Cybersecurity for Digital Development

From norms to national capabilities

Cyber resilience is now a development, trust, and stability issue — and ITU's value is in translating multilateral cooperation into practical national capabilities.

cybersecurity@itu.int

13-03-2026

Why ITU’s work matters in cybersecurity

The unique value of ITU lies in bridging multilateral legitimacy and country-level implementation.

Multilateral legitimacy

Trusted platform for dialogue, coordination, standardization and policy alignment.

Technical and policy convening power

Ability to foster collaboration between governments, technical communities, academia and industry partners.

Country-level implementation support

Capacity-building pathways that turn principles into institutions, skills, and practice.

Cyber resilience cannot be built by diplomacy alone — or by technical actors alone. It requires both.

How ITU delivers

Measure. Build. Convene.

Measure

- Assess commitment gaps
- Benchmark maturity
- Identify priorities
- National Cyber Risk assessments
- Assess Readiness

Build

- Support institutions
- Strengthen strategies and skills
- Advance protection frameworks around Critical Infrastructures

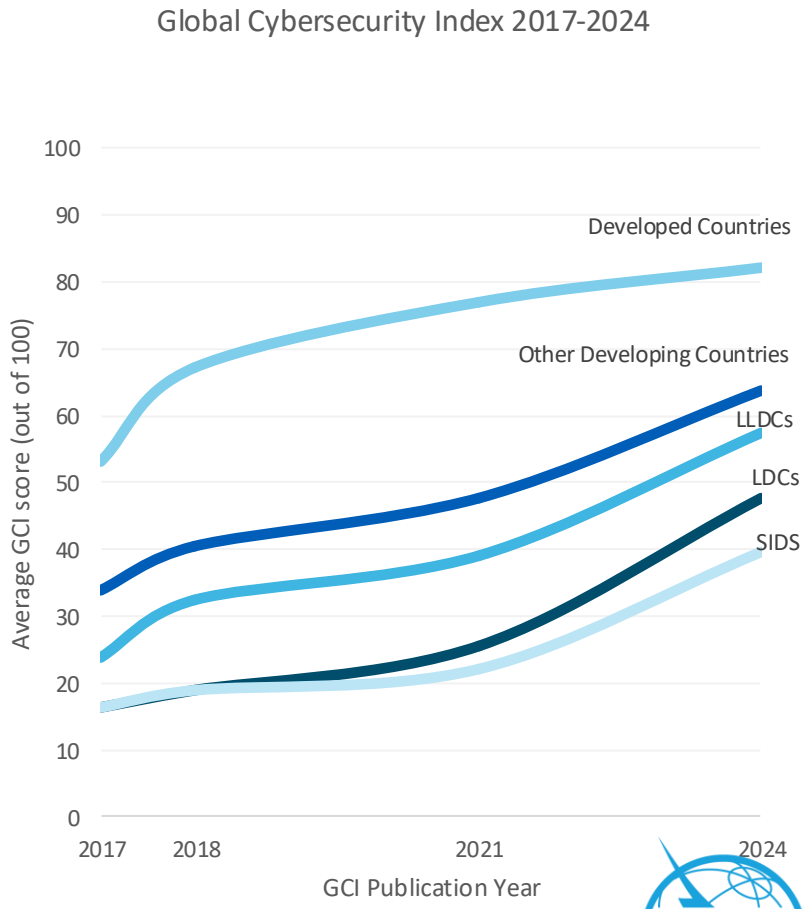
Convene

- Bring together governments
- Mobilize ITU Membership and partners
- Scale delivery through cooperation
- Cyberdrills and Tabletop Exercises (Policy & Technical)

Cyber resilience requires evidence, institutions, and cooperation — not isolated projects.

We provide targeted technical support based on mandates, feedback from Member States, and data

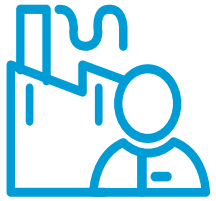
Resolution	Topics addressed
Plenipotentiary Res 130 (Rev. Bucharest, 2022)	Information sharing, international cooperation, cybersecurity frameworks, capacity development, awareness raising, institutional capacity, SMEs, infrastructure, Global Cybersecurity Index, Global Cybersecurity Agenda
Plenipotentiary Res 179 (Rev. Bucharest, 2022)	Child Online Protection (COP), international cooperation
WTDC Res 45 (Rev. Baku 2025)	Information sharing, international cooperation, capacity development, vulnerable populations, Global Cybersecurity Index, cybersecurity frameworks,
WTDC Res 67 (Rev. Baku 2025)	Child Online Protection (COP), international cooperation
WTDC Res 69 (Rev. Baku 2025)	CIRTs, international cooperation, capacity development, information sharing
WTSA Res 50 (New Delhi, 2024)	Cybersecurity standards, international cooperation, emerging risks, awareness raising, information sharing
WTSA Res 52 (New Delhi, 2024)	Spam, international cooperation
WTSA Res 58 (New Delhi, 2024)	CIRT, international cooperation



ITU works in partnership with local actors, governments, regional organizations, and companies

Governments

Czech Republic, Germany, Italy, Kingdom of Saudi Arabia, UAE, Republic of Korea, UK

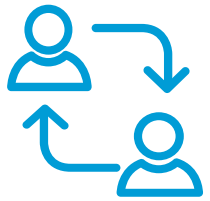


Private Sector

Axon Consulting, BitSight Technologies, Deloitte, Dreamlab, Immuniweb, Lego, Meta, Microsoft, NRD CyberSecurity, Roblox, Silensec, TikTok and others

International & Regional organizations

AU, ENISA, European Commission, CRASA, ECOWAS, FIRST, GFCE, Internet Society, INTERPOL, OAS, UNCTAD, UNCTT, UNDESA, UNESCO, UNDP, UNICEF, UNICRI, UNIDIR, UNODC, World Bank, World Economic Forum, and others



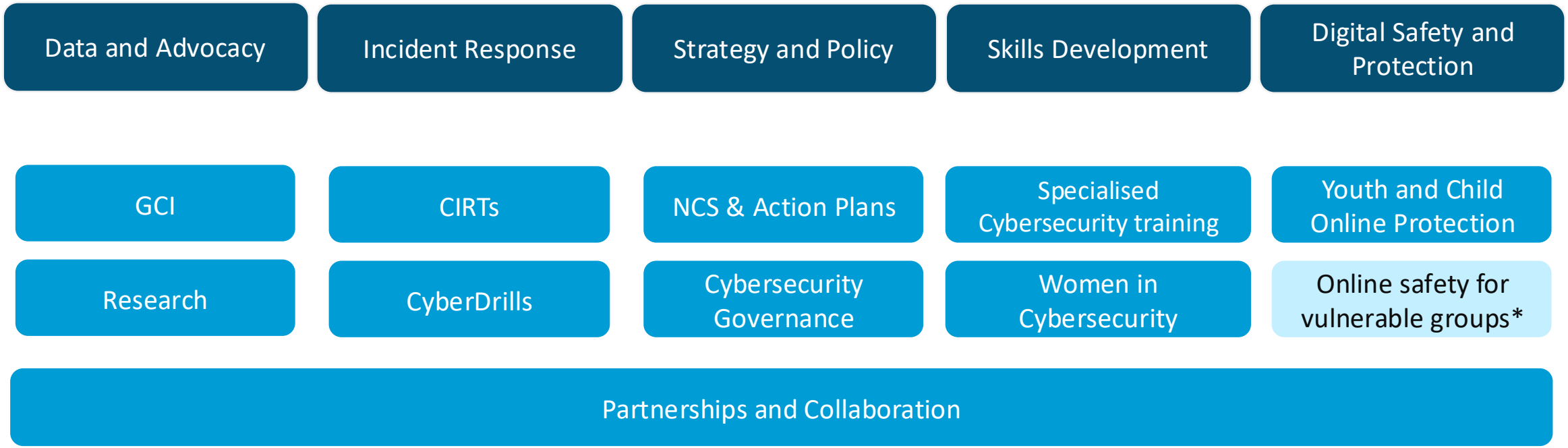
Academia, Civil Society NGOs

ASPI International Cyber Policy Centre, Chatham House, DCAF, Geneva Centre for Security Policy, Child Helpline International, 5Rights Foundation, Western Sydney University, and others

ITU Regional Presence

14 Regional and area offices

ITU Cybersecurity works across:



- * Planed – NEW, Targeting youth, persons with disabilities, elderly and women and girls

Data and Advocacy

Global Cybersecurity Index

Measuring the gap: evidence for action

172 countries

participated directly in the Global Cybersecurity Index

140+ experts

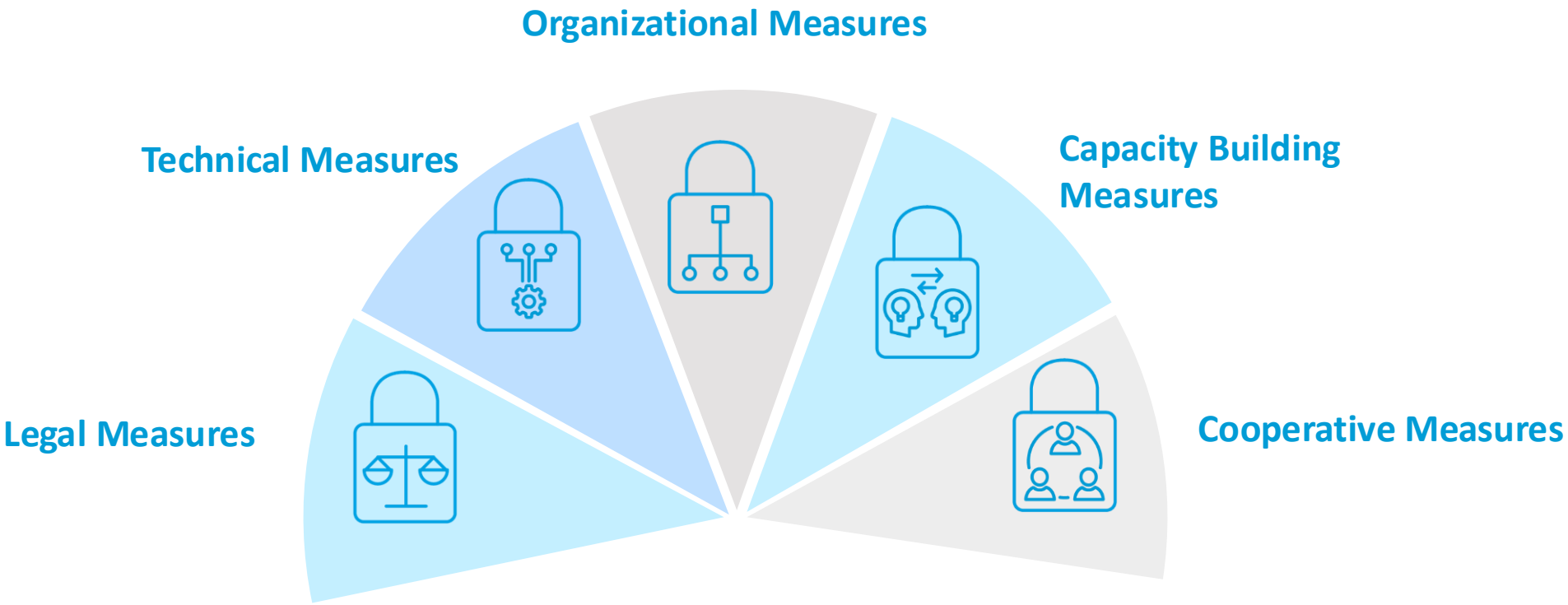
contributed to the input to the methodology assessment and evidence base questionnaire design

Why this matters

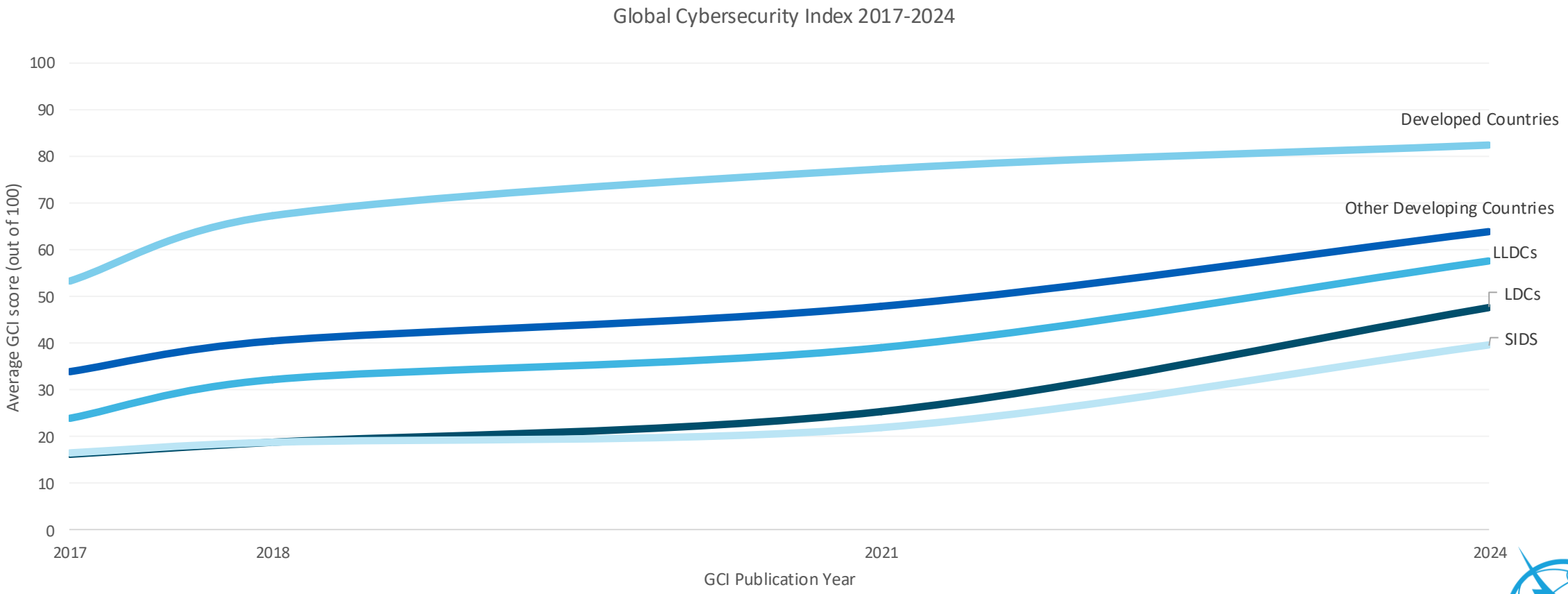
- Evidence turns cyber capacity building from aspiration into prioritization.
- Comparative commitment baselines help governments, partners, and donors direct support more effectively.
- The GCI's findings on LDCs and SIDS make the equity case visible.

Measurement of commentment is not a ranking exercise for us.
It is a Policy and Capacity Development tool.

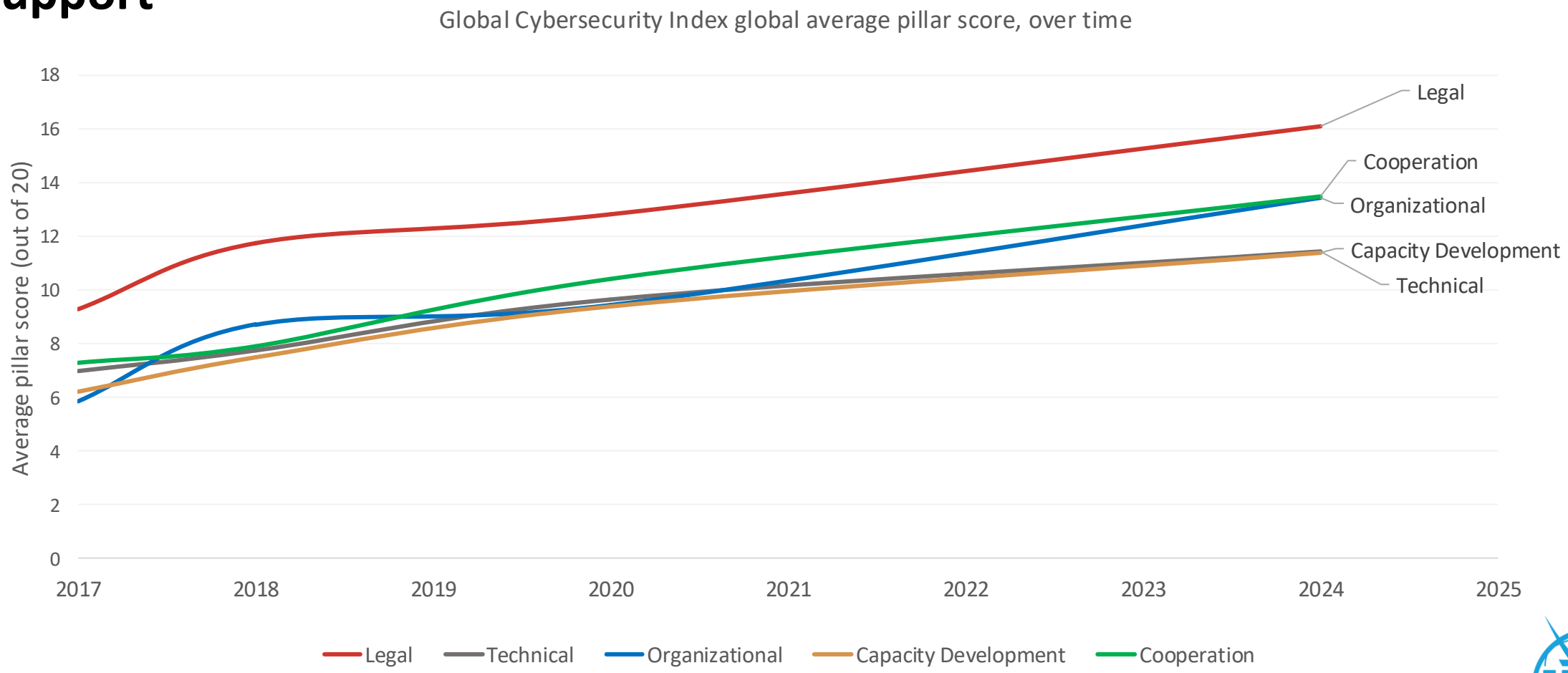
GCI takes a holistic approach to countries cybersecurity commitments



LDCs are starting to close the cyber capacity gap, but need support to solidify gains. SIDS need additional support



Globally, capacity development and technical measures need more support



Incident Response & Resilience

Building global cyber resilience

A sustainable development approach:
From assessments to establishment of institutions and capabilities

85+
national CIRT assessments completed

24 / 6
CIRTs established / enhanced

160+
countries engaged through CyberDrills

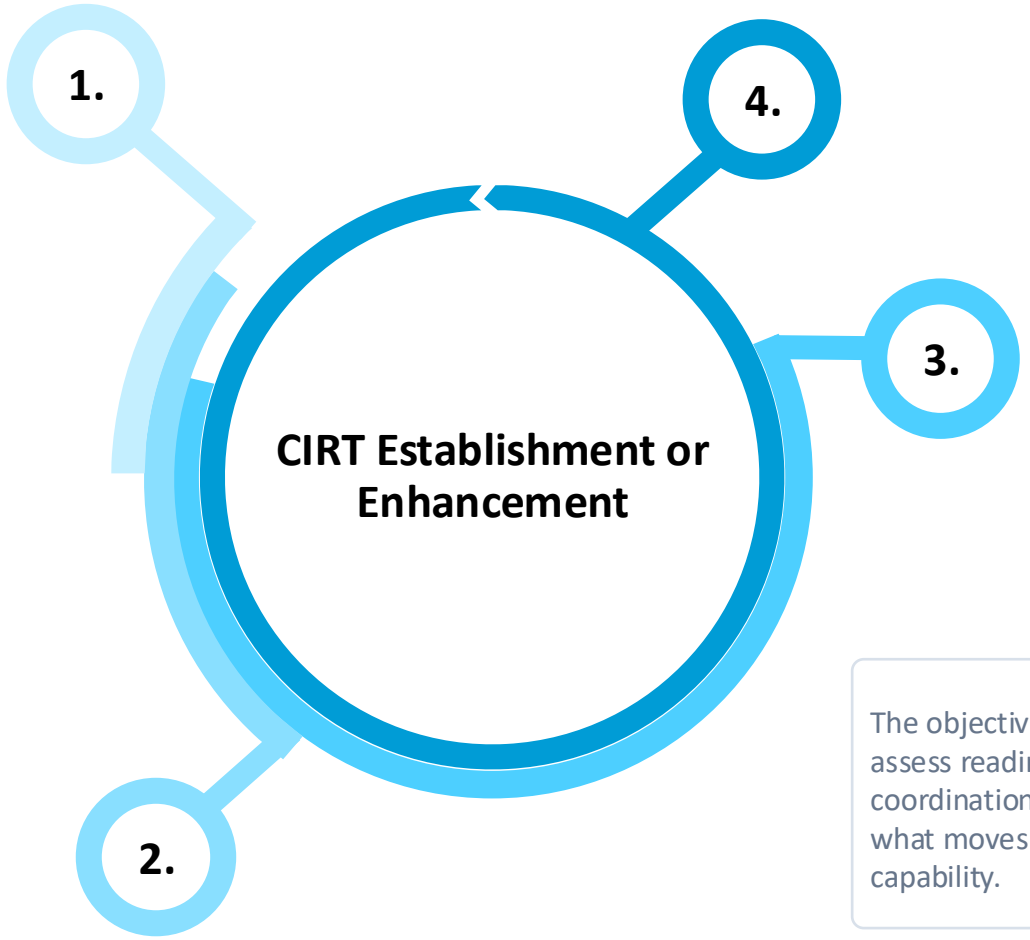
5+
Ongoing CIRT Implementations

13

ITU's Methodology for CIRT establishment & enhancement lifecycle

CIRT Readiness/Maturity Assessment:
Measuring the readiness for CIRT establishment/ enhancement

Design:
Preparing detailed design for the CIRT, including implementation processes and tools, engagement plan, networks design, training plans, etc.



Establishment:
Implementing infrastructure, building relationships with stakeholders, constituency, mandate, processes, services, launching operations, etc.

Enhancement:
Setting up additional services or improving existing service delivery for CIRT.

The objective is not a set of isolated activities. It is a sequence: assess readiness, establish or strengthen institutions, exercise coordination, and anchor the work in national strategy. That is what moves cybersecurity from a workshop topic to state capability.

CyberDrills:
Sustainable Capacity Development and Confidence Building Measures

- Hands-on exercises for national CIRTs
- Platform for cooperation and information sharing on good practices and current cybersecurity issues
- Publication - CyberDrill Framework
- Delivered over **60** national, regional and global CyberDrills since 2012
- Engaged over **160** countries

Recent and Upcoming CyberDrills can be found at:

https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

Cybersecurity Strategy and Policy

National Cybersecurity Strategies: development support

Activities:

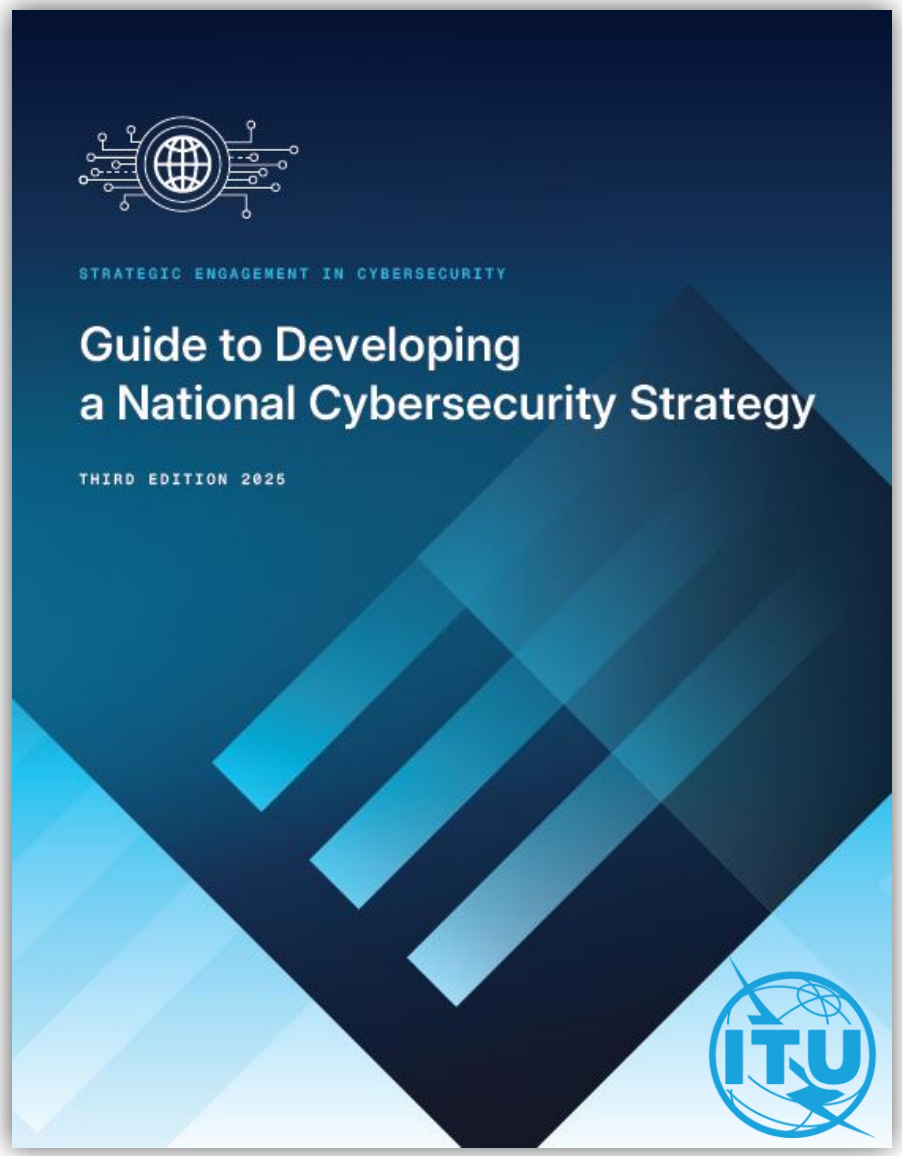
- National Cybersecurity assessments
- Facilitation of NCS and Action Plan Development
- Trainings and Human Capacity Development
- Technical Assistance
- Tabletop Exercises

Guide to Developing a National Cybersecurity Strategy

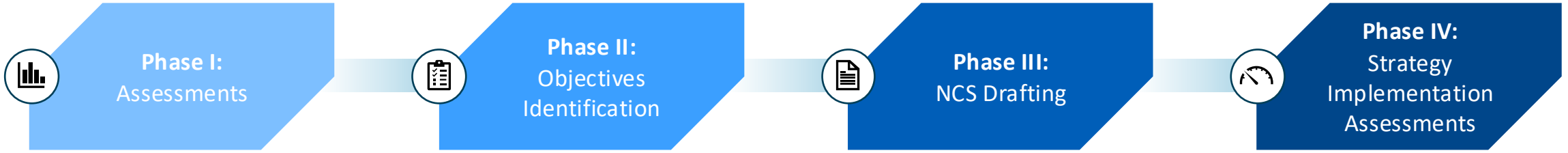
A community-based developed guide for countries and organizations

- 3rd Edition (dec.2025) developed by more than 37 contributors from international organizations, the private sector, academia, and civil society.
- Expert-recommended principles for national cybersecurity strategies
- Inspires strategic thinking and support global leaders in cybersecurity strategy

https://ncsguide.org/



ITU's Methodology: National Cybersecurity Strategy (NCS) and Action Plan Development



Assessments (GCI, CMM, NCRA) and **documentation review**, including digital development strategies

Identification of **cybersecurity objectives** of the country based on **country assessment** and **validation workshops**

Facilitate the drafting process of the **NCS**, including support with the drafting of the **NCS Action Plan** and validation workshops

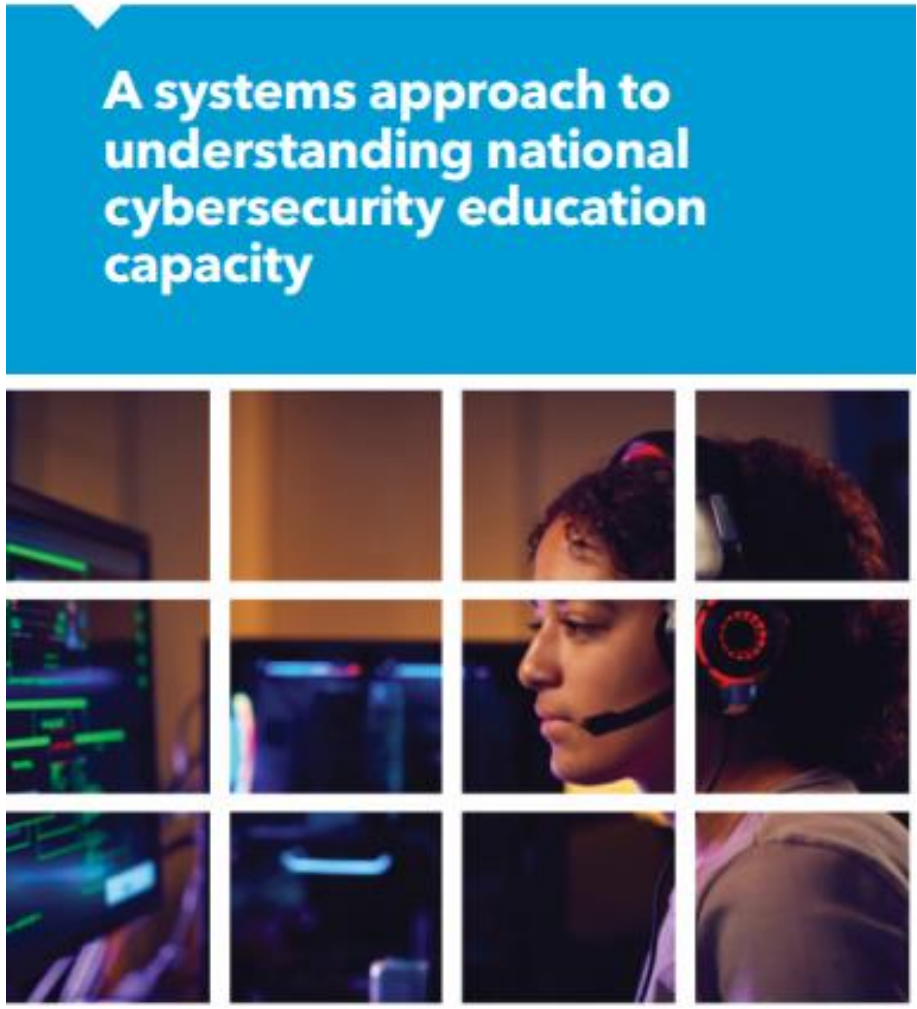
Strategy Implementation and monitoring and evaluation of the **Action Plan implementation** (country's responsibility)

GCI – Global Cybersecurity Index
CMM - Capacity Maturity Model Assessment
NCRA – National Cyber Risk Assessment
NCS – National Cybersecurity Strategy

Skills Development

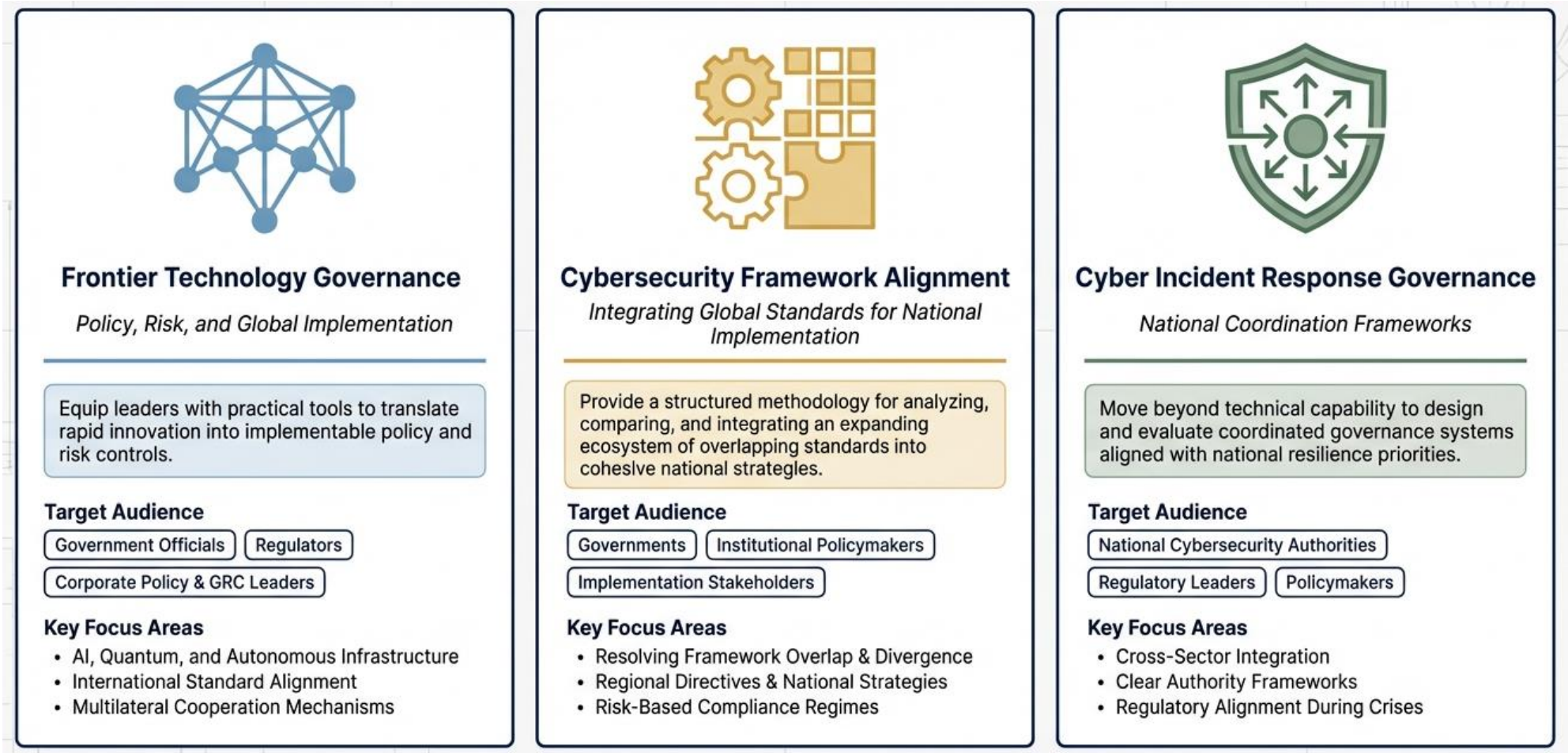
Skills Development: Research and Insights

- Analysis and insights in the full cybersecurity education ecosystem—policies, institutions, programs, and skills pipelines—to understand strengths, gaps, and opportunities for sustainable development.
- Stakeholder engagement and collaboration for sustainable workforce development strategies. Our research and partnerships focus on designing adaptable, long-term approaches that strengthen national cybersecurity education capacity and support the continuous evolution of the workforce.



Skills Development: Self-paced Cybersecurity training (coming soon)

ITU is developing a new portfolio of free cybersecurity policy and governance training for policy makers, national cybersecurity authorities, regulators available on the ITU Academy as self-paced courses



Skills Development: Her CyberTracks

A Cybersecurity Capacity Building program for Women funded by Germany FFO, the EU Commission, and Italy's MAECI, co-implemented with GIZ in Africa, the Americas, Asia Pacific, Eastern Europe and the Balkans

6-month blended training including online self-paced and live instructor courses, 1 week in person regional training, personalized mentoring and networking sessions

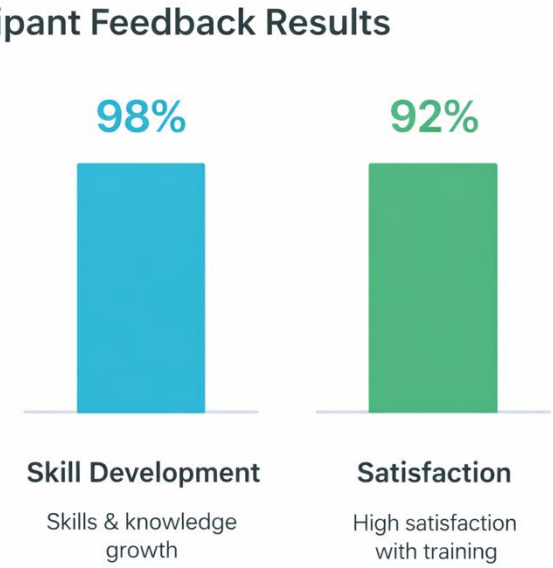
	Policy & Diplomacy CyberTrack	Incident Response CyberTrack	Criminal Justice CyberTrack	Cyber & AI CyberTrack
Content	Concepts and processes on national and international cybersecurity policy & diplomacy	Basic incident response skills, use of entry-level tools and techniques. AI-enhanced incident management and its risks	Frameworks and tools to contribute to cybercrime investigations and prosecution. Human rights. AI and ethical digital investigations	Risks and opportunities of AI in cyber, Policy and regulation related to AI and Cyber, AI cybersecurity readiness, international cooperation on cyber and AI issues
Target Group	Policymakers, technical profiles	Technical experts (CERT/SOC, systems administrators)	Law enforcement, prosecutors	Policymakers, technical profiles

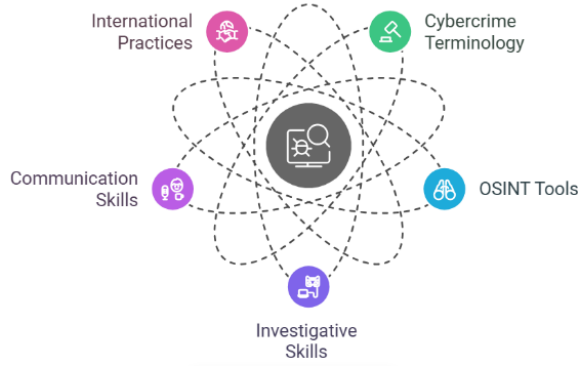
Her CyberTracks: a global program

2026 target countries:
ITU Member States of **Africa region**: Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Congo, Côte d'Ivoire, Dem. Rep. of the Congo, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, South Africa, South Sudan, Tanzania, Togo, Uganda, Zambia, Zimbabwe
ITU Member States of **Americas region**: Antigua and Barbuda, Bahamas, Barbados, Belize, Bolivia, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Honduras, Jamaica, Mexico, Panama, Paraguay, Peru, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, Uruguay
ITU Member States of **Arab region**: Algeria, Comoros, Djibouti, Egypt, Libya, Mauritania, Morocco, Somalia, Sudan, Tunisia
ITU Member States of **Asia and the Pacific region**: Bangladesh, Bhutan, Cambodia, Fiji, Indonesia, Kiribati, Lao P.D.R., Maldives, Marshall Islands, Micronesia, Nepal, Papua New Guinea, Philippines, Samoa, Solomon Islands, Thailand, Timor-Leste, Tonga, Tuvalu, Vanuatu, Vietnam
ITU Member States of **CIS region**: Armenia
ITU Member States of **Europe region**: Albania, Bosnia and Herzegovina, Moldova, Montenegro, Republic of North Macedonia, Serbia, Ukraine

Her CyberTracks: Outcomes & Impact

- **> 550 participants**
- **Increased expertise** on cybersecurity policy and diplomacy, incident management skills and cybercrime investigations and prosecution
- **Long term impact:** Regional & cross-regional professional network; strengthened information-sharing and increased cyber resilience within and across regions ; Career acceleration for mentees; Increased professional confidence
- **Key skills developed**:





Digital Safety and Protection

Child Online Protection

Activities and Output

- Development and implementation of global recommendations on Child Online Protection, Online Safety and Children's Rights online
- Development of National Child Online Protection Frameworks
- Capacity building for policy-makers, ICT Industry, educators, carers
- Development of educational tools on online safety for children (app, game, trainings)
- Child Consultations and Participation
- Awareness raising on Child Online Protection in Sports
- Coordination of Global Collaborations
- Provision of a Platform for intersectoral Dialogue and Knowledge Sharing (CWG COP, *Industry Connect* event series)

Child Online Protection Capacity Building

Academic and non-academic staff

Parents and carers

ITU and UNICEF
ICT industry

Policy-makers

Learning Objectives

- Understand children's behaviour online
- Identify online risks and harm to children
- Know how to appropriately respond to and report harm online
- Develop a multi-stakeholder coordinated national child online protection strategy
- Deep-dive into online child sexual exploitation and abuse (CSAM)
- Advocate for and support children's rights in the digital environment

Capacity Building for children

with children: co-creation with the ITU Child Online Protection child advisory board

Self-paced trainings: Online Safety for Children

E-learning for children aged 9 to 18: www.itu.int/COP/Training

The Game and App - *Complementing skills development: learn through play*

Web Game - Ages 9 to 12

Sango's adventures: Discover online safety

Web Application co-created with UNICEF

Ages 13 to 17

AskMe: Your online safety friend

ITU's Child Online Protection – Intersectoral Collaboration

Child Online Protection in, through and around sports.

ITU Policy Brief on Child online protection in sports

Testimonials: ITU/SCORT partnership impact video

Help children live in a world free from violence through ICTs - Protection through online Participation

Research & Data collection: Understand how children use the internet to access protection

Report: Global Principles for policymakers, ICT industry, and helplines

Good practices: Evidence on different types of systems to be made accessible

Provide Recommendations and a common understanding on Child Rights in the context of AI

Joint Statement: Convene UN and regional organizations to co-sign a joint statement on child rights and AI + 30+ contributors from CSOs and ICT Industry

Event: Launching event in Q4 2025

With the contributions of:

Proof point 3

Building inclusive and trusted future digital societies

Since 2022, ITU's COP efforts have had global reach

2500+
Parents and Educators participated in trainings

170,000
Children were reached through COP activities

26
countries that translated COP guidelines into national (non-UN) languages

50+
partners engaged in the COP ecosystem

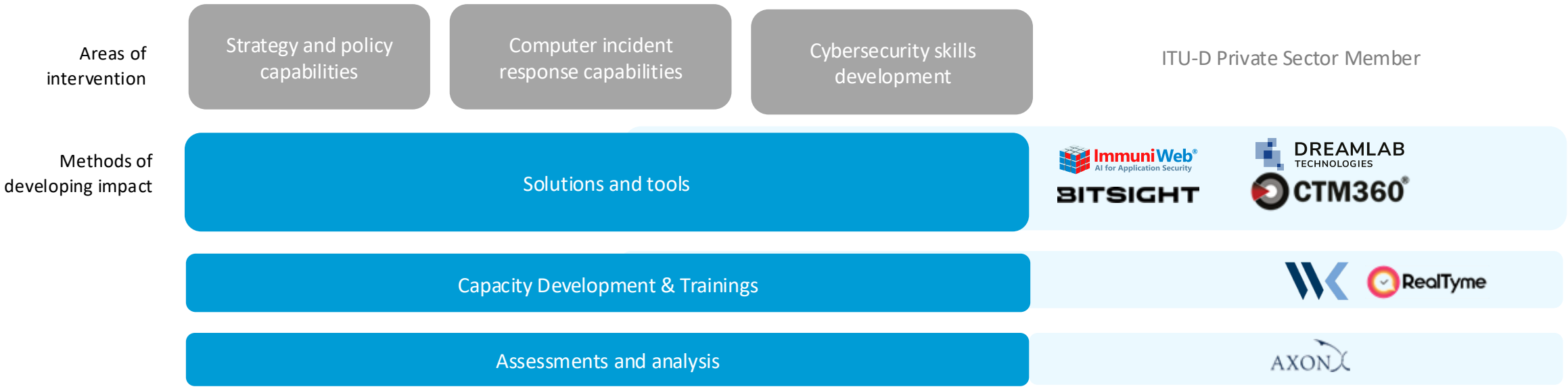
1000+
government stakeholders participated in train the trainer activities

35+
beneficiary countries

10
Self-paced trainings

Partnerships, Collaboration and Projects

With ITU-D Private Sector Members, Cyber for Good Project reduces cyber capacity gaps for LDC's and SIDS'



Cyber for Good supports Partner2Connect Focus Area 1, Pillar 3

Founding contributors: Republic of Korea and ITU

Cyber for Good Project: Scaling delivery through partnerships

34 of 45 LDCs

supported through Cyber for Good

+6 SIDS – are currently being supported

9 members

contributing through ITU-D partnership channels

$4.35M

in in-kind support over 3 years

What this model does well

- Reduces barriers for LDCs and SIDS to access expertise, tools, and training.
- Uses structured cooperation rather than ad hoc sponsorship.
- Shows how public-interest objectives can be scaled through practical burden-sharing.

For us partnerships are not the message. They are the scaling mechanism.

ITU

itu.int/cyb

cybersecurity@itu.int