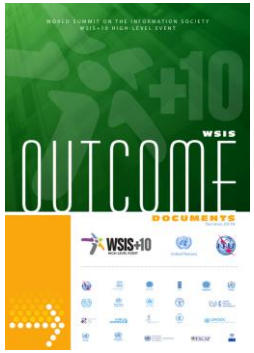
Cybersecurity @ ITU

WSIS Action Line C5: Building Confidence and Security in the use of ICTs

Rouda AlAmir Ali
Programme Officer
ITU Arab Regional Office

world summit
on the information society
Geneva 2003 - Tunis 2005



working together towards 2025
World Summit on the Information Society
Turning targets into action
Geneva 2003 | Tunis 2005 | New York 2015

ITU

WSIS FORUM
8-12 APRIL 2019
Geneva, Switzerland

ITU's 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.

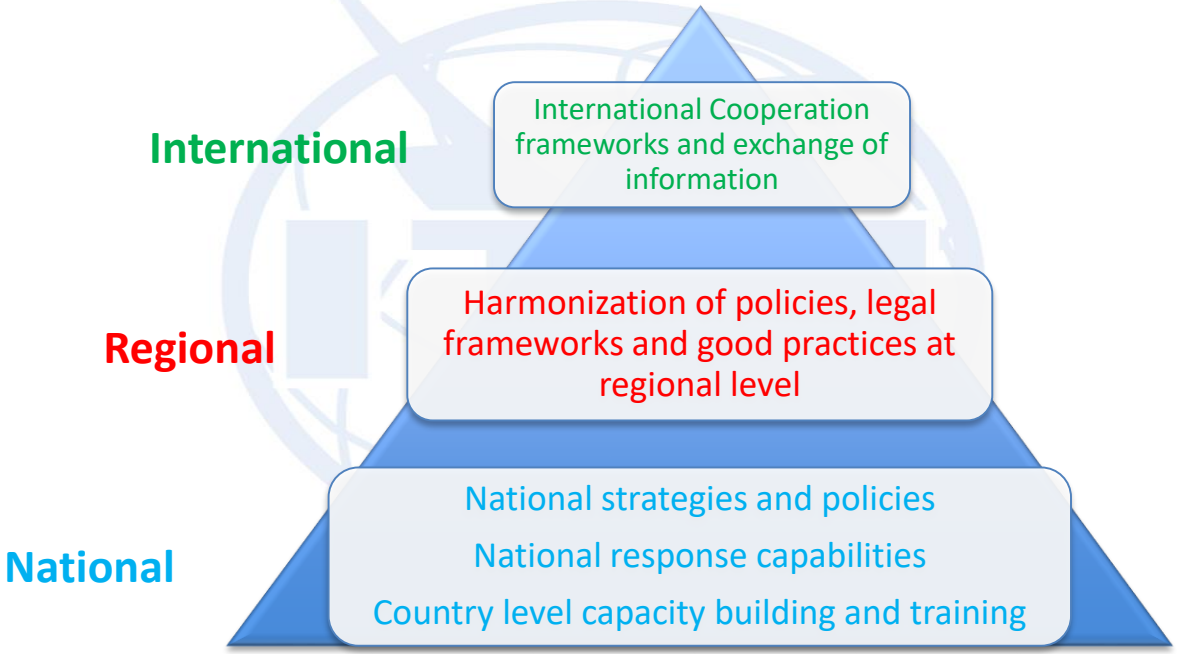
GCA GLOBAL CYBERSECURITY AGENDA

Child Online Protection

Building confidence and security in the use of ICTs is widely present in a number of ITU Resolutions produced by ITU's major policy making conferences: Plenipotentiary Conference (PP), World Telecommunication Development Conference (WTDC) and World Telecommunication Standardization Assembly (WTSA)

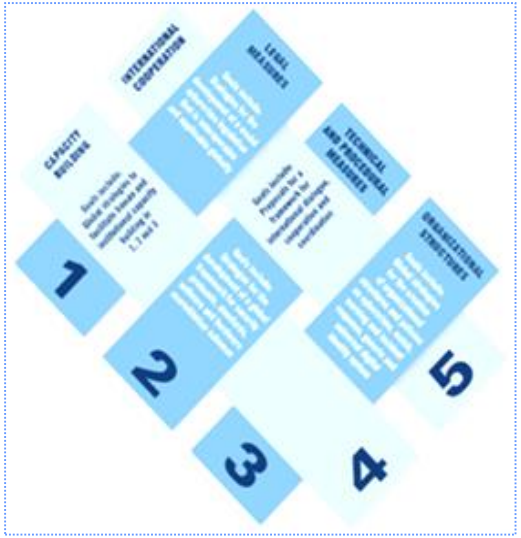
Coordinated Response

Need for a multi-level response to the cybersecurity challenges



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.



Launched in 2007

WTDC 17 Arab Regional Initiative

ARB2: Confidence and security in the use of telecommunications/ICTs

Objectives and Expected Results

Objective: To promote confidence and security in the use of ICTs, child online protection and combatting all forms of cyberthreat, including the misuse of information and communication technologies.

Expected results:

Assisting countries to:

1) issue policy guidelines, regulatory and technical frameworks and necessary measures and to provide information to meet their needs pertaining to this Initiative, specifically in the area of child online protection and combatting all forms of cyberthreat;

2) continue to sharpen awareness of the strategies to be followed with regard to the technical teaching and research materials which Arab university students are to be provided and taught to build confidence and security in the use of ICTs;

3) protect Arab children and young people from offensive and harmful content on the Internet, particularly by helping to enact laws, legislation and strategies in this area and raising the awareness of children and young people of the risks by launching awareness campaigns, workshops and training programmes and making use of the Arab Regional Cybersecurity Centre;

4) develop ICT applications to help protect children online and combat all forms of cyberthreat, in collaboration with relevant bodies;

5) organize training courses and seminars on protecting critical telecommunications/ICT infrastructure;

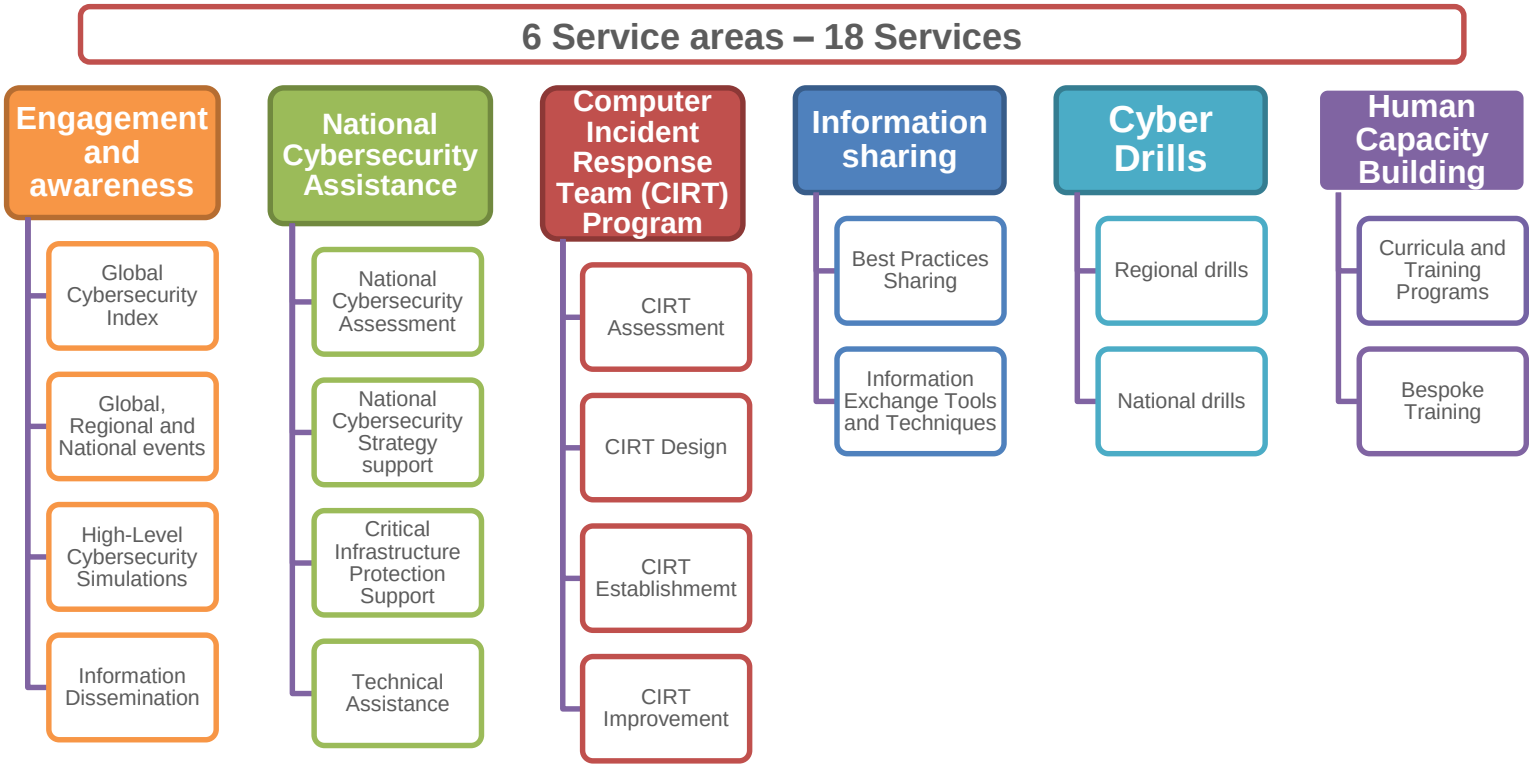
6) prepare training programmes and provide experts to specialized academic institutions to educate and instruct university students and academics in building confidence in the use of ICTs; exchange information in this regard;

7) establish national computer incident response teams (CIRTs) in the Arab region with optimum coordination among them and between them and CIRTs in the other regions.

Proposed Four Years Action Plan

Exp Res	2018	2019	2020	2021
ARB 2/1		Development of Strategies and Guidelines for the proper technical teaching and research materials on building confidence and security in the use of ICTs		Assistance to selected countries on the development of cybersecurity policy and strategy
ARB 2/2	Regional Forum for Building Partnership in Field of Cybersecurity with Academia		Training workshop for Academia on the strategies that ITU developed for the proper technical teaching and research materials on building confidence and security in the use of ICTs	
	Annual Regional Cybersecurity Summit			
ARB 2/3	Technical assistance to selected Arab countries in the development and/or implementation of their respective COP Action plans		Training workshop on COP	
	COP Challenge			
ARB 2/4		Launch a campaign for development of COP App for Arab region		Launch a campaign for development of application for Arab region on cybersecurity
ARB 2/5	Workshop on Cybersecurity for Essential Services (Health, Education, Finance, etc..)		Training workshop on critical infrastructure protection	
ARB 2/6			Development of training curricula on building trust in the use of ICTs	Regional Academia meeting on cyber security
ARB 2/7	• Regional Cyber Drill for the Arab Region • Arab Cybersecurity Cooperation Team (ACCT) meeting • Assistance to selected country for the establishment of national CIRT			

ITU's Development Sector & Cybersecurity



ITU Global cybersecurity Index (GCI)

GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States ***cybersecurity commitment*** with regard to the five pillars identified by the High-Level Experts and endorsed by the GCA.

"GCI is a capacity building tool, to support countries to improve their national cybersecurity"

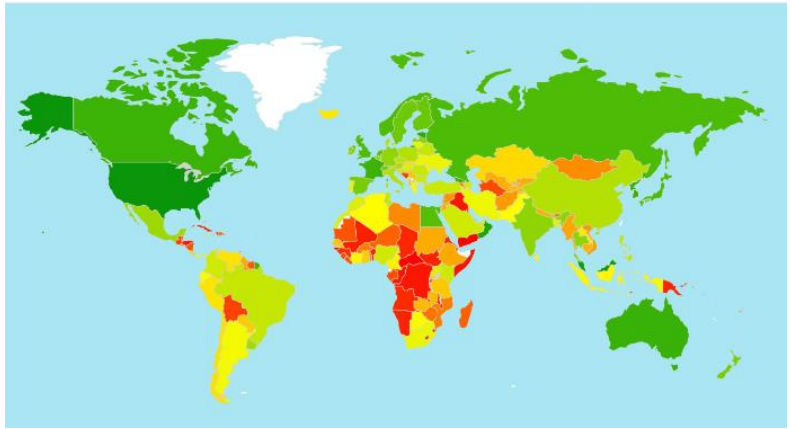
GCI overall approach

Goals

- Help countries identify areas for improvement
- Motivate action to improve relative GCI rankings
- Raise the level of cybersecurity worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity

World Heat Map

Level of commitment: from Green (highest) to Red (lowest)



Global and Regional Results 2017
Based on responses by 134 Countries

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

GCI overall approach

The GCIv3 includes 25 indicators and 50 questions. The indicators used to calculate the GCI were selected on the basis of the following criteria:

- relevance to the five GCA(Global Cybersecurity Agenda) pillars and in contributing towards the main GCI objectives and conceptual framework;
- data availability and quality;
- possibility of cross verification through secondary data.

How to improve GCI score and position

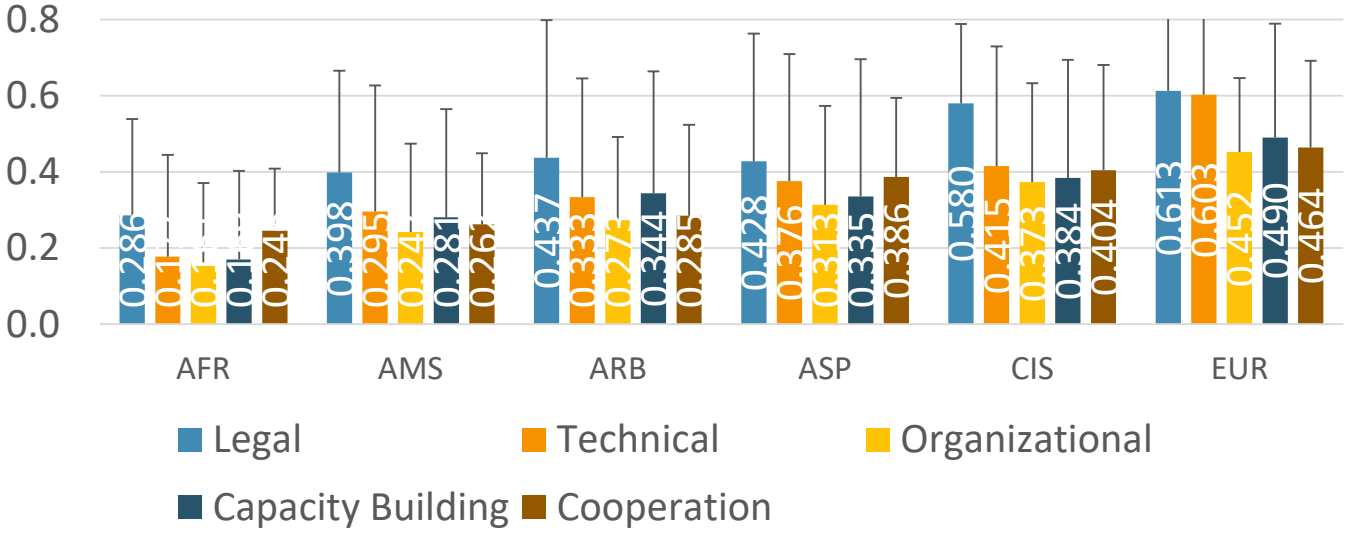
1. Commit to Cybersecurity!
2. Make continuous progress in all 5 pillars!
3. Make all relevant data available!
4. Cooperate when and where possible!
5. Actively participate in GCI!

GCIv2 Global Top Ten

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

Maximum score is 1

Global pillars' average by region



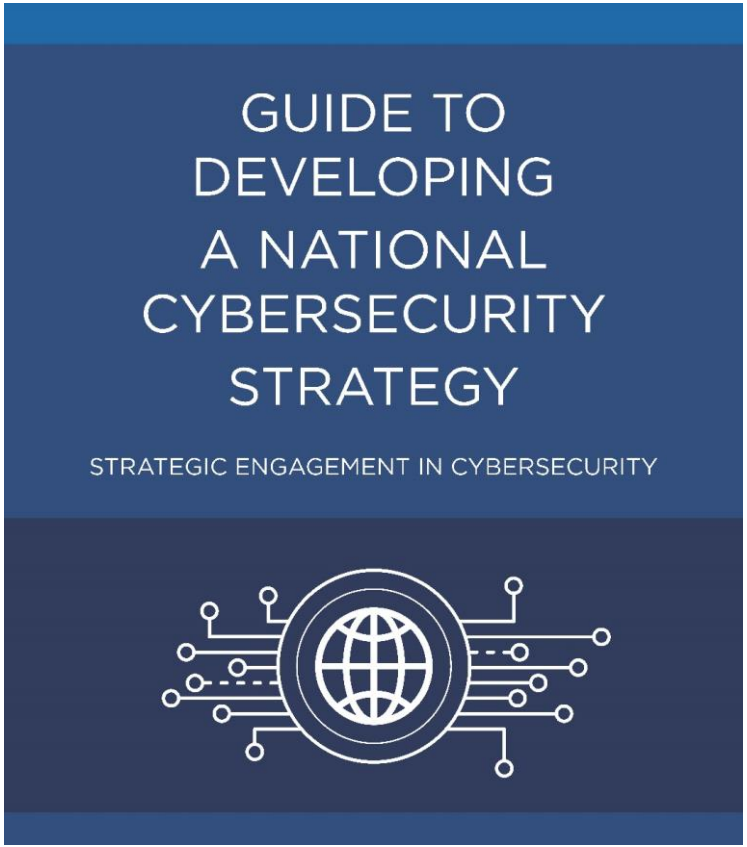
CIRT Programme

National CIRTs are in the first line of cyber-response

102 National CIRTs Worldwide

Need to fill the gaps

- Providing incident response support;
- Dissemination of early warnings and alerts;
- Facilitating communications and information sharing among stakeholders;
- Developing mitigation and response strategies and coordinating incident response;
- Sharing data and information about the incident and corresponding responses;
- Publicizing best practices in incident response and prevention advice;
- Coordinating international cooperation on cyber incidents;



The Commonwealth Cybercrime Initiative

CCDCOE

CTO

Global Cyber Security Capacity Centre

Deloitte.

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

ITU

Microsoft

Potomac Institute for Policy Studies

United Nations UNCTAD

RAND Corporation

The World Bank
IBRD • IDA | World Bank Group

Released in September 2018@ITU Telecom World

National Cyber Security Guide

A Joint Effort by 12 Partners

- Co-authored Multi-stakeholder approach

All project partners contribute their knowledge and expertise in the National Cyber Security domain, thereby providing a high added value to the toolkit definition

- Produced one reference guide on devising a national cybersecurity strategy to be followed by implementation in countries
- The reference guide represents a comprehensive one-stop resource for countries to gain a clear understanding of the purpose and content of a national cybersecurity strategy, as well as actionable guidance for how to develop a strategy of their own.
- It lays out existing practices, relevant models and resources, as well as offers an overview of available assistance from other organizations. An accompanying support tool assists evaluation of the strategy.

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx


GUIDE TO
DEVELOPING
A NATIONAL
CYBERSECURITY
STRATEGY
STRATEGIC ENGAGEMENT IN CYBERSECURITY

Purpose

Guides national leaders and policy-makers in the development of defensive responses to cyber-threats, in the form of a National Cybersecurity Strategy

A unique resource. A framework agreed on by organisations with demonstrated and diverse experience in the topic and builds on their prior work in this space

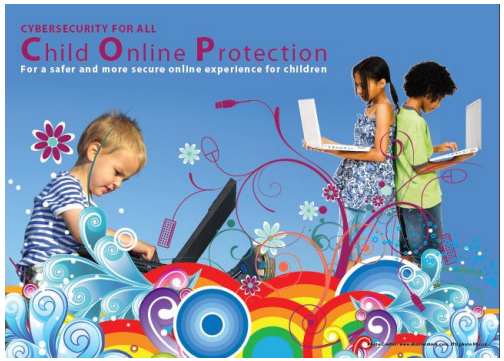
It offers policy-makers a holistic, high-level overview of existing approaches and applications, and a reference to additional and complementary resources that can inform specific national cybersecurity efforts.

Scope

Focuses on protecting civilian aspects of cyberspace. Does not cover aspects related to developing offensive and defensive capabilities

Provides indications on "**what**" should be included in a National Cybersecurity Strategy, as well as on "**how**" to build, implement and review it

Child Online Protection Initiative



The COP Initiative aims at bringing together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere.

Key Objectives:

- Identify risks and vulnerabilities to children in cyberspace
- Create awareness
- Develop practical tools to help minimize risk
- Share knowledge and experience

ITU meetings dealing with Cybersecurity

ITU Study Groups

- A platform for information exchange between ITU Member States and Sector Members (industry, academia etc.)
- ITU-D Study Group 2
  - Question 3/2: Securing information and Communication networks: Best practices for developing a culture of Cybersecurity
- ITU-T Study Group 17: Security
  - Standardization work on cybersecurity

International Policy-making Conferences

- World Telecommunication Standardization Conference (WTSA)

- World Telecommunication Development Conference (WTDC)

- ITU Plenipotentiary Conference 2018 in Dubai

WSIS Forum

- Annual multistakeholder event taking stock of the progress made in the implementation of the WSIS Summit Outcomes including AL C5 on “Building Confidence and Security in the use of ICTs”

- Linkage between the implementation of WSIS Action Lines and the Sustainable Development Goals (SDGs) (WSIS-SDG Matrix)

ITU's role in a nutshell

Neutral Global Convener

Technical Assistance / Capacity Building

Standardization

Knowledge Base

ITU : I Thank U

www.itu.int