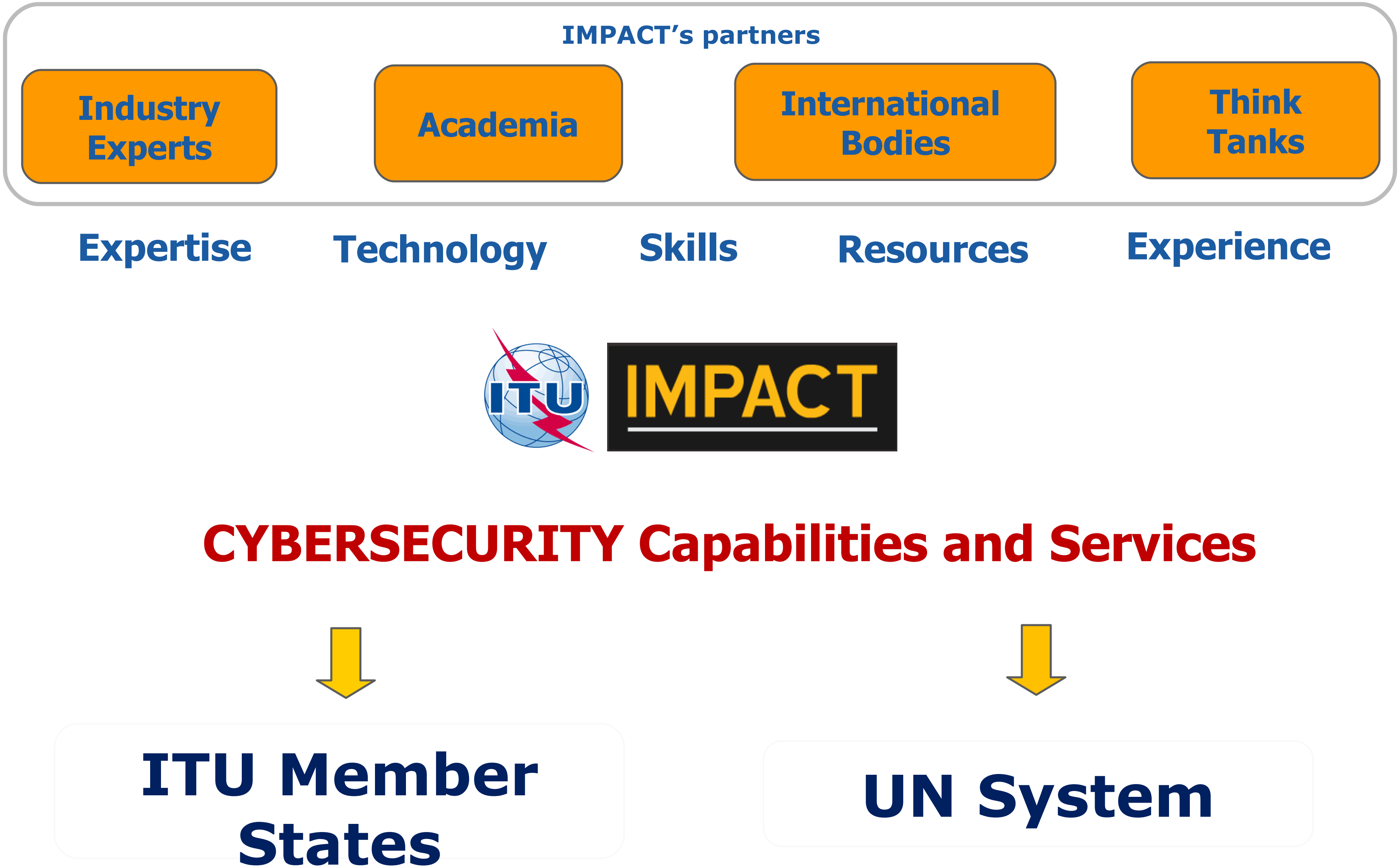
IMPACT is the cybersecurity executing agent of the United Nation’s (UN) specialized agency, ITU, bringing together governments, academia and industry experts to enhance the global community’s capabilities in dealing with cyber threats.

A Global Partnership



....plus 200 Universities around the world

ITU–IMPACT strategy



IMPACT's partners

Industry Experts

Academia

International Bodies

Think Tanks

Expertise

Technology

Skills

Resources

Experience

IMPACT

CYBERSECURITY Capabilities and Services

ITU Member States

UN System

Global Response Centre

- ***Network Early Warning System (NEWS)***
  - Cyber threat reference centre
  - Aggregation of cyber threats across the globe
  - Collaboration with global industry partners
- ***Electronically Secure Collaborative Application Platform for Experts (ESCAPE)***
  - Key experts and personnel from Member States (ICT Ministry, law enforcement, regulators, cybersecurity experts,…)
  - Facilitate & coordinate with Member States during cyber attacks

Services for Member States

As of today, some 137 countries joined ITU-IMPACT

- Region A – Americas – ***22 Countries***
  - Antigua and Barbuda, 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 – ***38 Countries***
  - Afghanistan, Bangladesh, Bhutan, Brunei Darussalam, Fiji, India, Indonesia, 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

Services for Member States

Computer Incident Response Team (CIRT)

ITU performed readiness assessment in 29 countries

Member State	Assessment Status
Afghanistan	Completed in October 2009
Uganda, Tanzania, Kenya, Zambia	Completed in April 2010
Nigeria, Burkina Faso, Ghana, Mali, Senegal, Ivory Coast	Completed in May 2010
Maldives, Bhutan, Nepal & Bangladesh	Completed in June 2010
Serbia, Montenegro, Bosnia, Albania	Completed in November 2010
Cameroon, Chad, Gabon, Congo, Sudan	Completed in December 2010
Cambodia, Lao, Myanmar, Vietnam	Completed in October 2011
Gambia, Senegal, Niger, Togo	November 2011

7 countries are now moving to the implementation phase

Member State	
Sudan	Montenegro (signing stage)
Zambia (proposal issued)	Mongolia
Kenya (proposal issued)	Burkina Faso
Nigeria (proposal issued)	

UN Delivering-As-One

- The United Nations Chief Executive Board (CEB) has given high priority to Cybersecurity, following a proposal from the ITU Secretary General, on a UN-wide strategy.
- ITU and UN ODC have been identified as lead UN bodies in Cybersecurity and cybercrime.
- ITU is facilitating the process toward a UN harmonized policy on Cybersecurity that would positively affect the achievement of Cybersecurity at national, regional and international level.

ITU – UNODC MoU

Legal Measures

Capacity Building and Technical Assistance

Intergovernmental and expert meetings

Joint Study

Sharing knowledge and information

Is it enough?

- More coordination/cooperation/communication is required within the country (bottom-up approach)
- More coordination/cooperation/communication is required at regional and international level (top-down approach)
- The different constituencies of different organizations must be able to share views, exchange information and properly communicate.

➢ The initial step done by UN ODC and ITU in leasing "ICT" with "cybercrime" should be replicated to involve the other groups and constituencies at the global level as well as involving relevant bodies (e.g. INTERPOL, NATO, OSCE, OECD, IPU, UNDESA, etc)

THANK YOU

For further information
www.itu.int/cybersecurity
cybersecurity@itu.int