

Cybersecurity Regulation in Practice

Institutional mandates, collaboration and
operator obligations

Evidence from the ITU World Telecommunication/ICT Regulatory
Survey, G5 Benchmark and Global Cybersecurity Index

ITU-D Study Group 2 workshop | 12 October 2026

Regulatory and Market Environment Division



Telecom networks are critical infrastructure under sustained attack

4×

rise in ransomware attacks on telecom operators worldwide, 2022–2025
24 → 90 incidents a year

444

data-theft incidents against telecom and ISP operators in 2025
133 stolen databases listed on the dark web

~70%

of 2025 telecom ransomware attacks were concentrated in the Americas
Europe and Asia-Pacific followed

"As digital interdependence deepens faster than our ability to govern it, collaboration is no longer optional. It is the foundation of digital resilience. "

Sources: Cyble, Telecommunications Sector 2025 Threat Landscape Report (Jan 2026); ITU, UNDRR and Sciences Po, "When Digital Systems Fail" (May 2026).

Cybersecurity regulation needs clear roles and working arrangements

01



MANDATE

Who is responsible?

02



COORDINATION

How do institutions
work together?

03



OBLIGATIONS

What must operators
do?

04



SUPERVISION

Who checks compliance
and requires corrective
action?

Countries organize these functions differently. Responsibilities can be shared, provided roles and working arrangements are clear.

G5 and GCI measure different aspects of national readiness

G5 Benchmark

Collaborative digital regulation across four pillars

National collaborative governance; policy design principles; digital development; digital economy policy agenda.

G5 groups (score out of 100)

Leading	80–100
Advanced	60–<80
Transitional	30–<60
Limited	0–<30

Global Cybersecurity Index

National commitment to cybersecurity across five pillars

Legal, technical and organizational measures, capacity development and cooperation.

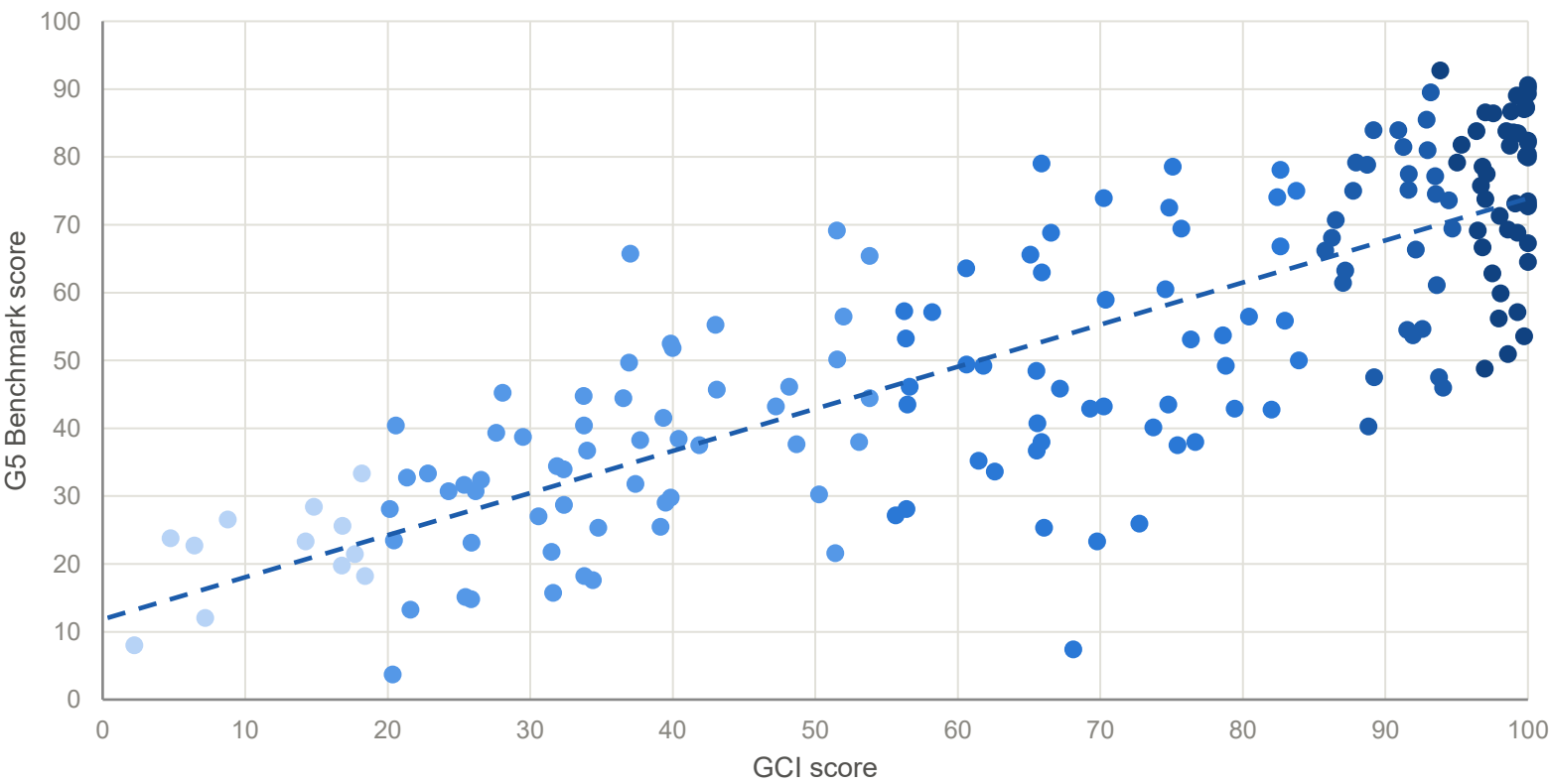
GCI tiers (score out of 100)

T1 Role-modelling	95–100
T2 Advancing	85–<95
T3 Establishing	55–<85
T4 Evolving	20–<55
T5 Building	0–<20

Sources: ITU G5 Benchmark methodology, Table 4 (pp. 13–14); GCI 2024, tier methodology (p. 133). Group boundaries differ.

Cybersecurity commitment and collaborative regulatory maturity are strongly associated

Each dot is one country. Position is its GCI score (horizontal) against its G5 Benchmark score (vertical); color deepens with GCI tier.



$r = 0.81$

GCI TIER

- T1 · Role-modelling
- T2 · Advancing
- T3 · Establishing
- T4 · Evolving
- T5 · Building

The relationship is substantial, but the indices measure different constructs and reference periods. The result identifies association, not causality.

191 countries scored in both indices. Dashed line is the linear fit ($r = 0.81$).

National structures and arrangements for collaboration

National structures

GCI 2024

161

countries have an agency responsible for national cybersecurity

139

countries have an active national computer incident response team (CIRT)

Arrangements involving the ICT regulator

G5 Benchmark 2025 · formal collaboration or the same authority

101

economies: ICT regulator and cybersecurity authority

19% increase in the recorded count since 2021

60

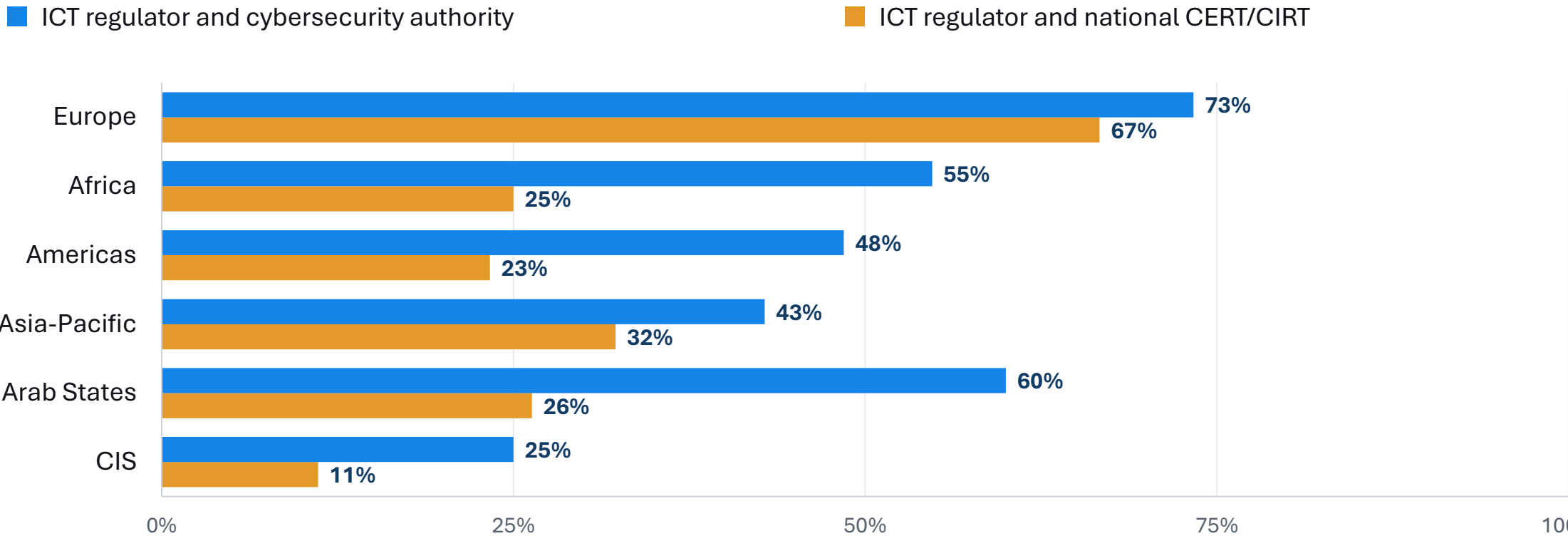
economies: ICT regulator and national CERT/CIRT

7% increase in the recorded count since 2021

Institutional presence and arrangements for cooperation are distinct measures.

Collaboration arrangements vary by relationship and region

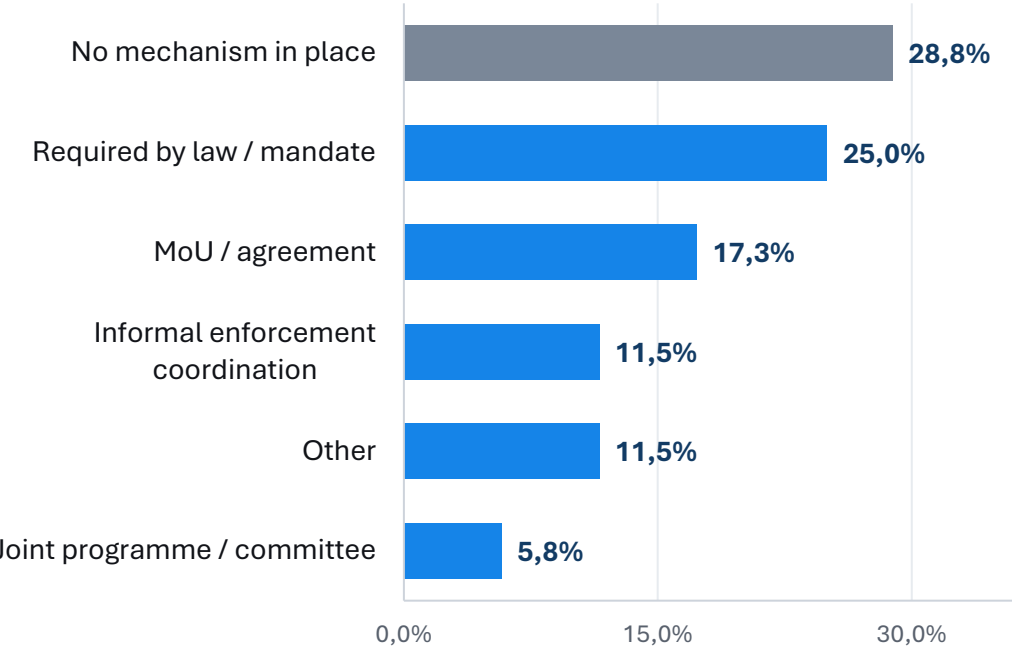
Formal collaboration or responsibilities within the same authority



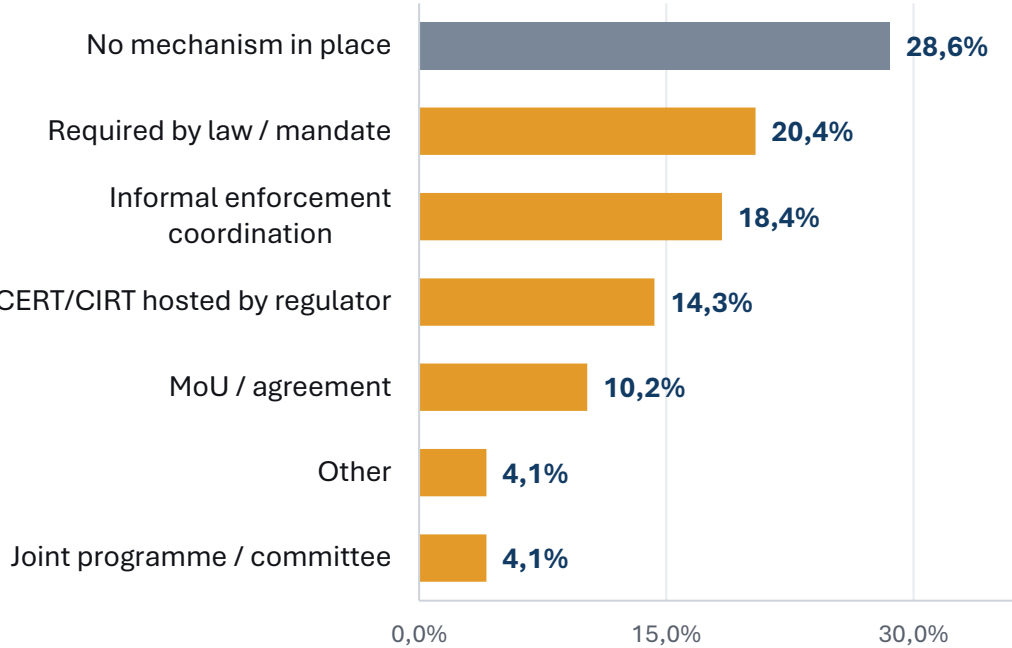
Each region records a higher share for the cybersecurity-authority relationship.

Collaboration is organized through several mechanisms

ICT regulator and cybersecurity authority



ICT regulator and national CERT/CIRT



Legal mandates and agreements provide a basis for cooperation. Some respondents report no mechanism in place.

Source: ITU Regulatory Survey 2024, two separate questions and respondent groups. All response categories are shown. These are not breakdowns of the G5 totals.

Legal coverage varies across areas of cybersecurity

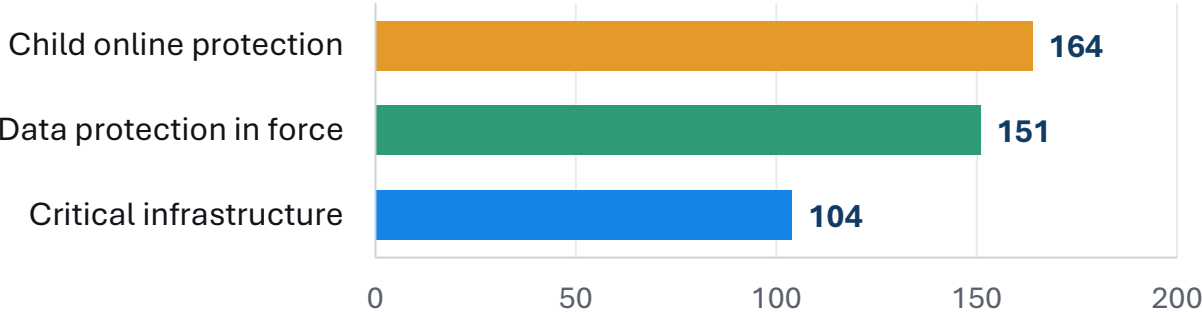
177

countries have a data-protection, privacy or breach-notification measure in force or in progress

46

regulators report online-safety and customer-security requirements for all operators and service providers

Selected legal measures in GCI 2024



National legislation sets the wider context. Sector duties still need clear notification routes and supervisory responsibilities.

Sources: GCI 2024, pp. 2 and 16 (national legal measures); ITU Regulatory Survey 2024 (46 responding regulators). Legal categories overlap and differ in scope.

Priorities for cybersecurity collaboration

- 01** | **Collaboration belongs in the cybersecurity discussion**

Higher G5 scores tend to accompany higher GCI scores. Governance deserves attention alongside cybersecurity commitments.
- 02** | **National models differ**

National agencies and CIRTs are widespread. Recorded arrangements connecting them to ICT regulators vary by relationship and region.
- 03** | **Working arrangements need to be explicit**

Clear roles, notification routes and supervisory responsibilities are practical priorities for implementation.

Institutions and operators should know who must act, what is required and how they will work together.