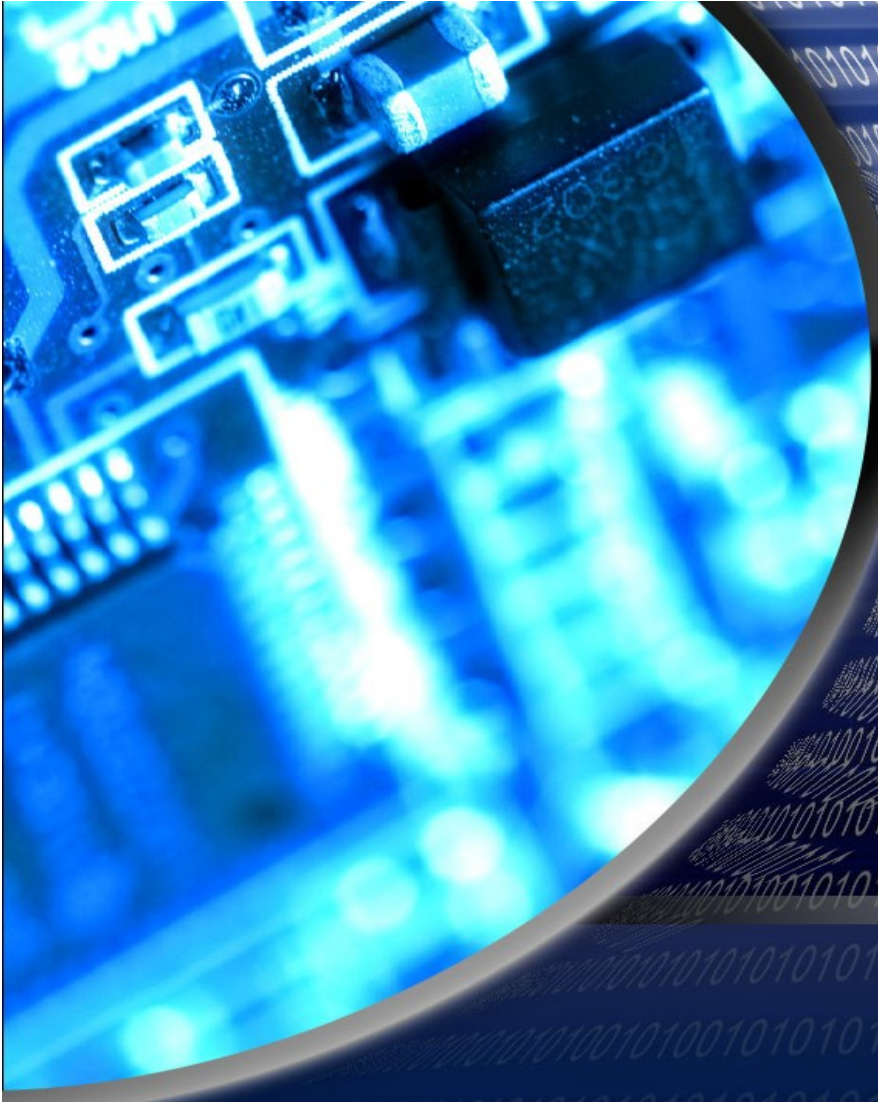


ITU Work on National Cybersecurity Strategies

Regional Cyber Drill for the Americas Region
Quito, Ecuador, 27 June 2016

Luc Dandurand
Head of ICT Applications and Cybersecurity Division
Telecommunications Development Bureau, ITU

ITU: A Brief Overview

Committed to Connecting the World

International Telecommunication Union

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.

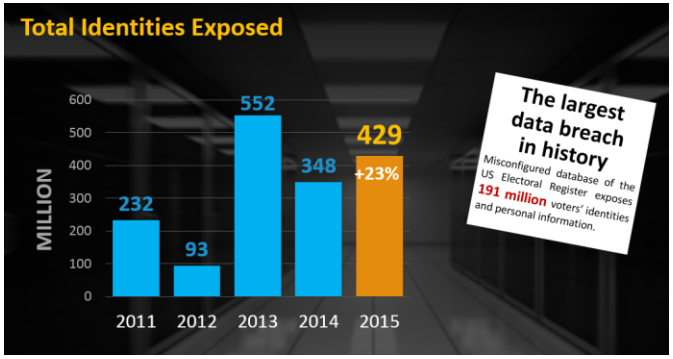
ITU-R: ITU's Radio-communication Sector globally manages radio-frequency spectrum and satellite orbits that ensure safety of life on land, at sea and in the skies.

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

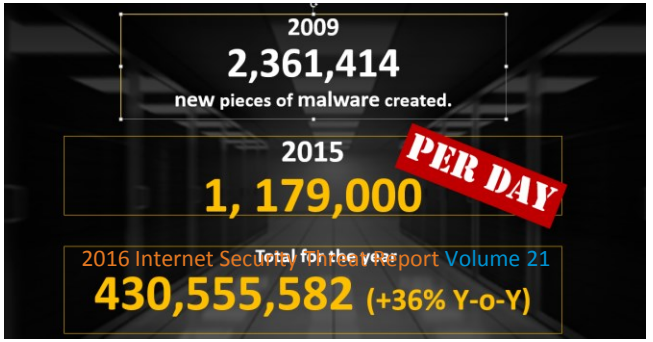
ITU-D: ITU's Development Sector fosters international cooperation and solidarity in the delivery of technical assistance and in the creation, development and improvement of telecommunication/ICT equipment and networks in developing countries.

The 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
  - Internet of Things and Smart Society initiatives will dramatically accelerate these trends



- Statistics and reports show that cyber-threats are on the rise



- Developing countries most at risk as they adopt broader use of ICTs

- Need to build cybersecurity capacity
  - Protection is crucial for the socio-economic wellbeing of a country in the adoption of new technologies

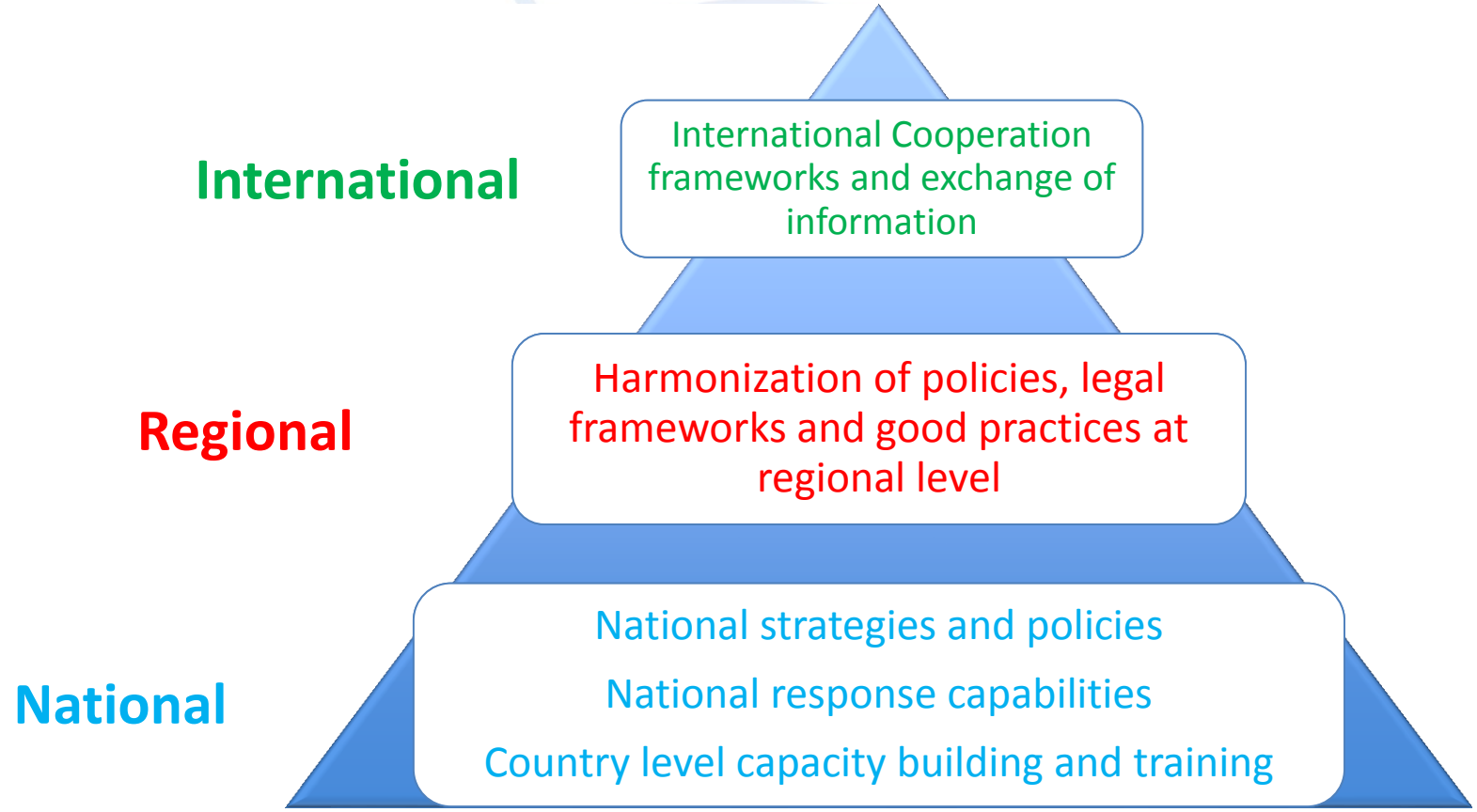
Key Cybersecurity Challenges

- Lack of adequate and interoperable national and 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
- 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.

For many, cybersecurity is still not seen as a cross-sector, multi-dimensional concern, but rather as a technical/technology problem.

Need for a Coordinated Response

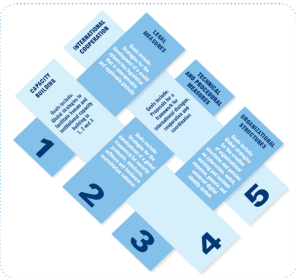
Need for a multi-level response to the cybersecurity challenges



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.

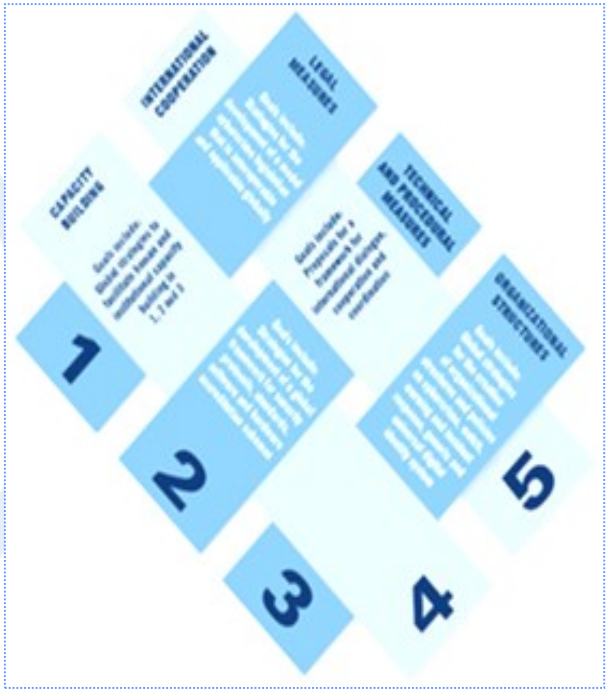
GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

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



BDT Cybersecurity Program: Building Confidence and Security in the Use of ICTs

- Engagement and Awareness (GCI, Events, Publications)
- National Cybersecurity Strategy (NCS) Support
- Computer Incident Response Team (CIRT) Program
- Cyber Drills
- Information Sharing
- In-Country Technical Assistance
- Human Capacity Building

Global Cybersecurity index - GCI

Global Cybersecurity Index

The GCI measures the commitment of countries to cybersecurity in the 5 pillars of the Global Cybersecurity Agenda:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- Cooperation

Goals

- help countries identify areas for improvement
- motivate them to take action to improve their GCI ranking
- help harmonize practices
- foster a global culture of cybersecurity

Final Global and Regional Results 2014 are on ITU Website

2016 Version Ongoing!

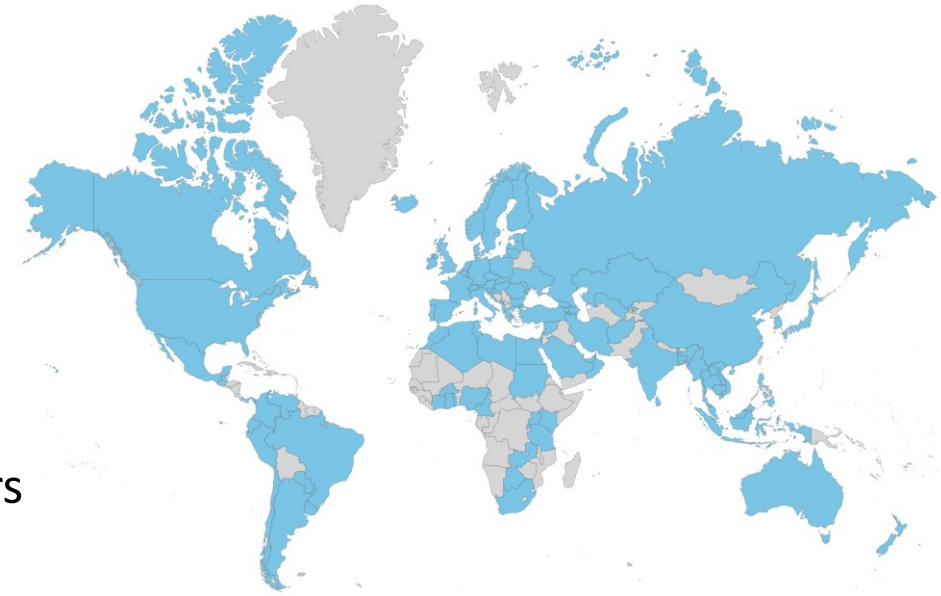
Analysis of 134 responses has started

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

National CIRTs
The First Line of Cyber-Response

Responsible for:

- Coordinating incident response
- Dissemination of early warnings and alerts
- Facilitating communications and information sharing among stakeholders
- Developing mitigation and response strategies
- Publishing best practices in incident response as well as prevention advice;
- Coordinating international cooperation on cyber incidents;



102 National CIRTs Worldwide

Need to fill the gap!

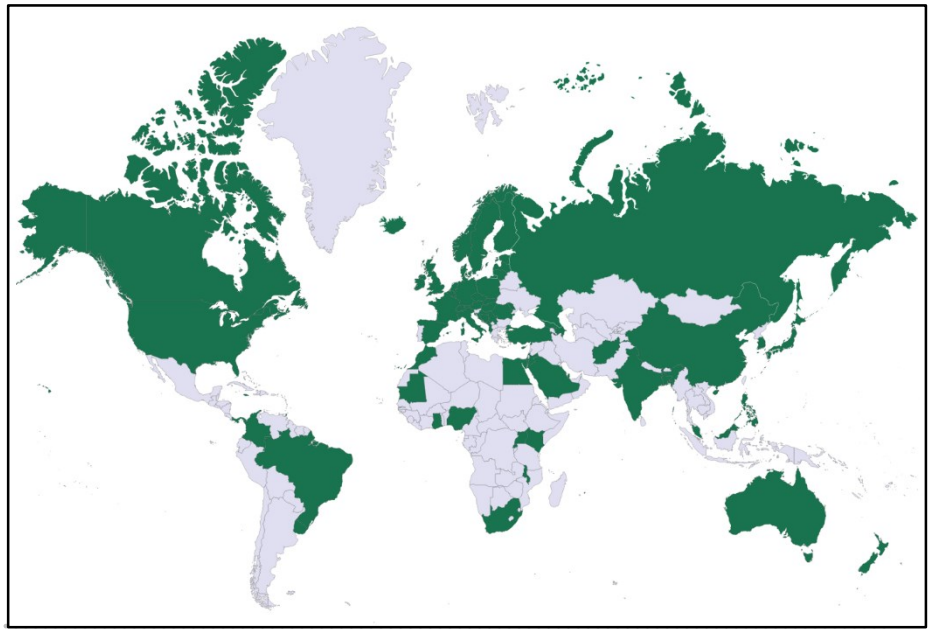
Upcoming "Guide on Being Strategic about Cybersecurity"

BDT Efforts to Assist Member States
in Producing a
National Cybersecurity Strategy

National Cybersecurity Strategies

Developing a Reference Guide to help Member States produce a National Cybersecurity Strategy

- Only 72 out of the ITU's 193 Member States have a National Cybersecurity Strategy
- New guide developed under open consultation and multi-stakeholder approach, and will replace ITU's previous National Cybersecurity Strategy Guide



National Cyber Security Guide
A Joint Effort by 15 Partners

All project partners contribute their knowledge and expertise in the National Cyber Security domain

Overview of the NCS Guide

- Overarching Principles for an NCS
  - Cross-cutting, fundamental aspects applicable to the NCS development process and the NCS content
- Strategic Areas and Good Practices
  - The key elements to be considered for inclusion in an NCS
- Process to develop an NCS
  - Captures the key actions of the NCS elaboration and review cycle
- Supporting reference materials
  - Points to relevant literature

Overarching Principles

- Comprehensiveness and Inclusiveness
- Human Rights and Fundamental Values
- Socio-Economic Prosperity
- Multi-Stakeholder Approach
- Vision
- Allocation of Roles and Responsibilities
- Intra-Governmental Coordination
- Risk Management
- Coherent use of National Cybersecurity Policies and Standards

Strategic Areas and Good Practice

- Strategic Areas are logical groupings that put a set of related aspects together
  - Helps break down and structure the analysis work
- Good Practice identifies the elements that should be considered for inclusion in an NCS.
  - No mandatory elements; each Country free to choose which to include, and to adapt them to its specific needs.

Strategic Area 1: Governance

Covers the Good Practice for steering the development of a NCS and its implementation plan, outlining organizational and positional authorities (determination of responsibilities) within the government and multi-stakeholder cooperation mechanisms. It also includes allocation of human and financial resources, and describes the NCS review cycle.

Strategic Area 2: Risk-Managed Resilience

Covers the Good Practice regarding ensuring ICT systems and information are well protected according to a risk-managed approach and are able to withstand cyber-attacks. Overall, this strategic area helps governments focus on the development of regulations, standards, and policies that form the national cybersecurity framework.

Strategic Area 3: Preparedness and Incident Response

Covers the Good Practice for the detection of cyber attacks, and the response to cyber incidents of national interest in a coherent manner, with continuous improvement of response capabilities and coordination.

Strategic Area 4: Critical Infrastructure

Covers the Good Practice for the identification and protection of critical digital assets and infrastructures, covering the traditional critical services such as water, telecommunications, transportation, energy, finance, etc.)

Strategic Area 5: Capability Development and Awareness

Covers the Good Practice for the advancement of national cybersecurity capabilities through national procurement of capabilities, as well as Research and Development (R&D). Also covers the Good Practice for the development of programs to increase cybersecurity awareness, education and skills development, and the development of a specialized workforce.

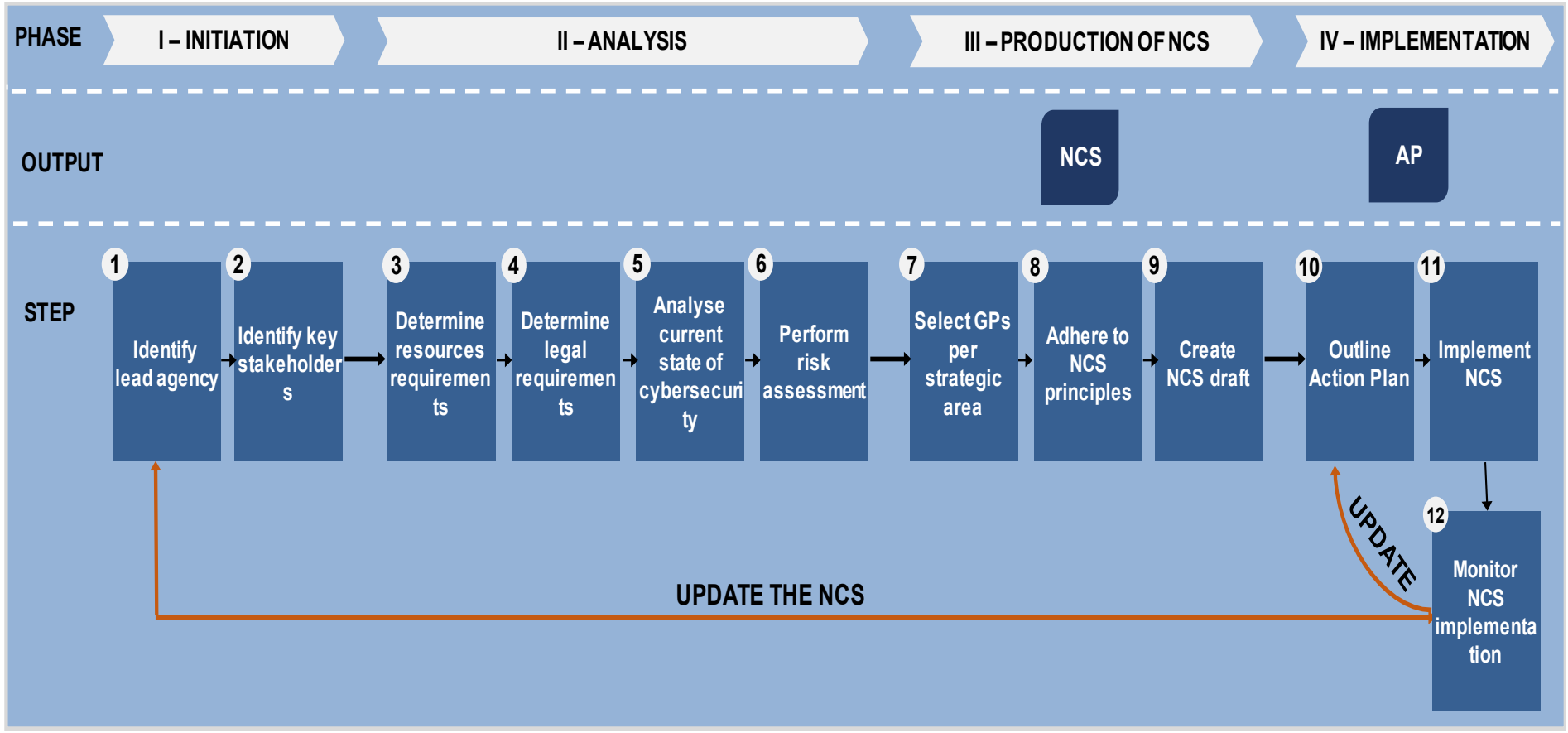
Strategic Area 6: Criminal Justice

Covers the Good Practice for the formalization of a legal framework defining illegal cyber activities and establishing the agencies that will enforce the legal framework (e.g. police, prosecutors, judges).

Strategic Area 7: International Collaboration

Covers the Good practice for outreach, partnership, and information sharing activities among nations and governments in order to give governments the ability to leverage existing capabilities and knowledge.

Process for the Development of an NCS



Thank You

cybersecurity@itu.int