Multi-level cybersecurity governance frameworks for public administration

LASARIS SEMINAR

28.04.2022

Františka Romanovská, 433528@mail.muni.cz

LAB OF SOFTWARE ARCHITECTURES AND
INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

lasaris

Goals and Content

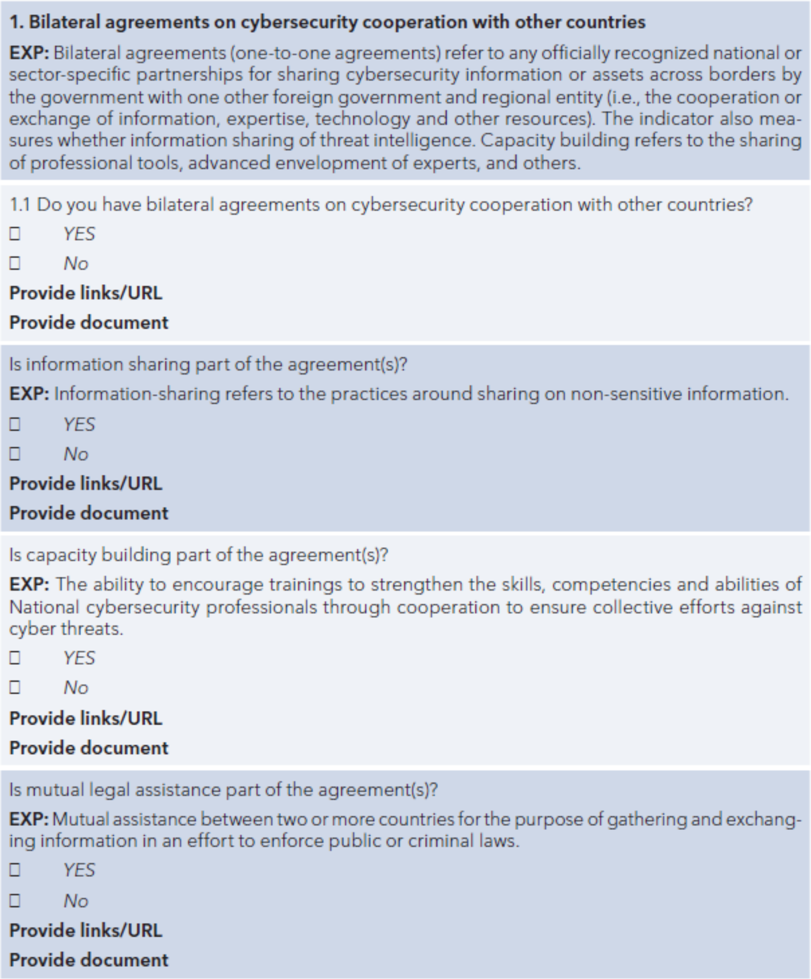
- Global Cybersecurity Index
- Multi-level cybersecurity governance in the context of public administration
- Approach comparison of selected territorial units
- Regional cybersecurity framework

Global Cybersecurity Index

- Initiative of the International Telecommunication Union (United Nations), from 2015
- Capacity development tool as it identifies areas for improvement
- Reports aim to evaluate commitments to cybersecurity of individual countries
- The report is used by countries to:
  - Facilitate discussion
  - Gather insight about national cybersecurity initiatives
  - Compare their efforts
  - Benchmarking
- GCI evolves – questionnaires are updated to reflect changes

GCI – How is the report created?

- 5 pillars, 20 indicators, 82 questions – the questions evolve in time
- No reponse collected: publicly available data are used
- Focal points
- Score 0 – 100, each pillar max 20 points



1. Bilateral agreements on cybersecurity cooperation with other countries

EXP: Bilateral agreements (one-to-one agreements) refer to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government and regional entity (i.e., the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether information sharing of threat intelligence. Capacity building refers to the sharing of professional tools, advanced envelopment of experts, and others.

1.1 Do you have bilateral agreements on cybersecurity cooperation with other countries?

□ *YES*

□ *No*

Provide links/URL

Provide document

Is information sharing part of the agreement(s)?

EXP: Information-sharing refers to the practices around sharing on non-sensitive information.

□ *YES*

□ *No*

Provide links/URL

Provide document

Is capacity building part of the agreement(s)?

EXP: The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.

□ *YES*

□ *No*

Provide links/URL

Provide document

Is mutual legal assistance part of the agreement(s)?

EXP: Mutual assistance between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

□ *YES*

□ *No*

Provide links/URL

Provide document

Pillars

Legal measures

- Existence of legal cybersecurity frameworks
  - Data Protection Regulations
  - Critical Infrastructure Regulations
- Minimum foundation for cybersecuriy capabilities

Technical measures

- Existence of technical institutions
  - CIRT
- Existence of framework dealing with cybersecurity
- Minimum-security criteria and accrediation for software
- National/sector-specific agencies

Pillars cont.

Organisational measures

- Existence of coordination institutions, policies, and strategies at the national level
- Identification of cybersecurity goals and strategic and delivery plans
- Definition of roles and responsibilities, governance model and supervisory body

Capacity development measures

- Socio-economical and political context
- Research and development
- Education and training programmes
- Certified experts
- Public sector agencies for capacity building
- Public awareness campaigns

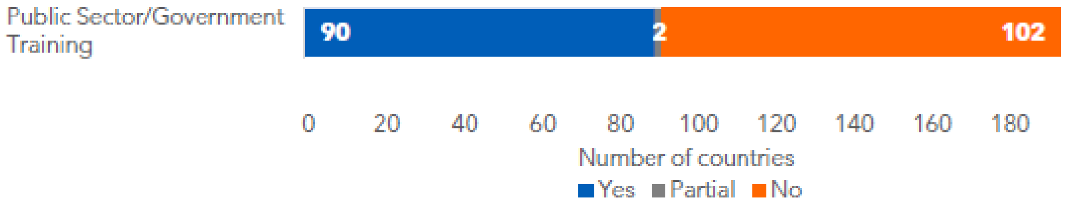
Pillars cont.

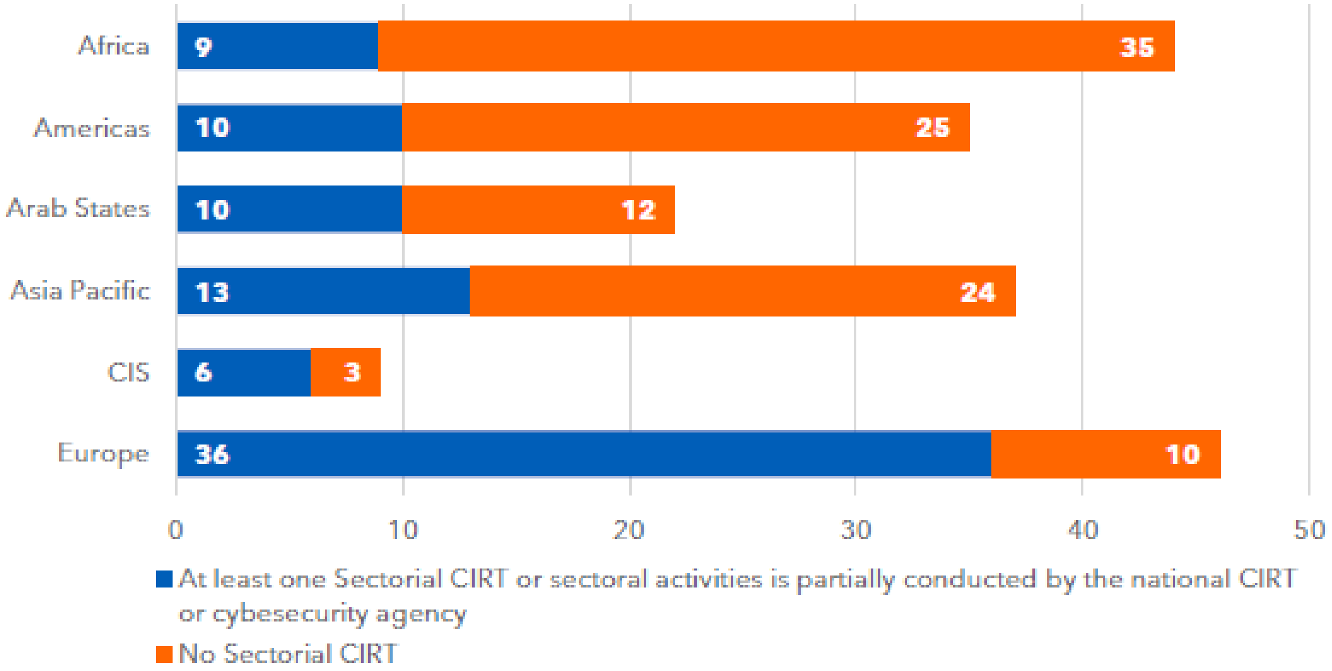
Cooperative measures

- Existence of partnership and cooperative frameworks
  - Between corporations, public agencies, and countries
- Information sharing networks

GCI report for 2020

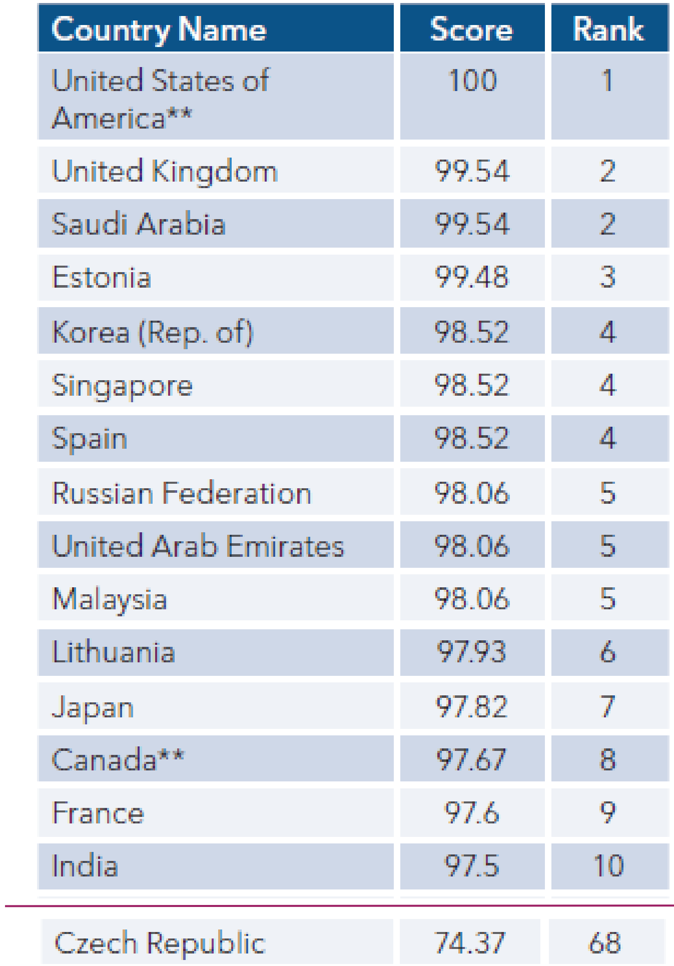
- Progress in legislation regarding privacy, unauthorized access, and online safety
- Emphasis on establishing strategies (to build capacity and mitigate cyber risks)
  - 2/3 of countries have a national cybersecurity strategy
- Online identity protection and data theft legislation lack attention
- 131 implemented CIRTs
  - Only 1/3 has sector-specific CRITs
  - Lack of sector-specific training





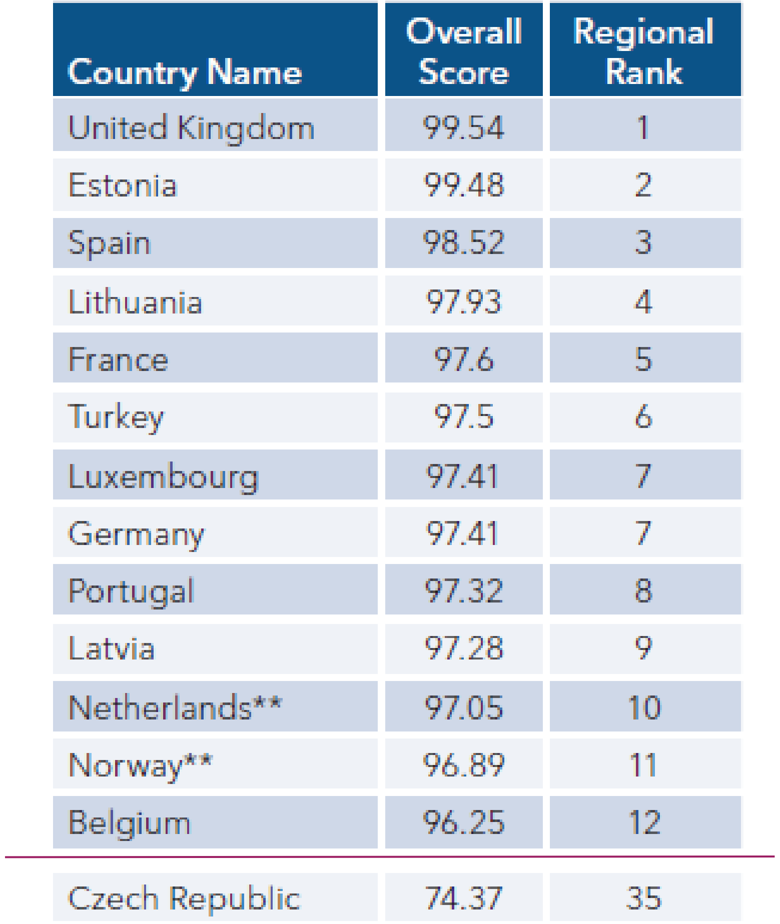
GCI 2020 – Ranking

Global



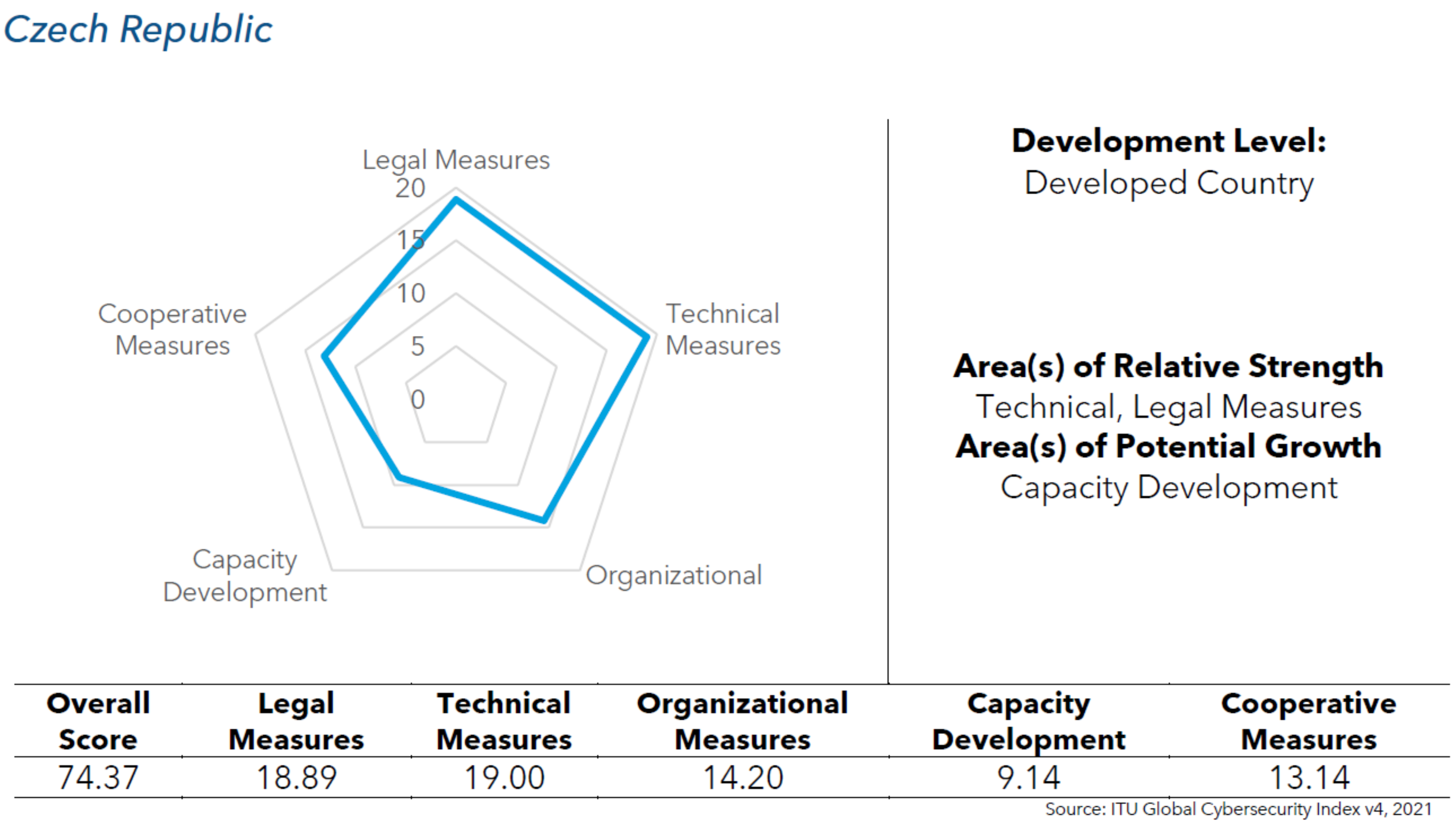
Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Czech Republic	74.37	68

Europe



Country Name	Overall Score	Regional Rank
United Kingdom	99.54	1
Estonia	99.48	2
Spain	98.52	3
Lithuania	97.93	4
France	97.6	5
Turkey	97.5	6
Luxembourg	97.41	7
Germany	97.41	7
Portugal	97.32	8
Latvia	97.28	9
Netherlands**	97.05	10
Norway**	96.89	11
Belgium	96.25	12
Czech Republic	74.37	35

GCI 2020 – Czech Republic



Czech Republic

Development Level:
Developed Country

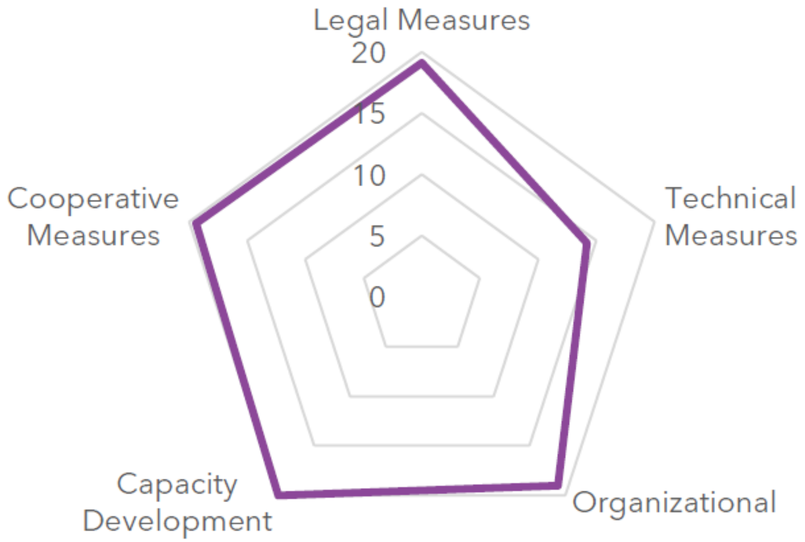
Area(s) of Relative Strength
Technical, Legal Measures
Area(s) of Potential Growth
Capacity Development

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
74.37	18.89	19.00	14.20	9.14	13.14

Source: ITU Global Cybersecurity Index v4, 2021

GCI 2020 - Australia

Australia



Development Level:
Developed Country

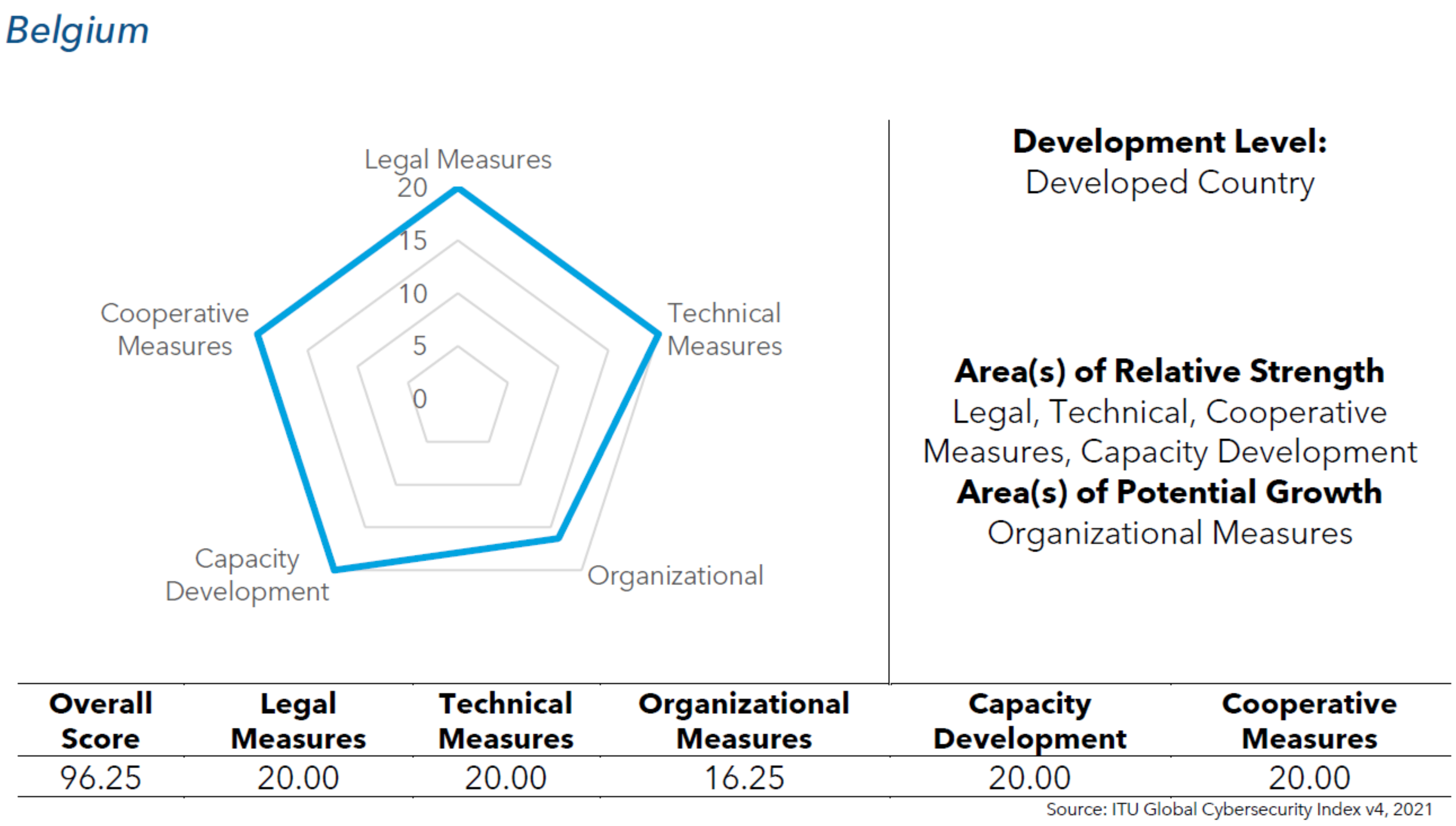
Area(s) of Relative Strength
Capacity Development, Cooperative Measures, Legal Measures

Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.47	20.00	19.08	18.98	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

GCI 2020 - Belgium



Belgium

Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures, Capacity Development
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
96.25	20.00	20.00	16.25	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Multi-level governance of cybersecurity

- Different responsibilities for different levels of governmental institutions
  - State, region, district, city
- EU's Regulation on the internal market in electricity (sectoral)
- EU: focus on EU's agencies and the national governments
  - Regions and municipalities in the background
- Limitation: cybersecurity of a member state is a sensitive matter
- Advantages: closer connection to local and reginal cybersecurity actors, possible improvement of GCI ranking

Australia's national cybrsecurity strategy

- GCI ranking globally: 12, regionally: 5 (97.47)
- Improving cybersecurity through actions of different stakeholders
  - Governments, business, community
- Strong presence of public-private partnership
  - The Government and large businesses will help SMEs with their cybersecurity
- No explicit mention of cybersecurity governance on regional (state) levels
- Actions of the government that mention state/territorial/local governments:
  - Improving incident response procedures witih the state and territory governments in cooperation with private sector and the Government
  - Providing technical assistance and supporting law enforcement to [...] state, and territory law enforcement agencies
  - Investing in expansion of Joint Cyber Security Centres

Belgium's national cybersecurity strategy

- GCI ranking globally: 19, regionally: 12 (96.25)
- Three regions has their own governments with several authorities
- GCI: everyting except Organistional measures perfect

  VS Belgium's cybersecurity strategy: insufficient capacity
- Cybersecurity is considered a shared responsibility
  - Citizens, companies, government services, and organisations of vital interest
- Cybersecurity is considered a federal matter ⟶ managed on the national level
  - No regional responsibilities are mentioned in the strategy

High-level Comparison

Australia

- Technical, Organisational, Cooperative Measures
- Cybersecurity = shared responsibility
  - Governments, business, community
- No explicit mention of cybersecurity governance on regional (state) levels; however
  - Improving incident response procedures witih the state and territory governments
  - Providing technical assistance and supporting law enforcement to […] state, and territory law enforcement agencies
  - Joint Cyber Security Centres

Belgium

- Organisational Measures
- Cybersecurity = shared responsibility
  - Government services, organisations of vital interest, companies, citizens
- No mention of cybersecurity governance on regional levels

Victoria and Queensland States

Victoria

- The first Australian state with its own cyber strategy
- The current strategy has 5-year duration
- Current strategy has three main missions:
  1. Safe and reliable governmental services
  2. Vibrant cyber economy
  3. Cyber-safe place to work, live, and learn

Queensland

- Queensland's government has cybersecurity department
  - Doesn't have a cybersecurity strategy
- The department
  - Provides information about cybersecurity incident
  - Operates team that assist in solving incidents
  - Offers training related to cybersecurity
  - Provides cybersecurity services

Brussels-Capital and Flemish Regions

Brussels-Capital Region

- Whitepaper Towards a regional Cybersecurity plan (by Brussels Regional Informatics Centre and Brussels Prevetion & Security)
  - Methodological framework as a response to cyber threats
  - Estalish cybersecurity on the regional level
  - Focus on raising awareness and managin IT policies, establish a knowledge and training centre
- Cybersecurity plan for the region
  - Regional Cybersecurity Centre

Flemish Region

- Focus on the private sector
- Foundation for the Cybersecurity action plan (in making)
  - Solely focused on the private sector, secondary focus on research
  - No development of governmental organisations is required
    - GCI Organisational measures = least developed
- Action plan should focus on economic sector and the capacity of human resources

Low-level Comparison

- Both countries with high GCI score – no focus on multi-level governance
  - No clear guidance
- Highly nonuniform
  - Cybersecurity strategy
  - Cybersecurity services for the public sector
  - Focus on the private sector
- Regional Cyber Centre as a space for cooperation, no further elaboration

Regional cybersecurity framework

- Multi-level cybersecurity governance
  - Closer connection to regional stakeholders
- Regional cybersecurity centre
  - Space for cooperation
  - Provision of service for public administration in the region
  - Education and training
- GCI
  - Technical: Sectoral CIRT/CSIRT/CERT + awareness activities + information sharing
  - Organisational measures: Question concern only national level
  - Capacity development measures: sector specific public awarenes campaigns, national sector-specific educationl programmes/training/courses, government incentive to encourage capacity development
  - Cooperative measures: Public-private partnership

Resources

- CGI report 2020: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- Kaklauskaité, M. (2020). Multi-level Governance in Cybersecurity: What Role for the European Regions? *European Cybersecurity Journal*, *6*, 44–51. https://cybersecforum.eu/wp-content/uploads/2020/08/ECJ-VOLUME-6-2020-ISSUE-1.pdf
- European Parliament and Council of the European Union. (2019). Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) . *Official Journal of the European Union*, 54–124. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943
- Australian Government. (August 2020). *Australia's Cyber Security Strategy 2020.* Tech. rep. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
- Brussels Regional Informatics Centre. (2018). *Towards a regional cybersecurity plan.* Tech. rep. https://bric.brussels/en/news_publications/publications/papers/towards-a-regional-cybersecurity-plan-september-2018
- Queensland Government Customer and Digital Group. (December 2021). Cyber Security. *Cyber Security*. https://www.qgcio.qld.gov.au/information-on/cyber-security
- Victorian Government Melbourne. (April 2021). *Victoria's Cyber Strategy 2021.* Victorian Government Melbourne. https://www.vic.gov.au/sites/default/files/2021-06/DPC_Cyber%20Security%20Strategy_Accessible%20PDF.pdf
- Centre for Cyber Security Belgium. (May 2021). *Cybersecurity Strategy Belgium 2.0 2021-2025*. Tech. rep. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
- Vlaamse minister van Werk, Economie, Wetenschap, Innovatie, en Sport. (2019). *Quaternota aan de Vlaamse regering.* Tech. rep. https://www.ewi-vlaanderen.be/sites/default/files/quaternota_aan_de_vlaamse_regering_-_vlaams_beleidsplan_cybersecurity.pdf