ITU Global Cybersecurity Index
Europe’s commitment in cybersecurity

Marco Obiso
Cybersecurity Coordinator
ITU

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 cybersecurity awareness worldwide
- Help to identify and promote best practices
- Foster a global culture of cybersecurity

134 responses in 2016– primary research

193 countries analysed - secondary research

LEGAL

- Cybercriminal Legislation
- Substantive law
- Procedural cybercriminal law
- Cybersecurity Regulation

TECHNICAL

- National CIRT
- Government CIRT
- Sectoral CIRT
- Standards for organisations
- Standardisation body

ORGANIZATIONAL

- Strategy
- Responsible agency
- Cybersecurity metrics

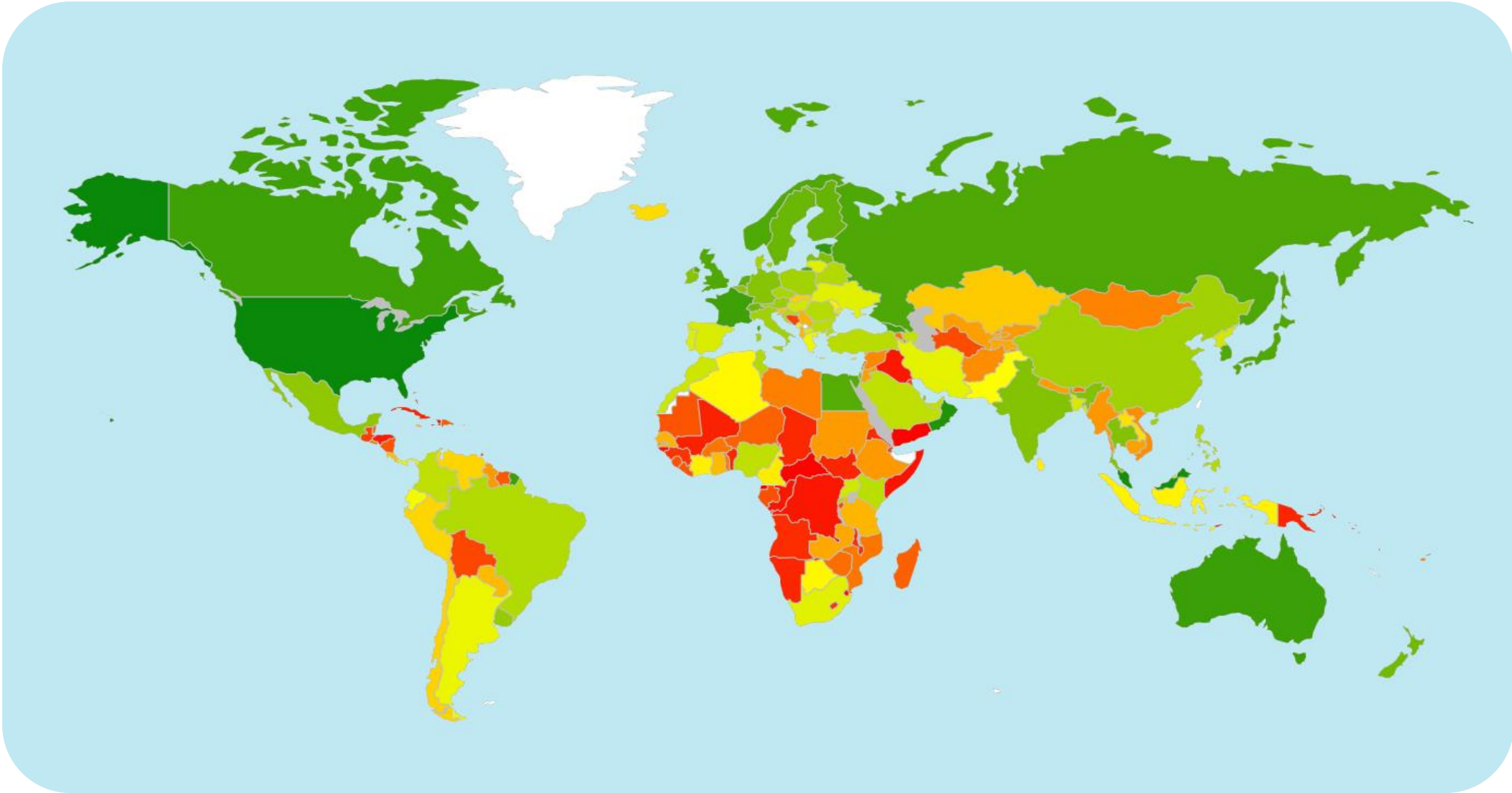
CAPACITY BUILDING

- Public awareness
- Professional training
- National education programmes
- R&D programmes
- Incentive mechanisms
- Home-grown industry

COOPERATION

- Intra-state cooperation
- Multilateral agreements
- International fora
- Public-Private partnerships

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

GCI Europe region

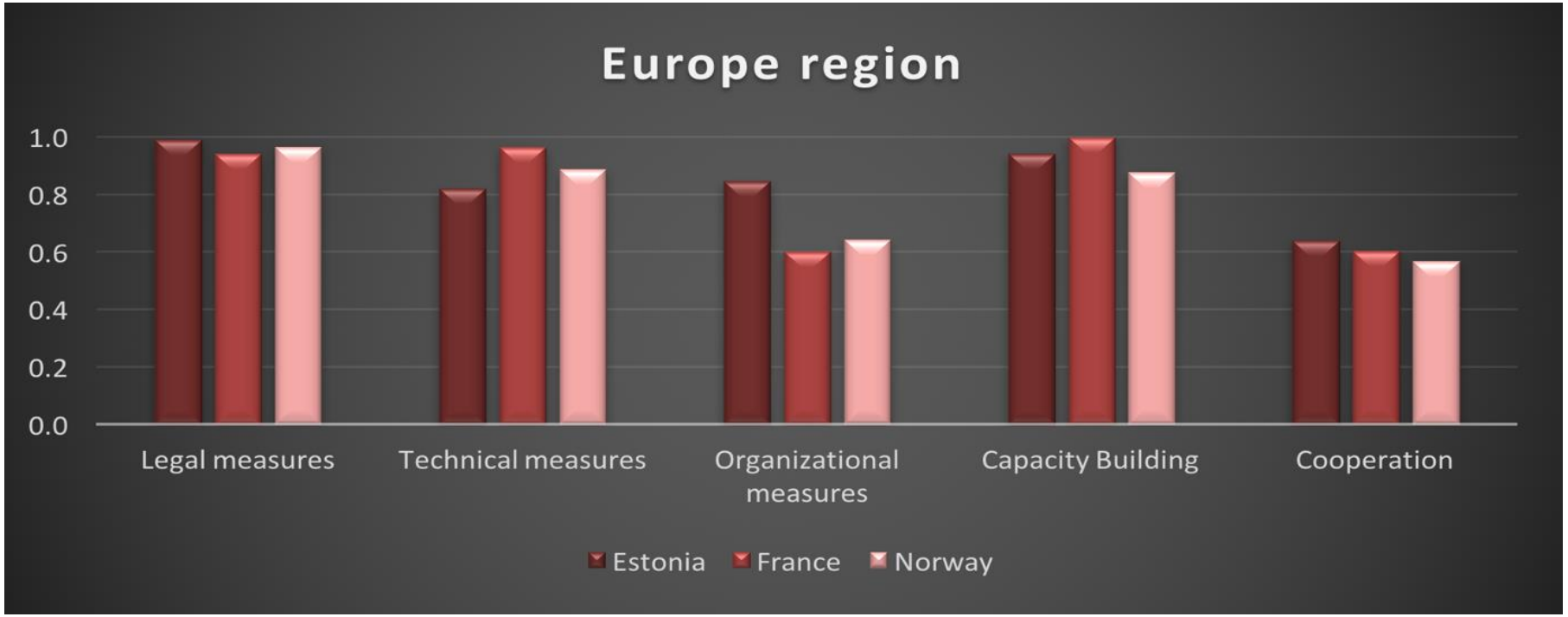
43 Countries : Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, The Former Yugoslav Republic of Macedonia, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, Vatican, United Kingdom

- Out of **43** Member States in Europe, **34** countries responded to the GCI survey in 2016 (primary research)
- **9** countries did not respond and ITU carried out research on their behalf (secondary research)

GCI TIERS FOR EUROPE REGION

Leading stage			
Estonia	0.846	Latvia	0.688
France	0.819	Germany	0.679
Norway	0.786	Ireland	0.675
United Kingdom	0.783	Belgium	0.671
Netherlands	0.760	Austria	0.639
Finland	0.741	Italy	0.626
Sweden	0.733	Poland	0.622
Switzerland	0.727	Denmark	0.617
Spain	0.718	Czech Republic	0.609
Israel	0.691	Luxembourg	0.602
Maturing stage			
Croatia	0.590	Cyprus	0.487
Romania	0.585	Greece	0.475
Turkey	0.581	Montenegro	0.422
Bulgaria	0.579	Malta	0.399
Hungary	0.534	Iceland	0.384
Macedonia	0.517	Slovakia	0.362
Portugal	0.508	Slovenia	0.343
Lithuania	0.504	Albania	0.314
		Serbia	0.311
Initiating stage			
Monaco	0.236	Bosnia and Herzegovina	0.116
Liechtenstein	0.194	Andorra	0.057
San Marino	0.174	Vatican	0.040

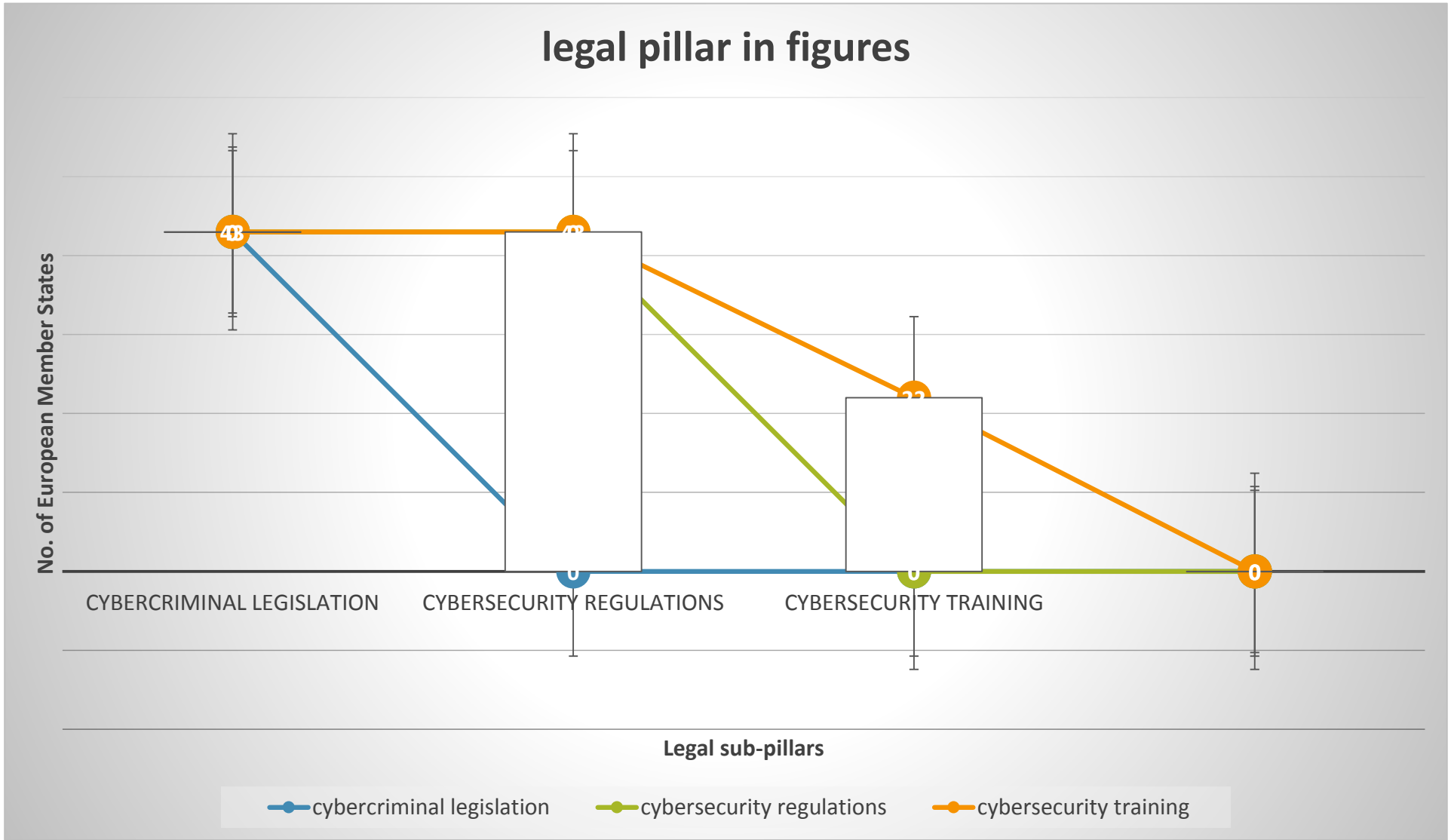
Top three ranked countries in Europe



Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
France	0.81	0.94	0.96	0.6	1	0.61
Norway	0.78	0.96	0.89	0.64	80.8	0.57

Illustrative practices

1. Legal



Illustrative practices

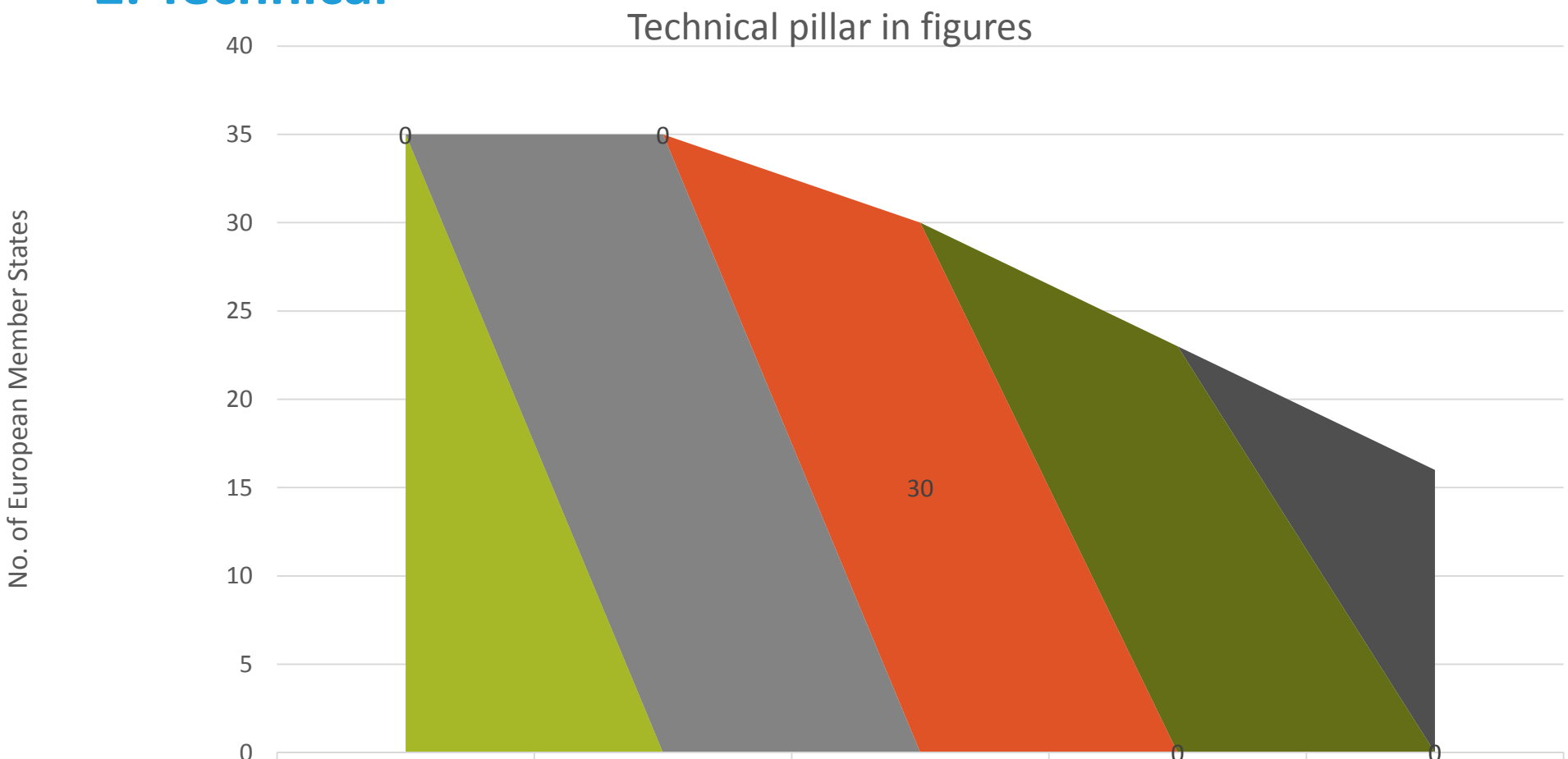
1. Legal

Hungary has trainings available for law enforcement and judiciary conducted by different organizations such as the International Law Enforcement Academy (ILEA), the Central European Police Academy (of which Hungary is a member with other Member States), and the Hungarian National Tax and Customs Administration (NTCA) .

Turkey's law requires private sector, public sector and critical infrastructure operators to implement cybersecurity measures. Legislation exists detailing the liability and the responsibility of Internet service providers, digital signature and e-transaction and finally the protection of privacy.

Illustrative practices

2. Technical



	National CIRT	Government CIRT	Sectorial CIRT	Standard framework	Standard certification
Standard Certication					16
Standard framework				23	
Sectorial CIRT			30		
Government CERT		35			
National CIRT	35		Technical sub-pillars		

Illustrative practices

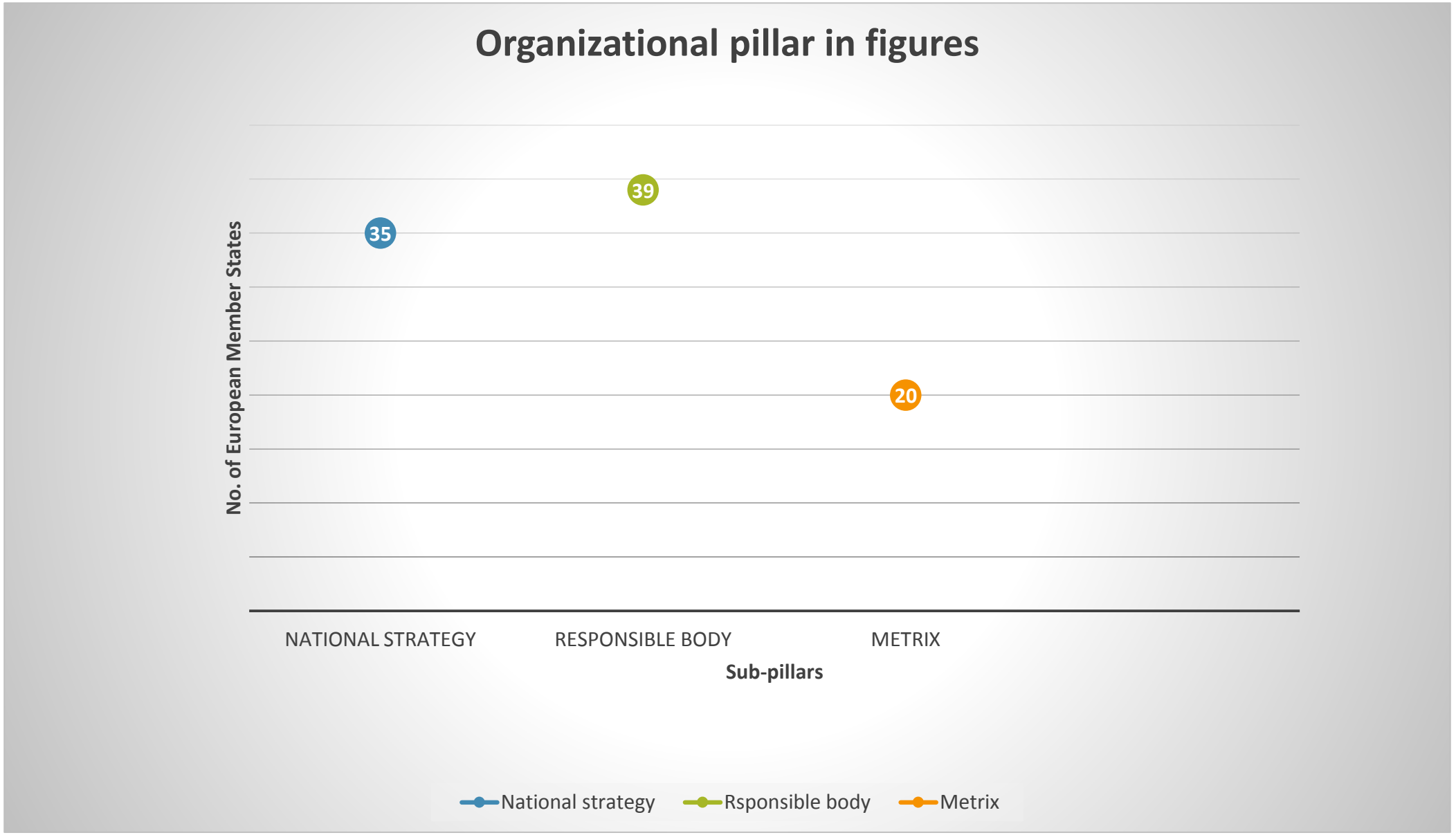
2. Technical

Slovakia benefits from a computer security incident response team with national responsibilities (CSIRT.SK) which was established by the Ministry of Finance. This entity ensures protection and support of national infrastructure including the Critical Information Infrastructures (CII). CSIRT.SK is in constant collaboration with authorities, different organizations of the private sector and international counterparts. It also contributes to raising awareness concerning certain areas of information security

Serbia created the AMRES CSIRT (the Serbian Academic Network) with a mission to enhance the level of security to ICT systems and infrastructures. In order to protect cyberspace, it collaborates and builds various projects with other international entities**.** Its competencies are defined by the "Decision on the establishment of AMRES". AMRES CSIRT is an institution where incidents are reported, analysed and handled. Raising awareness within the academic community about cybersecurity is another of its objectives

Illustrative practices

3.Organizational



Illustrative practices

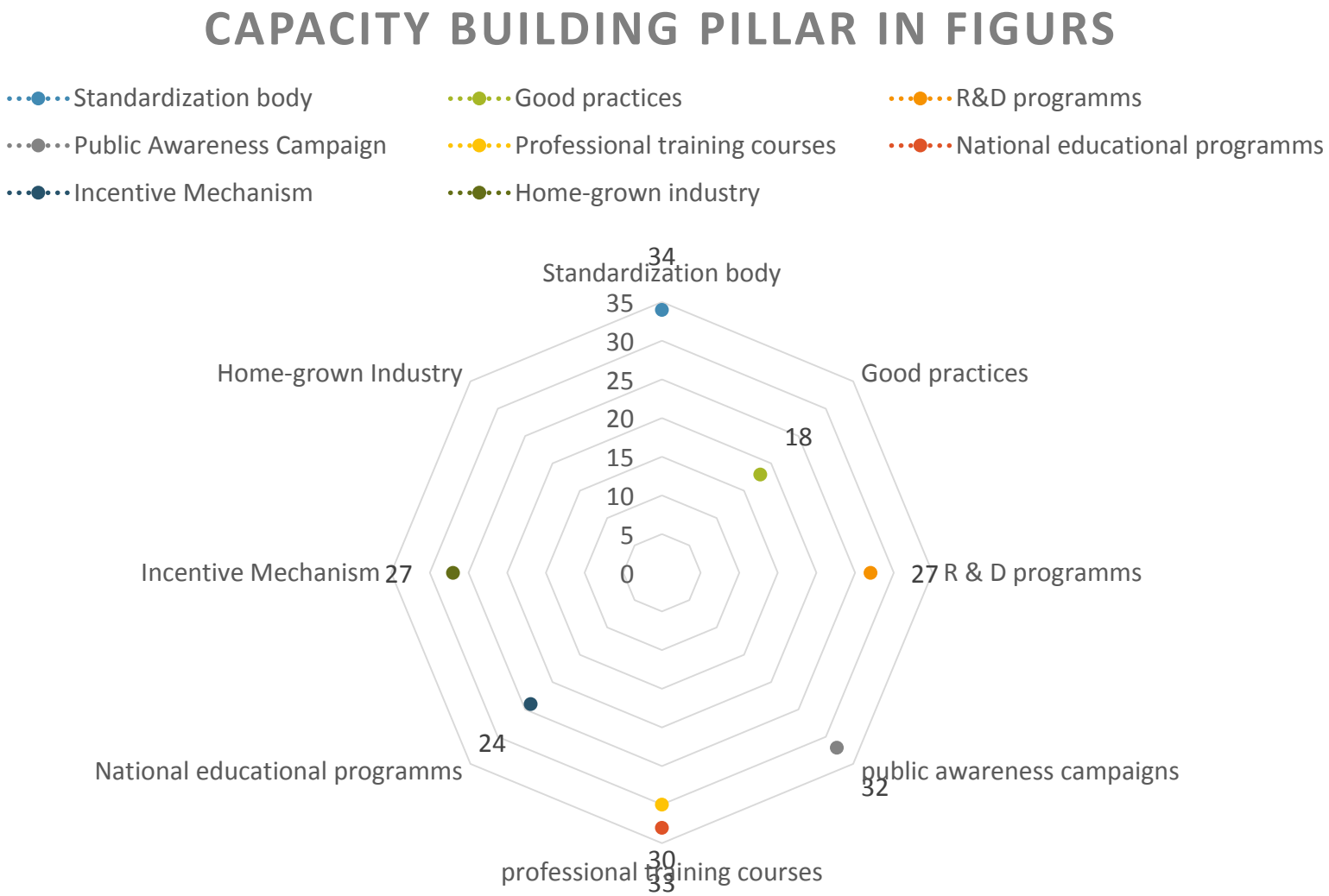
3.Organizational

United Kingdom issued its second five year National Cyber Security Strategy in 2016. The Strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.

Netherlands uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report. The National Cyber Security Centre (NCSC) compiles disclosure reports, security advisories and incidents using a registration system. The metrics allow trends to be observed and acted upon.

Illustrative practices

4.Capacity building



Illustrative practices

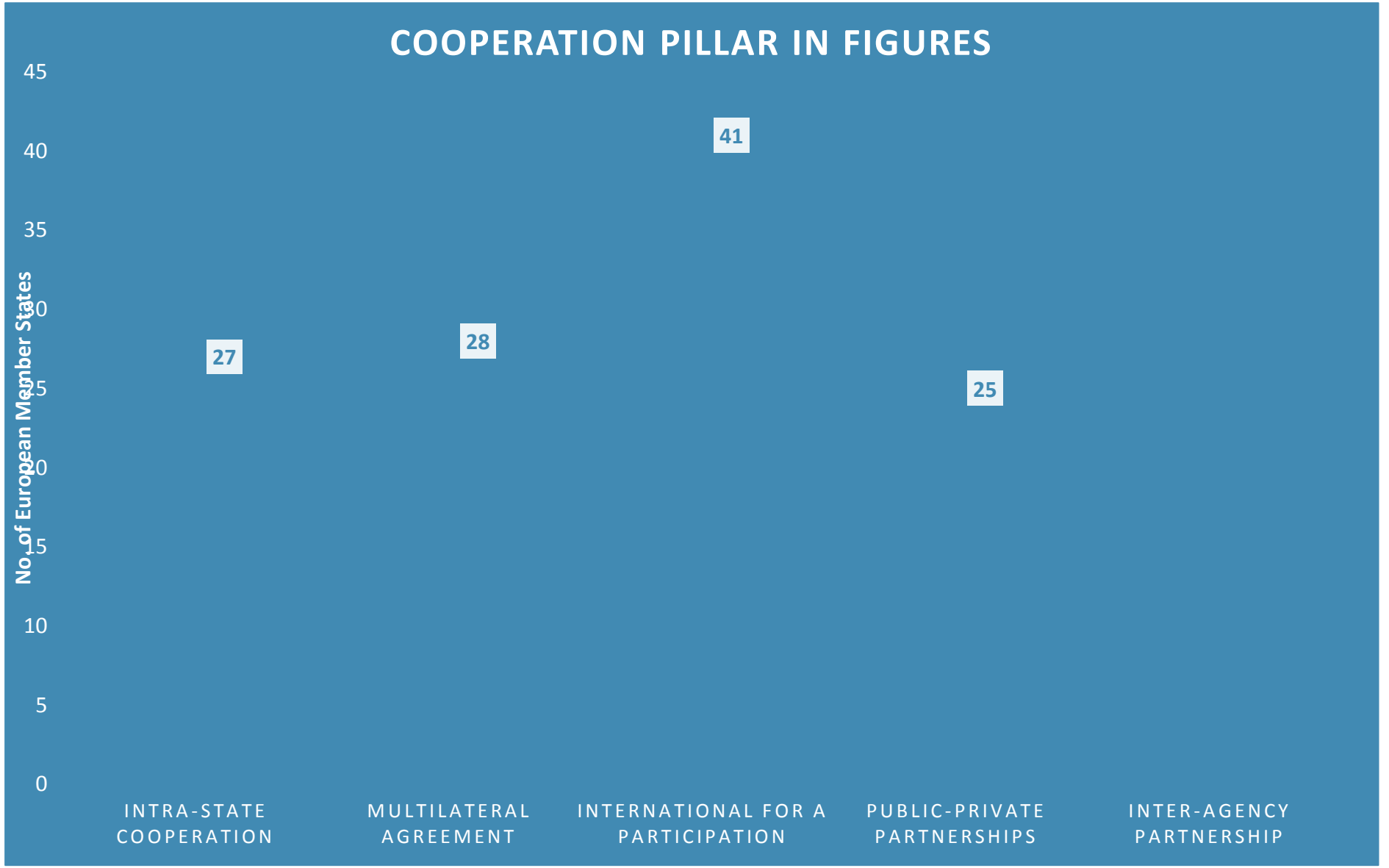
4. Capacity building

Romania created the National Standardization Organization to produce relevant national standards on processes, tools and technologies for software products and systems in the area of security in information technology. It also tests the standardization integrity of encryption algorithms, authentication services and algorithms for confidential services in compliance with accepted international standards http://www.asro.ro/

Switzerland established MELANI in 2008, a collaboration model with three partners, namely GovCert.ch, Service for Analysis and Prevention (SAP) and the Federal IT Steering Unit (FITSU). MELANI has 4 pillars - prevention, early warning, damage limitation and analysis of causes of crisis. Within MELANI, there is the Reporting and Analysis Center for Information Assurance where partners collaborate regarding the security of computer systems' area, Internet and the protection of critical national infrastructures

Illustrative practices

5. Cooperation



Illustrative practices

5. Cooperation

United Kingdom

- The UK and China agree to establish a high-level security dialogue to strengthen exchanges and cooperation on security issues such as non-proliferation, organized crime, cyber crime and illegal immigration. The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage
- Cyber Security information Sharing Partnership (CiSP)

Denmark, Finland, Iceland, Norway and Sweden

- Nordic National CERT Collaboration. This incudes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region.

Illustrative practices

5. Cooperation

EU - European Union Agency for Network and Information Security (ENISA)

- Coordinates information sharing among its member states in the European Union.
- It develops and promotes a culture of network and information security in society to assist in the proper functioning of the internal market.
- Committed on CTI – Regular meetings on the subject - https://www.enisa.europa.eu/events/cti-eu-event/enisa-cti-eu-event

Cybersecurity Cooperation actions @ ITU

PARTNERSHIPS for initiatives

Global Cybersecurity Index – call for new partners

- Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre, Korea Internet & Security Agency, NTRA Egypt, Potomac Institute of Policy Studies, Red Team Cyber, UNICRI, University of Technology Jamaica, UNODC, World Bank

National Cybersecurity Strategy Reference Guide

- CCI, CTO, ENISA, GCSP, GCSCC University of Oxford, Intellium, Microsoft, NATO CCDCOE, OECD, OAS, Potomac Institute, RAND Europe, UNCTAD and World Bank

Child Online Protection – a whole community

Cybersecurity Cooperation actions @ ITU

EVENTS 2016-2017

Regional Cyberdrills for National CSIRTs/CIRTs/CERTs

- Knowledge exchange through team work in handling cyberattack scenarios
- Joint Europe/CIS exercise, 21-23 November 2017, Chisinau, Moldova

Regional Cybersecurity Seminars

- Bulgaria 2016 jointly with ENISA

Co-organizers

- 11th International Conference "Keeping Children and Young People Safe Online", 19-20 September 2017, Warsaw, Poland
- Cybersecurity-Switzerland, 7-8 December 2017

Thank you!

cybersecurity@itu.int

www.itu.int