# ITU Global Cybersecurity Index

## Joint ALERT Cyberdrill for Europe & CIS regions,Chisinau 2017

Rosheen Awotar-Mauree
Programme Officer
ITU Office for Europe

# ITU Overview

*Founded in* **1865**

*A specialized agency of the UN with focus on Telecommunication / ICTs*

**193** Member States
**567** Sector Members
**159** Associates
**104** Academia

**ITU-R**: ITU's Radio-communication Sector globally manages radio-frequency spectrum and satellite orbits that ensure safety of life on land, at sea and in the skies.

**ITU-T**: ITU's Telecommunication Standardization Sector enables global communications by ensuring that countries' ICT networks and devices are speaking the same language.

Headquartered in Geneva,
**4** Regional Offices
**7** Area Offices.

**ITU-D**: ITU's Development Sector fosters international cooperation and solidarity in the delivery of technical assistance and in the creation, development and improvement of telecommunication/ICT equipment and networks in developing countries.

# Services in Cybersecurity

CELEBRATING 25YEARS OF ACHIEVEMENTS ITU-D 1992 2017

### *Engagement and awareness*

- Global Cybersecurity Index
- Global, Regional and National events
- High-Level Cybersecurity Simulations
- Information Dissemination

### *National Cybersecurity Assistance*

- National Cybersecurity Assessment
- National Cybersecurity Strategy support
- Critical Infrastructure Protection Support
- Technical Assistance

### *Computer Incident Response Team (CIRT) Program*

- CIRT Assessment
- CIRT Design
- CIRT Establishmemt
- CIRT Improvement

### *Information sharing*

- Best Practices Sharing
- Information Exchange Tools and Techniques

### *Cyber Drills*

- Regional drills
- National drills

### *Human Capacity Building*

- Curricula and Training Programs
- Bespoke Training

# ITU Office for Europe EURregion@itu.int

**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

## WTDC-14: 5 Regional Initiatives for 2014 to 2017

EUR1: Spectrum management and transition to digital broadcasting

EUR2: Development of broadband access and adoption of broadband

EUR3: Ensuring access to telecommunications/ICTs in particular for persons with disabilities

EUR4: Building confidence and security in the use of telecommunications/ICTs

## WTDC-17: 5 Regional Initiatives for 2018 to 2021

# ITU Regional Initiative 4 in Europe (EUR4)

**Objective: To build confidence and security in the use of telecommunications /ICTs**

## Some Actions 2016-2017

- ITU – Council of Europe: High Level Round Table on COP, 10 October 2016
- ITU-ENISA Regional Cybersecurity Forum for Europe, 29-30 November 2016, Bulgaria
- Benchmark of national initiatives on COP in the Central and Eastern European Countries
- Central European Cybersecurity public-private dialogue platform, Romania [co-organized - annual]
- National CIRT Implementation, Cyprus [2017-2018]
- CIRT Assessment, Bosnia & Herzegovina, November-December 2017
- International Conference "Keeping Children and Young People Safe Online", Poland [co-organized - annual]
- ITU ALERT International Cyber Drill Exercise for the Europe & CIS Regions, Moldova , 21-23 November 2017
- Western European Cybersecurity public-private dialogue platform, Switzerland, 7-8 December 2017

# 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

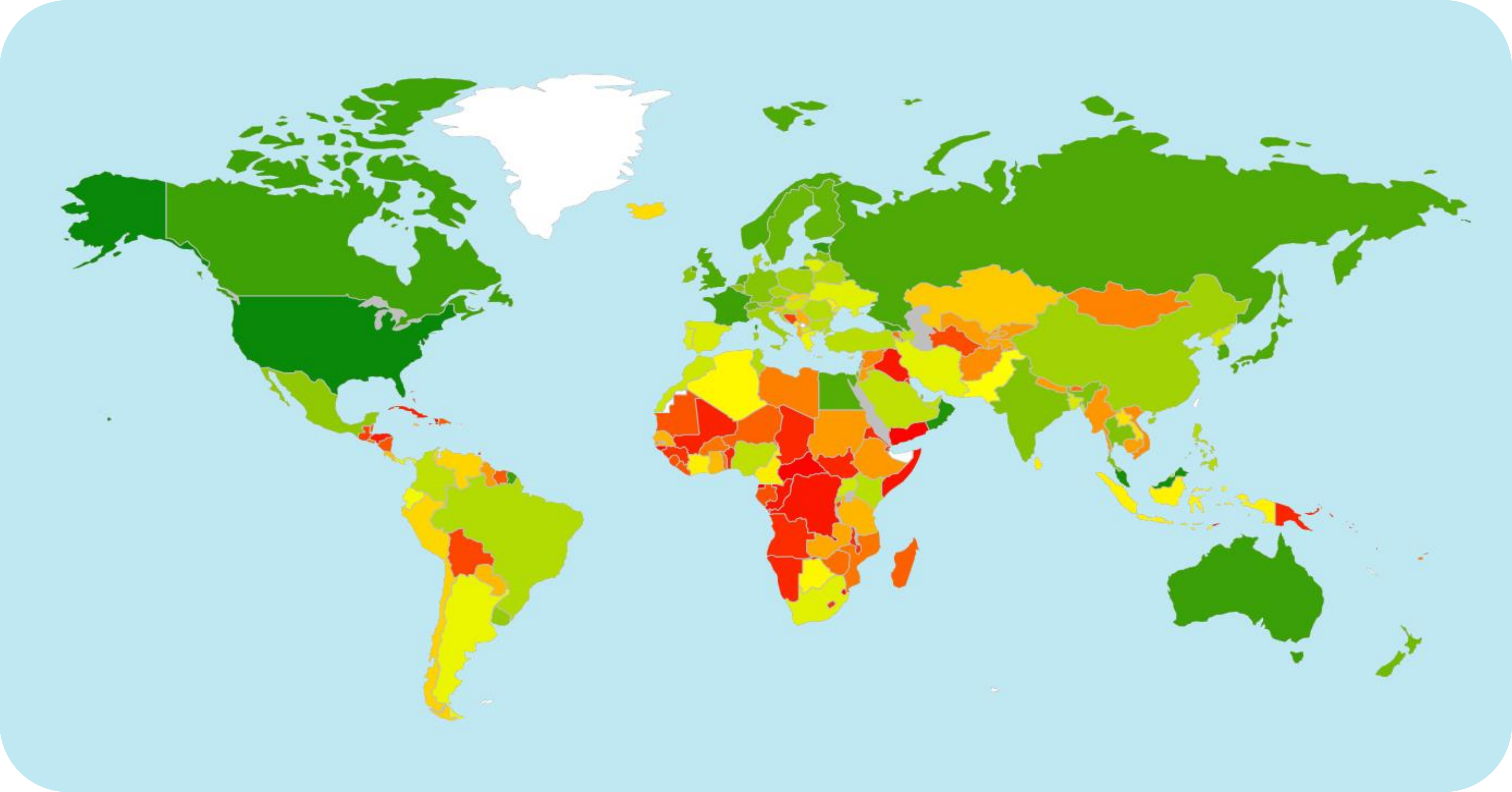
## Capacity Building

- 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



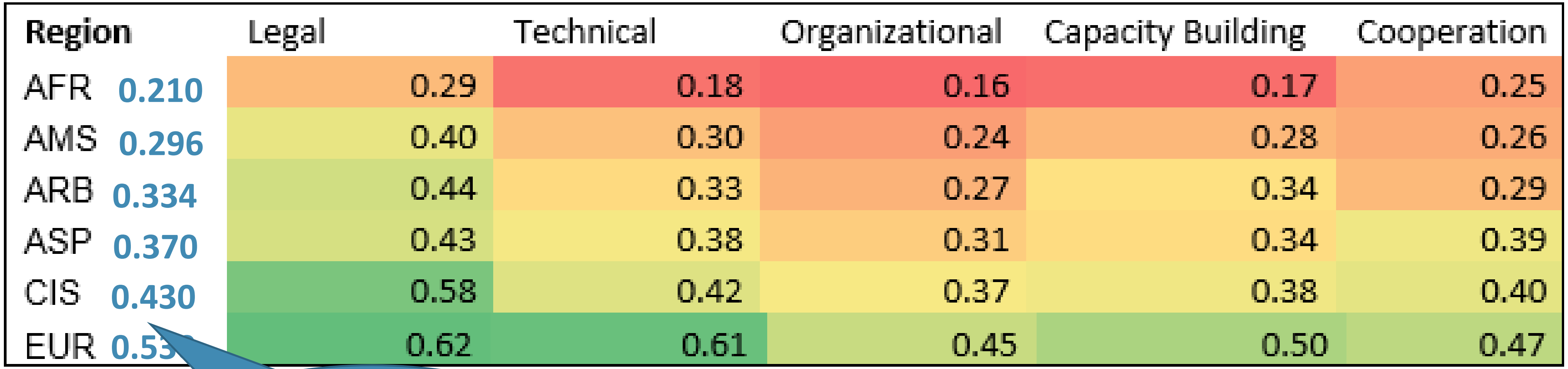
Commitment levels 🟩 High 🟨 Medium 🟥 Low

# 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

# Heat map – regional perspective



| Region | | Legal | Technical | Organizational | Capacity Building | Cooperation |
|---|---|---|---|---|---|---|
| AFR | 0.210 | 0.29 | 0.18 | 0.16 | 0.17 | 0.25 |
| AMS | 0.296 | 0.40 | 0.30 | 0.24 | 0.28 | 0.26 |
| ARB | 0.334 | 0.44 | 0.33 | 0.27 | 0.34 | 0.29 |
| ASP | 0.370 | 0.43 | 0.38 | 0.31 | 0.34 | 0.39 |
| CIS | 0.430 | 0.58 | 0.42 | 0.37 | 0.38 | 0.40 |
| EUR | 0.53 | 0.62 | 0.61 | 0.45 | 0.50 | 0.47 |

Regional Score on a maximum on 1

# GCI for ITU Europe & CIS region

**43 Countries EUROPE** : 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

**11 Countries CIS :** Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine, Uzbekistan

## GCI TIERS out of 54 countries

- *Leading stage* refers to the **22** countries (i.e., GCI score in the 60th percentile and higher) that demonstrate high commitment.
- *Maturing stage* refers to the **22** countries (i.e., GCI score between the 30th and 59th percentile) that have developed complex commitments, and engage in cybersecurity programmes and initiatives.
- *Initiating stage* refers to the 10 countries (i.e., GCI score less than the 30th percentile) that have started to make commitments in cybersecurity.

# Some responses for Europe & CIS regions

**Out of 54**

- ✓ 24 countries have Cybercriminal legislation
- ✓ 32  countries have Cybersecurity  legislation
- ✓ 20 countries have Cybersecurity training on regulation and laws
- ✓ 35 countries have National CIRTs
- ✓ 43 countries have Government CIRTs
- ✓ 34 countries have sectoral CIRTs
- ✓ 38 countries have an entity responsible for Child Online Protection
- ✓ 7  countries use Cybersecurity metrics at national level
- ✓ 12 countries have standardization bodies handling Cybersecurity
- ✓ 23 countries have good practices in Cybersecurity
- ✓ 17 countries have R&D programmes in Cybersecurity

# Some Noteworthy practices

**Georgia** established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing.

**United Kingdom** issued in 2016 its second five years *National Cyber Security Strategy*. 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.

# Some Noteworthy practices

**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 on.

**UK and China** agreed 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/

# Some Noteworthy practices

**Switzerland** has an 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

**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.

# Countries & GCI ...

- Countries compare their own progress over time
- Questionnaire used as a basic roadmap to enhancing cybersecurity
- Identify and share practices

**Collaborate on the GCI initiative**

- Open consultation for Questionnaire development
- Data sharing and validation

# 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

**ITU STUDY GROUPS – Membership driven**

ITU-D Study Group2 Question3

- Securing information and communication networks:

Best practices for developing a culture of cybersecurity new mandate

ITUWTDC
BUENOS AIRES 2017
9-20 October

ITU-T Study Group 17 : Security

- Develop recommendations for future standards including in Cybersecurity

ITU-R Study Groups

- Securing radiocommunications

# Thank you

eurregion@itu.int

www.itu.int