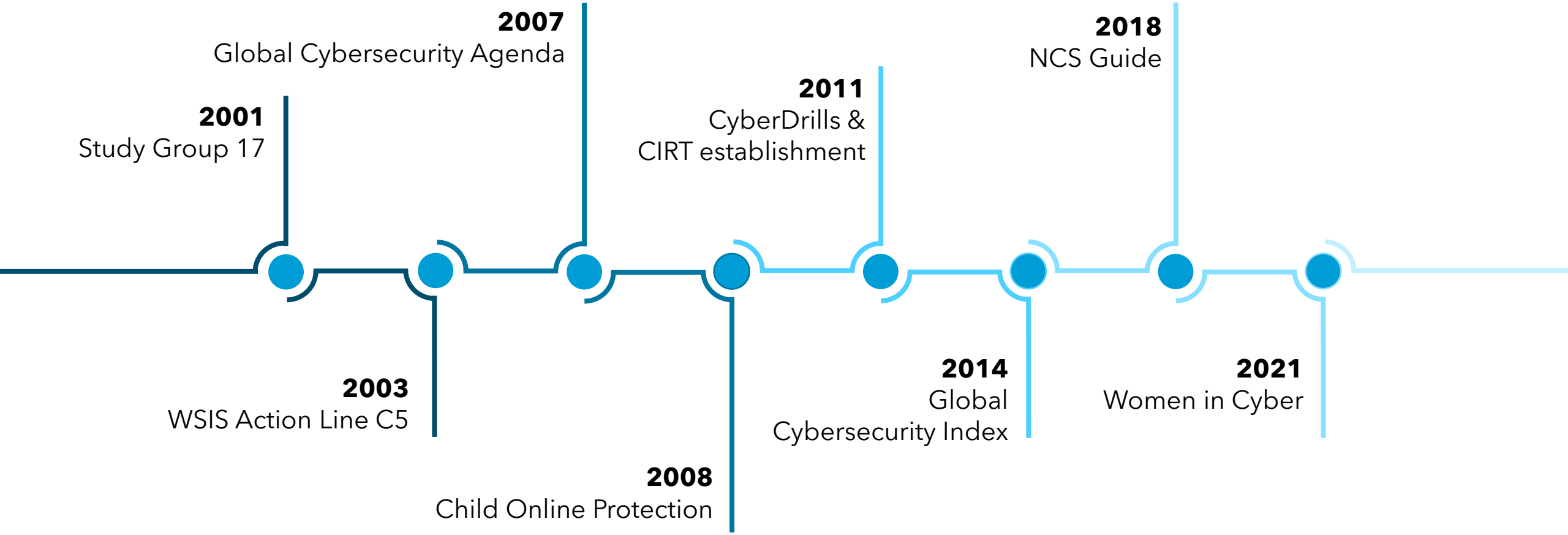
ITU efforts in developing cybersecurity capacity

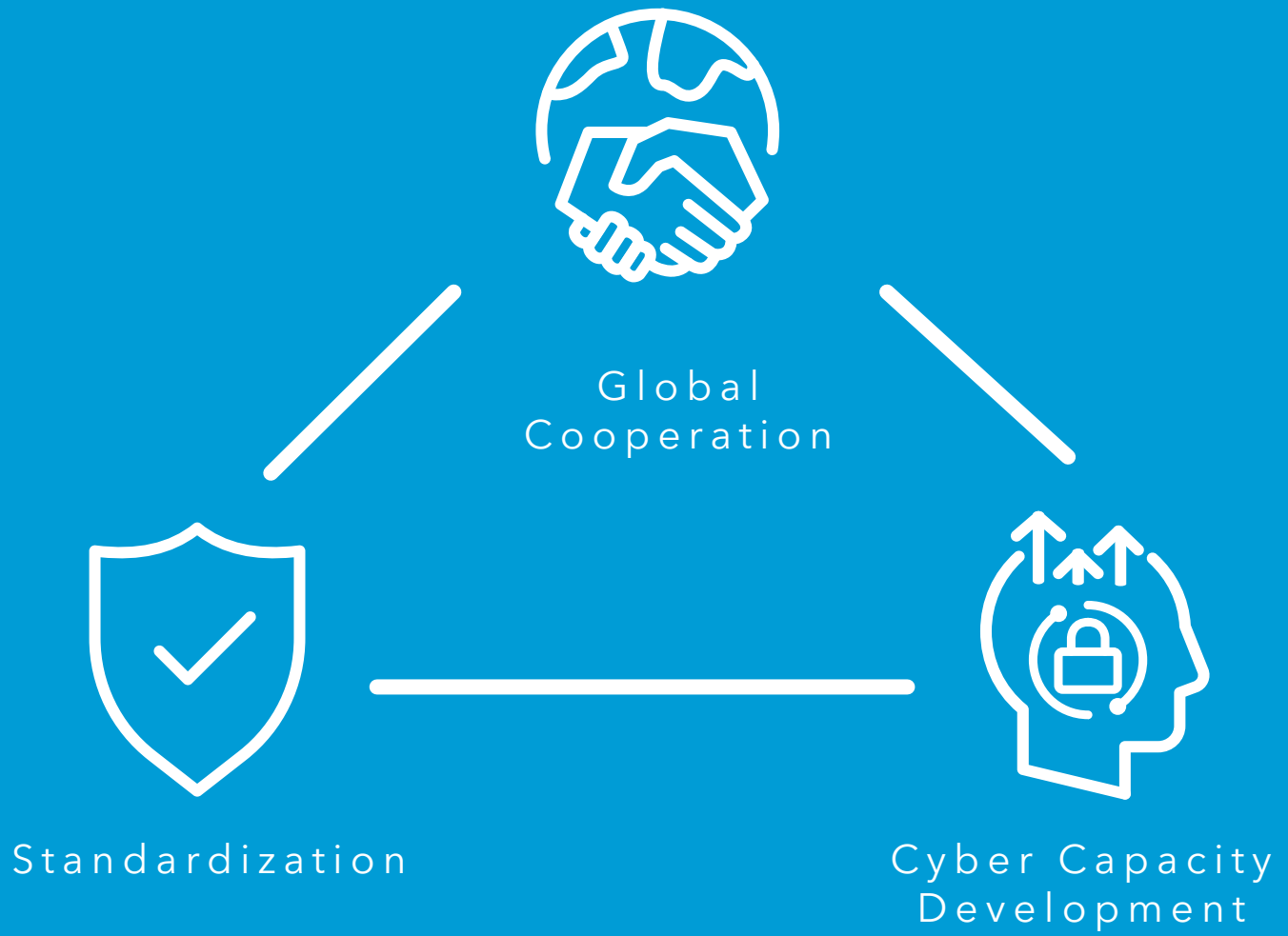
cybersecurity@itu.int

May 2023

ITU and Cybersecurity: a Timeline



ITU's Role in Cybersecurity



ITU Plenipotentiary Conference (PP):

Resolution 130 (Rev. Dubai 2018
Resolution 174 (Busan 2014)
Resolution 179 (Rev. Dubai 2018)

ITU World Telecommunication Development Conference (WTDC):

Resolution 45 (Dubai 2014)
Resolution 67 (Buenos Aires 2017)
Resolution 69 (Buenos Aires 2017)

ITU World Telecommunication Standardization Assembly (WTSA):

Resolution 50 (Rev. Geneva, 2022)
Resolution 52 (Hammamet 2016)
Resolution 58 (Rev. Geneva, 2022)

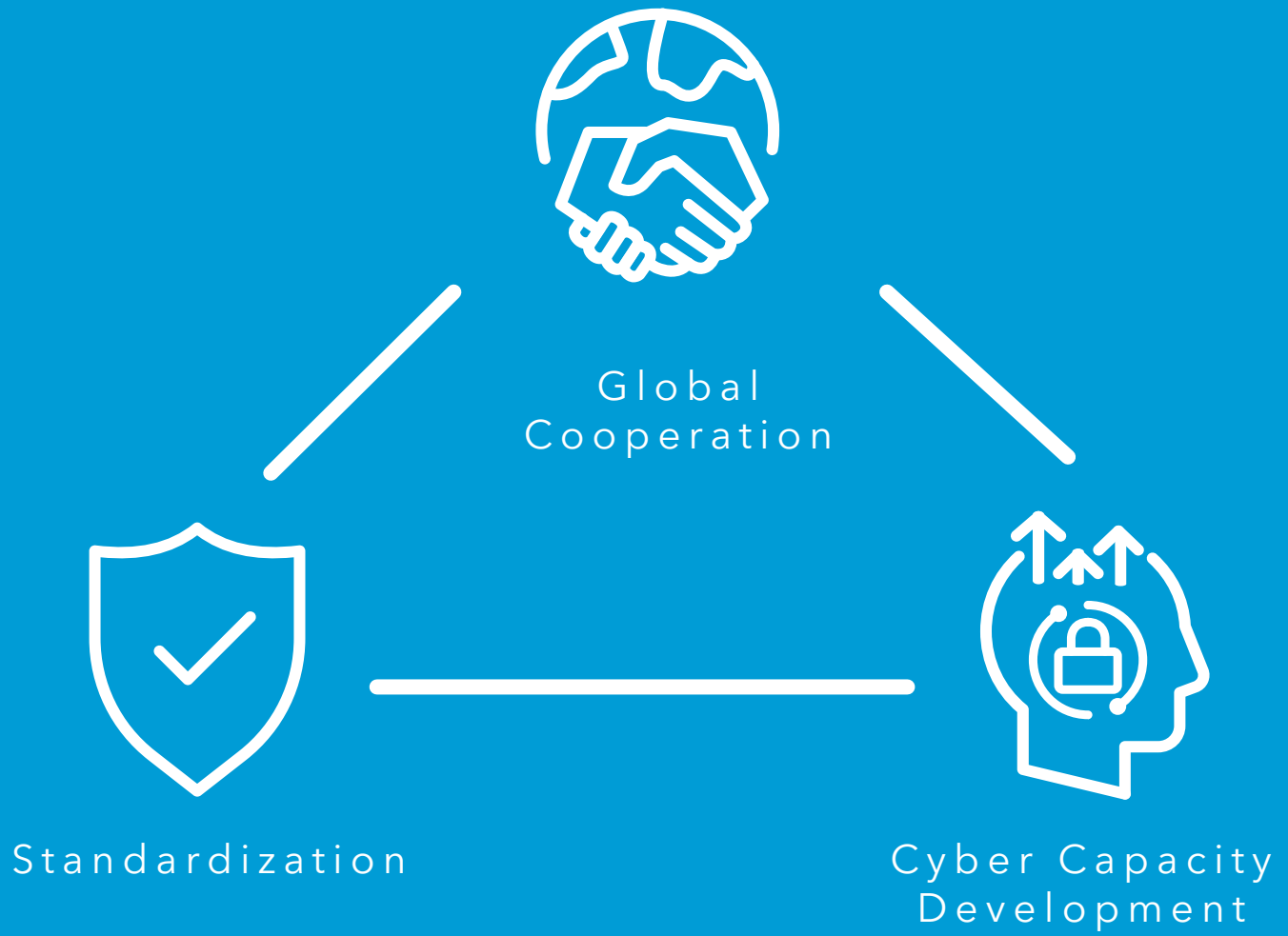
Related Study Group :

ITU-D STUDY GROUP 2 (2018 - 2021): Question 3/2:

Kigali Action Plan 4.5
Implementation of Inclusive and secure telecommunications/ICTs for sustainable development priority outcomes

- Increased digital literacy and public awareness of cybersecurity issues
- Stronger consumer protection in Member States
- Increased access for all to training programmes in digital skills
- Support for Member States to develop National Cybersecurity Strategies and Computer Incident Response Teams
- Enhanced capacity of telecommunication/ICT professionals to support the digital economy and strengthened digital skills
- Increased secured online services, including Child Online Protection, and mobilization of resources for marginalized groups and persons with specific needs
- Mobilizing investment in secure and resilient telecommunication/ICT infrastructure, particularly in underserved areas
- Utilize the ITU's unique partnerships to adequately resource and support capacity building and cybersecurity activities

ITU's Role in Cybersecurity



ITU's role in promoting global cooperation

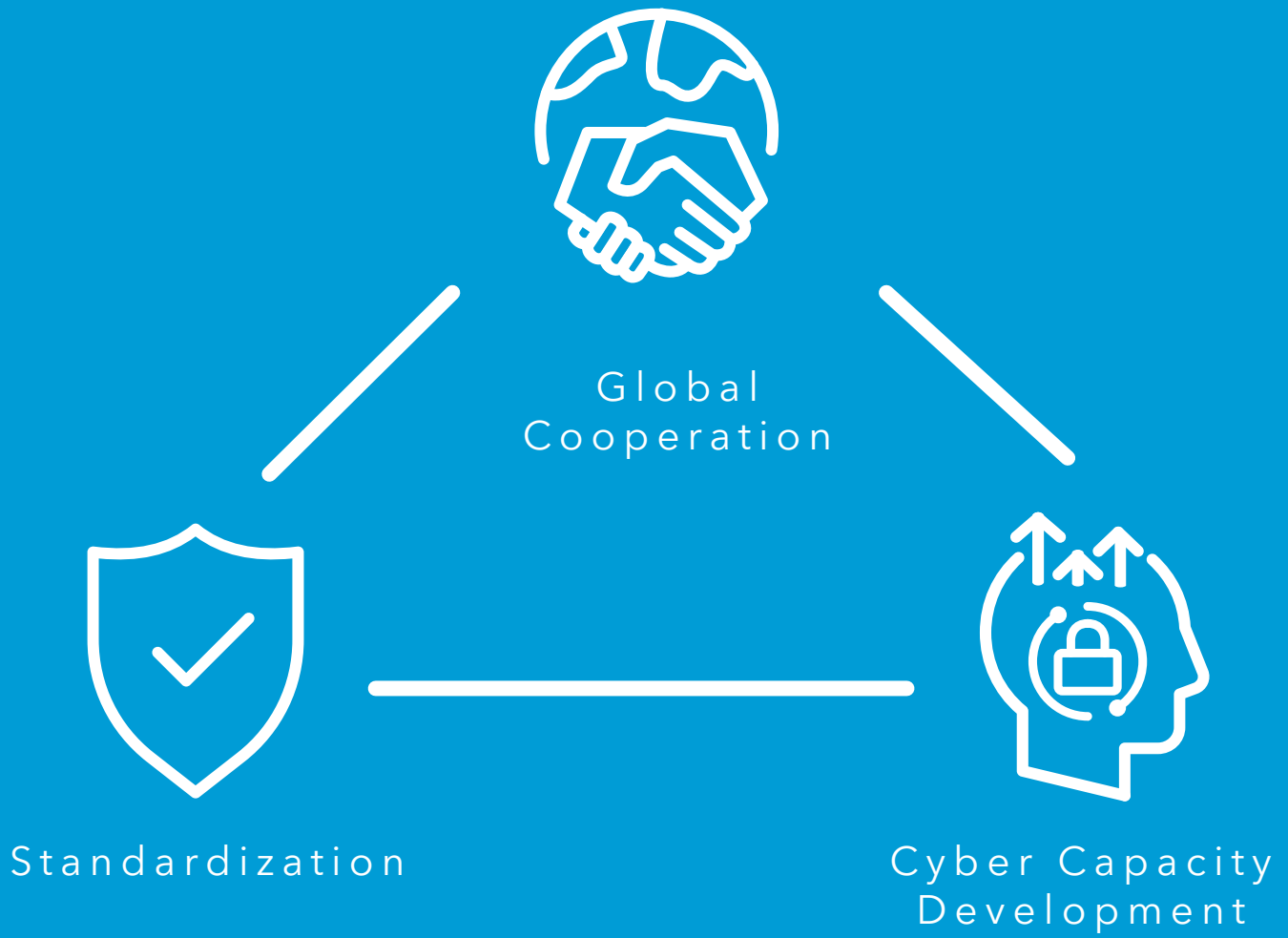
2007

Global Cybersecurity Agenda (GCA) was launched by ITU Secretary General

GCA is a framework for international cooperation in cybersecurity

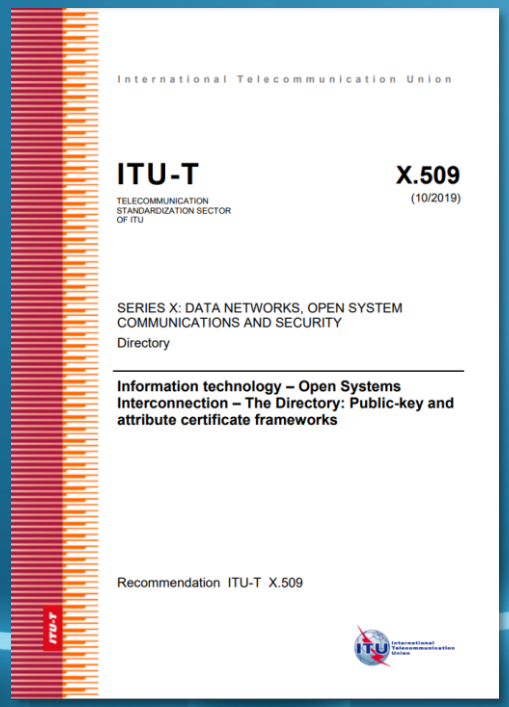
Inter-UN Processes	NGOs	Private Sector	Regional Organisations	Academia

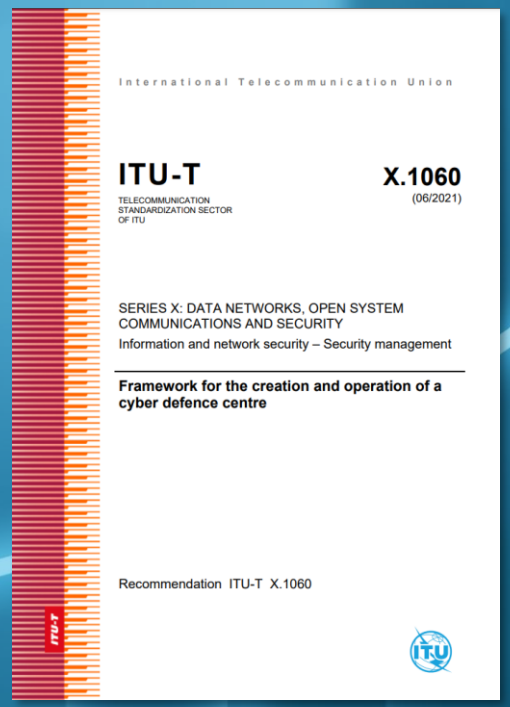
ITU's Role in Cybersecurity

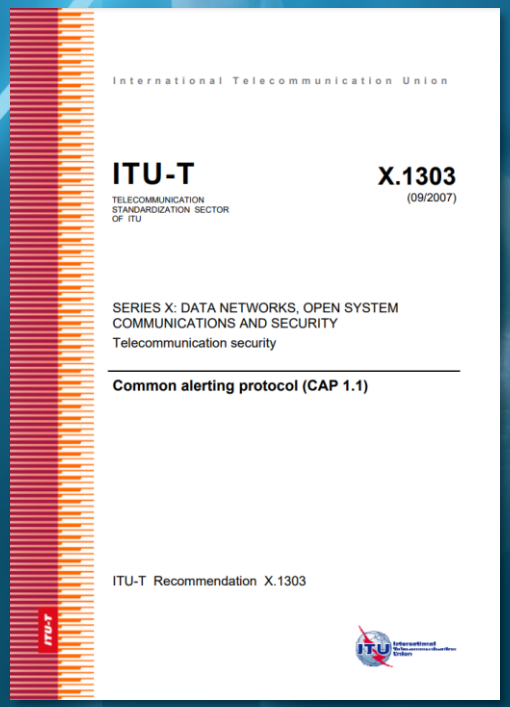


ITU's role in developing international standards and recommendations

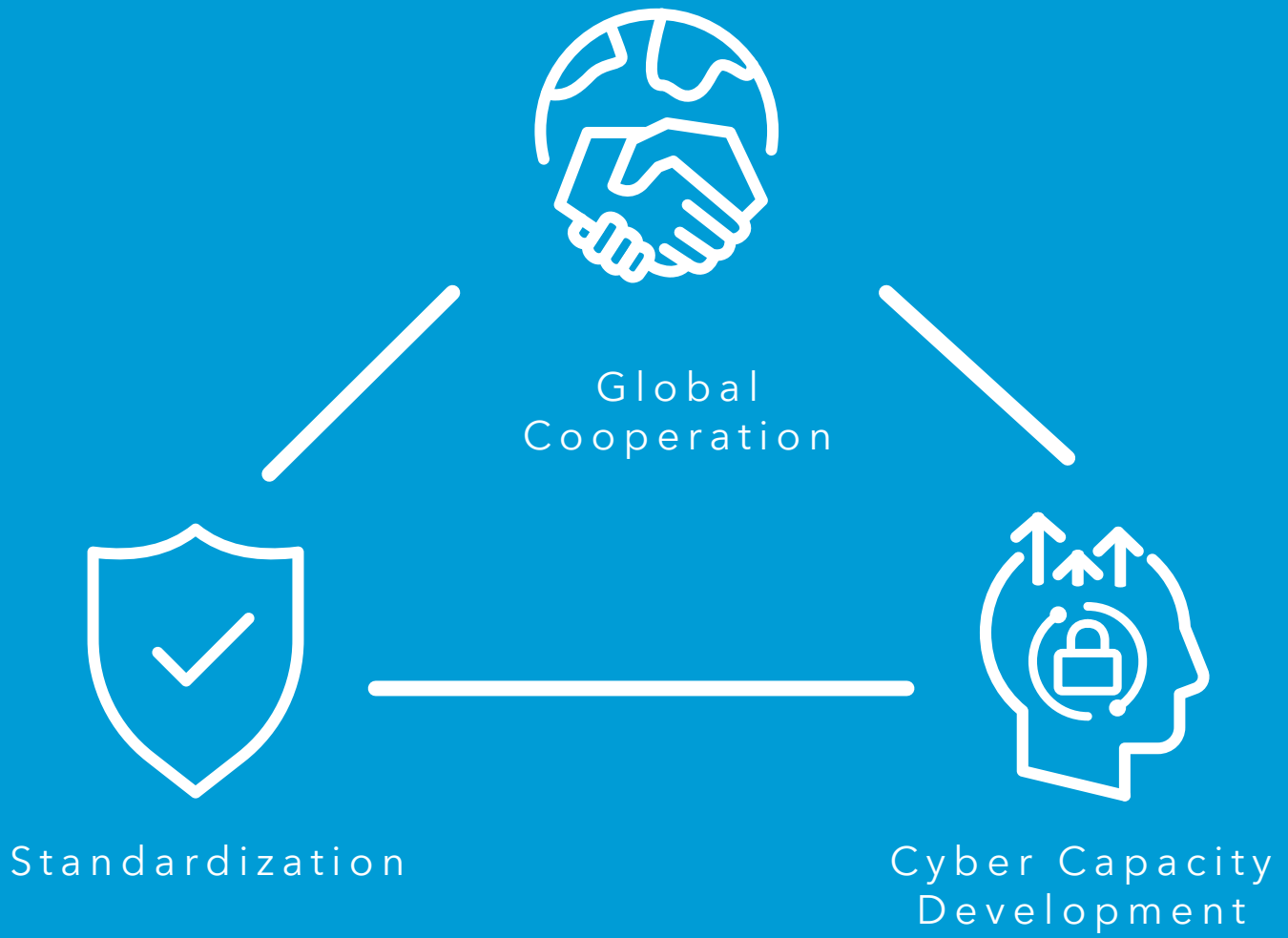
230+ ITU-T X-series Recommendations on ICT security







ITU's Role in Cybersecurity



ITU Cybersecurity Development aims to provide

Areas of intervention	Incident Response	Cybersecurity Strategy	Cybersecurity Inclusion	Data and Advocacy
Methods of developing impact	CIRTs	NCS & Action Plans	Child Online Protection	GCI
	CyberDrills	Assessments	Women in Cyber	Partnerships
	Training	Advisory	Youth for Cyber	Reports

Partnerships (Cyber for Good)

ITU's role in providing capacity building and technical assistance

Areas of intervention

- Incident Response
- Cybersecurity Strategy
- Cybersecurity Inclusion
- Data and Advocacy

Means of developing impact (Products and Services)

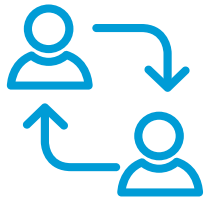
- Solutions and tools (Frameworks, Guidelines and Data)
- Project Implementations Through Partnerships (i.e Cyber for Good, National CIRTs, etc.)
- Capacity Development (training, mentoring, fellowships, content development, on-the-job training)
- Establish networks of practice and support
- Training, TTXs & Workshops

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

Governments

Private Sector

Regional organizations



Civil Society

ITU Regional Presence

Annex

National CIRT establishment & enhancement

Mandate

PP Res 130 *(Rev. Bucharest, 2022)*

- continue identifying best practices **(…) establishing CIRTs**, and promoting the related operating framework of CIRTs to review the reference guide for the Member States… the use of ICTs, including the establishment of CIRTs
- to collaborate with relevant organizations, through the **exchange of best practices** in building confidence and security in the use of ICTs, including the establishment, development and implementation of national CIRTs, especially in developing countries;
- to encourage their national **CIRTs to collaborate with other national and subnational governmental agencies** as appropriate, and other CIRTs and stakeholders

WTDC Res 69 *(Rev. Kigali, 2022)*

- to establish national CIRTs, including CIRTs responsible for government-to government cooperation (…)
- to facilitate exchanging **best practices** among their national CIRTs;
- to encourage the use of **emerging telecommunications/ICTs to enhance technical capabilities of CIRTs**;

WTSA Res 58 (Rev. Geneva, 2022)

Activities

- National CIRT Assessments: Defines the readiness to implement a national CIRT
- CIRT establishment: after the CIRT assessment, we assist with planning, implementation, and operation of the CIRT
- ITU's continued collaboration with the newly established CIRT ensures that support remains available, and institutions can be further enhanced

Impact:

- 85 CIRT assessments completed
- 23 CIRTs established
- 6 CIRTs enhanced

CyberDrills: information sharing & hands-on capacity building

Mandate

PP Res 130 *(Rev. Bucharest, 2022)*

- to invite all countries to take part in these activities, such as **cyberdrills**, among others

WTDC Res 69 *(Rev. Kigali, 2022)*

- providing CIRTs with **capacity development**, particularly in areas of new and emerging telecommunications/ICTs, through the ITU regional and area offices, taking into account the financial resources;
- preparing the **training programmes** necessary for this purpose and continuing to provide support as required to those developing countries that so wish;

Activities

- Hands-on exercises for national CIRTs
- Platform for cooperation and information sharing on good practices and current cybersecurity issues
- Production of "CyberDrill Framework"

Impact

- Over 36 regional and global CyberDrills since 2012
- Over 120 countries involved

Upcoming CyberDrills:

- Africa Regional CyberDrill(May 2023, Malawi)
- America Regional CyberDrill (June 2023, Dominican Republic)
- South America CyberDrill (Sept 2023, Chile)
- Arab and CIS inter-regional CyberDrill (Oct 2023, UAE)
- EU and ASP interregional CyberDrill (Oct 2023, TBD)
- Global CyberDrill (Nov 2023)

National Cybersecurity Strategies: development support

Mandate

PP Resolution 130 *(rev. Bucharest)*

- *to support development of* ***national and/or regional cybersecurity strategies*** *towards building national capabilities for protecting against and dealing with cyberthreats in accordance with the principles of international cooperation*
- *to support ITU initiatives on cybersecurity, including the GCI, and the Global Network Resiliency Platform, in order to* ***promote national strategies and the sharing of information*** *on efforts across industries and sectors;*

Activities:

- National Cybersecurity assessments
- Facilitation of NCS Development and Implementation
- Trainings and Human Capacity Development
- Technical Assistance

Impact:

- Convened 20+ partners to create new NCS guide
- Conducting NCS development activities
- Running table-top exercises in intervention countries

Policy support

Women in Cyber Programme

Mandate

PP Resolution 130 (rev. Bucharest)

- *to promote the growth and development of a **diverse and skilled cybersecurity workforce** that is able to address and mitigate cyber risks, and promote the importance of effective qualifications and professional career pathways;*
- *to support the membership to **address cybersecurity skills shortages** by encouraging people to enter the cybersecurity profession and **promoting the employment of women in the cybersecurity field**;*
- *to maintain, develop and promote a repository of best practice on measures that facilitate and **encourage people to choose a career in cybersecurity**.*

Activities

- Trainings (technical and soft skills)
- Guided mentorship & role modeling

Impact:

- 73 countries from the Global South
- 2 editions
- 300+ mentees, 100+ mentors
- 95% of mentees have reported an improved awareness of the different career paths in cybersecurity thanks to the WiC programme.
- 97% of mentees have reported increased confidence being a woman in cybersecurity

Her CyberTracks

- *Her CyberTracks* : align, improve, develop, and scale existing offerings for cyber capacity building
- A complementary and one-stop holistic curriculum that integrates capacity building, mentoring, employment opportunities, and networking.
- 2023: Launch of the Policy & Diplomacy Track to promote women's representation and participation in international cybersecurity processes and organizations.

Three action areas :

- Build the required capacity for women to contribute to a secure and resilient cyberspace
- Inspire the next generation of women leaders in cybersecurity through role models & networking
- Empower women to pursue new pathways and actively shape cyber policies and norms

Global Cybersecurity Index

Mandate

PP Res 130 (Rev. Bucharest, 2022)

- to consider the results of the GCI to guide ITU cybersecurity-related initiatives, especially taking into account the gaps identified through the GCI process
- to engage in the improvement of the GCI process, including the discussion on the methodology, structure, weightage and questions, using the GCI expert group

WTDC Res 45 (Rev. Kigali 2022)

- to consider the results of the Global Cybersecurity Index (GCI) to guide BDT cybersecurity-related initiatives, especially taking into account the gaps identified through the GCI process

Activities

- Produces the only global measure of state-level cybersecurity activities
- 4 editions since 2015
- Provide individual, deep dive country reports
- Next period of data collection underway

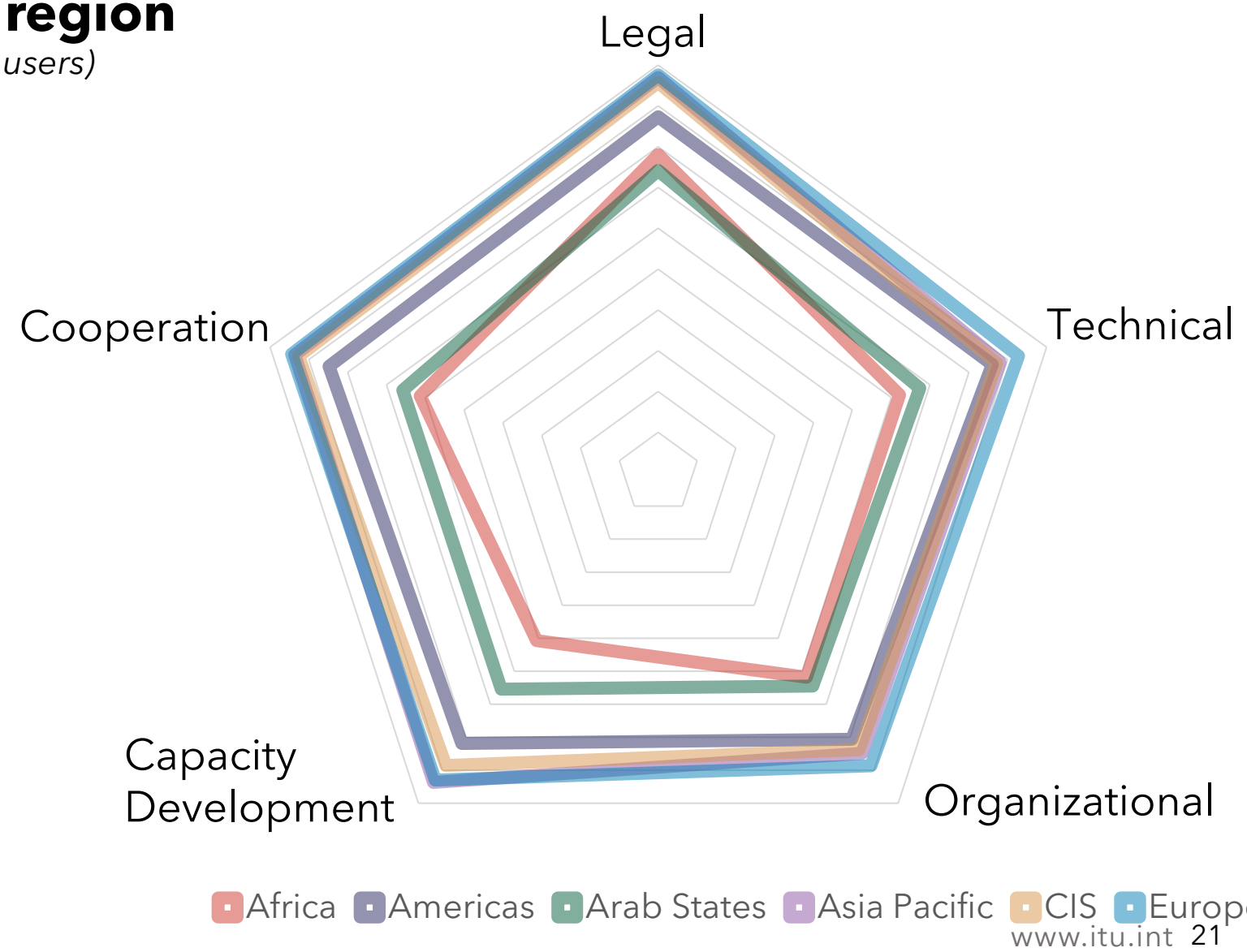
Impact

- Measures and guides ITU activities around cybersecurity
- Used by governments to drive cybersecurity improvements
- Over 140 participants in Expert Group
- Cited in over 2,100 scholarly articles

Average performance by region

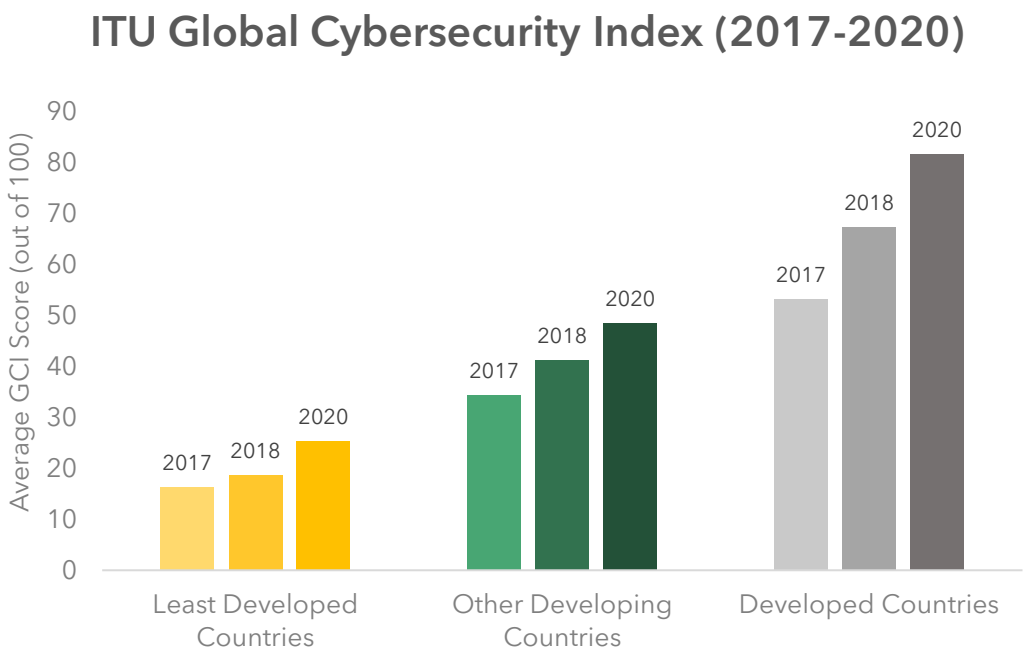
(weighted average, by number of internet users)

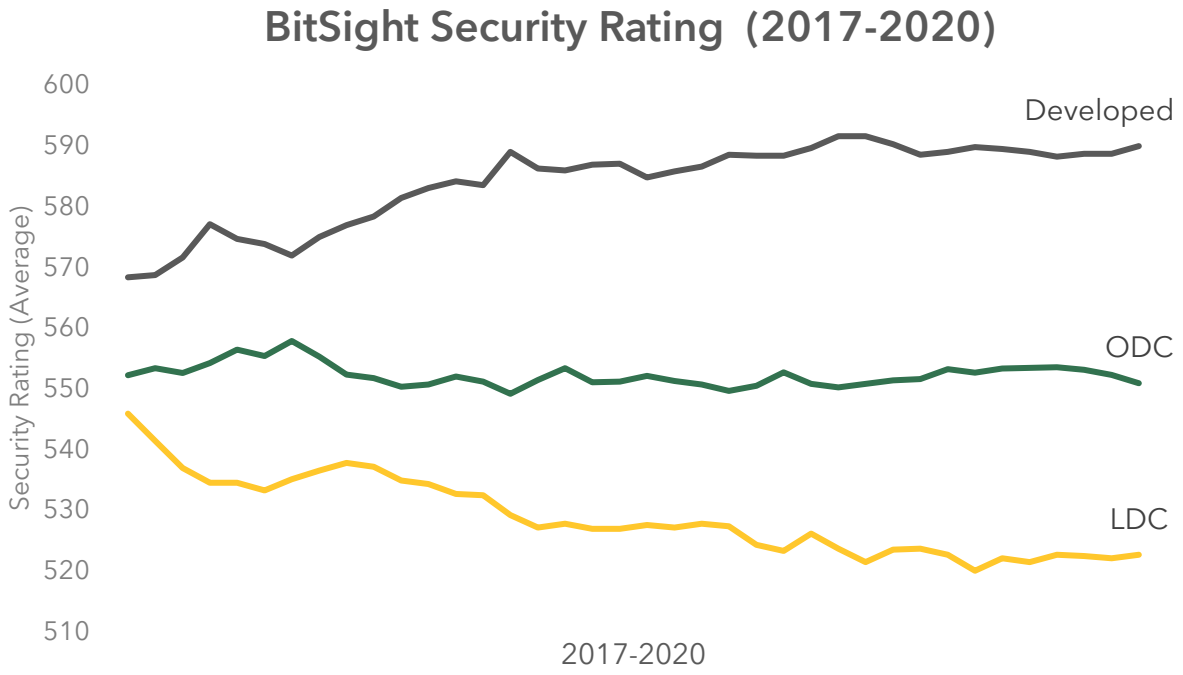
- Every region has a country which has commitments to GCI cybersecurity measures
- The right mix of Legal, Technical, Organizational, Capacity Development, and Cooperation measures depends on countries' priorities and strengths
- Overcoming challenges requires government, private sector actors, civil society, and academia working together



Cybercapacity gaps persist, with developing countries underperform in cybersecurity, and are not catching up

Not all are ready to receive support, and need foundational trainings
Other countries need access to advanced tools, services, and trainings to build their digital ecosystems





Sources: BitSight, 2017-2020, UN Population Program, ITU ICT Indicators

Note: ODC (Other Developing Countries)

Cyber for Good

Mandate

PP Res 130 (Rev. Bucharest, 2022)
WTDC Res 45 (Rev. Kigali 2022)

Activities

- Connecting LDCs with ITU-D cybersecurity Private Sector Members
- Focus on low barrier-to-entry and exit trainings, services, and tools

Impact

- 16 LDCs working with 3 different companies to improve their cybersecurity posture
- Working with 5 ITU-D Sectors

ITU

itu.int/cybersecurity

cybersecurity@itu.int