WTO Cybersecurity Webinar

ITU Global Cybersecurity Index Overview

8 October 2020

Caroline Troein, Grace Acayo

ITU builds technical and human capacity in ICTs

ITU is the United Nations specialized agency for ICTs.

Founded in 1865, it works to facilitate international communications, ensure seamless interconnections, and improve ICT access to underserved communities worldwide. ITU is committed to connecting all the world's people – wherever they live and whatever their means.

193

MEMBER STATES

+700

INDUSTRY & INTERNATIONAL ORGANIZATIONS

+150

ACADEMIA MEMBERS

ITU works across three main areas:

ITU Development

Bridging the digital divide

ITU Radiocommunication

Coordinating radio-frequency spectrum and assigning orbital slots for satellites

ITU Standardization

Establishing global standards

Trade Implications of Cybersecurity Risk

Cybersecurity is the biggest threat to the global economy over the next decade*

33%

Increase in mobile ransomware 2018-2019**

78%

Increase in supply chain attacks 2018-2019**

0.8%

Of the global economy was lost due cybercrime in 2019, nearly $600 billion. Cybercrime will result in a loss of $90 trillion in net economic impact by 2030. ***

*Source: EY

**Source: Symantec

*** Source: CSIS&McAfee

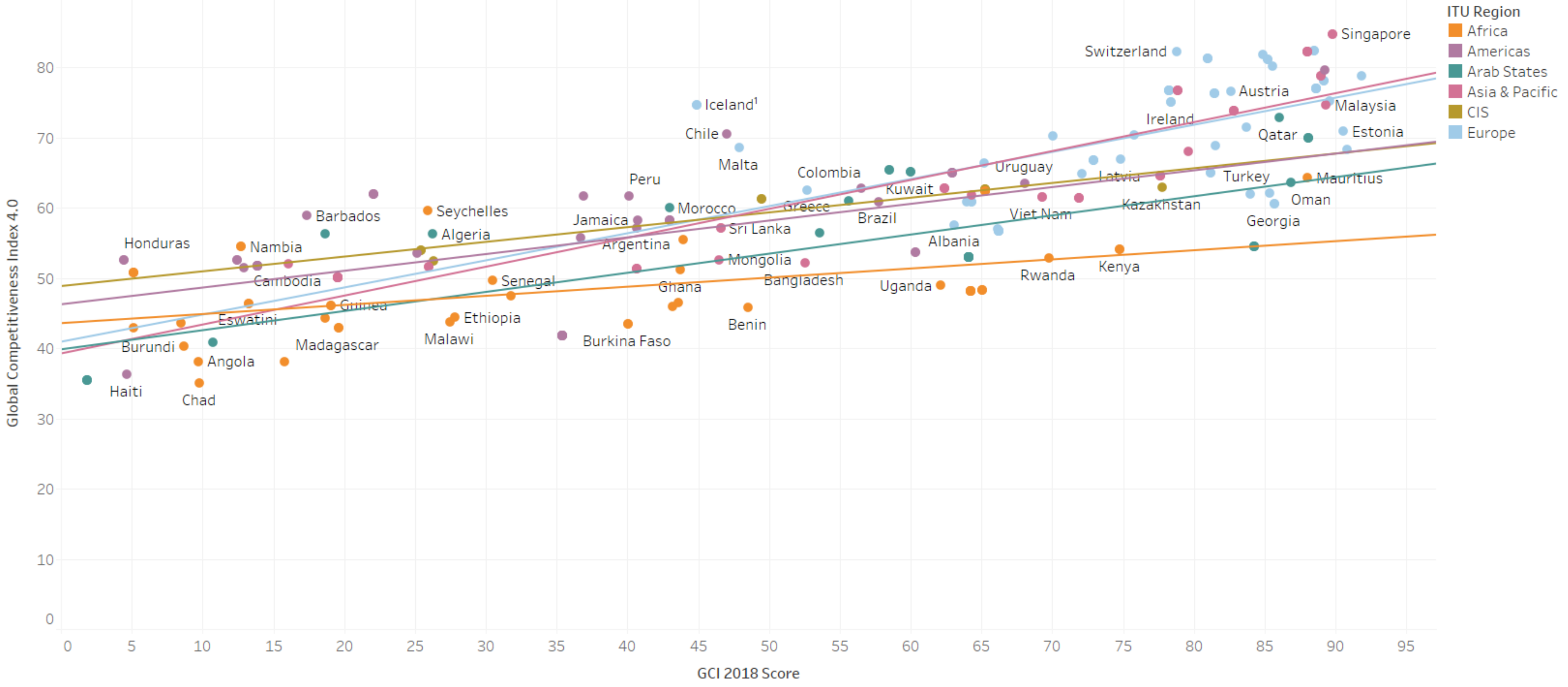
Why does cybersecurity matter for global trade?

Trade is enabled by interoperability and trust

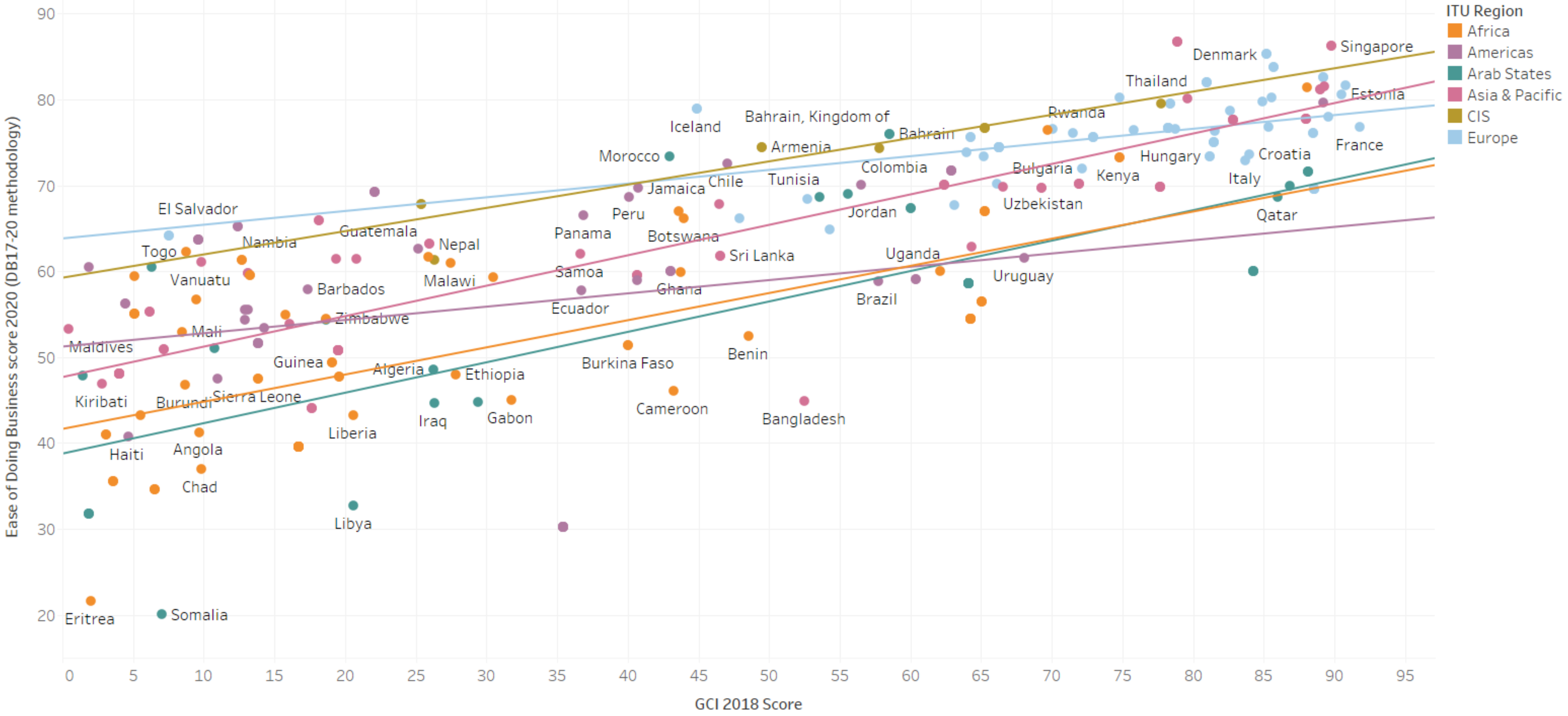
Examples of cybersecurity in trade:

- Payment security
- Free data flow to enable information sharing
- Cyber espionage/ corporate espionage
- Protection against malicious attacks
- Supply chain security

GCI 2018 versus WEF Global Competiveness Index 2019



GCI 2018 generally correlates with World Bank Doing Business scores, except for in the Americas



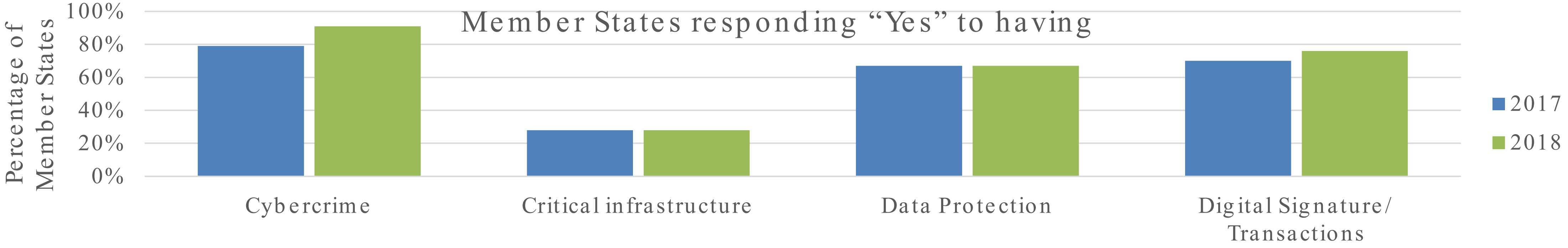
Trade Implications of National Cybersecurity Policies

The Global Cybersecurity Index (GCI) builds on five pillars, which represent key cybersecurity measures relevant to Member States

- Legal
- Technical
- Organizational
- Capacity Development
- Cooperation

Countries are increasingly adopting of cyber-security laws and regulations

- Most cybersecurity laws are broad, covering multiple sectors
- Cybercrime laws and acts: several models harmonise the content worldwide, such as the Budapest Convention of 2001
- GDPR forced countries to update existing data protection regulations
- Cybersecurity related certifications of products and procurement processes are becoming increasingly important



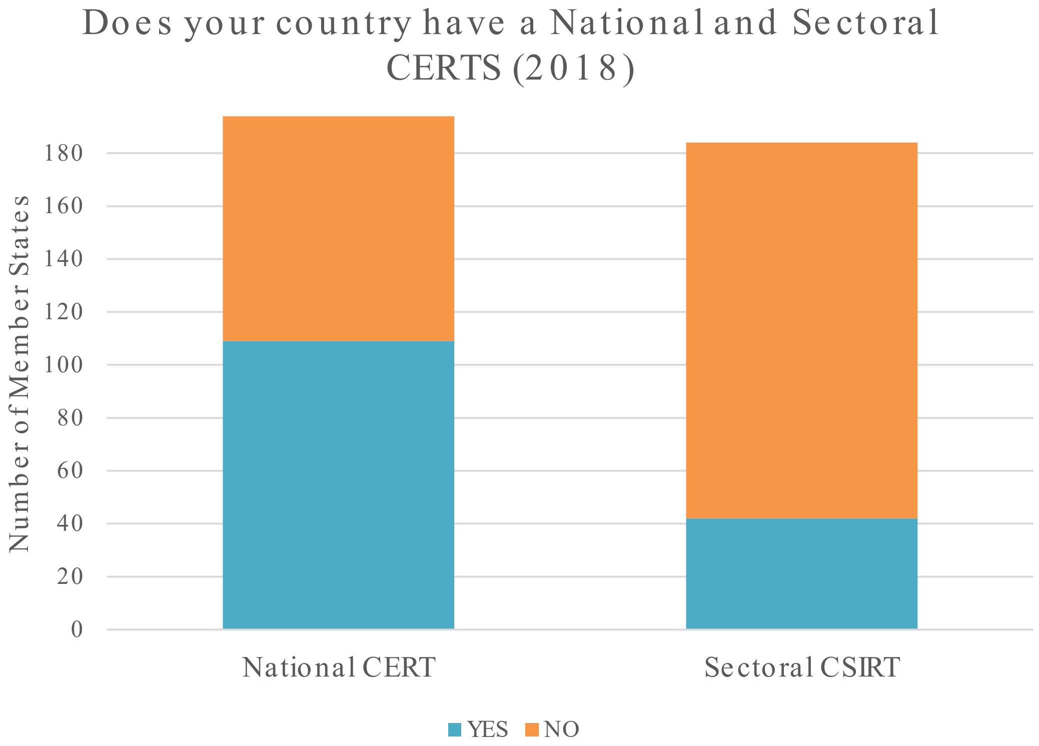
National Cybersecurity Strategies (NCS) rarely address trade issues

- An NCS defines the maintenance of resilient and reliable national critical information infrastructures including the security and the safety of citizens
- 104 Member States have national strategies related to cybersecurity
- Common features identified in cybersecurity policies include:
  - The protection of critical information infrastructure
  - A national resiliency plan
  - Some have clear action plan for government implementation on cybersecurity governance
  - Cybersecurity Responsible Agencies responsible for implementing the national cybersecurity strategy/policy

CERT/CIRT/CSRIT can improve the security and reliability of the digital ecosystem

CIRT/CSIRT/CERT are organizational entities responsible for coordinating and supporting response to computer security events or incidents responses

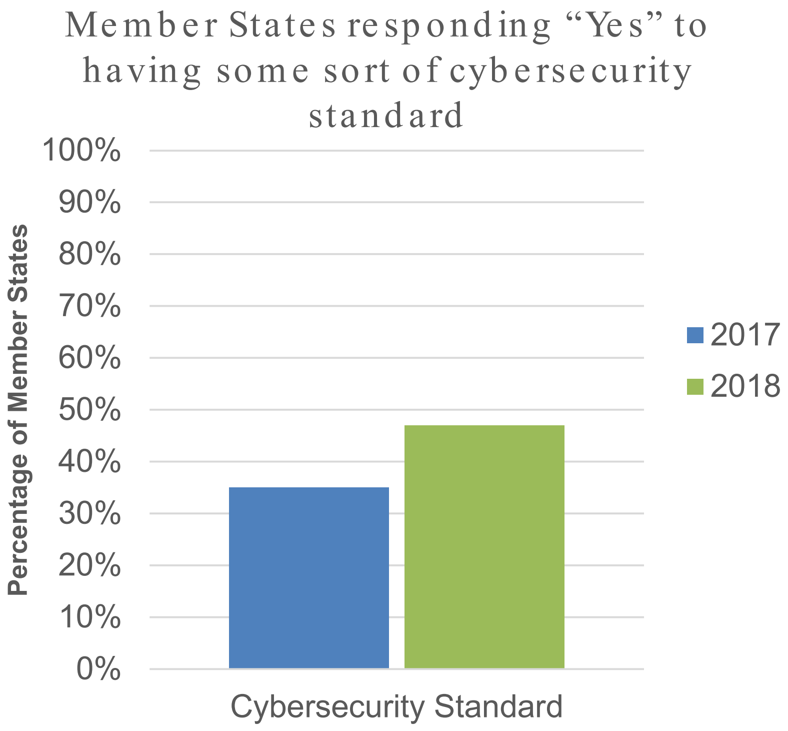
Most of the Sectoral CERT/CIRT/CSRIT are established within the financial sectors, a few in the academic sector



ICT Product Regulation, Standard Development, and International Regulatory Cooperation

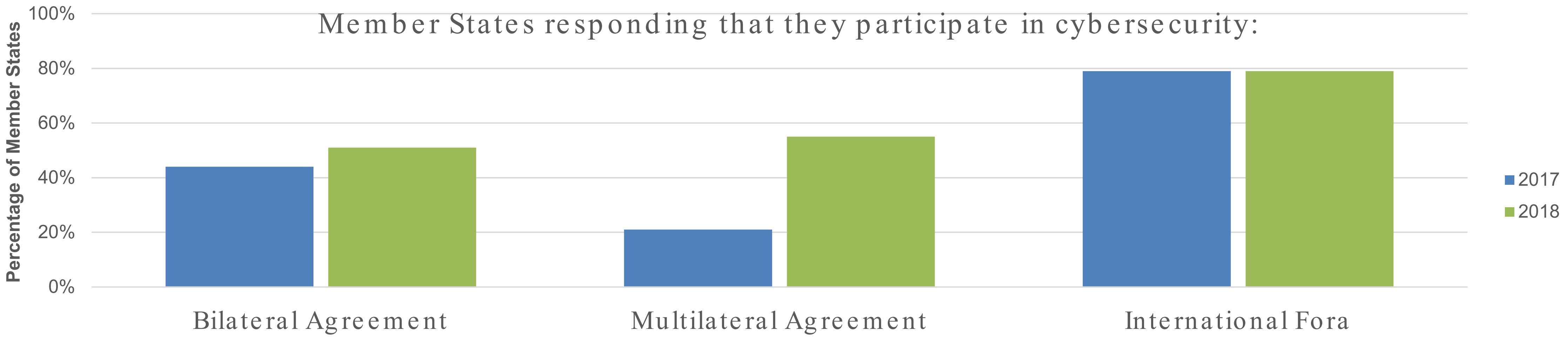
ICT and critical infrastructure are shaped through different international cybersecurity standards

- Standards address security requirements, building a common level of security, providing tools for operators etc.
- Many governments are developing national standards or adopting existing standards (especially ISO 27000 series, NIST)
- Governments often support increasing national and international certifications as it brings several benefits for both trade and security



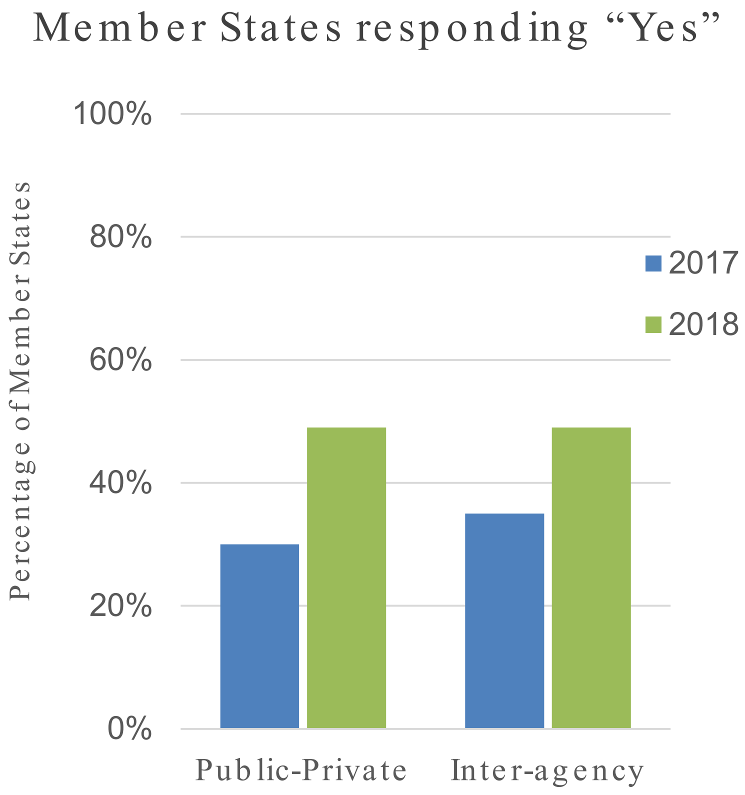
Cooperation Measures enables the creation of a more comprehensive cybersecurity

- International cooperation needs to be strengthened in order to effectively improve international trade and deal with cybercrime which easily transcends national borders.
- The Global Cybersecurity Agenda is one example of countries coming together to cooperate on cybersecurity.



Public-private partnerships and inter-agency partnerships are crucial

The Public-Private partnerships are important in connecting diverse public and sector stakeholders to exchange information and guiding policymaking on trade issues around the world



Inter-agency Partnerships in cybersecurity in the domestic level are found:

- Police officers and law enforcement agents
- Judicial and other legal actors including Lawyers, Judges, solicitors, Barristers, Attorneys and paralegals
- Communication/ICT Ministries and CERT teams

Good practices identified by the GCI

High scoring countries in the GCI tend to have:	Potential Impact on trade
Cybersecurity acts and regulations	Standards and requirements for products sold in a country (ex. Standards, GDPR)
National Cybersecurity Strategies (NCS)	Security protocols, import/export control (ex. Encryption sales)
National CERTs	Increased operating costs, sharing trade secrets, freeloaders, improve reliability of services
Public awareness campaign	Shape what products consumers buy, how they use products (ex. Privacy and home security system)

itu.int/gci
gci@itu.int

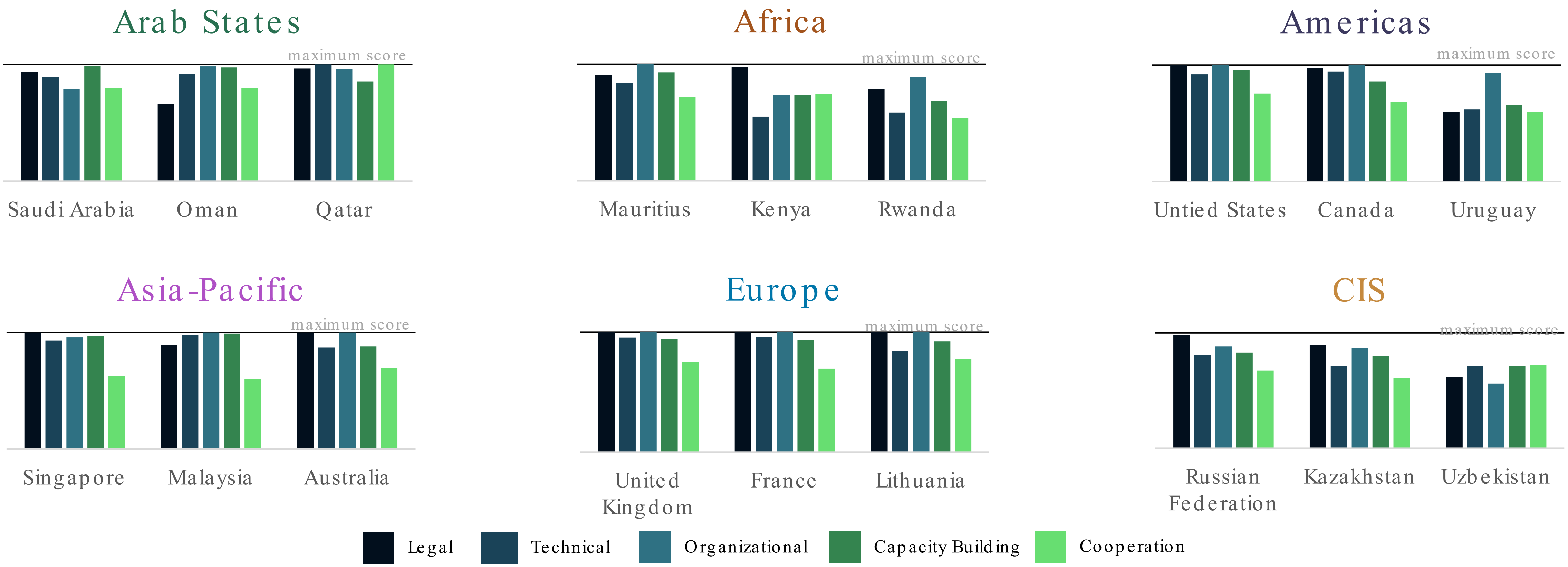
itu.int/cybersecurity
cybersecurity@itu.int

Appendix

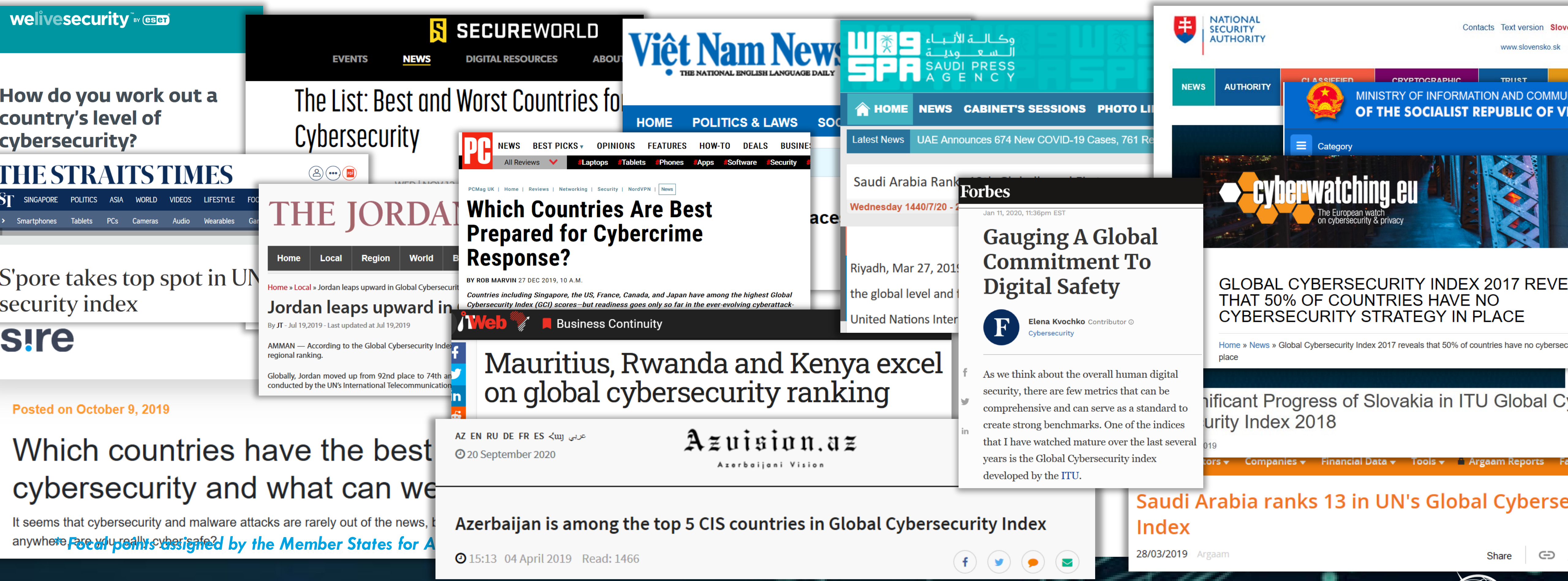
The Global Cybersecurity Agenda (GCA) is a framework for international cybersecurity cooperation

- Launched 13 years by the ITU in 2007
- Designed for cooperation, efficiency, encouraging collaboration, and building on existing initiatives
- The framework is regularly reviewed and updated by Member States, with relevant experts and stakeholders
- The GCA informs cybersecurity strategy and shapes international cooperative efforts
- For more: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Top GCI performers have diverse competitive advantages across the GCI pillars



The Global Cybersecurity Index (GCI) is internationally recognized as a measure of cybersecurity commitments by states



welivesecurity BY eset

How do you work out a country's level of cybersecurity?

Posted on October 9, 2019

Which countries have the best cybersecurity and what can we

It seems that cybersecurity and malware attacks are rarely out of the news, b anywhere. Are you really cyber-safe?

*Focal points assigned by the Member States for A

THE STRAITS TIMES

SINGAPORE POLITICS ASIA WORLD VIDEOS LIFESTYLE FOO

Smartphones Tablets PCs Cameras Audio Wearables Ga

S'pore takes top spot in UN security index

SECUREWORLD

EVENTS NEWS DIGITAL RESOURCES ABOUT

The List: Best and Worst Countries for Cybersecurity

THE JORDAN

Home Local Region World B

Home » Local » Jordan leaps upward in Global Cybersecurit

Jordan leaps upward in

By JT - Jul 19,2019 - Last updated at Jul 19,2019

AMMAN — According to the Global Cybersecurity Index regional ranking.

Globally, Jordan moved up from 92nd place to 74th an conducted by the UN's International Telecommunication

Việt Nam News

THE NATIONAL ENGLISH LANGUAGE DAILY

HOME POLITICS & LAWS SOC

PC

NEWS BEST PICKS OPINIONS FEATURES HOW-TO DEALS BUSINES

All Reviews #Laptops #Tablets #Phones #Apps #Software #Security

PCMag UK | Home | Reviews | Networking | Security | NordVPN | News

Which Countries Are Best Prepared for Cybercrime Response?

BY ROB MARVIN 27 DEC 2019, 10 A.M.

Countries including Singapore, the US, France, Canada, and Japan have among the highest Global Cybersecurity Index (GCI) scores—but readiness goes only so far in the ever-evolving cyberattack-

iTWeb Business Continuity

Mauritius, Rwanda and Kenya excel on global cybersecurity ranking

SPA وكالة الأنباء السعودية SAUDI PRESS AGENCY

HOME NEWS CABINET'S SESSIONS PHOTO LI

Latest News UAE Announces 674 New COVID-19 Cases, 761 Re

Saudi Arabia Rank

Wednesday 1440/7/20 -

Riyadh, Mar 27, 2019 the global level and United Nations Inter

Forbes

Jan 11, 2020, 11:36pm EST

Gauging A Global Commitment To Digital Safety

Elena Kvochko Contributor
Cybersecurity

As we think about the overall human digital security, there are few metrics that can be comprehensive and can serve as a standard to create strong benchmarks. One of the indices that I have watched mature over the last several years is the Global Cybersecurity index developed by the ITU.

AZ EN RU DE FR ES عربي

20 September 2020

Azvision.az
Azerbaijani Vision

Azerbaijan is among the top 5 CIS countries in Global Cybersecurity Index

15:13 04 April 2019 Read: 1466

NATIONAL SECURITY AUTHORITY

Contacts Text version Slov

www.slovensko.sk

NEWS AUTHORITY CLASSIFIED CRYPTOGRAPHIC TRUST

MINISTRY OF INFORMATION AND COMMU OF THE SOCIALIST REPUBLIC OF VI

Category

cyberwatching.eu
The European watch on cybersecurity & privacy

GLOBAL CYBERSECURITY INDEX 2017 REVE THAT 50% OF COUNTRIES HAVE NO CYBERSECURITY STRATEGY IN PLACE

Home » News » Global Cybersecurity Index 2017 reveals that 50% of countries have no cybersec place

nificant Progress of Slovakia in ITU Global C urity Index 2018

019

tors Companies Financial Data Tools Argaam Reports

Saudi Arabia ranks 13 in UN's Global Cyberse Index

28/03/2019 Argaam

Share

The GCI is a composite index that measures key aspects of state-level cybersecurity practices

Key Statistics

First released: 2015

Past editions: 3

Member States Participating: 164 (of 194)

Mentions in scholarly articles: 821*

Current questionnaire: 82 questions

The GCI is designed to

- ✓ Drive awareness global cybersecurity
- ✓ Share best practices
- ✓ Drive continuous cybersecurity improvement
- ✓ Build capacity in ITU Members

The GCI developed through a multistakeholder process, with Member States, civil society, academia, and private sector

Preparation & Survey Distribution

Complete

Questionnaire review with the consultation group

Approval of questionnaire through the Study Group meeting

Official invitation sent and Survey conducted

Data Collection & Weightage Model

Ongoing

Member States submit completed Questionnaires

Weightage Expert Group meets, members submit weightage recommendations

Data Quality Check & Analysis

Ongoing

Questionnaire submissions are cross-checked

Member States are invited to validate ITU-GCI team verification

Questionnaires are scored and weighted

Results Publication

End-2020

Report compiled and published

Upcoming for ITU Cybersecurity

For the GCI

- In the process of submitted questionnaire data validation.
- Weightage Expert Group meeting 15 October 2020
- Publication tentatively scheduled for end 2020
- Working to expand the application of the GCI, including:
  - Creation of a Self-Assessment tool, based on GCI, that cities or regions can use to assess their cybersecurity maturity
  - Targeting ITU operations based on needs identified by the GCI

Other ITU Cybersecurity activities

- Global and regional CyberDrill 2020 ongoing until end of the year.
- ITU Cybersecurity webinar 19 October 2020
- Consultation meeting for the second review of the National Cybersecurity Strategies Guide (NCS)-started end of September to mid-year 2021.
- Ongoing National CIRT/CERT/CSIRT Assessments, Design and Establishment of Member States requests