ITU Global Cybersecurity Index
Key Findings

Borderless Cyber USA 2017

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 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

GCI Indicators

Legal

- Cybercriminal legislation
- Cybersecurity regulation
- Cybersecurity training on regulation and laws

Technical

- National CIRT
- Government CIRT
- Sectoral CIRT
- Standards implementation framework for organizations
- Standards and certification for professionals

Organizational

- Strategy
- Responsible agency
- Cybersecurity metrics

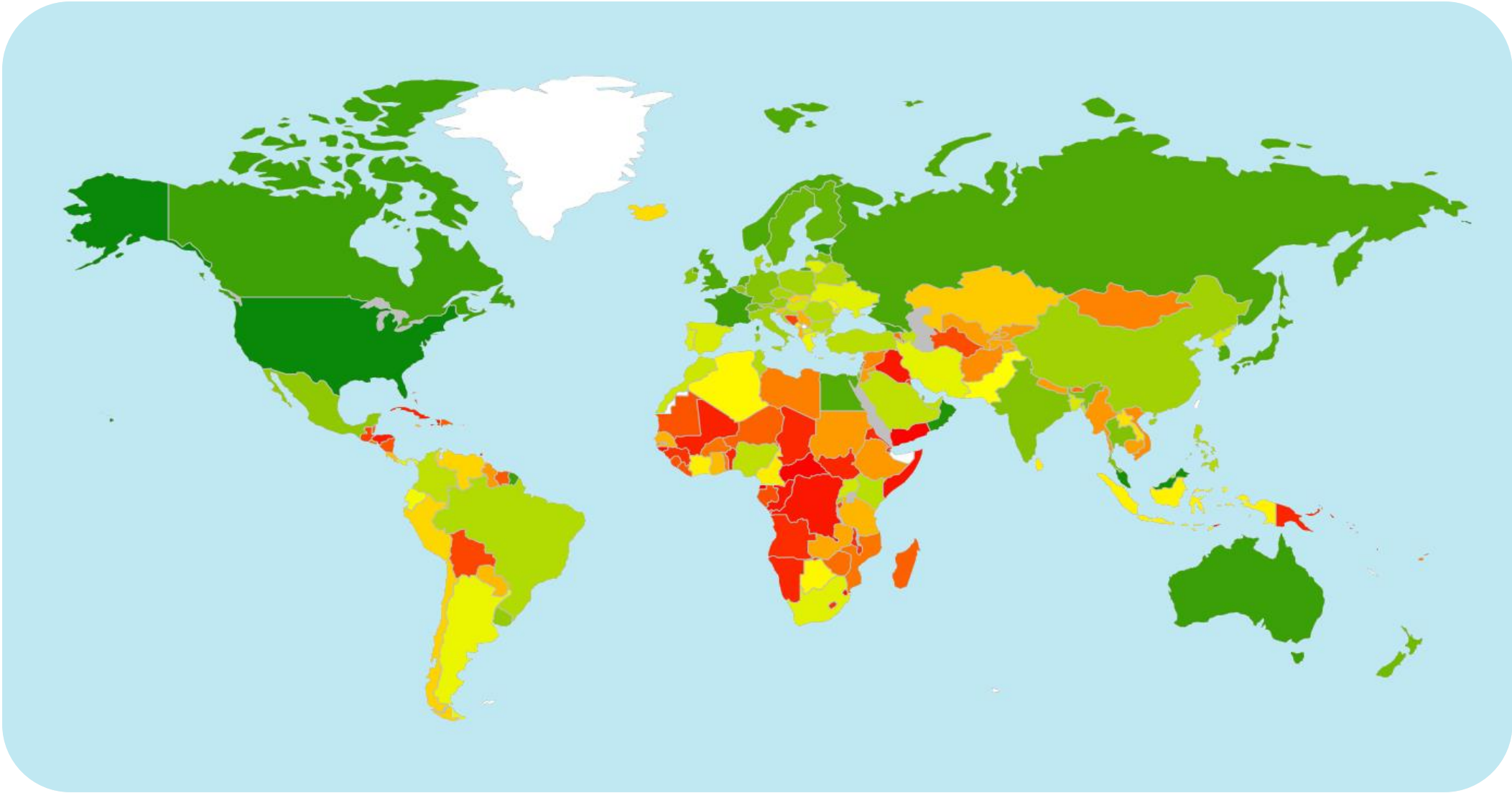
Capacity Building

- 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

Cooperation

- Bilateral agreements
- Multilateral agreements
- International fora participation
- Public-private partnerships
- Interagency partnerships

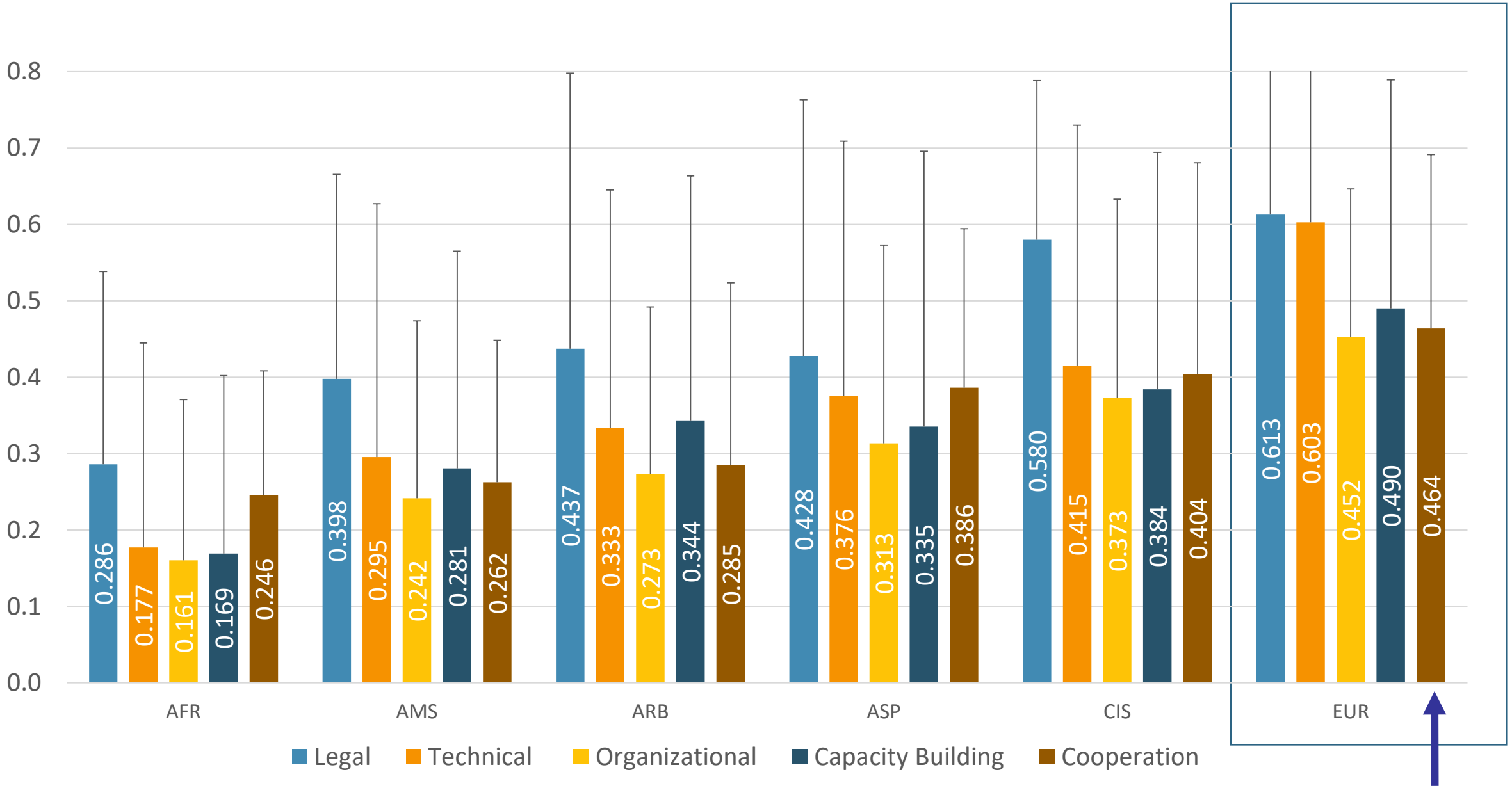
Heat Map



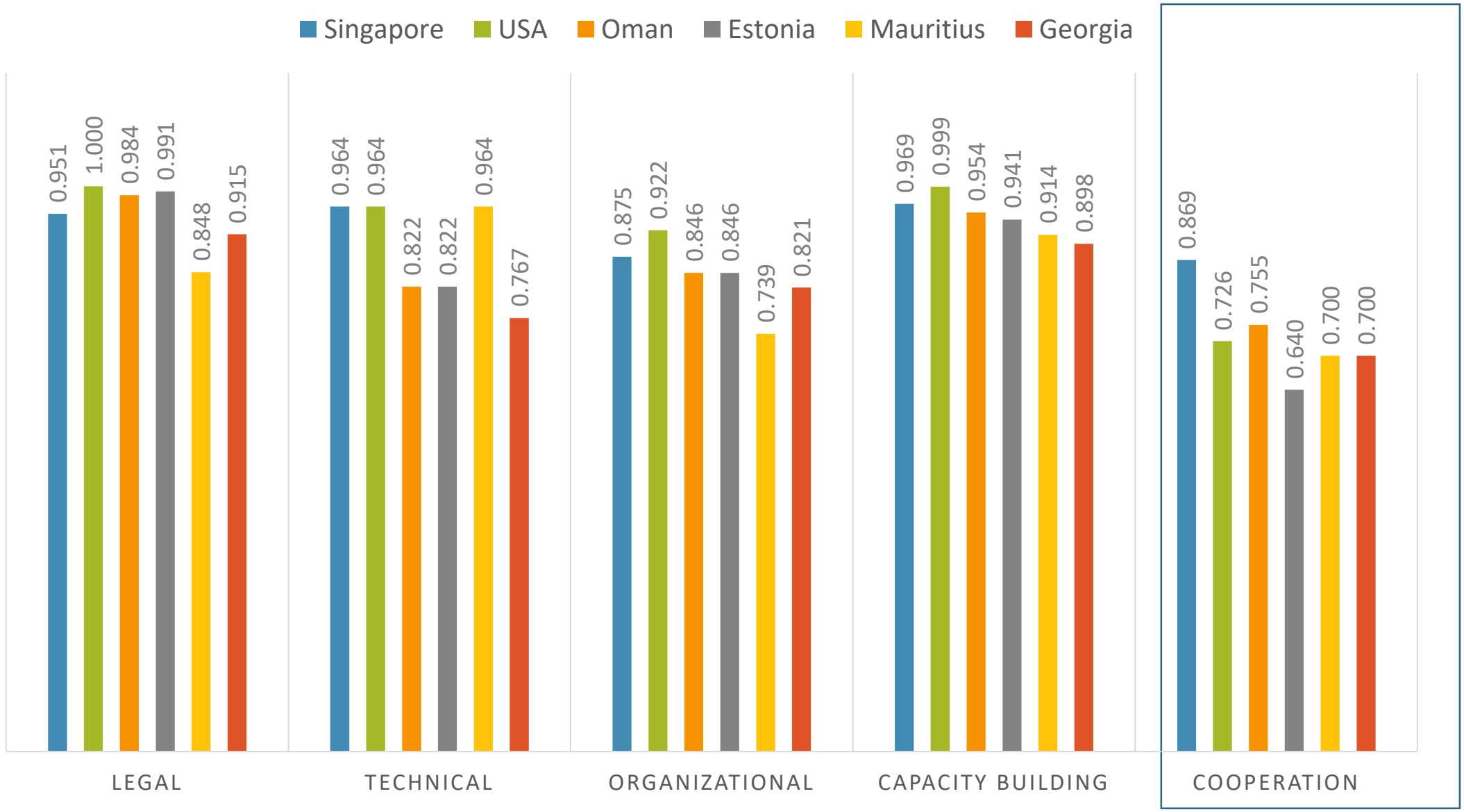
Top Ten

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

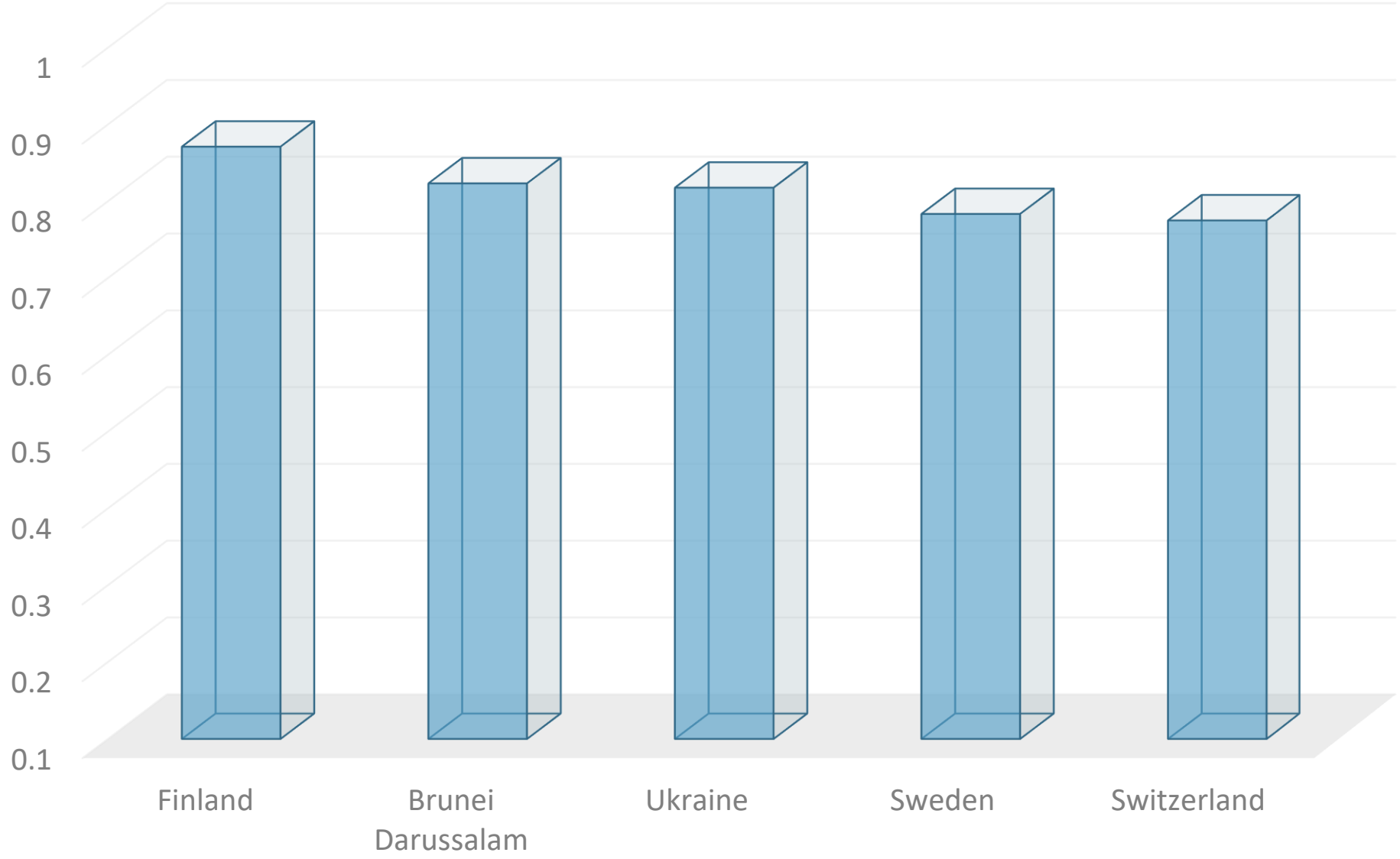
Average by region



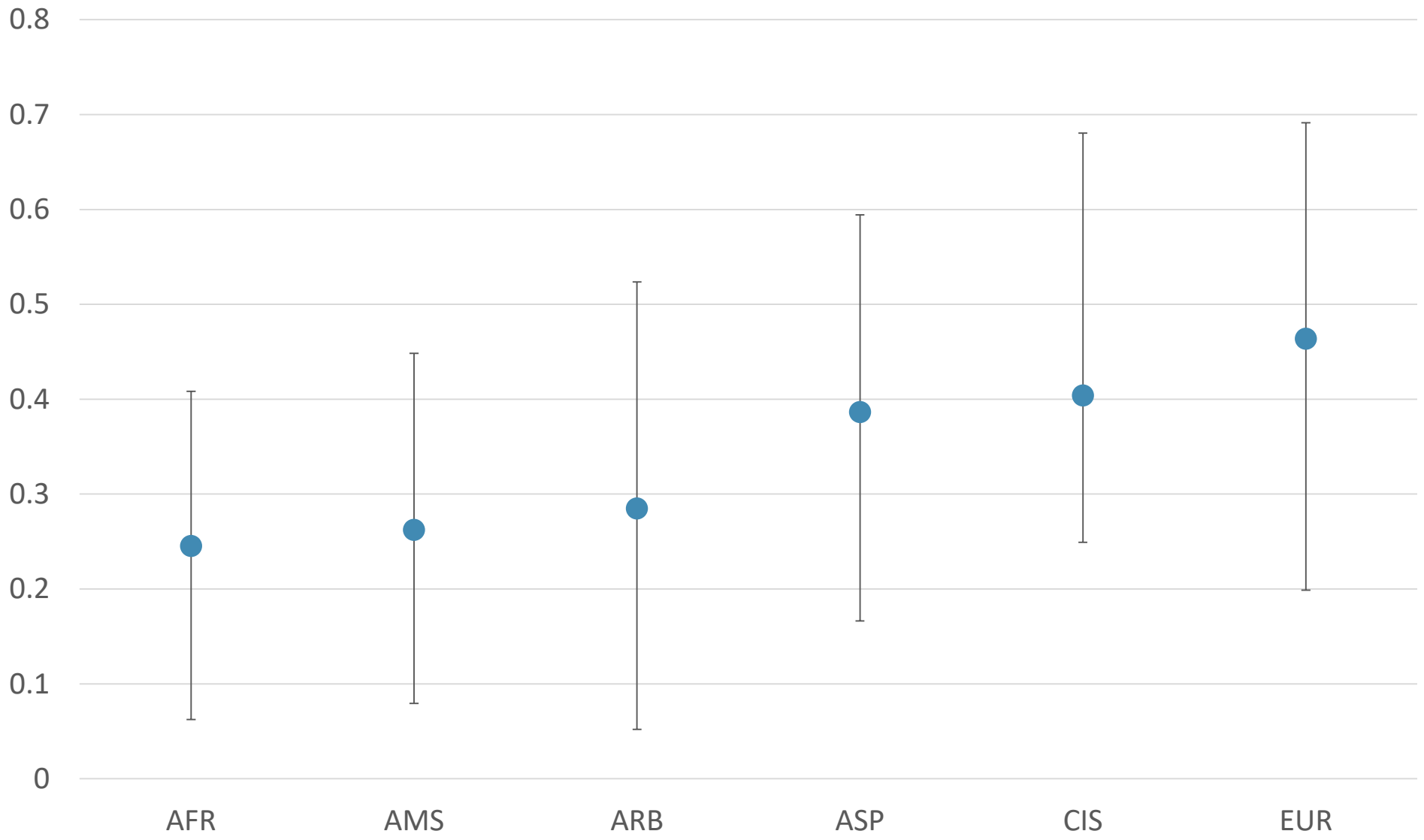
Top 5 countries – Best commitment by pillar



Best commitment on cooperation



Cooperation average by region



Noteworthy practices – Cooperation

UK

- 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) - https://www.cert.gov.uk/cisp/

USA

- USA started its first cross-government security information sharing agreement in 2015 - https://www.ise.gov

Noteworthy practices – Cooperation (2)

South Africa

- A national cybersecurity hub, mandated by the National Cybersecurity Policy Framework (NCPF) in 2012, as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. it coordinates cybersecurity response activities, and facilitates information and technology sharing - https://www.cybersecurityhub.gov.za

Switzerland

- Association of experts. Privately managed companies and government agencies together in the event of a cyber incident, to quickly deliver a diagnosis in case of severe cyber incidents - https://www.swiss-cyber-experts.ch/cms/index-en.html

Noteworthy practices – Cooperation (3)

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

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.