ITU activities in cybersecurity

Farid Nakhli
Programme Officer
ITU Regional Office for CIS

Baku, Azerbaijan, 5th September 2018

About ITU

ITU is the United Nations **specialized agency for information and communication technologies** (ICTs)

Founded in Paris in 1865 as the International Telegraph Union

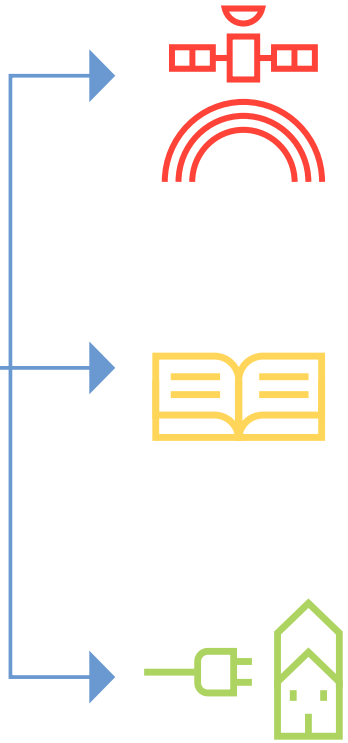
More than 150 years of experience and innovation

ITU Sectors

What we do

‘Committed to Connecting the World’

3 Sectors



ITU Radiocommunication

Coordinating radio-frequency spectrum and **assigning** orbital slots for satellites

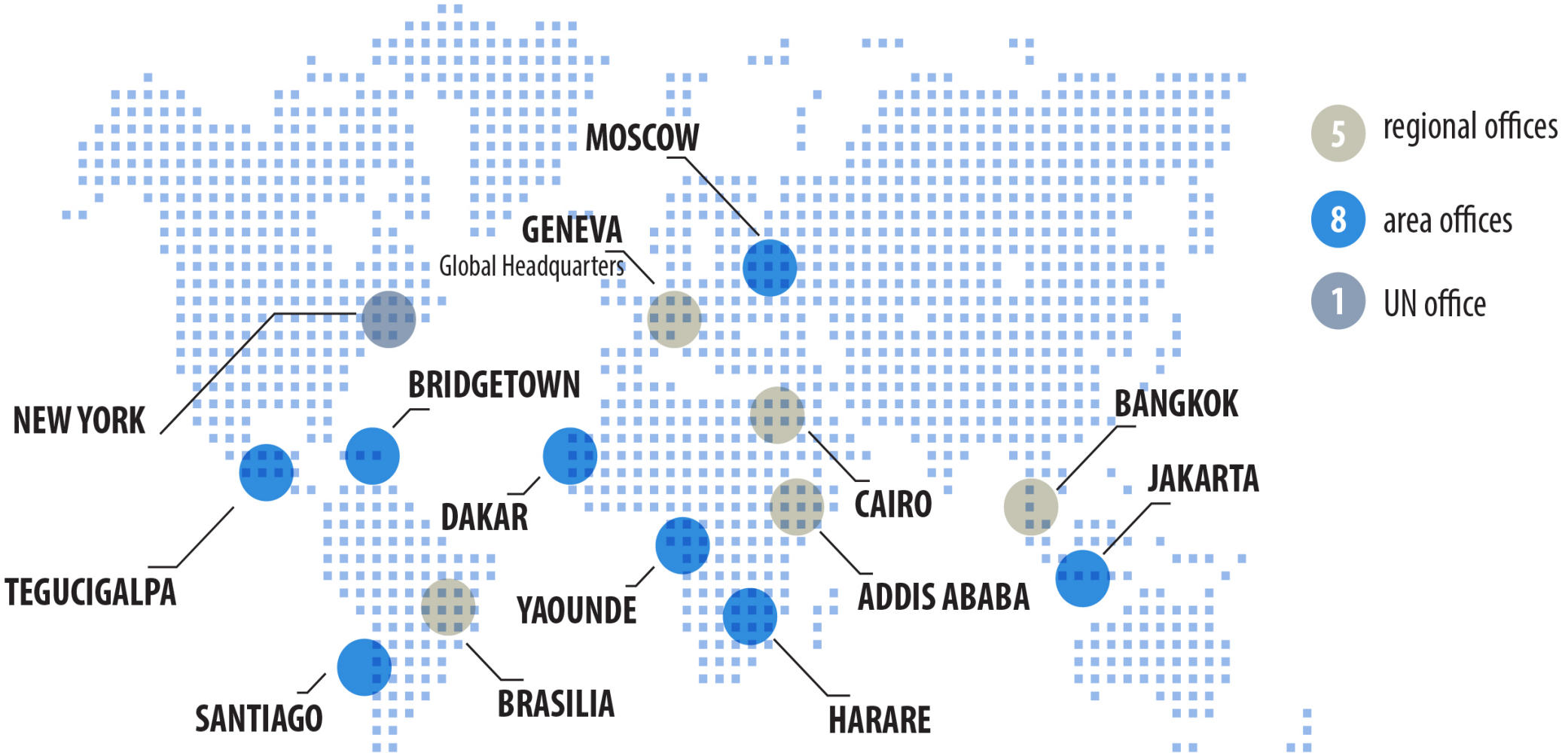
ITU Standardization

Establishing global standards

ITU Development

Bridging the digital divide

Global presence



ITU members

193

MEMBER STATES

+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

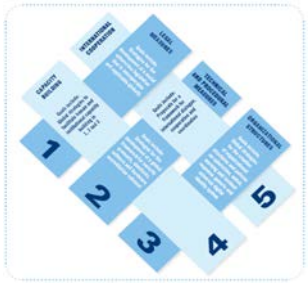
+150

ACADEMIA MEMBERS

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**

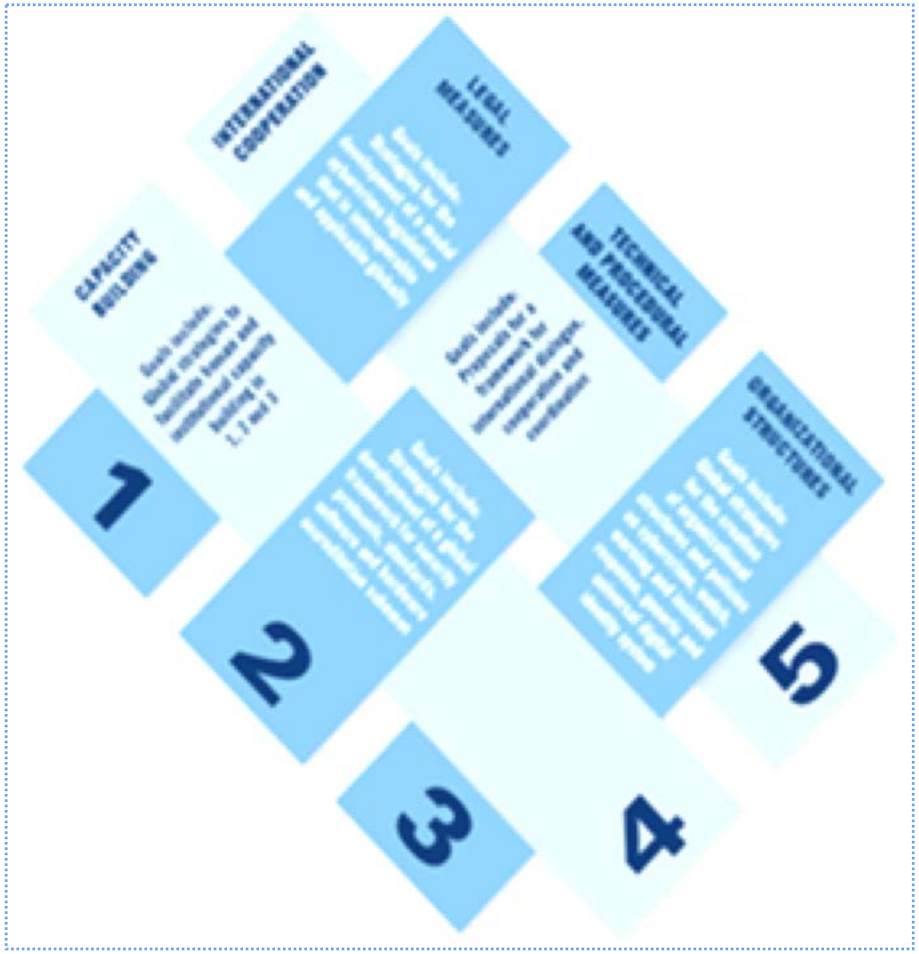
2008 to date
ITU Membership endorsed the GCA as the ITU-wide strategy on international cooperation.

GCA GLOBAL CYBERSECURITY AGENDA

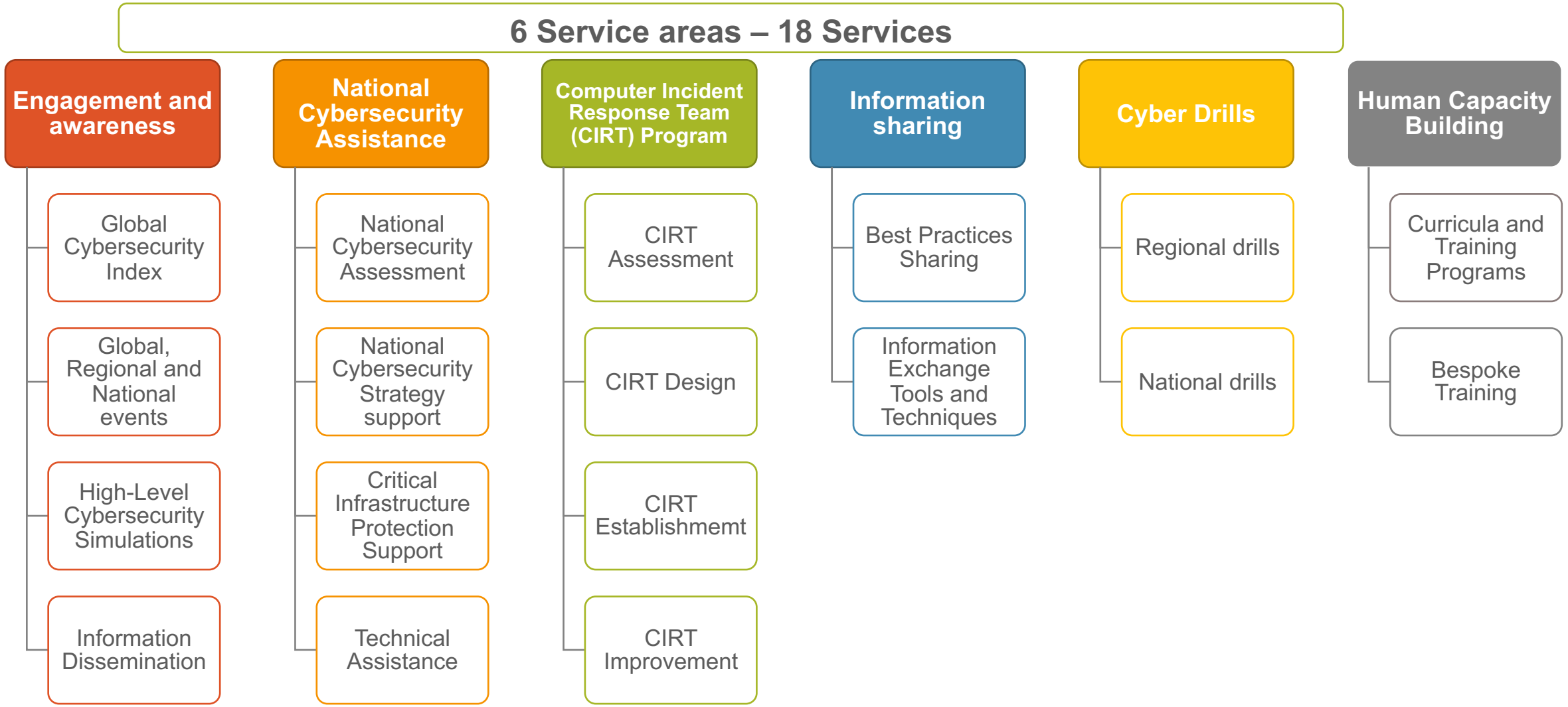
Building confidence and security in the use of ICTs is widely present in **PP and Conferences**' resolutions. In particular WTSA 12, PP 10 and WTDC 10 produced Resolutions (WTSA 12 Res 50, 52, 58, PP Res 130, 174, 179, 181 and WTDC 45 and 69) which touch on the most relevant ICT security related issues, 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
- Since its launch, GCA has attracted the support and recognition of leaders and cybersecurity experts around the world.



BDT Cybersecurity Program



GCI overall approach

Objective

The Global Cybersecurity Index (GCI) measures each ITU Member States' level of cybersecurity commitment in 5 main areas

- Legal - Technical – Organizational - Capacity Building - Cooperation

Goals

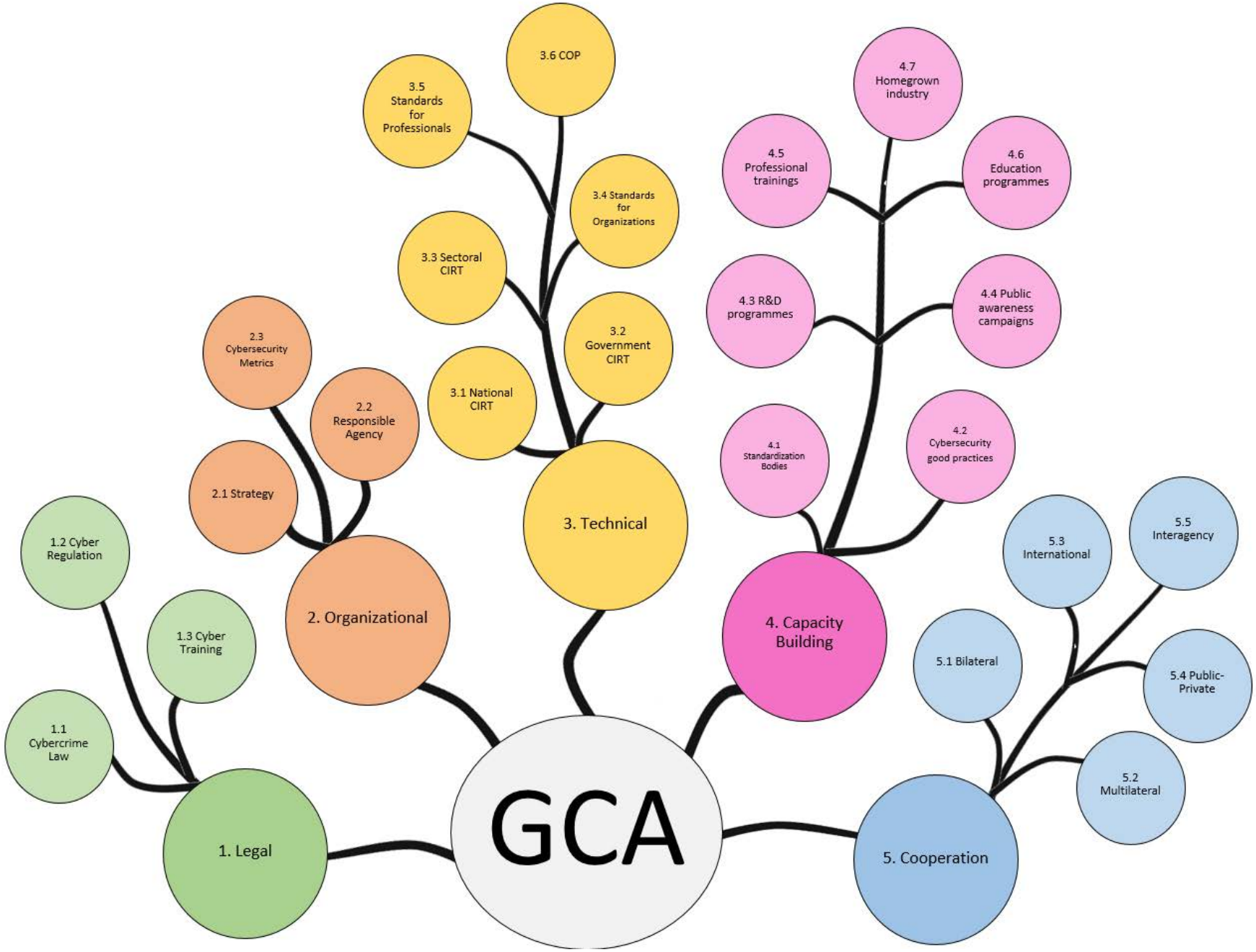
- Help countries identify areas for improvement
- Motivate action to improve relative GCI rankings
- Raise the level of cybersecurity worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity

134 responses – primary research

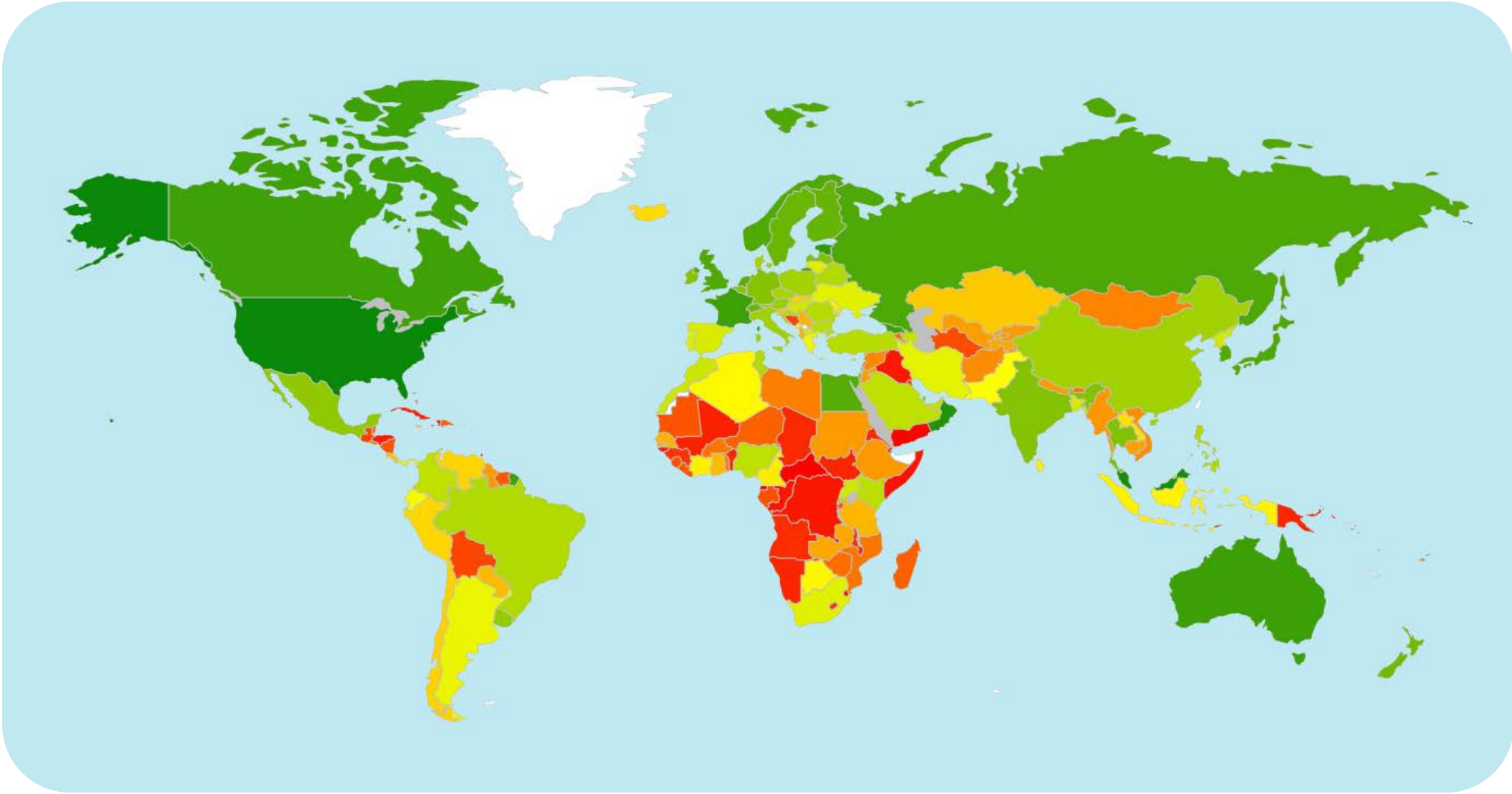
193 countries analysed - secondary research

24 Indicators based on the 5 pillars of the Global Cybersecurity Agenda (GCA)

Legal	Technical	Organizational	Capacity Building	Cooperation
• Cybercriminal legislation • Cybersecurity regulation • Cybersecurity training on regulation and laws	• National CIRT • Government CIRT • Sectoral CIRT • Standards implementation framework for organizations • Standards and certification for professionals	• Strategy • Responsible agency • Cybersecurity metrics	• Standardization bodies • Best practice • R & D programmes • Public awareness campaigns • Professional training courses • National education programmes and academic curricula • Incentive mechanisms • Home-grown cybersecurity industry	• Bilateral agreements • Multilateral agreements • International fora participation • Public-private partnerships • Interagency partnerships


GCA
1. Legal
1.1 Cybercrime Law
1.2 Cyber Regulation
1.3 Cyber Training
2. Organizational
2.1 Strategy
2.2 Responsible Agency
2.3 Cybersecurity Metrics
3. Technical
3.1 National CIRT
3.2 Government CIRT
3.3 Sectoral CIRT
3.4 Standards for Organizations
3.5 Standards for Professionals
3.6 COP
4. Capacity Building
4.1 Standardization Bodies
4.2 Cybersecurity good practices
4.3 R&D programmes
4.4 Public awareness campaigns
4.5 Professional trainings
4.6 Education programmes
4.7 Homegrown industry
5. Cooperation
5.1 Bilateral
5.2 Multilateral
5.3 International
5.4 Public-Private
5.5 Interagency

Heat Map



Commitment levels High Medium Low

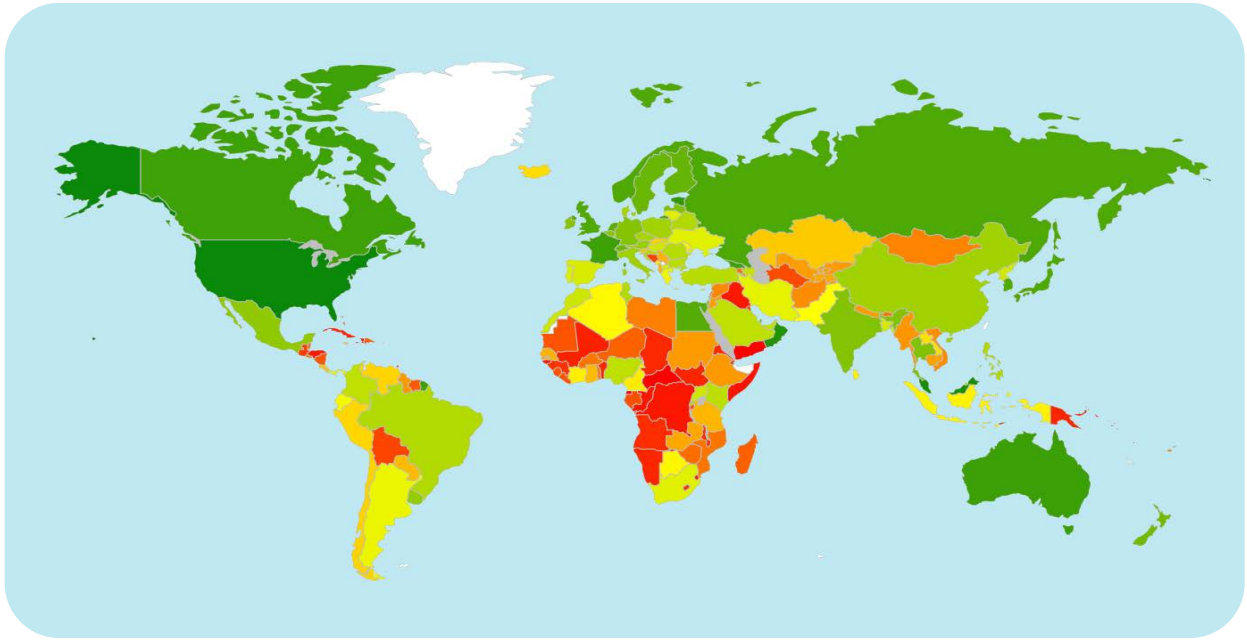
Global Top Ten

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

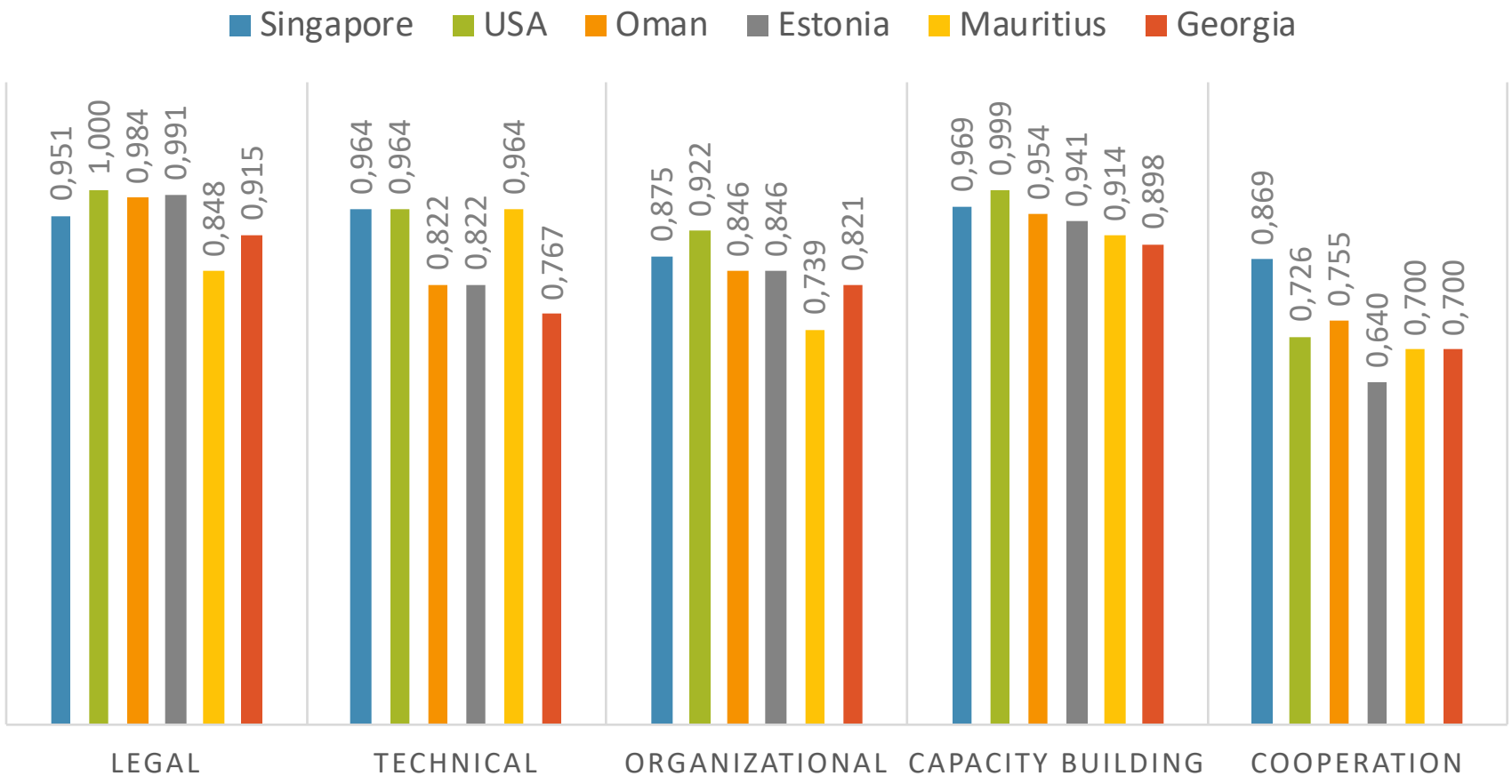
Maximum score is 1

2017 GCI global Participants

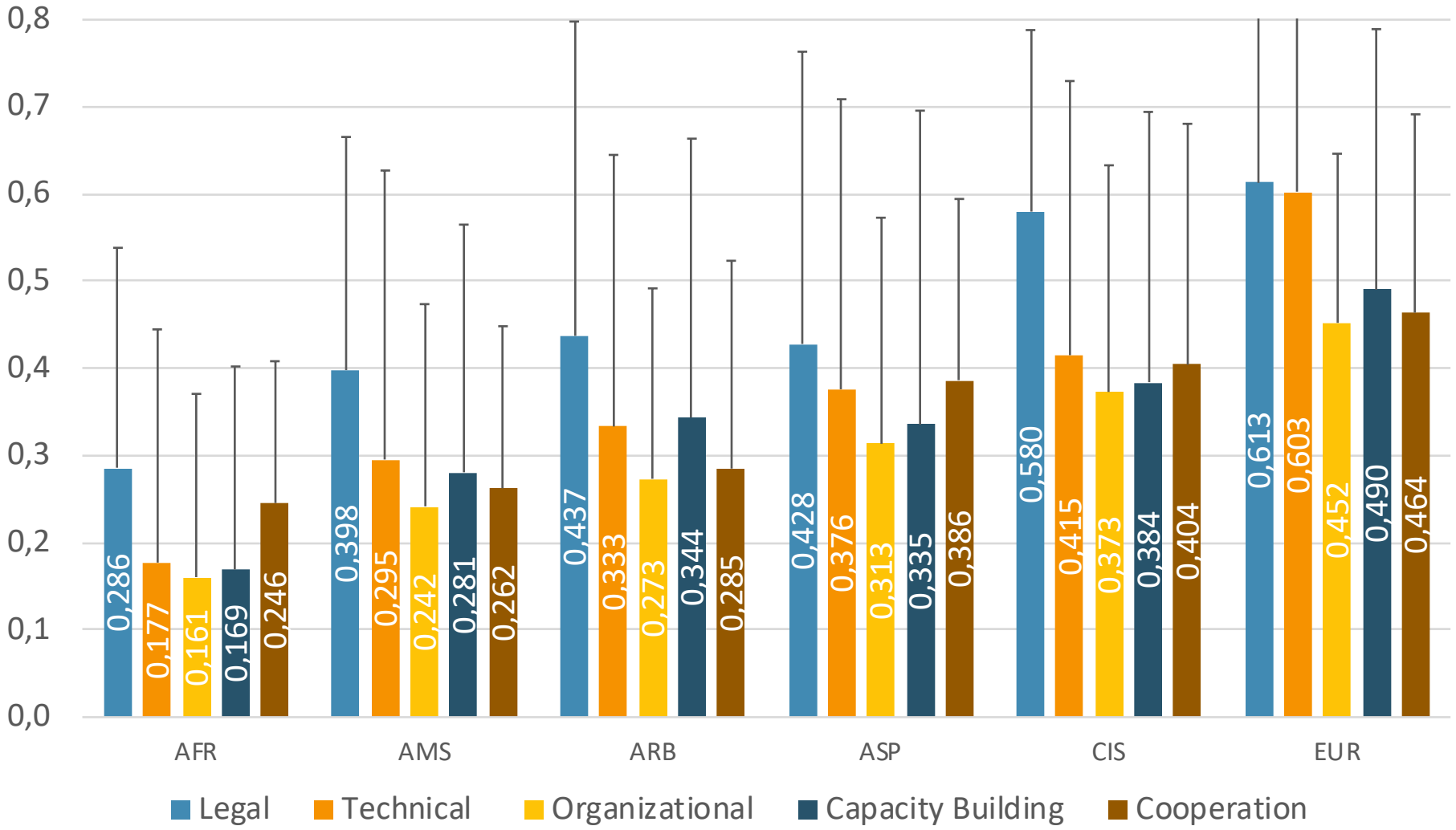
Region	Africa	Americas	Arab States	Asia-Pacific	CIS	Europe	Global
Responses	29	23	16	25	7	34	134
Non responses	15	12	5	13	5	9	59
Total of participants	44	35	21	38	12	43	193



TOP 5 ITU MEMBERS:
BEST COMMITMENT BY PILLARS



Global pillars' average by region

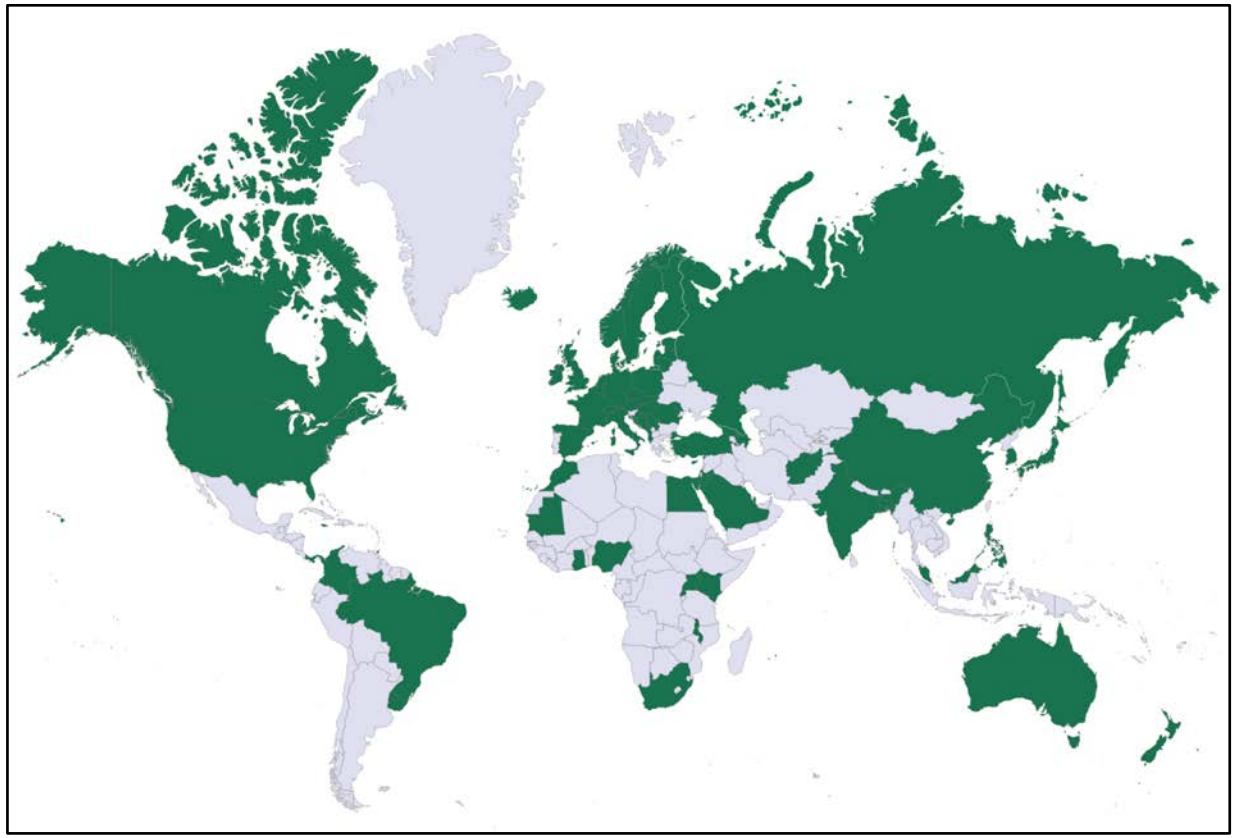


National Cybersecurity Strategies

- Policy document, Strategy document, Action Plan
- Process for review and enhancement
- Standalone document or embedded in other strategies …
- Actionable, Sustainable
- A public document or not …
- Currently over **72** countries have published National Cybersecurity Strategies
- The oldest was issued in 2004 and the latest in 2015..

Some repositories are

- ITU *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx*
- ENISA *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world*
- NATO CCDCOE *https://ccdcoe.org/strategies-policies.html*



Source: ITU

National Cyber Security Strategy (NCS) Toolkit

Examples of Topics To Be Addressed

- The role, objectives and scope of a National Cyber Security Strategy in a line with the UN SDGs
- The definition/publication/review process: the Governance Model
- National and International Standards and government compliance program
- Critical Infrastructure Protection and integration with other national security/emergency programs
- National Risk Management program
- National Incident Response/CERT - integration/alignment with Military/Intelligence
- Implementation strategies for the Government
- Implementation strategies for Private Sector
- The definition/publication/review process: the Awareness Programme
- Aspects not typically covered by public strategies that should be considered and addressed

Components of Toolkit

Reference Guide

- **A single resource** for any country to gain a clear understanding of National Cyber Security Strategy in terms of:
  - the **purpose and content**
  - how to go about **developing a strategy,** including **strategic areas and capabilities**
  - the relevant **models and resources** available
  - the **assistance available** from various organisations and their contact details
- FORMAT: 15-20 page Word / PDF

Evaluation Tool

- **A simple tool** that allows national governments and stakeholders to:
  - Evaluate their **current status in each of the strategic areas** identified in the reference guide
  - Evaluate their **current status in cyber security lifecycle management**
  - Easily **identify key areas** for improvement
  - Provide a means for **measuring improvements** over time
- FORMAT: Excel or web-based worksheet

Co-authored and Co-owned by Partners

Five key elements to consider when designing a toolkit

	1 GEOGRAPHIC FOCUS	2 TARGET STRATEGY APPLICABILITY	3 AREAS OF IMPROVEMENT	4 LINKAGE/REFERENCE TO OTHER MODELS	5 DESIGNED FOR ASSESSING IMPROVEMENTS
DEFINITION	Which countries / regional areas the model / tool focuses on	Designed to define a strategy or to evaluate an existing strategy	Helps to identify areas of improvement and how to address them	Establishes links to existing guidelines /references	Includes functionality for measuring improvements over time
PARAMETER	▪ **Global:** Designed for use in all countries ▪ **Regional:** Tailored for use in a specific region / political alliance	▪ **New:** Provides guidance in developing a new strategy ▪ **Existing:** Helps to evaluate existing strategies	▪ **Identify:** Identifies improvement areas ▪ **Address:** Provides solutions for improvement areas	▪ **Global:** Refers to globally focused models ▪ **Regional:** Refers to regionally focused models	▪ **Indicators:** Best practice indicators for each component of the strategy that can be measured repeatedly over time

By leveraging the strengths of existing guidelines and evaluation tools across these elements…

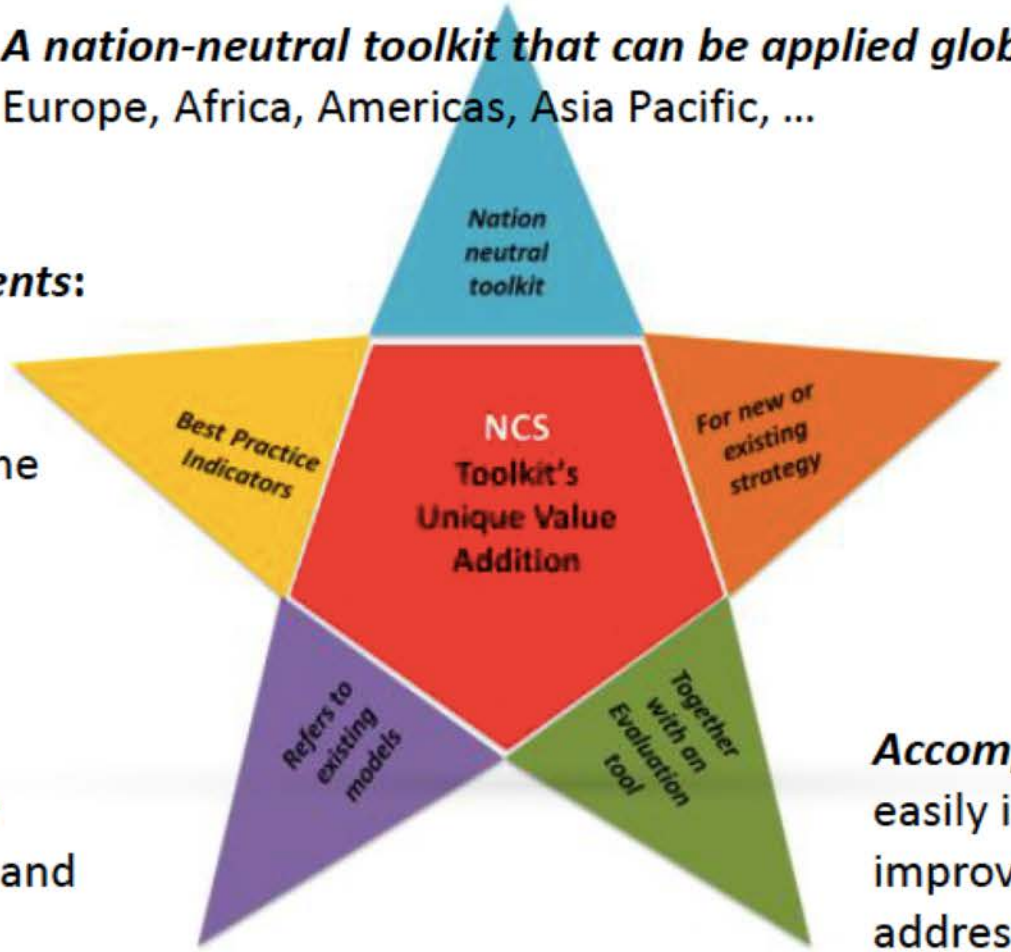
Models / Tools	Geographic Focus		Target Strategy Applicability		Areas of improvement		Linkage/reference to other models		Designed for assessing improvements
	Global	Regional	New	Existing	Identify	Address	Global	Regional	Indicators
ITU National Cyber Security Toolkit (This project)	X	X	X	X	X	X	X	X	X
ITU – National Cybersecurity Strategy Guide (2011)	X		X						
Oxford Martin School – Cyber Capability Maturity Model (2014)				X	X				
CTO – Commonwealth Approach For Developing National Cyber Security Strategies (2014)		X							
Microsoft – Developing a National Strategy for Cybersecurity (2013)			X						
CCDCOE - National Cyber Security Framework Manual (2012)	X		X						
OECD - Cybersecurity Policy Making at a Turning Point (2012)			X						
OAS – Cyber Security Program (2004)		X	X						

…we can achieve our goal of adding value to members by creating a framework that leverages global best practices

Strengths of NCS Toolkit

***A nation-neutral toolkit that can be applied globally*:**
Europe, Africa, Americas, Asia Pacific, …

***Measuring improvements*:**
provide best practice indicators to assess improvements over time



***Pragmatic reference guide can be used by all countries, including micro-countries*:** developed strategies, new strategies under development, …

Reference to other guidelines/references:
link to existing models and evaluation tools

Accompanying evaluation tool:
easily identify key areas for improvement and how they can be addressed

We have also defined the basic Reference Guide structure consisting of five main sections

WORK IN PROGRESS

National Cyber Security Toolkit

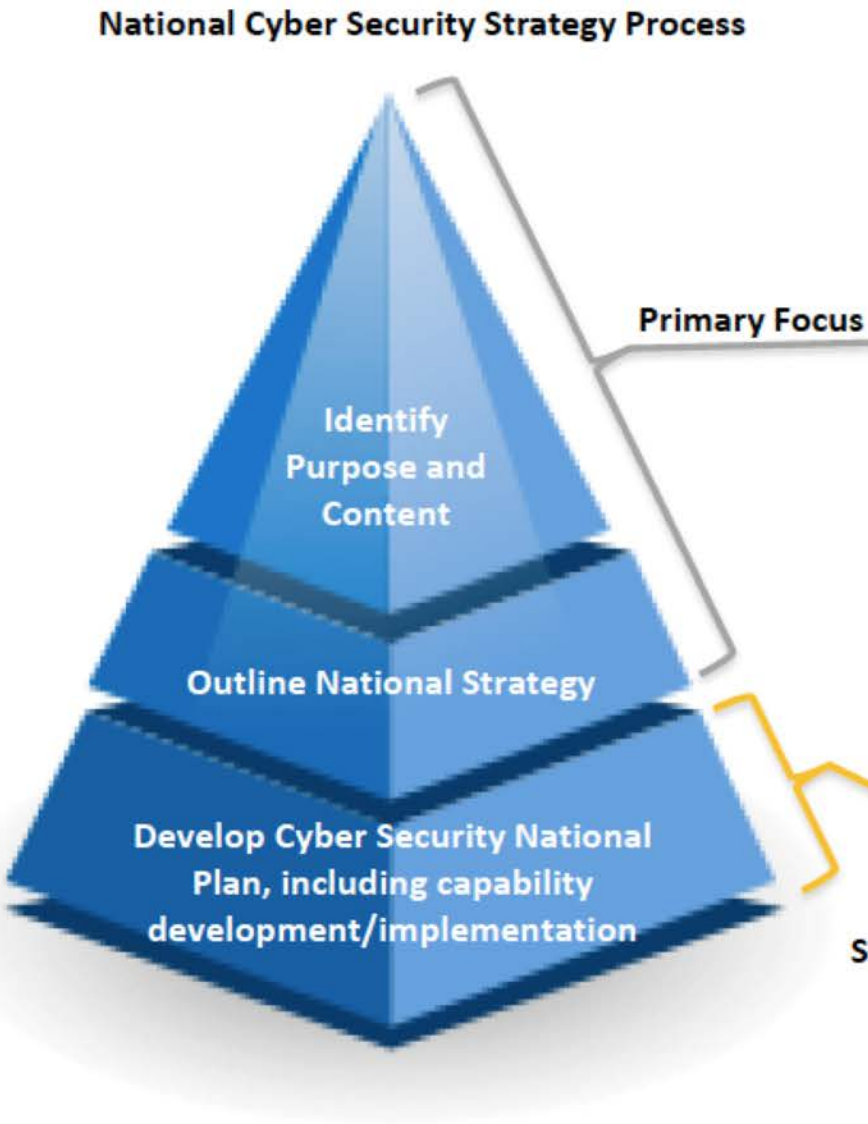
REFERENCE GUIDE

Est. 15-20 pages

Structure of Reference Guide

1. **Toolkit Description**
   - Position relative to other guides
   - Target Audience
   - How to Use
2. **Strategic Areas to Address**
   - Macro areas that a national strategy should address
   - Public vs. confidential areas
3. **Implementation Guidelines**
   - PDCA approach in national terms
   - Elements relevant to implementation that should be outlined in the strategy
4. **Development Blueprint**
   - Basic project approach for writing or improving a national strategy
   - Lessons learned on what to avoid
5. **Supporting Material References**
   - Direct links to supporting material to support writing the strategy
   - Cross-references to other tools

Positioning and functionality of the toolkit



Primary Focus

- The NCS Toolkit will provide national policy developers with a **means to evaluate their current status and identify areas for improvement** regarding:
  - Identifying the **purpose and content** of their own national cyber security strategy
  - Outlining the **strategic areas** that their national cyber security strategy should address
  - Defining a **management lifecycle process** to govern the implementation of the strategy
  - Establishing a **structured process** for strategy development
  - Finding **additional resources** to support strategy development

Secondary Focus

- The NCS Toolkit will provide national policy developers with **links to other best practice guidelines** for insights on how to:
  - Develop National Plan
  - Evaluate the current **maturity levels of** their national **cyber security capabilities**
  - **Compare their strategies / capabilities** against peers through ranking systems and criteria
  - ...more

National CIRTs are in the first line of cyber-response

- 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;
- Publicising best practices in incident response and prevention advice;
- Coordinating international cooperation on cyber incidents;

Around 103 National CIRTs Worldwide

CIRT assessment

ITU is helping countries to establish their National Computer Incident Response Team (CIRT), which serves as a national focus point for coordinating cybersecurity incident response to cyber attacks in the country. The objective of the CIRT Assessment is to define the readiness to implement a national CIRT.

ITU has to date completed CIRT assessments for **71** countries.

Africa: Angola, Botswana, Burkina Faso, Burundi, Cameroon, Central African Republic, Chad, Congo (Dem Rep), Congo (Republic), Côte d'Ivoire, Gabonese Republic, Gambia, Ghana, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mozambique, Niger , Nigeria, Rwanda, Senegal, Sierra Leone, Swaziland, Tanzania, Togolese Republic, Uganda , Zambia, Zimbabwe
Americas: Anguilla, Antigua, Barbados, Bolivia, Dominica , Dominican Republic , Ecuador, Grenada, Honduras, Jamaica , St Kitts & Nevis, St Lucia, St Vincent & The Grenadines, Suriname, Trinidad and Tobago
Arab region: Comoros, Djibouti, Jordan, Lebanon, Mauritania, Palestine, Sudan
Asia & Pacific: Afghanistan, Bangladesh , Bhutan, Cambodia, Fiji, Laos, Maldives , Myanmar, Nepal , Vanuatu, Vietnam
Europe & CIS: Albania , Armenia, Cyprus, Macedonia, Monaco, Montenegro, Serbia

CIRT establishment

After the assessment, the initiative assists with planning, implementation, and operation of the CIRT. Continued collaboration with the newly establish CIRT ensures that support remains available.

ITU has established **National CIRTs in 14 countries**: Barbados, Burkina Faso, Côte d'Ivoire, Cyprus (Governmental CIRT) + National CSIRT, Ghana, Jamaica, Kenya, Lebanon, Macedonia, Montenegro, Tanzania, Trinidad and Tobago, Uganda, Zambia.

CIRT Implementations **in progress in 5 countries**: Burundi, Cyprus (National CIRT), Gambia, Palestine and Zimbabwe.

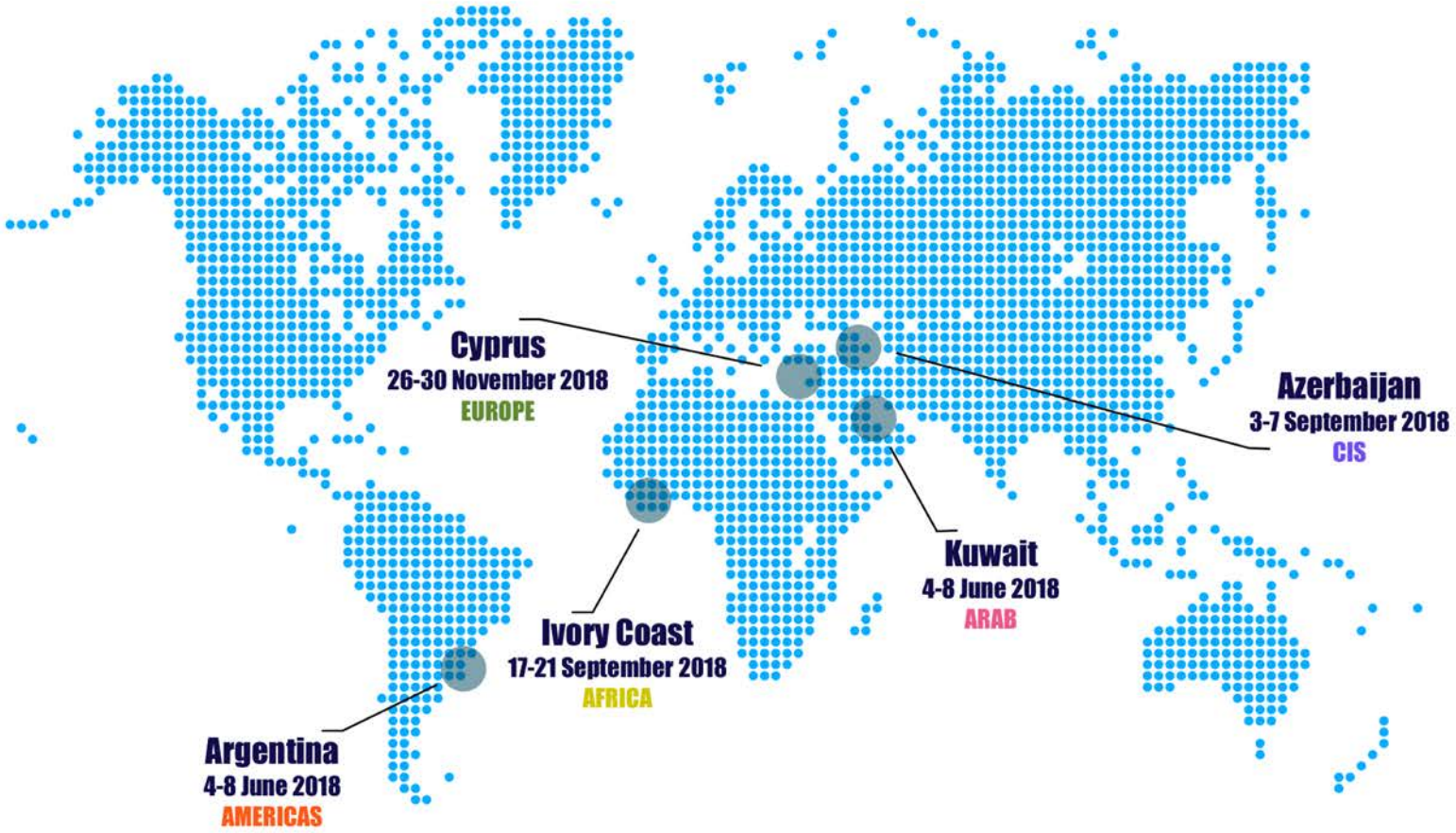
CIRT **enhancement in progress in 1 country**: Kenya

Regional Cyber drills

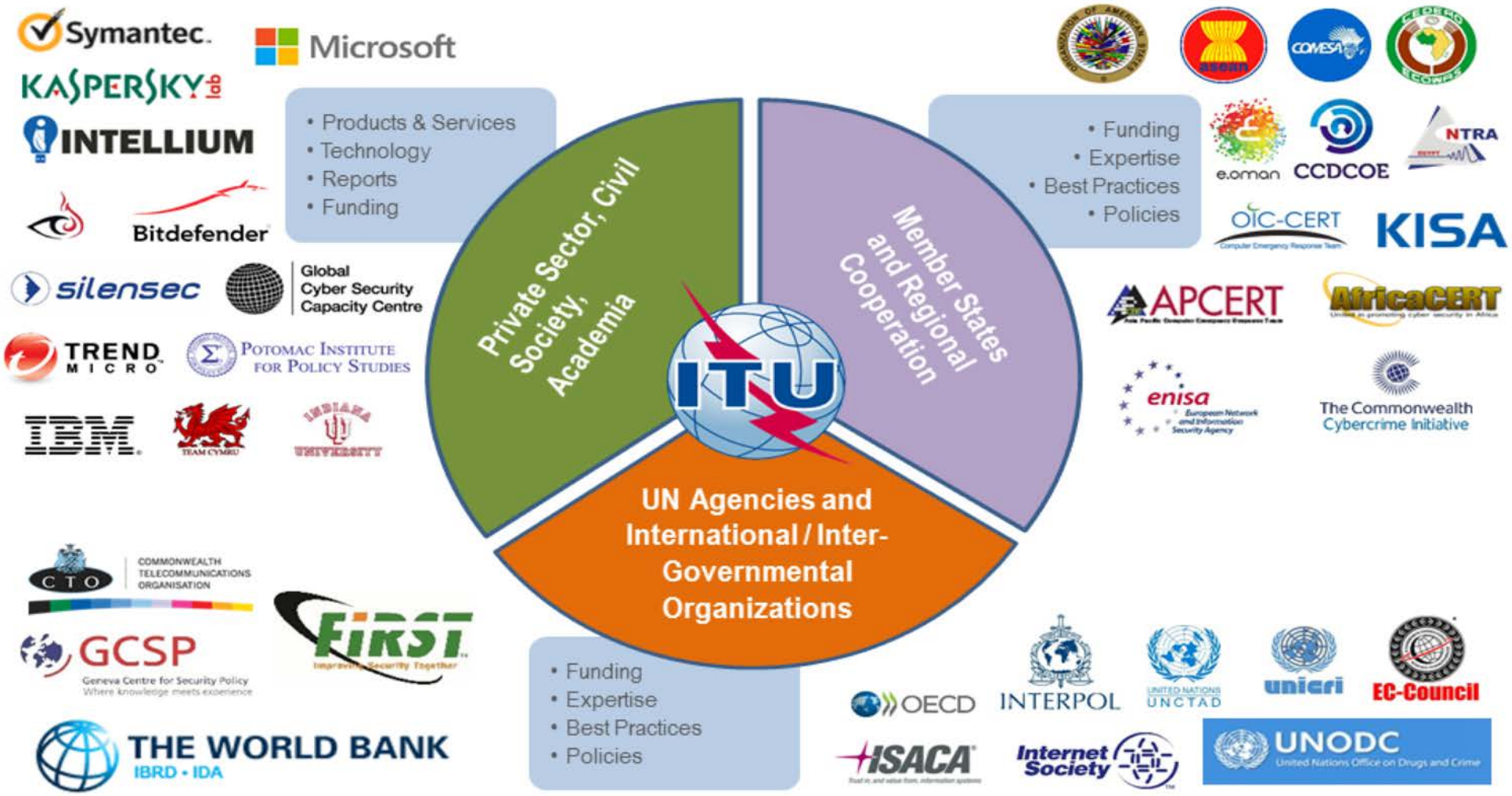
The ITU regional cyberdrills are annually events held for the purpose of:

- Enhancing Cybersecurity capacity and capabilities through regional collaborations and cooperation;
- Enhancing the awareness and the capability of countries to participate and to contribute to the development and deployment of a strategy of defeating a cyber threat;
- Strengthening International Cooperation between Member States to ensure continued collective efforts against cyber threats;
- Enhancing Member States' and incident response capabilities and communication;
- Assisting Member States to develop and implement operational procedures to respond better to various cyber incidents, identify improvements for future planning CIRT processes and operational procedures.

Regional Cyber drills: 2018



Multi-Stakeholder Partnership



THANK YOU