

Global Cybersecurity Index 2017 Europe

Draft Report



Acknowledgments

This report has been produced by the International Telecommunication Union (ITU) with the support of Michael Minges. The Cybersecurity Team of the ITU would like to express its appreciation to the cybersecurity regional focal points for their input to the regional Cybersecurity Index (GCI) work and report.

The report was elaborated and written with the support of Grace Acayo, Lena Lattion and Yulia Kozyavina.

DRAFT

Table of Contents

1	Executive Summary.....	4
2	Introduction.....	5
3	GCI Scope and Framework	7
3.1	Background	7
3.2	Reference model	7
3.3	Conceptual framework	8
4	Key Findings	12
4.1	Heat Map of National Cybersecurity Commitments	12
4.2	GCI Groups for the Europe Region	12
4.3	Europe commitment in figures	15
5	Europe region in the Global ranking	20
5.1	Comparing Europe with ICT Development Index	20
6	Regional Outlook	23
7	Illustrative practices by pillar	24
7.1	Legal	24
7.2	Technical	28
7.3	Organizational.....	33
7.4	Capacity building.....	37
7.5	Cooperation	45
8	Conclusion	51
	Annex 1: Abbreviations.....	52
	Annex 2: ITU Member states from Europe - cybersecurity commitment score.....	53
	Annex 3: An illustration of all countries in the region and their score for each pillar is presented below.	54
	Annex 4: Tables and figures	56

1 Executive Summary

This report is an analysis for the Europe Region of the results of the Global Cybersecurity Index (GCI). The GCI is an index that measures the commitment of Member States to cybersecurity. The GCI does not measure the number of attacks or level of cybercrime within each Member State but rather Member States' involvement in, and commitment to, cybersecurity practices.

The GCI aligns with the ITU Global Cybersecurity Agenda (GCA)¹ and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment.

The GCI was developed through an established methodology, the ITU study groups² and different multi-stakeholder consultations, in order to analyze the existence of cybersecurity tools and form an overview of the developing commitments of governments in six regions – Americas, Arab, Africa, Asia-Pacific, CIS and Europe.

The Index provides information regarding the level of development of the different pillars varying from country to country and highlights the challenges Member States experience in the matter of cybersecurity, as illustrated by the scores of each pillar of the Global Cybersecurity commitment.

A detailed review of the GCI data is provided to present a more accurate picture of the cybersecurity situation in Europe. This includes: a regional outlook and specific practices which distinguish the region and give an insight into the achievements of the pillars employed in the GCI.

This report concludes that collaboration in the field of cybersecurity is urgent and essential to achieving the 2030 Sustainable Development Goals and the successful implementation of the Connect 2020 Agenda for Global Telecommunication/ICT Development³.

¹ <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

² <http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybex.aspx>

³ <http://www.itu.int/en/connect2020/Pages/default.aspx>

2 Introduction

Information and communication technologies' (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half of the world's population used the Internet (3.5 billion users⁴) and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020⁵. Yet, just as in the real world, digital space is exposed to a variety of cybersecurity threats that can cause immense damage.

Cybersecurity threats remain at the forefront of the public consciousness, whether in the form of ransomware attacks, cyber-enabled fraud or State-on-State actions. The ransomware industry continues to affect member states, businesses and consumers, by regularly destabilizing access to the data until a ransom payment is made to cybercriminals. To prevent such misuse of ICT resources, governments, the private sector and civil society need to cooperate and put into effect a cybersecurity system to reduce threats, enhance confidence in the use of electronic devices and services and build mitigation strategies.

Over the past decade, great leaps have been made in the promulgation of international and regional tools aimed at countering cybercrime. Countries increasingly recognize the need for legislation in this area and some conventions related to cybercrime have been adopted. However, there are large regional differences, with some countries reporting insufficient legislation in this regard.

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has stepped up its efforts to better protect the continent. It has adopted a set of legislative proposals, in particular on network and information security, and earmarked more than €600 million for research and innovation in cybersecurity projects from 2014-2020. The NIS Directive (The Directive on security of network and information systems) adopted by the European Commission was the first EU-wide legislation on cybersecurity that aims to provide legal measures to boost the overall level of cybersecurity in the EU⁶.

Furthermore, the Commission has also fostered cooperation within the EU and with other partners on the global stage. The Commission has further strengthened its approach in the past year by putting cybersecurity at the heart of its political priorities: trust and security are at the core of the Digital Single Market Strategy presented in May 2015, while the fight against cybercrime is one of the three pillars of the European Agenda on Security adopted in April 2015. In July 2016, delivering on these strategies, the Commission presented additional measures to boost the cybersecurity industry and to tackle cyber-threats⁷.

Nonetheless, there is still a visible gap between countries in terms of knowledge, awareness and capacity to deploy the strategies, capabilities and programmes in the field of cybersecurity. Sustainable developments in this area should ensure the safe and adequate use of ICTs as well as economic growth. Cybersecurity is no longer only a government concern. Today, the industries, the governments and the citizens need to respond, protect and design strategies toward raising awareness and capacity building.

⁴ www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

⁵ www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

⁶ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

⁷ http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

The ITU oversees the development of the knowledge, awareness and capacity in member countries. This report specifically relates to the European Region. This region comprises of 43 Member States; 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 and the United Kingdom.

In this context, under Resolution 130 (Rev. Busan, 2014) the ITU, together with Member States, has established the Global Cybersecurity Index (GCI) to promote government strategies and the sharing of information on efforts across industries and sectors. This report aims to implement EUR4 from the WDTC and build further confidence and security in the use of Telecommunications/ICTs. This comes under Sustainable Development Goal 7, to ensure access to affordable, reliable, sustainable and modern energy for all.

The methodology used is explained in more detail in the main Global Cybersecurity Index which can be found on the website of the ITU⁸ but in sum the GCI is a composite index which combines 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States' cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. The methodology for the GCI tasked the ITU and the expert group with developing a questionnaire for the purpose of information gathering, collecting and analysing data with the key objective of building capacity at the national, regional and international level. An analysis of the data collected is set out in the Report below.

⁸ <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx>

3 GCI Scope and Framework

3.1 Background

The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. Specifically, Member States are invited “to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors”.

A first iteration of the GCI was conducted in 2013-2014 in partnership with ABI Research, and the final results have been published.

Following feedback received from various communities, a second iteration of the GCI was planned and undertaken. This new version was formulated around an extended participation from Member States, experts and industry stakeholders as contributing partners (namely World Bank and Red Team Cyber as new GCI partners joining the Australia Strategic Policy Institute, FIRST, Indiana University, INTERPOL, ITU-Arab Regional Cybersecurity Centre in Oman, Korea Internet & Security Agency, NTRA Egypt, The Potomac Institute of Policy Studies, UNICRI, University of Technology Jamaica and UNODC) who all provided support with the provision of secondary data, response activation, statistical analysis, qualitative appreciation amongst other.

The data collected via GCI 2017 for ITU-D Study Group 2 Question 3 (SG2Q3) surveys have been analyzed by the Rapporteur and co-Rapporteur for inclusion in the SG2Q3 final report. GCI partners have been active in providing expertise and secondary data as appropriate, while the UN office of ICT (New York) has also initiated collaborative work. ITU is also working in a multi-stakeholder collaboration led by the World Bank to elaborate a toolkit on “Best practice in Policy/Legal enabling Framework and Capacity Building in Combatting Cybercrime”. ITU is providing support on the component on capacity building from a cybersecurity perspective based on GCI 2017 data.

An enhanced reference model was thereby devised. Throughout the steps of this new version, Member States were consulted using various vehicles including ITU-D Study Group 2 Question 3/2, where the overall project was submitted, discussed and validated.

3.2 Reference model

The GCI is a composite index combining 25 indicators into one benchmark measure to monitor and compare the level of ITU Member States’ cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the GCA. These pillars form the five pillars of GCI.

The main objectives of the GCI are to measure:

- the type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- the progress in cybersecurity commitment of all countries from a global perspective;
- the progress in cybersecurity commitment from a regional perspective;
- the cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering a global culture of cybersecurity.

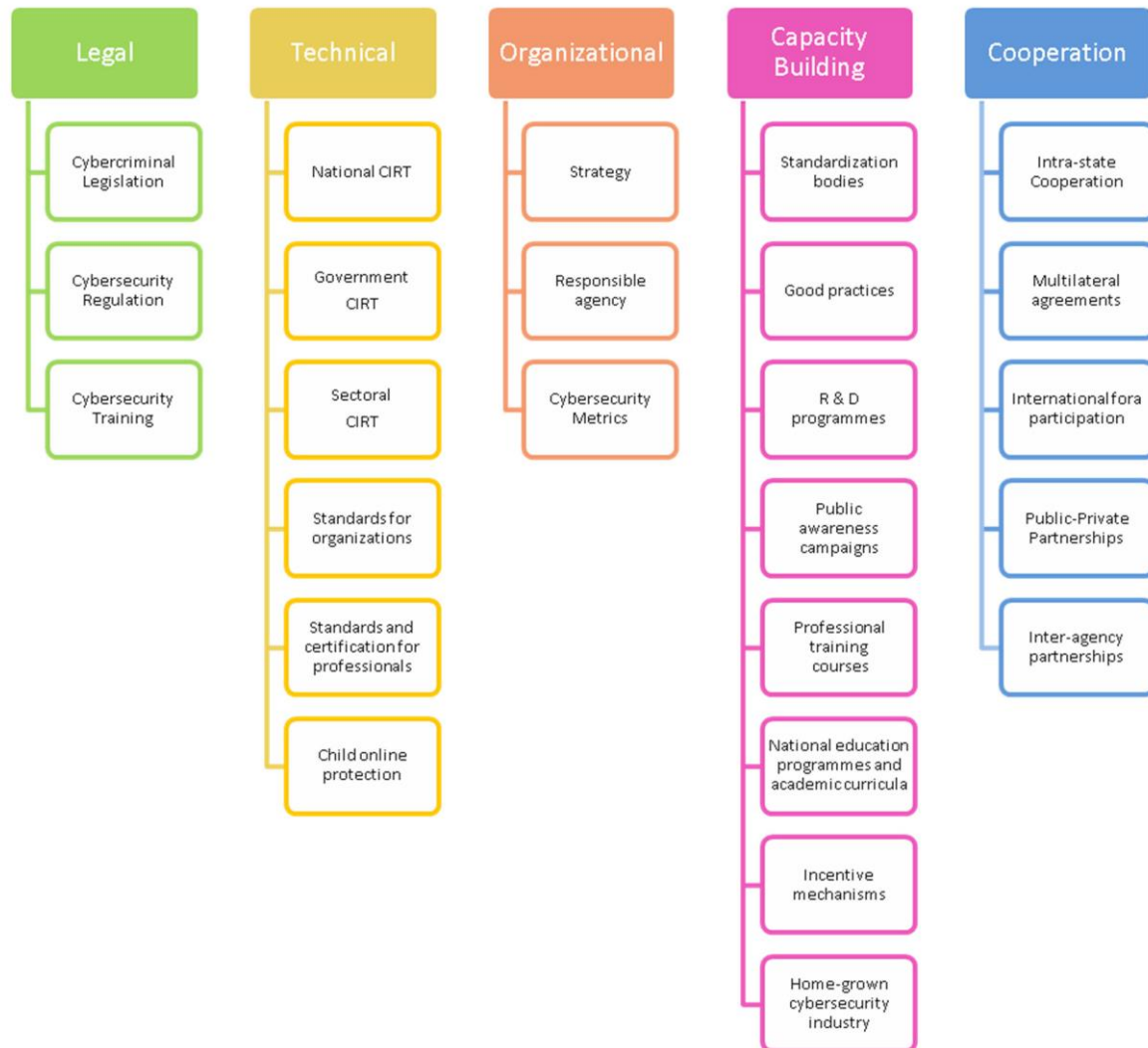
3.3 Conceptual framework

The five pillars of the GCI are briefly explained below:

1. **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.
3. **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
4. **Capacity Building:** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Each pillar was then further divided in sub-pillars (Figure 3.3.1).

Figure 3.3.1: GCI pillars and sub-pillars



The questionnaire was elaborated on the basis of these sub-pillars. The values for the 25 indicators were therefore constructed through 157 binary questions. This was done in order to achieve the required level of granularity and ensure accuracy and quality on the answers.

Figure 3.3.2 below represents all the five pillars from GCA with their indicators.

Figure 3.3.2: GCA tree structure illustrating all pillars (simplified)

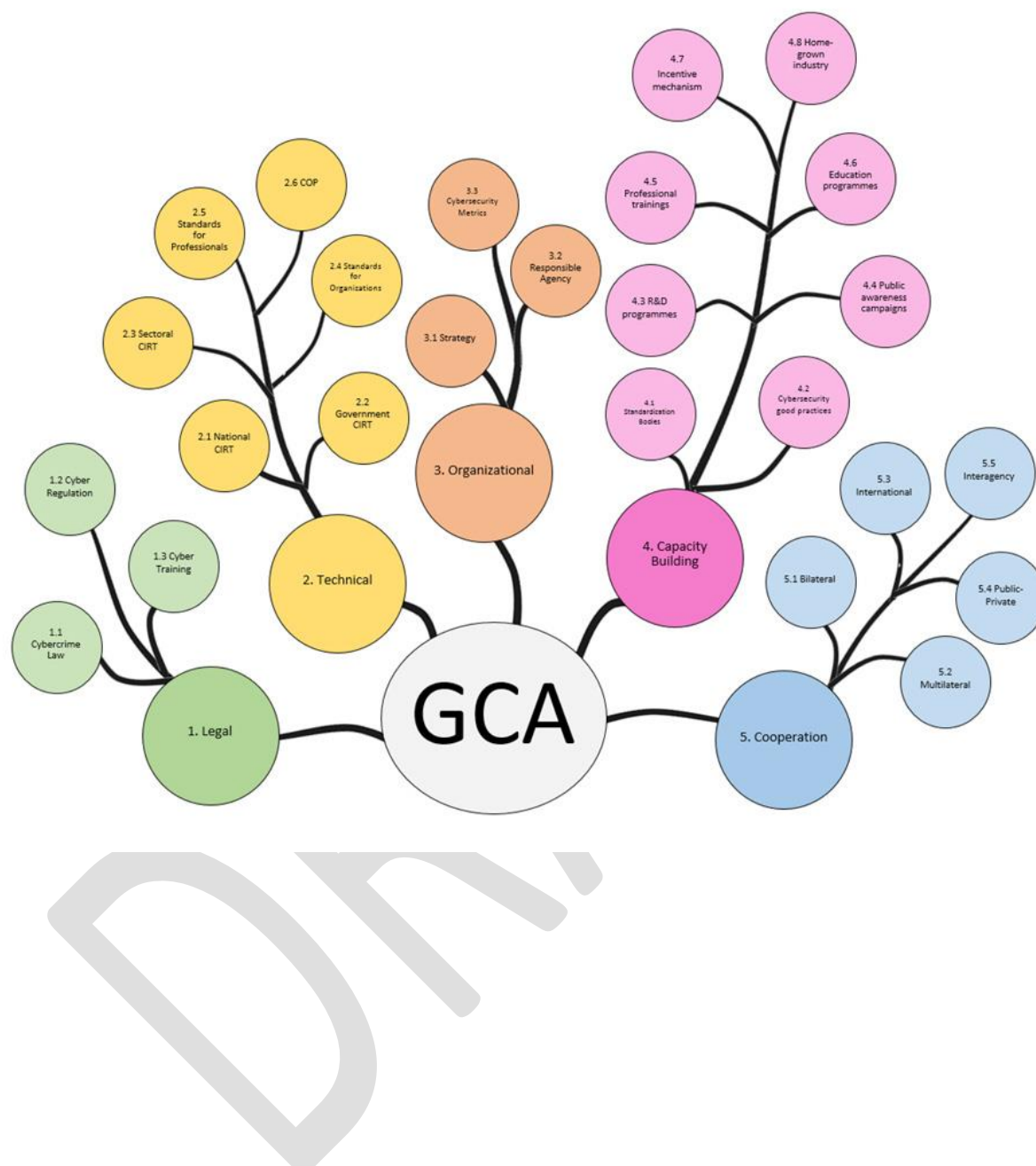
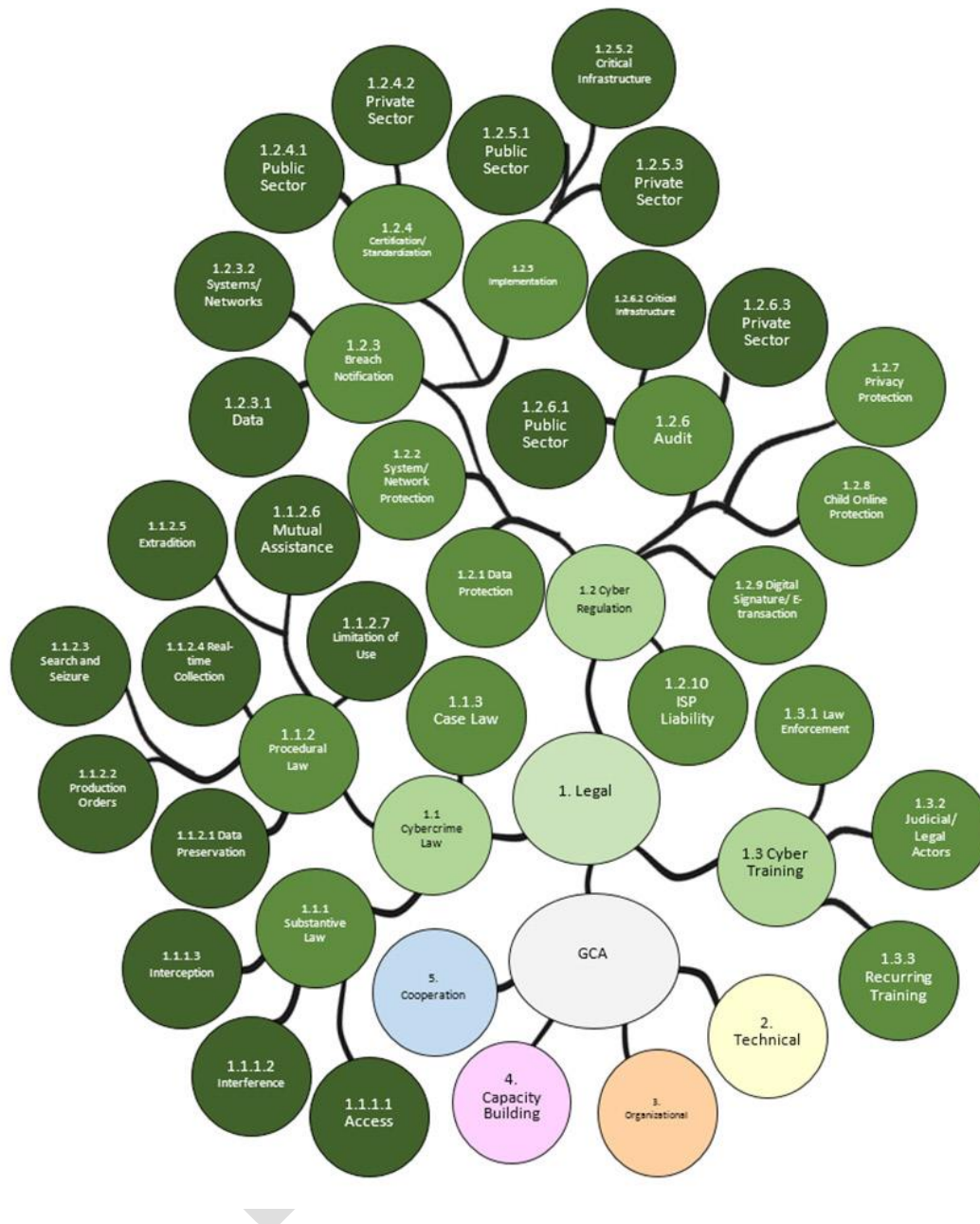


Figure 3.3.3 below illustrates the relationship between the GCA, the pillars, sub-pillars and questions (expanded only for the legal pillar due to space considerations).

Figure 3.3.3: GCI tree structure illustrating Legal pillar



4 Key Findings

This section presents the key findings of the GCI 2017 for the Europe region, which were drawn from the results of the GCI survey conducted in 2016 and presented in 2017 under the five pillars of the GCA agenda: Legal, Technical, Organizational, Capacity building and Cooperation measures. These findings indicate how active and committed the Europe region is to cybersecurity and also present some of the new improvements illustrated in each country.

4.1 Heat Map of National Cybersecurity Commitments

Out of the 43 Member States in Europe, quite a high level of cybersecurity commitment can be observed, especially in the North of Europe, as the heat map below illustrates.

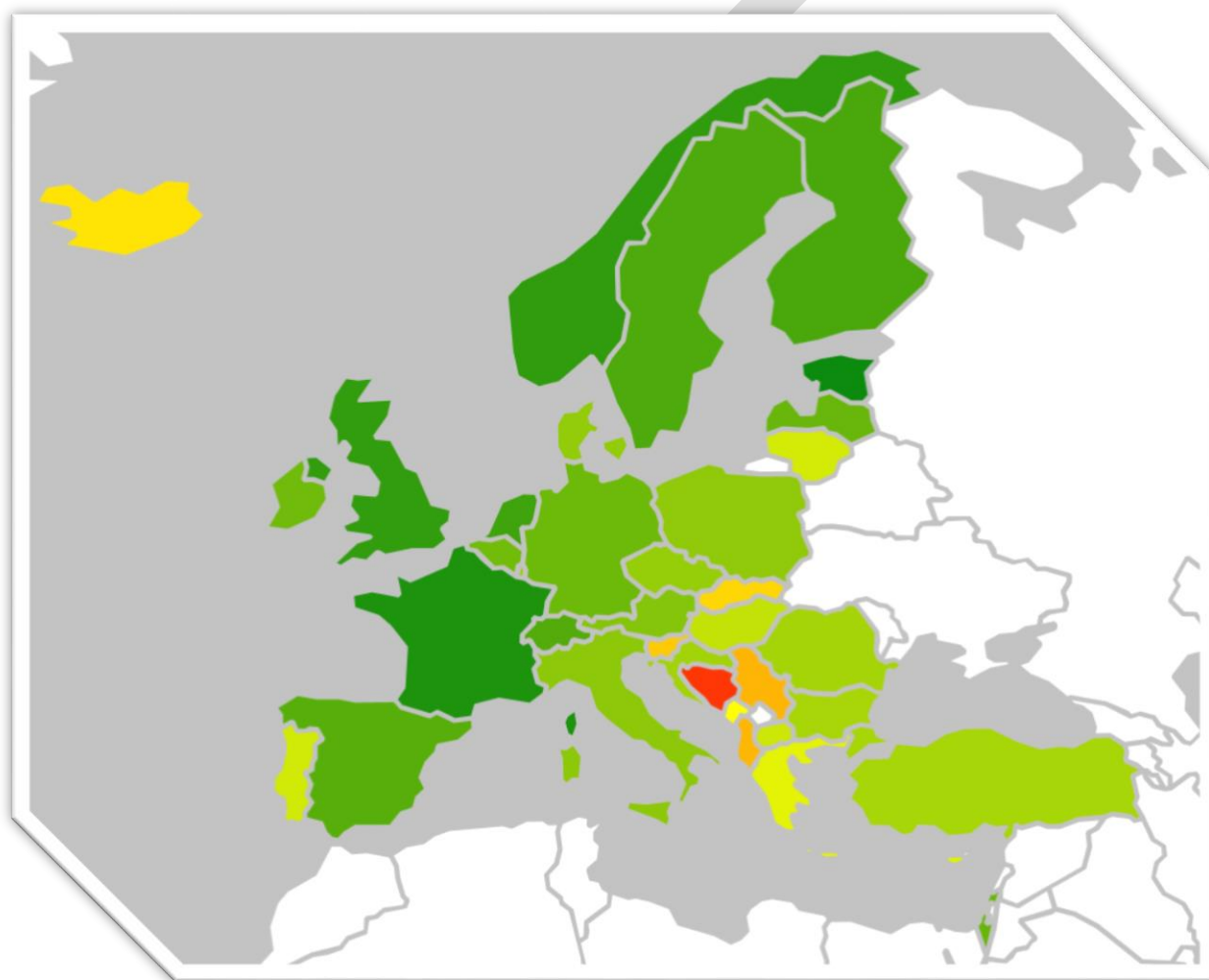


Figure 4.1.1: GCI Heat Map of the Europe region

Level of commitment from Green (highest) to Red (lowest)

4.2 GCI Groups for the Europe Region

Europe's Member States were classified into three categories by their GCI score (Table 4.2.1). The commitment to cybersecurity of the European region is well illustrated in the heat map above and the table, where most countries are in the leading and maturing stages.

- *Leading stage* refers to the 20 countries (i.e., GCI score in the 60th percentile and higher) that demonstrate high commitment.
- *Maturing stage* refers to the 17 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 6 countries (i.e., GCI score less than the 30th percentile) that have started to make commitments in cybersecurity.

DRAFT

Leading stages	
Estonia	Latvia
France	Germany
Norway	Ireland
United Kingdom	Belgium
Netherlands	Austria
Finland	Italy
Sweden	Poland
Switzerland	Denmark
Spain	Czech Republic
Israel	Luxembourg
Maturing stages	
Croatia	Cyprus
Romania	Greece
Turkey	Montenegro
Bulgaria	Malta
Hungary	Iceland
TFYR of Macedonia	Slovakia
Portugal	Slovenia
Lithuania	Albania
	Serbia
Initiating stages	
Monaco	Bosnia and Herzegovina
Liechtenstein	Andorra
San Marino	Vatican

Table 4.2.1: A breakdown for GCI tiers for the Europe Region

4.3 Europe commitment in figures

Below is a table showing how many countries in Europe have a specified cybersecurity indicator out of the 43 countries in the region. This analysis consists of 34 countries that responded to the survey and the information for the remaining 9 countries that was collected by ITU.

Legal in figures:



Technical in figures:



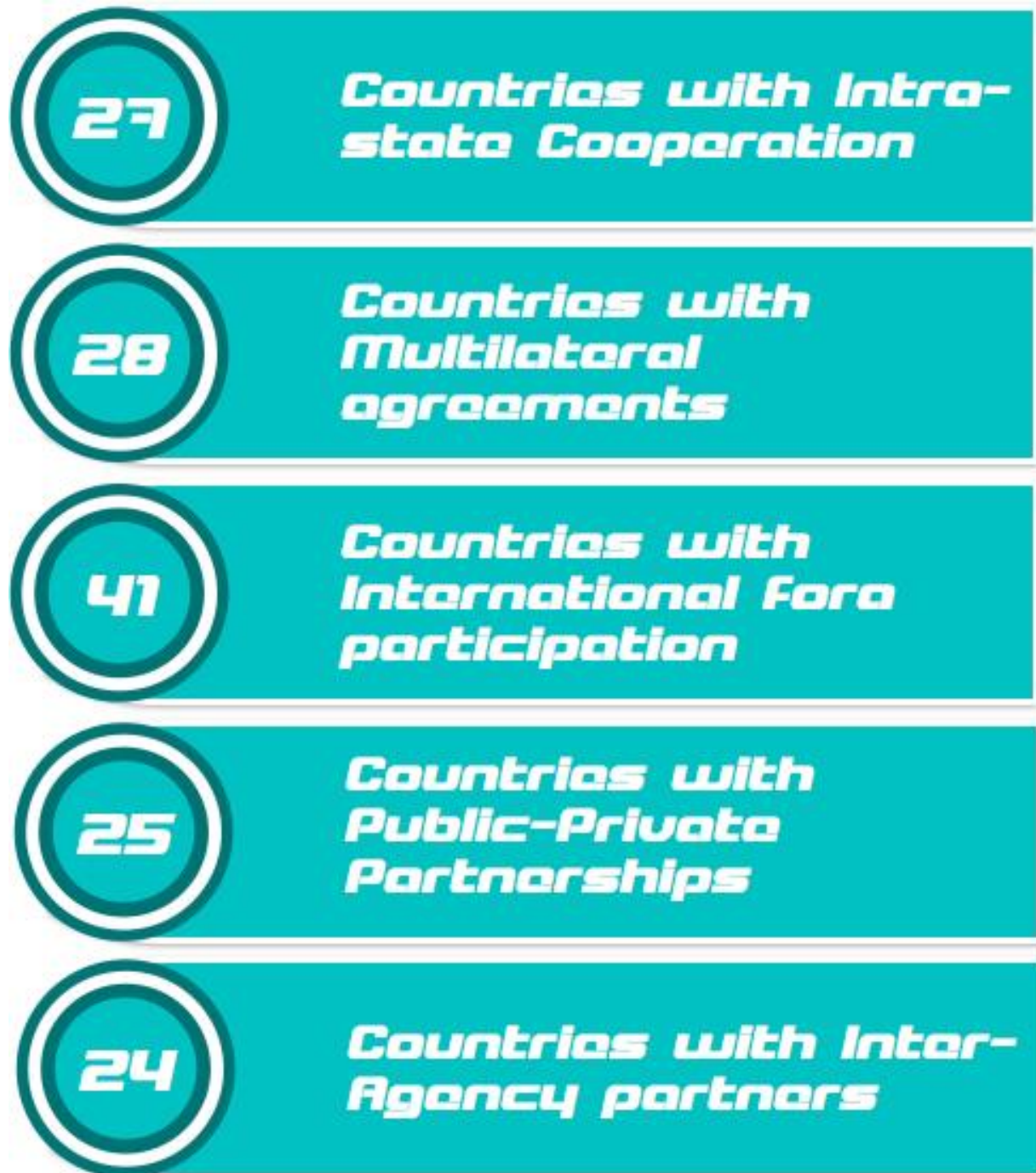
Organizational in figures:



Capacity Building in figures:



Cooperation in figures:



5 Europe region in the Global ranking

Two countries of the Europe region were present in the top ten globally in GCI 2017, showing that Europe is highly committed in cybersecurity actions.

Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
USA	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

Table 5.1: Top ten most committed countries

As the GCI shows, there is a wide gulf in cyber commitment around the globe. This gap exists between and within regions.

Further, cybersecurity related commitments are often unequally distributed with countries performing well in some pillars and less so in others. Cybersecurity is an ecosystem where laws, organizations, skills, cooperation and technical implementation need to be in harmony to be most effective.

Additionally, cybersecurity is not just a concern of the government but also needs commitment from the private sector and consumers. Thus, it is important to develop a cybersecurity culture where citizens can share ideas to improve their nation.

5.1 Comparing Europe with ICT Development Index

A qualitative comparison has been performed to raise awareness of the importance of investing in cybersecurity as an integral component of any national ICT development strategy.

This section is not intended to provide a thorough and exhaustive statistical analysis, but rather an indication on how cybersecurity can relate to existing national processes, in order to emphasize the importance of investing in and being committed to cybersecurity.

Comparing GCI scores to notable ICT for Development Indices does not reveal an especially close relationship, as experience shows that countries which score high in terms of ICT for Development do not necessarily invest in cybersecurity with the same level of commitment, and vice versa.

For example, comparing the GCI with the ITU ICT for Development Index (IDI), shows that some countries are performing much better in the GCI than their level of ICT development

would suggest. The following figures show the comparison between the GCI and IDI, with each graph identifying the top three countries for each region.

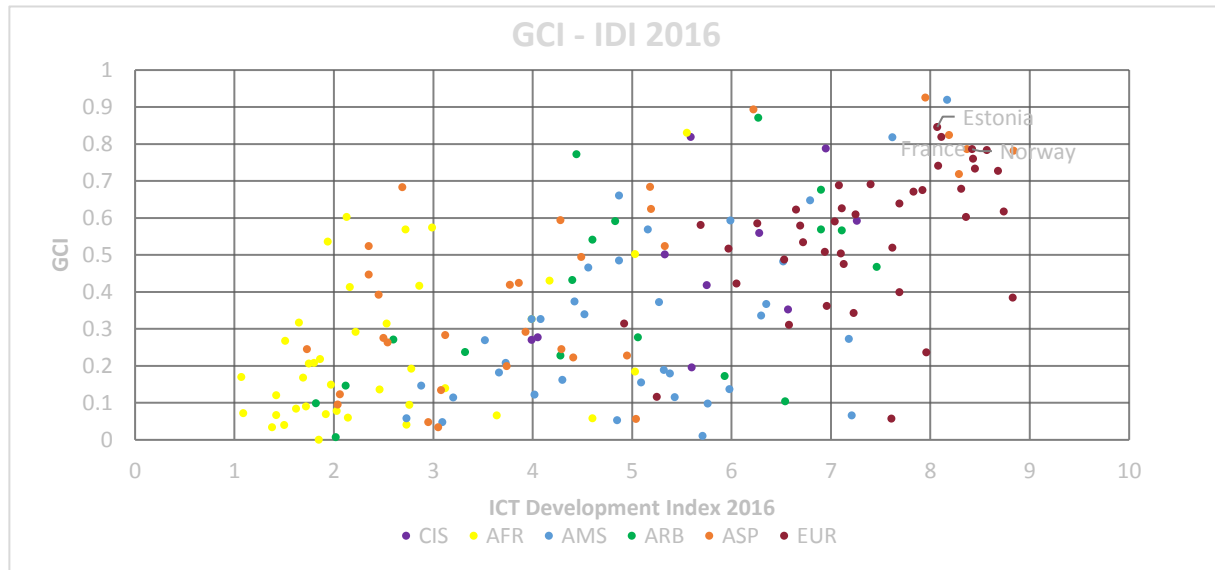


Figure 5.1.1: Global comparison of GCI and IDI

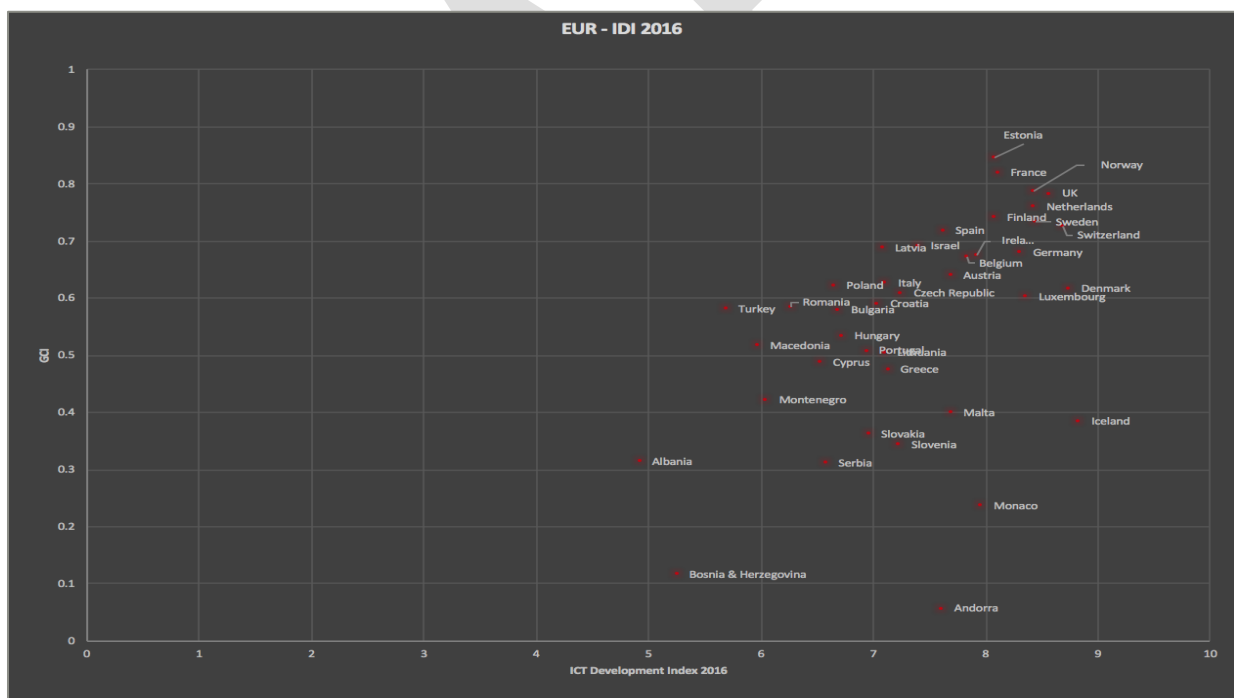


Figure 5.1.2 Comparison of the GCI and IDI in the Europe region

The “regional scorecard” summarizes the countries’ level of commitment to every pillar and sub-pillars (green for high, yellow for medium, and red for low).

	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	LEGAL MEASURES	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	TECHNICAL MEASURES	Strategy	Responsible agency	Cybersecurity metrics	ORGANIZATIONAL MEASURES	Standardization bodies	Cybersecurity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	CAPACITY BUILDING	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Inter-agency partnerships	COOPERATION	GCI
Albania	Red	Yellow	Red	Red	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Andorra	Red	Red	Red	Red	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Austria	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Belgium	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Bosnia and Herzegovina	Red	Yellow	Red	Red	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Bulgaria	Red	Green	Green	Yellow	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Croatia	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Cyprus	Red	Yellow	Green	Yellow	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Czech Republic	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Denmark	Red	Green	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Estonia	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Finland	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
France	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Germany	Green	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Greece	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Hungary	Green	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Iceland	Yellow	Yellow	Green	Yellow	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Ireland	Green	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Israel	Green	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Italy	Red	Green	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Latvia	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Liechtenstein	Green	Yellow	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Lithuania	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Luxembourg	Yellow	Green	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Malta	Red	Green	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Monaco	Yellow	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Montenegro	Red	Yellow	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Netherlands	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Norway	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Poland	Green	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Portugal	Yellow	Green	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Romania	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
San Marino	Yellow	Yellow	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Serbia	Green	Red	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Slovakia	Yellow	Red	Red	Red	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Slovenia	Red	Green	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Spain	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Sweden	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Switzerland	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
The former Yugoslav Republic of Macedonia	Red	Green	Red	Red	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Turkey	Green	Green	Red	Yellow	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
United Kingdom	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow

Figure 5.1.3: Europe region scorecard

6 Regional Outlook

During the active data collection phase of the GCI 2017 exercise, 34 of the 43 European countries responded to the survey.

Figure 6.1 illustrates the average GCI score for all countries in each region for the respective pillar. Scores that fall below the 33rd percentile have a red background, scores that are between the 33rd to 65th percentiles have a yellow background and scores that lie above the 65th percentile have a green background. There is scope for improvement since most regions have an average score for the different pillars (i.e., lying between 33rd and 65th percentiles). For more information on the percentile, refer to the Global Cybersecurity Index report.

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

Figure 6.1: Average pillar scores by region

The exception here is Europe, where average scores are high across all pillars even if a bit lower in the organizational pillar. Given Europe's high level of IT development, it is not surprising that the region overall is doing well in all five pillars of the GCI, despite a few countries in the region with low marks. Below are the top three countries from the European region.



Estonia is the highest-ranking nation in the Europe region. Estonia enhanced its cybersecurity commitment after a 2007 attack. This included the introduction of an organizational structure that can respond quickly to attacks as well as a law that requires all vital services to maintain a minimal level of operation if they are cut off from the Internet⁹. The country also hosts the headquarters of the NATO Cooperative Cyber Defence Centre of Excellence¹⁰.



France is the second highest ranked in the Europe region, scoring a perfect 100 in capacity building. There is widespread cybersecurity training available in the country, and the National Agency for Information System Security (ANSSI in French) publishes a list of dozens of universities that provide recognized accredited cybersecurity degrees¹¹.



Norway is ranked third in Europe with its highest score in the legal pillar. Apart from laws dealing with cybersecurity, Norway has also conducted research on its cybersecurity culture including surveying citizens about the degree to which they will accept monitoring of their online activities.¹²

⁹ <http://www.nextgov.com/cybersecurity/2015/01/heres-what-us-could-learn-estonia-about-cybersecurity/103959/>

¹⁰ <https://ccdcoe.org>

¹¹ <https://www.ssi.gouv.fr/particulier/formations/formation-et-cybersecurite-en-france/>

¹² <https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf>

7 Illustrative practices by pillar

This chapter identifies noteworthy and thought-provoking practices in cybersecurity across the various GCI pillars. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken from their focus areas. The table below shows sub-pillars and Member States who responded positively to having such laws or elements in their public system, compared to the number of countries worldwide.

7.1 Legal

Examples for this pillar illustrate practices in national cybercrime legislation regarding unauthorized access, data and system interference or interception, and misuse of computer systems.

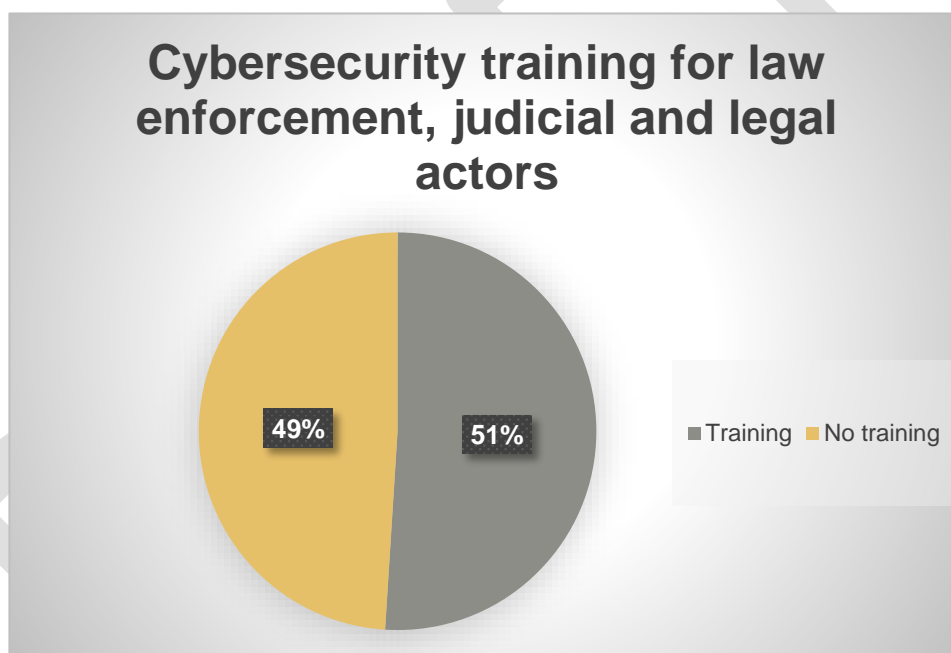




Figure 7.1.1: Cybersecurity training

Europe is generally well committed in this pillar, although there is room for improvement in cybersecurity training. Given that only half of the European Member States have capacity building programs for law enforcement and the judicial system, efforts need to be enhanced, particularly for those who are most likely going to handle cybersecurity crimes (Figure 7.1.1).


On the positive side, those countries who are already providing cybersecurity training always carry out the training exercise on a regular basis for law enforcement as well as other types of legal actors.


7.1.1 Cybercrime legislation

 **Liechtenstein** is excelling in this sector, having all the GCI items such as different substantive laws regarding cybercrime as well as procedural cybercriminal laws¹³.

 In **Norway**, specific legislation and regulation related to cybersecurity has been enacted through the following instruments: Electronic Commence Act; Electronic Communication Act; Personal Data Act; Electronic Signature Act, Act concerning Electronic Money Institutions; Freedom of Information Act; and the Act relating to Protective Security Services¹⁴.


7.1.2 Cybersecurity regulation

 In **Estonia**, regulation on Security Measures for information systems of Vital Services and Related Information assets requires entities engaged in “Vital services” to each appoint an individual to notify the Estonian Information System Authority in the event of a security incident, including cyber security incidents¹⁵.

 **Turkey** has legislation on cybersecurity that can be found in the main website for Turkish laws. Such as on E-Commerce for data, network and system protection, and a regulation that provides details regarding breach notifications. It also has articles concerning the framework for certification and standardization for the public and private sectors. The law requires private sector, public sector and critical infrastructure operators to implement cybersecurity measures.¹⁶

7.1.3 Cybersecurity training

 **Hungary** has training available for law enforcement and the 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)¹⁷.

 In **France**, cybersecurity investigator officers undergo thorough interviews and are trained in methods of investigating cybercrime (first intervention, investigation on the internet and via social networks and Investigation under pseudonym). The cybercrime investigator is ideally a judicial police officer, a quality necessary for the execution of letters rogatory. In addition, they have the computer skills necessary to understand the methods of operation specific to the “cyber” universe¹⁸.

¹³ <https://www.gesetze.li/lilexprod/ifsshowpdf.jsp?lgblid=1988037000&version=16&signed=n&table sel=0>

¹⁴ http://eng.nkom.no/technical/confidentiality-and-privacy/digital-footprints/communications-protection/_attachment/8978? ts=1400a32ce79

¹⁵ https://www.ria.ee/public/KIHK/Security_measures_for_information_systems_of_vital_services_and_related_information_assets.pdf

¹⁶ <http://www.lawsturkey.com/law/5809-electronic-communications-law>

¹⁷ <http://www.nokitc.hu/nokitc/page.php?40>

¹⁸ <http://www.lapolice nationale recrute.fr/Fiches-metiers/Policier-investigateur-en-cybercriminalite>

Note: Below is a table of the legal sub-index and its score is calculated as a weighted average of the three indicators.

Country	Legal score	Cybercriminal legislation	Cybersecurity regulations	Law enforcement training
Estonia	0.991	1.000	0.972	1.000
Belgium	0.968	1.000	0.902	1.000
Norway	0.964	1.000	0.889	1.000
Spain	0.954	1.000	0.860	1.000
France	0.941	0.908	0.925	1.000
Netherlands	0.937	1.000	0.808	1.000
Greece	0.885	0.866	0.803	1.000
Hungary	0.821	0.957	0.501	1.000
United Kingdom	0.819	1.000	0.738	0.680
Sweden	0.803	0.912	0.798	0.674
Austria	0.800	0.862	0.841	0.680
Croatia	0.781	0.680	0.694	1.000
Lithuania	0.765	0.957	0.924	0.354
Finland	0.764	0.687	0.934	0.674
Czech Republic	0.754	0.687	0.605	1.000
Bulgaria	0.716	0.313	0.915	1.000
Latvia	0.681	0.954	0.670	0.354
Romania	0.677	1.000	0.605	0.354
Poland	0.670	1.000	0.908	0.000
Germany	0.670	1.000	0.906	0.000
Switzerland	0.660	0.954	0.605	0.354
Turkey	0.647	0.912	0.937	0.000
Israel	0.622	1.000	0.760	0.000
Luxembourg	0.590	0.680	0.705	0.354
Cyprus	0.577	0.440	0.640	0.680
Liechtenstein	0.571	1.000	0.605	0.000

Country	Legal score	Cybercriminal legislation	Cybersecurity regulations	Law enforcement training
Iceland	0.558	0.680	0.605	0.354
Portugal	0.533	0.634	0.906	0.000
Ireland	0.522	0.733	0.760	0.000
Monaco	0.472	0.588	0.773	0.000
San Marino	0.442	0.737	0.510	0.000
TFYR of Macedonia	0.439	0.500	0.773	0.000
Denmark	0.434	0.459	0.803	0.000
Serbia	0.433	0.908	0.288	0.000
Italy	0.423	0.457	0.773	0.000
Slovenia	0.411	0.453	0.741	0.000
Malta	0.367	0.367	0.705	0.000
Albania	0.310	0.387	0.506	0.000
Slovakia	0.285	0.680	0.095	0.000
Montenegro	0.285	0.320	0.506	0.000
Bosnia and Herzegovina	0.285	0.320	0.506	0.000
Andorra	0.207	0.367	0.213	0.000
Vatican	0.096	0.128	0.146	0.000

Table 7.1.1: Details of legal sub-index and its indicators per country

7.2 Technical

Examples for this pillar illustrate practices in areas such as the existence of technical institutions and industry standards and certification.

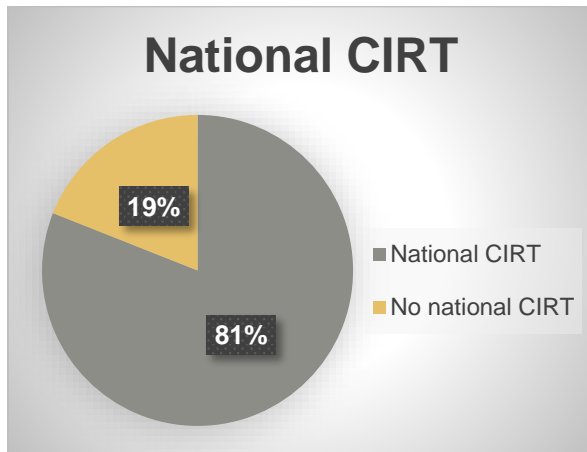


Figure: 7.2.1: National CIRT

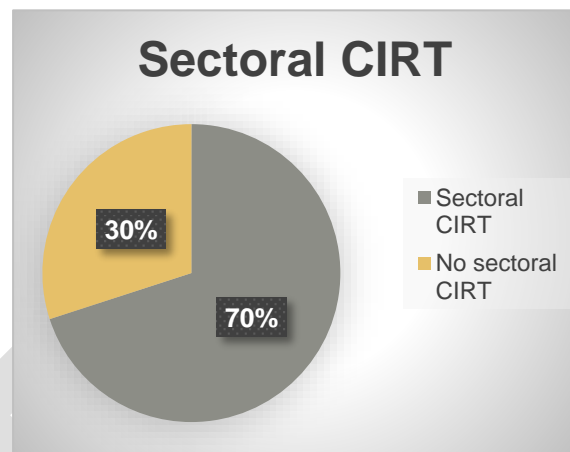


Figure: 7.2.2: Sectoral CIRT

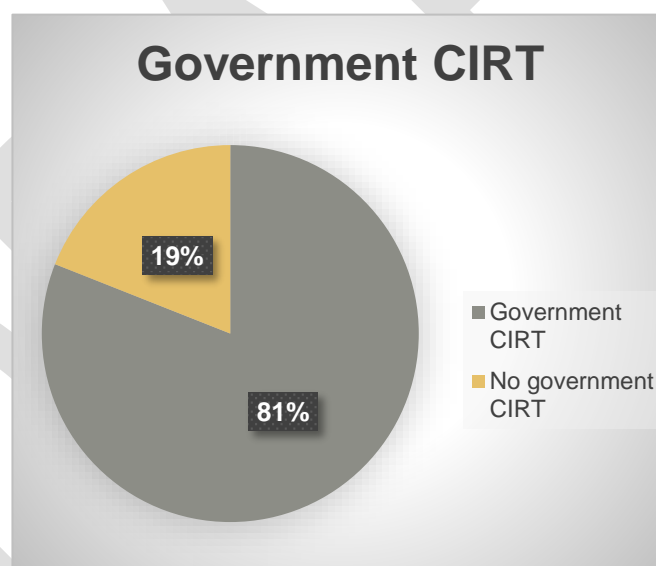


Figure: 7.2.3: Government CIRT

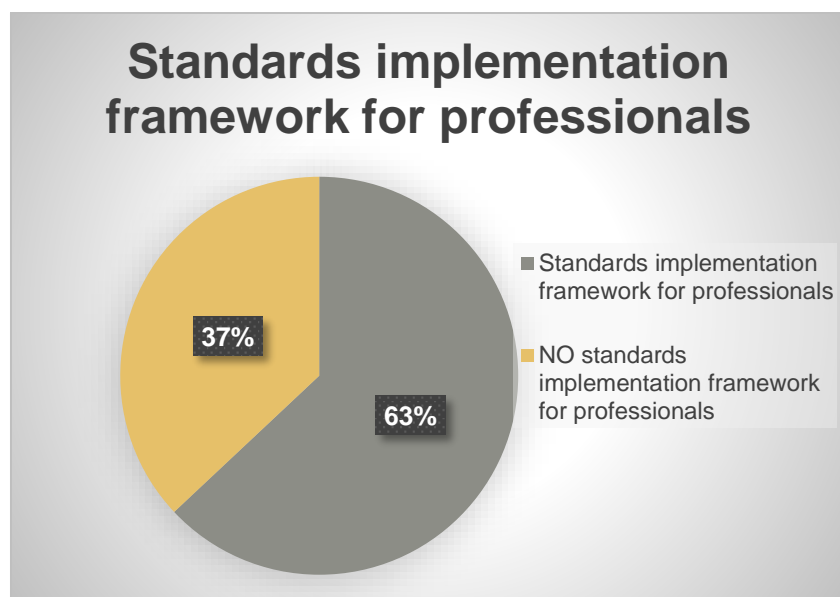


Figure: 7.2.4: Standards implementation for professionals

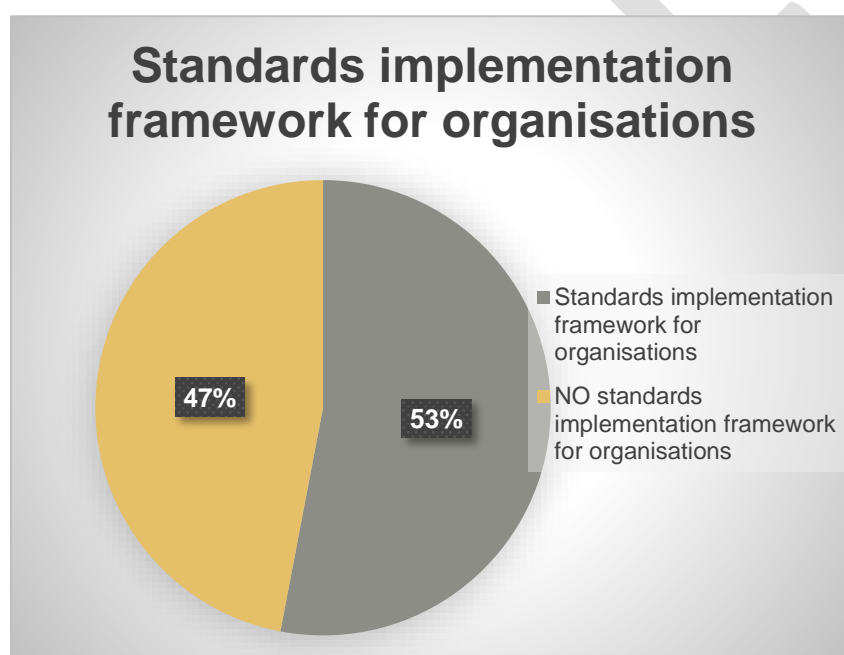




Figure: 7.2.5 Standards implementation framework for organisations


In this pillar, Europe is performing well in the CIRT (Cyber Incident Responses Team) area. Most countries have a national, a governmental and also a sectoral CIRT. The implementation of standards and certification frameworks needs improvement, especially for professionals, given the fact that only 16 countries provide it. Cybersecurity certification is an important component in today's world where hacking has become more and more dangerous and inevitable. It is a way of protecting IoT's, networks and data. Special criteria given by a certifying body enhances the protection of products and services against cyber threats. Increasingly, standards are needed to establish a common language through different cultures and countries. A standard is a framework recognized by a normalization body that provides a consensus on a service or a product and that details also its quality and security.

7.2.1 National CERT/CIRT/CSIRT


 **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 the 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 security¹⁹.

7.2.2 Government CERT/CIRT/CSIRT


 **Luxembourg** created a computer emergency response team (GOVCERT.LU) in 2011 to help in protecting government computer systems and data as well as specific infrastructures and is engaged at both national and international levels under the name of NCERT.LU²⁰. GOVCERT.LU is also a critical player in the event of a large cyber-attack affecting the country's ICT assets.

 **United Kingdom:** In collaboration with the Government Communications Head Quarters (GCHQ)²¹, the National Cybersecurity Centre as part of CyberFirst, supports the development of the UK's next generation of cyber professionals. They also work closely with cyber security educators and researchers to build a cyber-savvy workforce of the future and enhance the UK's knowledge and reputation as a producer of world-leading researchers. As part of the GCT scheme, they offer Certification of Cyber Security Training Courses and each training course is assessed against the nominated area(s) of the Institute of Information Security Professionals (IISP) Information Security Skills Framework²².

7.2.3 Sectoral CERT/CIRT/CSIRT

 **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 entities²³. Its competencies are defined by the "Decision on the establishment of AMRES"²⁴. 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.

7.2.4 Cybersecurity standards implementation framework for organizations

 **Hungary** has national regulations which lay out the framework for information security training for state and local government officials²⁵. The National University for Public Service (NKE) is charged with training and establishing a certification system²⁶. Certificates issued

¹⁹ <https://www.csirt.gov.sk>

²⁰ <https://www.govcert.lu/en/ncert.html>

²¹ <https://www.gchq.gov.uk/>

²² <https://www.gchq.gov.uk/news-article/cyberfirst-girls-competition-finds-worthy-winner>

²³ <https://www.amres.ac.rs/institucije/csirt>

²⁴ https://www.amres.ac.rs/dokumenti/amres/akti/osnivacki-akti/odluka_o_osnivanju_amres_sl_glasnik_28_10.pdf

²⁵ http://njt.hu/cgi_bin/njt_doc.cgi?docid=164331.250717

²⁶ <http://en.uni-nke.hu>

include information security risk assessment and the testing of electronic information systems.

Note: Below is a table of the Technical sub-index and its score is calculated as a weighted average of the six indicators.

Country Score	Technical score	National CIRT	Government CIRT	Sectoral CIRT	Standard implementation framework for organizations	Standards and Certification for professionals	Child online protection
France	0.964	1.000	1.000	1.000	1.000	1.000	0.755
United Kingdom	0.964	1.000	1.000	1.000	1.000	1.000	0.755
Germany	0.964	1.000	1.000	1.000	1.000	1.000	0.755
Ireland	0.910	0.777	1.000	1.000	1.000	1.000	0.755
Austria	0.898	1.000	1.000	1.000	1.000	0.535	0.755
Norway	0.889	1.000	1.000	1.000	0.540	1.000	0.755
Switzerland	0.852	1.000	1.000	1.000	0.540	1.000	0.514
Netherlands	0.848	1.000	1.000	1.000	1.000	0.465	0.490
Hungary	0.823	1.000	1.000	1.000	0.540	0.535	0.755
Estonia	0.822	1.000	1.000	0.000	0.997	1.000	0.755
Czech Republic	0.822	1.000	1.000	1.000	0.997	0.000	0.755
Italy	0.822	1.000	1.000	1.000	1.000	0.000	0.755
Israel	0.800	1.000	1.000	1.000	0.000	1.000	0.755
Denmark	0.800	1.000	1.000	1.000	0.000	1.000	0.755
Turkey	0.786	1.000	1.000	1.000	1.000	0.000	0.514
Portugal	0.758	0.736	1.000	1.000	1.000	0.000	0.755
Finland	0.756	1.000	1.000	0.000	1.000	0.535	0.755
Luxembourg	0.747	1.000	1.000	1.000	0.540	0.000	0.755
Sweden	0.745	1.000	1.000	0.000	1.000	1.000	0.248
Latvia	0.730	1.000	0.000	1.000	1.000	0.465	0.755
Belgium	0.688	0.451	1.000	1.000	1.000	0.000	0.755
Lithuania	0.658	1.000	1.000	1.000	0.000	0.000	0.755
Romania	0.658	1.000	1.000	1.000	0.000	0.000	0.755

Country Score	Technical score	National CIRT	Government CIRT	Sectorial CIRT	Standard implementation framework for organizations	Standards and Certification for professionals	Child online protection
Montenegro	0.658	1.000	1.000	1.000	0.000	0.000	0.755
Slovakia	0.632	1.000	1.000	1.000	0.540	0.000	0.000
Spain	0.622	1.000	1.000	1.000	0.000	0.000	0.514
Poland	0.613	0.451	1.000	1.000	0.540	0.000	0.755
Greece	0.604	0.777	1.000	1.000	0.000	0.000	0.755
Croatia	0.593	1.000	1.000	0.000	0.000	0.535	0.755
Bulgaria	0.551	0.777	1.000	0.000	0.540	0.000	0.755
Malta	0.539	0.509	1.000	1.000	0.000	0.000	0.755
Slovenia	0.452	0.736	1.000	0.000	0.000	0.000	0.755
Serbia	0.415	0.000	1.000	1.000	0.000	0.000	0.755
Cyprus	0.378	0.000	1.000	1.000	0.000	0.000	0.514
Iceland	0.376	0.491	0.000	1.000	0.000	0.000	0.755
Albania	0.343	0.285	1.000	0.000	0.000	0.000	0.755
TFYR of Macedonia	0.268	0.285	1.000	0.000	0.000	0.000	0.266
Liechtenstein	0.142	0.000	0.000	1.000	0.000	0.000	0.000
Bosnia and Herzegovina	0.126	0.000	0.000	0.000	0.540	0.000	0.248
Monaco	0.038	0.000	0.000	0.000	0.000	0.000	0.248
San Marino	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Andorra	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Vatican	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Table: 7.2.1: Details of Technical sub-index and its indicators per country

7.3 Organizational

Examples for this pillar illustrate practices where governments are organized by having a cybersecurity strategy, a coordinating agency and a compilation of indicators for tracking cybercrime.

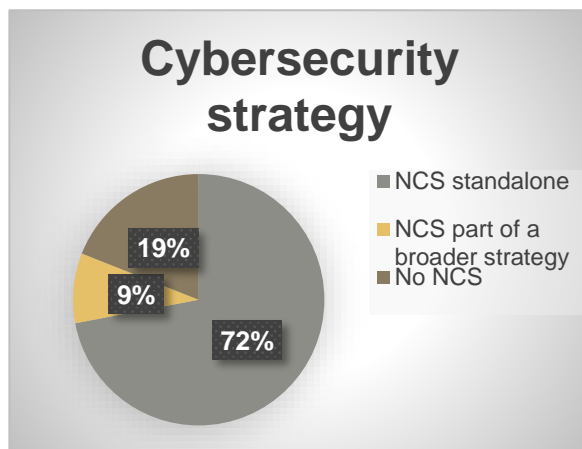


Figure 7.3.3: Cybersecurity strategy

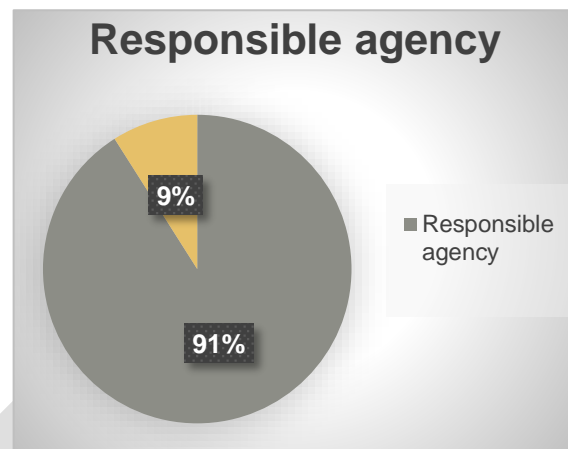


Figure 7.3.1: Responsible agency

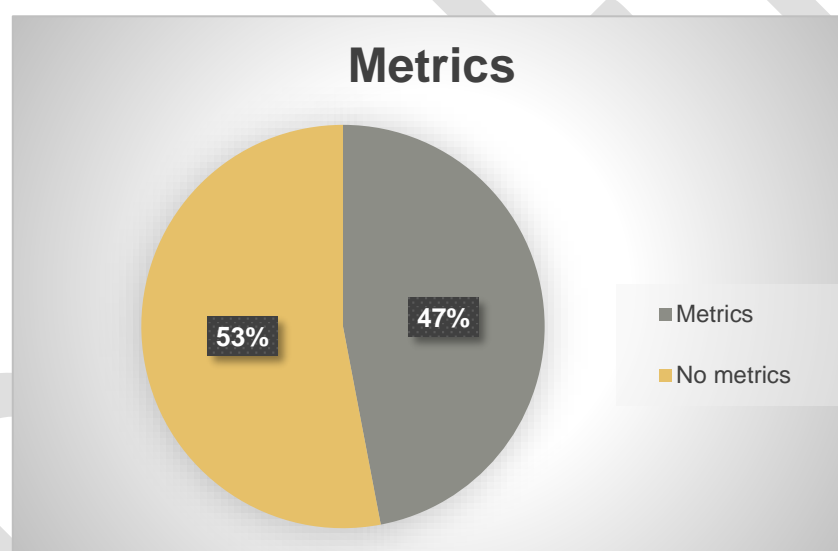



Figure 7.3.2: Metrics

One of the strongest commitments is to outline a cybersecurity strategy describing how the country will prepare and respond to attacks against its digital networks. Most European countries have a NCS (National Cybersecurity Strategy). A NCS is more efficient when it is standalone and includes a section on the protection of Critical Information Infrastructure (CII) as they are vulnerable to cyber-attacks which can be highly damaging to both the private and public sectors. In addition, a National Cybersecurity Strategy should include a resilience plan to foresee externalities/danger in a world of rapidly changing and alarming technologies. In Europe, more than 81% of all countries have a published cybersecurity strategy and 72% of them have a dedicated standalone strategy (Figure 7.3.1).


Regarding metrics used to measure cybersecurity, countries can invest in risk assessment on a regular basis. Effectively, as ICT developments and changes are increasing rapidly, it is not


worthwhile assessing risks, threats and vulnerabilities on a long-term basis. Risk assessment should be done regularly and in the short term with specific benchmarks. Also, the metrics used should be re-evaluated, innovated and improved as needs change with time and cybercrime is always in development. In addition, regular cybersecurity audits are fundamental to help control the quality of cybersecurity services. In Europe, just over 47% of countries release metrics on cybersecurity incidents. Only half possess a strong, regular risk assessment, with benchmarks that are rated and with mandatory regular audits. This challenges countries to objectively assess incidents based on the evidence and determine if protection measures are working.

7.3.1 Strategy


 **United Kingdom** issued its second five year National Cyber Security Strategy in 2016²⁷. 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 strategy.

7.3.2 Responsible agency

 **Spain** established the “Consejo Nacional de Ciberseguridad” in 2013. This council is responsible for reinforcing collaboration, cooperation and coordination between the different public administrations and the private sector regarding cybersecurity. It also provides help regarding the various decisions that need to be taken in the national and international fields²⁸.

 **Iceland** created the Cyber Security Council, appointed by the Minister of the Interior, which is responsible for overseeing the implementation of the National Cyber Security Strategy. In addition, a cyber security forum has been created as a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities.

7.3.3 Cybersecurity metrics

 **Netherlands** uses metrics annually in order to measure cybersecurity development at a national level, summarized in the Cyber Security Assessment Netherlands report²⁹. 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.

²⁷https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

²⁸<http://www.dsn.gob.es/es/sistema-seguridad-nacional/comités-especializados/consejo-nacional-ciberseguridad#collapseTwo>

²⁹<https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html>

Note: Below is a table of the organizational sub-index and its score is calculated as a weighted average of the three indicators

Country	Organizational Score	National Strategy	Responsible Bodies	Cybersecurity Metrics
Estonia	0.846	0.597	1.000	0.998
United Kingdom	0.787	0.613	1.000	0.771
Sweden	0.773	0.403	1.000	0.998
Turkey	0.703	0.613	1.000	0.474
Norway	0.643	0.248	1.000	0.751
Netherlands	0.632	0.391	1.000	0.524
Finland	0.629	0.212	1.000	0.751
France	0.603	0.315	1.000	0.524
Poland	0.581	0.293	1.000	0.474
Spain	0.569	0.248	1.000	0.494
Germany	0.566	0.216	1.000	0.524
Luxembourg	0.563	0.207	1.000	0.524
Israel	0.545	0.347	1.000	0.277
Switzerland	0.539	0.183	1.000	0.474
Czech Republic	0.512	0.282	1.000	0.247
Italy	0.500	0.250	1.000	0.247
Montenegro	0.500	0.250	1.000	0.247
Latvia	0.496	0.426	1.000	0.000
Bulgaria	0.495	0.111	0.500	0.998
Cyprus	0.494	0.422	1.000	0.000
Ireland	0.486	0.399	1.000	0.000
Malta	0.479	0.382	1.000	0.000
Austria	0.470	0.150	1.000	0.277
Slovenia	0.460	0.331	1.000	0.000
Iceland	0.458	0.325	1.000	0.000
Lithuania	0.457	0.324	1.000	0.000
Denmark	0.454	0.107	1.000	0.277
Belgium	0.445	0.293	1.000	0.000
Slovakia	0.416	0.216	1.000	0.000
Romania	0.413	0.207	1.000	0.000

Country	Organizational Score	National Strategy	Responsible Bodies	Cybersecurity Metrics
Croatia	0.404	0.183	1.000	0.000
Hungary	0.402	0.178	1.000	0.000
Portugal	0.391	0.150	1.000	0.000
Greece	0.334	0.000	1.000	0.000
Serbia	0.334	0.000	1.000	0.000
TFYR of Macedonia	0.334	0.000	1.000	0.000
Monaco	0.334	0.000	1.000	0.000
Albania	0.247	0.210	0.500	0.000
San Marino	0.167	0.000	0.500	0.000
Bosnia and Herzegovina	0.070	0.183	0.000	0.000
Liechtenstein	0.000	0.000	0.000	0.000
Andorra	0.000	0.000	0.000	0.000
Vatican	0.000	0.000	0.000	0.000

Table 7.3.1: Details of Organizational sub-index and its indicators per country

7.4 Capacity building

Examples of practices for capacity building include developing the technical and human resources for fighting cybercrime. This includes raising awareness about cybersecurity among the public, the existence of cybersecurity standards, the regulatory bodies, best practices guides, education initiatives and research and development.



Figure 7.4.1: Good practices

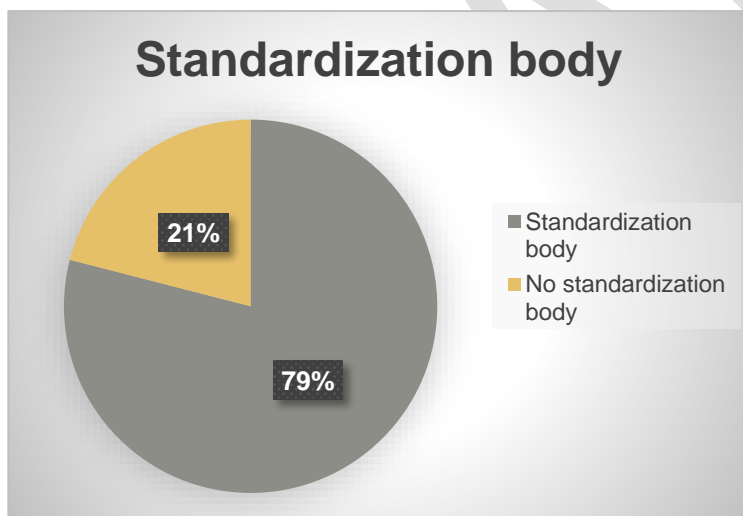


Figure 7.4.2: Standardization body

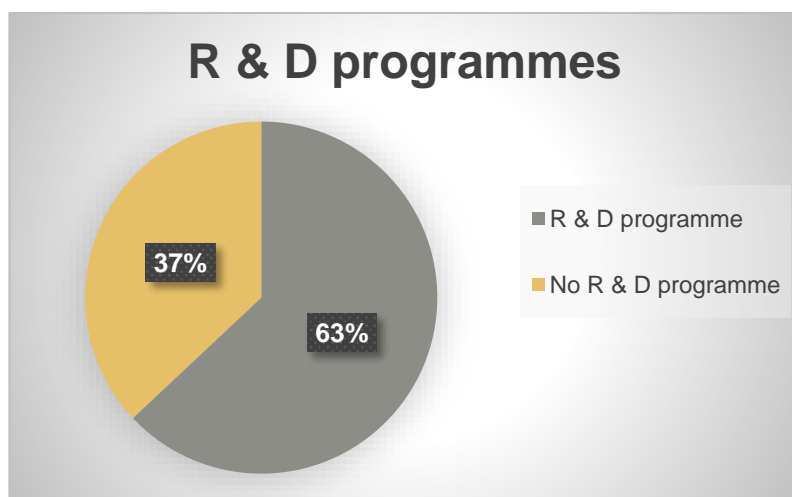


Figure 7.4.3: R & D programmes

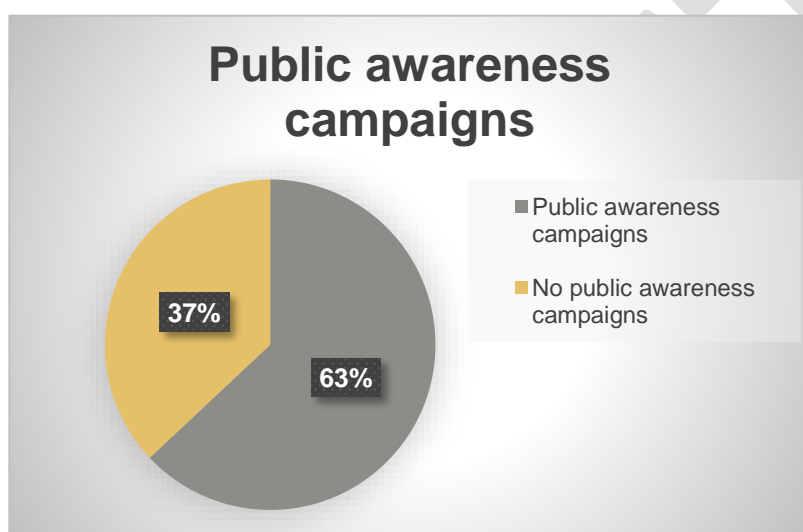


Figure 7.4.4: Public awareness campaigns

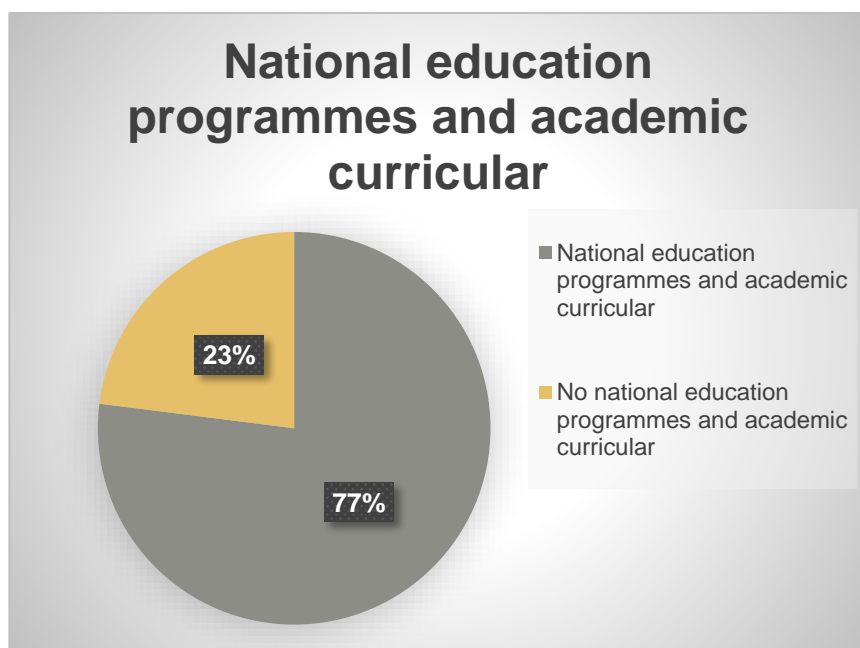


Figure 7.4.5 : National education programmes

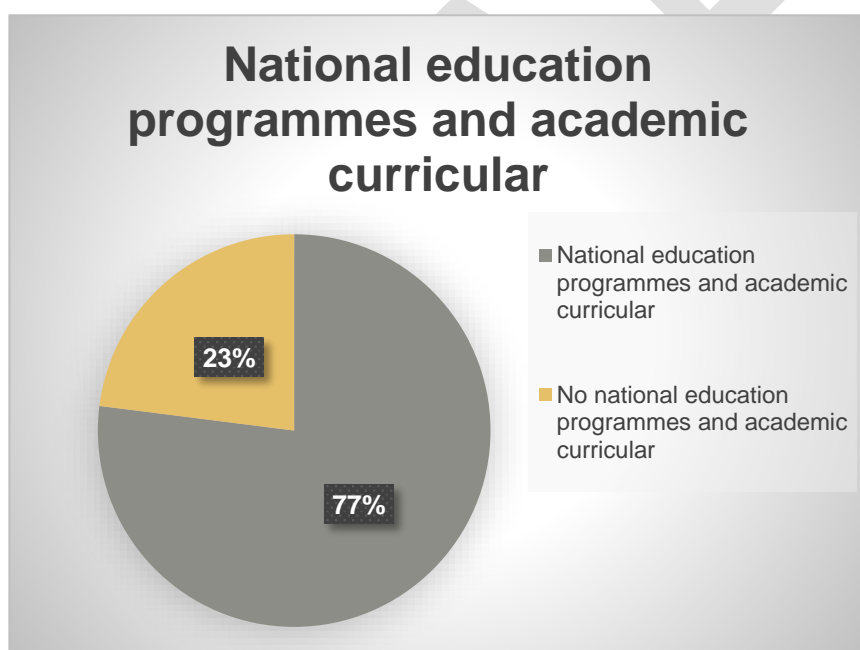


Figure 7.4.5 : National education programmes

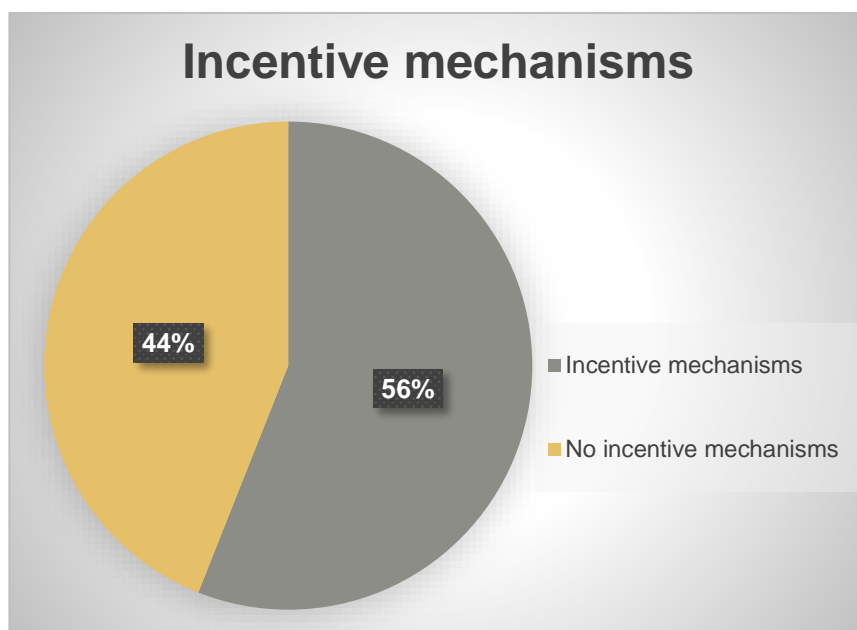


Figure 7.4.6 : Incentive mechanisms



Figure 7.4.7: Professional training courses

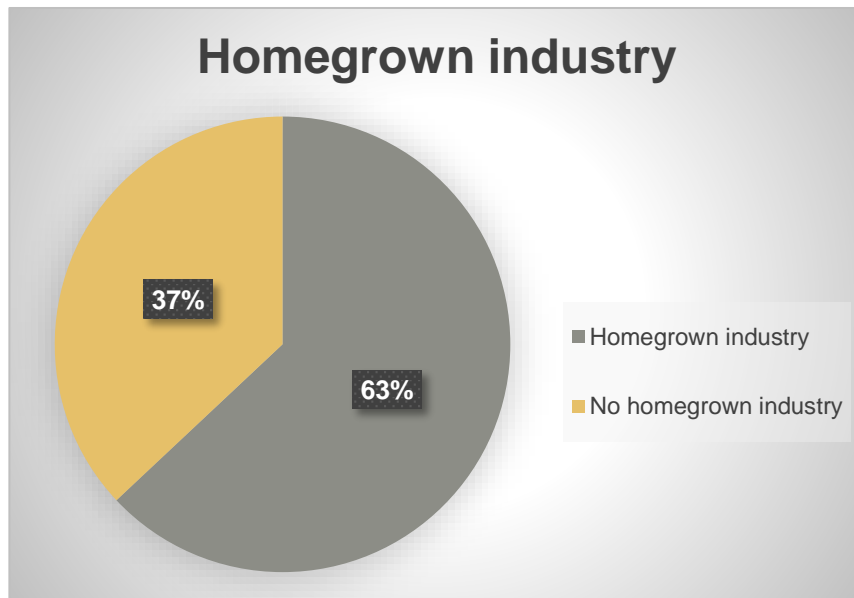


Figure 7.4.8: Home-grown industry


Almost all capacity building sub-pillars have a score above 60%, indicating that they have most of the specified elements.

Having a standardization body is more relevant when the body develops its own standards and adopts international ones. It is advantageous to have a body overseeing research and development programs as well as developing and providing training courses for professional and educational programs for all the different sectors within the country.


Publishing awareness campaigns are exceptionally important but need to be adapted for the different target audiences. Public campaigns are more effective if they deliver free accessible protection programs and software or service based solutions.

Finally, a government needs to encourage homegrown industry and in order to incite society to build a national cybersecurity industry, governments can create incentive mechanisms, such as financial advantages, authorizations etc.

7.4.1 Standardization bodies

 **Romania** created the National Standardization Organization³⁰ 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 standards³¹.

7.4.2 Good practice

 **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

³⁰ <http://www.asro.ro/>

³¹ <http://www.asro.ro/CTmementoSite.html#BM208>

(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 infrastructures³². MELANI is an institution that is open to serve all society to protect against cyber threats. A part of it is a closed section created for CIIIs in order to share encountered issues with the private sector and collaborating to figure out solutions to threats.

7.4.3 Cybersecurity research and development programs



Germany: In 2009 the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior (BMI) signed a cooperation agreement on IT security research. The IT Security Research program covers research and development in new information security technologies. The BMBF has been supporting three research centres since 2011 which bring together leading university and non-university establishments in cybersecurity³³.

7.4.4 Public awareness campaigns



Latvia has published a series of articles on its national CERT portal about free-of-charge security solutions including anti-viruses, firewalls, NoScript, etc.³⁴ Twice a year, the national CERT organizes a campaign where people can bring their computers for a check-up to see if they are infected, and it also distributes commercial anti-virus installations during the campaigns that are made available free-of-charge for one year.

7.4.5 Cybersecurity professional training courses



Bulgaria established the International Cyber Investigation Training Academy in 2009, which is a non-governmental organization³⁵. The academy aims to improve the qualification of specialists working in the field of cybersecurity. It has trained over 1300 people from both the public and private sectors.

7.4.6 National education programs and academic curricula



Belgium's universities offer a great variety of courses concerning various ICT areas such as Informatics, Artificial Intelligence, Crime control in the digital world, Governance, Information Security etc. In addition, Bachelor and Master degrees are both proposed in those areas. Courses related to the cyber world are proposed by more than 10 different universities around Belgium³⁶.

7.4.7 Incentive mechanisms



Israel's Prime Minister's Office has established promotions related to various fields of activity with the private, governmental and academic sectors. For instance, Kidma

³² <https://www.melani.admin.ch/melani/fr/home/generalites-concernant-melani/organisation.html>

³³ <https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html>


³⁴ <https://www.esidross.lv/category/bezmaksas-risinajumi/page/2/>

³⁵ <http://e-crimeacademy.com/>

³⁶ <https://www.b-ccentre.be/education/universities-2/>

(Advancement of Cyber Defense R&D) has been created to prioritize the cyber defense industry and funds have been invested for academic research in the field of cybersecurity in collaboration with the Ministry of Science and Technology. Israel has granted scholarships for students involved in academic degrees in the Cyber field, and adapted programs have been established in the field³⁷.

7.4.8 Home-grown cybersecurity industry

 **Ireland's** economy has the largest proportion of the Information and Communication sector compared to all other countries in Europe and is leveraging that advantage to grow its cybersecurity industry. The country is drawing on existing incentives and attractions with the aim of being a cybersecurity capital³⁸. These incentives include a favourable business environment and low taxes, a talented pool of highly skilled and multilingual workers and a good base for access to European markets³⁹.

Note: Below is a table of the Cooperation sub-index and its score is calculated as a weighted average of the eight indicators

Country	Capacity building scores	Standardization bodies	Good-practices	R & D programmes	Public awareness campaigns	Professional training courses	National education programmes and academic curricula	Incentive mechanisms	Home-grown cybersecurity industry
France	0.999	0.993	1.000	1.000	1.000	0.996	1.000	1.000	0.995
Israel	0.948	0.593	1.000	1.000	0.832	0.996	1.000	1.000	0.995
Estonia	0.941	0.993	1.000	1.000	1.000	0.996	1.000	0.500	0.995
Spain	0.914	0.593	1.000	1.000	1.000	0.996	1.000	1.000	0.448
United Kingdom	0.883	0.993	1.000	1.000	1.000	0.996	1.000	0.000	0.995
Norway	0.876	0.593	1.000	0.653	1.000	0.996	0.700	1.000	0.995
Switzerland	0.813	0.593	1.000	1.000	0.689	0.996	1.000	0.000	0.995
Ireland	0.801	0.593	1.000	0.318	0.922	0.996	1.000	0.500	0.995
TFYR of Macedonia	0.777	0.593	1.000	1.000	1.000	0.996	0.367	0.500	0.547
Latvia	0.745	0.993	1.000	0.664	1.000	0.697	0.633	0.500	0.448
Italy	0.724	0.593	1.000	1.000	0.574	0.996	0.367	1.000	0.000
Denmark	0.709	0.993	1.000	0.682	0.590	0.996	0.367	1.000	0.000
Czech Republic	0.678	0.593	1.000	1.000	0.922	0.697	0.000	1.000	0.000

³⁷ <http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Activities.aspx>

³⁸ <https://www.siliconrepublic.com/companies/cybersecurity-hub-ireland>

³⁹ http://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security/IDA_CYBER_SECURITY.pdf

Country	Capacity building scores	Standardization bodies	Good-practices	R & D programmes	Public awareness campaigns	Professional training courses	National education programmes and academic curricula	Incentive mechanisms	Home-grown cybersecurity industry
Finland	0.669	0.593	1.000	0.664	0.766	0.000	0.367	1.000	0.995
Turkey	0.653	0.993	0.000	0.653	1.000	0.996	0.367	1.000	0.547
Luxembourg	0.644	0.593	0.000	0.664	1.000	0.996	1.000	0.000	0.995
Germany	0.636	0.993	0.000	1.000	1.000	0.996	0.367	0.500	0.448
Croatia	0.635	0.593	0.000	1.000	0.000	0.996	1.000	1.000	0.547
Austria	0.612	0.593	0.000	1.000	1.000	0.363	1.000	0.500	0.448
Belgium	0.605	0.593	1.000	0.000	0.766	0.000	1.000	1.000	0.448
Bulgaria	0.597	0.593	0.000	0.653	1.000	0.996	1.000	0.000	0.547
Netherlands	0.575	0.593	0.000	1.000	0.676	0.996	0.367	0.500	0.547
Sweden	0.547	0.593	0.000	0.664	0.344	0.697	0.367	1.000	0.995
Portugal	0.532	0.000	0.000	0.318	0.766	0.996	1.000	0.500	0.547
Poland	0.531	0.593	0.000	1.000	0.746	0.363	1.000	0.000	0.547
Cyprus	0.528	0.593	1.000	0.318	0.254	0.363	1.000	0.000	0.547
Malta	0.484	0.593	1.000	0.000	0.254	0.363	1.000	0.500	0.000
Romania	0.443	0.993	0.000	0.000	0.922	0.661	0.333	1.000	0.000
Lithuania	0.287	0.000	1.000	0.000	0.234	0.000	0.367	0.000	0.448
Montenegro	0.286	0.593	0.000	0.000	0.000	0.996	0.367	0.500	0.000
Slovakia	0.276	0.593	0.000	0.318	0.000	0.335	1.000	0.000	0.000
Hungary	0.244	0.000	0.000	0.000	0.766	0.363	0.367	0.000	0.448
Slovenia	0.242	0.593	0.000	0.000	0.766	0.363	0.367	0.000	0.000
Greece	0.202	0.593	0.000	0.318	0.512	0.000	0.000	0.000	0.448
Monaco	0.160	0.593	0.000	0.000	0.000	0.000	0.000	1.000	0.000
Albania	0.155	0.000	0.000	0.000	0.508	0.000	0.633	0.000	0.000
Serbia	0.045	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.448
Iceland	0.044	0.593	0.000	0.000	0.000	0.000	0.000	0.000	0.000
San Marino	0.044	0.593	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Liechtenstein	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Bosnia and Herzegovina	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Country	Capacity building scores	Standardization bodies	Good-practices	R & D programmes	Public awareness campaigns	Professional training courses	National education programmes and academic curricula	Incentive mechanisms	Home-grown cybersecurity industry
Andorra	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Vatican	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Table 7.4.1: Details of Capacity building sub-index and its indicators per country

7.5 Cooperation

This pillar considers collaborative efforts across national and international domains and between the public and private sector.



Figure 7.5.1: Participation of international FORA

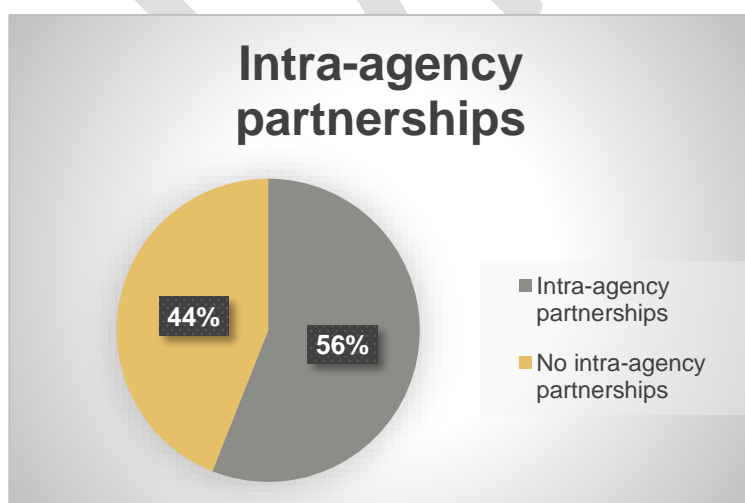


Figure 7.5.2: intra-agency partnerships

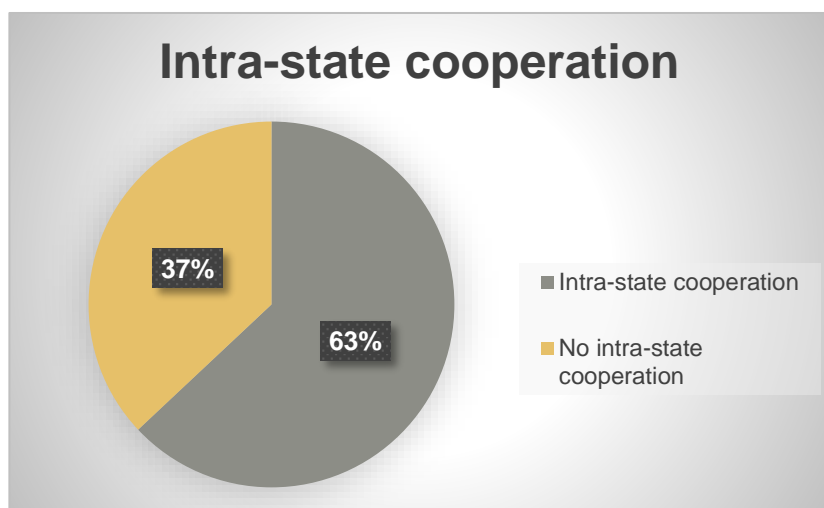


Figure 7.5.3: Intra-state cooperation

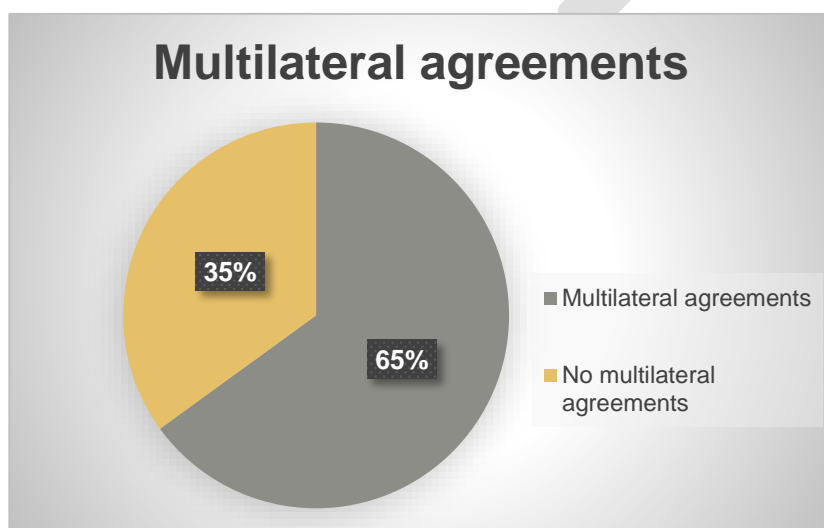


Figure 7.5.4: Multilateral agreements

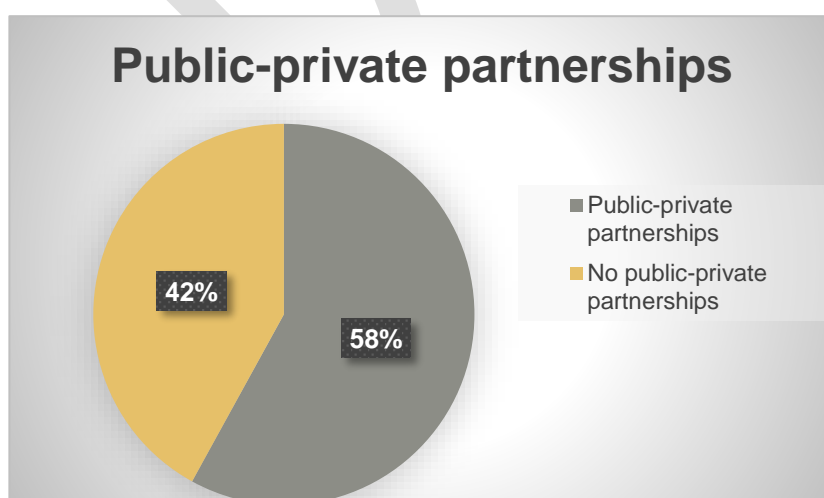



Figure 7.5.5: Public-private partnerships

The potential for cooperation is enhanced by participation in international cybersecurity events, with 95% countries replying affirmatively.






The strengthening of international, regional and national partnerships regarding cybersecurity issues with a view to sharing knowledge and best practices to prevent and combat cybercrime is an essential element in Cybersecurity. The scope of digital space is enormous and international cooperation is therefore required to further facilitate management of cybersecurity systems and make the process durable.

Overall, the importance of cooperation in Europe region is not well reflected. More than a third do not have any bilateral agreements with other regional nations or international organizations, nor multilateral or international agreements with more than two parties. For the Member States which do have an agreement, it is often informal and non-legally binding or pending a further ratification. In addition, almost half of all European countries do not have any partnerships between the public and the private sectors from foreign or local companies.

7.5.1 Intra-State Cooperation


 **TFYR of Macedonia** considers national and international cooperation a priority. It has bilateral agreements with more than 10 European countries and around 20 non-European countries. Also, TFYR of Macedonia is an active member of NATO since 2002 and takes part in International Peace Keeping missions. The EU cooperation is included in the framework of G7 where cybersecurity cooperation and knowledge exchange are already featured, and in bilateral agreements with the US, Japan, Canada, Australia, and India⁴⁰

7.5.2 Multilateral agreements

 **Denmark**,  **Finland**,  **Iceland**,  **Norway** and  **Sweden** collaborate through the Nordic National CERT Collaboration. This includes technical cooperation and cybersecurity exercises to assess and strengthen cyber preparedness, examine incident response processes and enhance information sharing in the region⁴¹.

7.5.3 Participation in international fora

Participation in international cybersecurity events, workshops and training is the one indicator where virtually all countries score high on the GCI. Most countries of the Europe region are members of the Forum of Incident Response and Security Teams (FIRST)⁴² and participate in international fora organized by the International Telecommunication Union.

 The **United Kingdom** is working with a local company Netcraft on cybersecurity initiatives.⁴³ This includes combatting phishing and malware hosted in the United Kingdom as

⁴⁰ http://www.epc.eu/documents/uploads/pub_7739_europeancybersecuritypolicy.pdf

⁴¹ <https://www.msb.se/en/Tools/News/Nordic-cyber-security-exercise-was-conducted-in-Linkoping/>

⁴² www.FIRST.org

⁴³ <https://news.netcraft.com/archives/2016/11/01/the-chancellor-of-the-exchequer-sets-out-plans-for-the-uk-government-to-work-with-netcraft.html>

well as phishing targeting the government⁴⁴. The partnership helped stop 34,550 potential attacks on government departments in the last six months of 2016, or 200 incidents a day.

7.5.4 Public-private partnerships



Finland is an active member of many organizations, such as the Council of Europe (CoE), the Organization for Security and Co-operation in Europe (OSCE) and the United Nations (UN). Finland has also joined the NATO Partnership for Peace and is engaged in cooperation with the organization in, for example, crisis management. There is also local partnership between Finnish company Codenomicon, which later was acquired by Synopsys and which develops the national IDS system and automatic incident reporting service with FICORA⁴⁵

7.5.5 Interagency partnerships



Italy is a Member State of the European Union⁴⁶. In 2016, the European Parliament adopted the Directive on the security of network and information systems (NIS directive) which entered into force in August 2016 for all EU Member States⁴⁷. This directive is the first EU-wide legislation on cybersecurity and has been adopted in order to strengthen Europe's cyber resilience, imposing all Member States to establish a CERT and a NCS. To this end, a EU Platform on Network and Information Security (NIS) has been created⁴⁸.

Note: Below is a table of the Cooperation sub-index and its score is calculated as a weighted average of the five indicators

Country	Cooperation scores	Intra-state Cooperation	Multilateral agreements	International fora participation	Public-Private Partnerships	Inter-agency partnerships
Finland	0.871	0.650	1.000	1.000	1.000	1.000
Netherlands	0.789	1.505	0.724	1.000	0.546	1.000
Latvia	0.784	0.425	0.724	1.000	1.000	1.000
Sweden	0.784	0.425	0.724	1.000	1.000	1.000
Switzerland	0.775	0.341	0.724	1.000	1.000	1.000
TFYR of Macedonia	0.755	1.164	0.724	1.000	0.546	1.000
Romania	0.712	0.766	0.276	1.000	1.000	1.000
Denmark	0.700	0.650	0.276	1.000	1.000	1.000
Poland	0.700	0.650	0.276	1.000	1.000	1.000
Ireland	0.678	0.425	0.276	1.000	1.000	1.000

⁴⁴ <https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk>

⁴⁵ <http://formin.finland.fi/public/default.aspx?nodeid=49303&contentlan=2&culture=fi-FI>

⁴⁶ https://europa.eu/european-union/about-eu/countries/member-countries_en

⁴⁷ <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>

⁴⁸ <http://www.apre.it/media/183485/martinelli.pdf>

Country	Cooperation scores	Intra-state Cooperation	Multilateral agreements	International fora participation	Public-Private Partnerships	Inter-agency partnerships
Italy	0.678	0.425	0.276	1.000	1.000	1.000
Estonia	0.640	1.075	0.276	1.000	0.546	1.000
Belgium	0.632	1.164	0.724	1.000	0.000	1.000
France	0.606	0.734	0.276	1.000	0.546	1.000
Germany	0.575	0.425	0.276	1.000	0.546	1.000
Israel	0.570	0.000	0.000	1.000	1.000	1.000
Norway	0.570	0.000	0.000	1.000	1.000	1.000
Spain	0.537	1.280	0.276	1.000	0.000	1.000
Croatia	0.532	0.000	0.276	1.000	0.546	1.000
Bulgaria	0.532	0.000	0.276	1.000	0.546	1.000
Albania	0.495	0.855	0.276	1.000	0.000	1.000
United Kingdom	0.492	0.425	0.276	1.000	1.000	0.000
Luxembourg	0.481	0.341	0.000	1.000	0.454	1.000
Cyprus	0.452	0.000	0.724	1.000	0.546	0.000
Iceland	0.452	0.000	0.724	1.000	0.546	0.000
Austria	0.430	0.855	0.000	1.000	0.000	1.000
Montenegro	0.394	0.000	1.000	1.000	0.000	0.000
Hungary	0.372	0.425	0.724	1.000	0.000	0.000
Lithuania	0.346	0.650	0.000	1.000	0.546	0.000
Portugal	0.344	0.000	0.000	1.000	0.000	1.000
Greece	0.329	0.000	0.724	1.000	0.000	0.000
Serbia	0.312	0.308	0.000	1.000	0.546	0.000
Czech Republic	0.303	0.425	0.000	1.000	0.454	0.000
Slovakia	0.223	0.000	0.276	1.000	0.000	0.000
Liechtenstein	0.223	0.000	0.276	1.000	0.000	0.000
San Marino	0.189	0.308	0.000	1.000	0.000	0.000
Turkey	0.158	0.000	0.000	1.000	0.000	0.000
Malta	0.158	0.000	0.000	1.000	0.000	0.000
Slovenia	0.158	0.000	0.000	1.000	0.000	0.000
Monaco	0.158	0.000	0.000	1.000	0.000	0.000
Vatican	0.094	0.467	0.000	0.297	0.000	0.000

Country	Cooperati ona scores	Intra-state Cooperation	Multilateral agreements	International fora participation	Public- Private Partnerships	Inter- agency partners hips
Bosnia and Herzegovina	0.086	0.855	0.000	0.000	0.000	0.000
Andorra	0.065	0.000	0.276	0.000	0.000	0.000

Table 7.5.1: Details of cooperation sub-index and its indicators per country

8 Conclusion

The new generation of cybercriminals do not need our approval or awareness to access valuable data, which could lead to the leak of personal data or theft of a large amount of money. As more people are now getting access to the internet all over the world, governments and the private sector need to increase their online presence due to a competitive market and the rapidly changing international scene. However, misuse of computers and communications systems happens every day. The explosion in global connectivity has given rise to the following questions: how do we ensure a state's security and how do we protect businesses in a highly technological age?

According to the analysis and data collected through the GCI survey, the Europe region has reached an advanced stage across all five pillars, with a marginal dip in the capacity building pillar. Improvements are needed in the home-grown industries, sharing of best practices across the different sectors as well as the development of National educational programmes.

The region is quite well advanced in the legal aspect of cybersecurity where all countries have at least cybercriminal laws and regulations. However one area to be improved as regards to the legal pillar would be the proper and continuous training of law enforcement (which includes police officers and enforcement agents, judicial and other legal actors such as judges, solicitors, barristers, attorneys, lawyers, paralegals, etc.).

Noteworthy in the Europe region is the exchange of good practices, policies, and information among Member States, and the aligned cybersecurity policies and strengthened operational cooperation. The EU cooperation with developing countries by providing support with the development of their National Cybersecurity Strategies is also noted. Their cooperation is also included in the framework of the G7, where cybersecurity cooperation and knowledge exchange are already featured, and in bilateral agreements with the US, Japan, Canada, Australia, and India.

A prevailing number of private cybersecurity companies are supported by government agencies concentrated in Europe. This tendency allows them to expand partnerships between Member States and the private sector with the objective of increasing awareness and reducing the risks of cybercrime. Moreover, with its advanced technologies and telecommunication capacity it is essential for Europe to share its best practices and strategies with other countries creating a huge market in cybersecurity and increasing connectivity within the region and globally.

In conclusion, the EU is on the right track, but with digitalization progressing at full speed and the evolving nature of cyber threats, the EU should embed cybersecurity principles in all relevant policies, innovation, investment, as well as in cooperation.

It is essential for the Global Cybersecurity Index to raise awareness of the importance of cybersecurity and promote knowledge exchange on the best practices in the field. In this regard, the ITU welcomes all Member States and industry stakeholders in the European region to actively participate in future efforts to enhance the current reference model. A lack of common approach may challenge the quality of the GCI and cooperation in cybercrime does matter. ITU therefore calls on Member States to take part in the upcoming GCI survey for 2018. Additionally, the ITU would like to thank all Member States and international partners for their valuable contribution to this GCI survey and the publication of this report.

Annex 1: Abbreviations

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Team
FIRST	Forum of Incident Response and Security Teams
GCA	Global Cybersecurity Agenda
GOVCERT	Governmental Computer Emergency Response Team
GCI	Global Cybersecurity Index
ICT	Information and Communication Technology
ITU	International Telecommunication Union
NCS	National Cybersecurity Strategy
UN	United Nations
R&D	Research and Development
NATO	North Atlantic Treaty Organization
ANSSI	National Agency for Information System Security
BMBF	Federal Ministry of Education and Research
NCSC	Nation Cyber Security Centre
IDI	ICT Development Index
GOVCERT.LU	Government Computer Emergency Response Team of Luxembourg
NCERT.LU	National Computer Emergency Response Team of Luxembourg

Annex 2: ITU Member states from Europe - cybersecurity commitment score

Europe Region	Score	Global Rank	Regional ranking
Estonia	0.846	5	1
France	0.819	8	2
Norway	0.786	11	3
United Kingdom	0.783	12	4
Netherlands	0.760	15	5
Finland	0.741	16	6
Sweden	0.733	17	7
Switzerland	0.727	18	8
Spain	0.718	54	9
Israel	0.691	20	10
Latvia	0.688	21	11
Germany	0.679	24	12
Ireland	0.675	26	13
Belgium	0.671	27	14
Austria	0.639	30	15
Italy	0.626	31	16
Poland	0.622	33	17
Denmark	0.617	34	18
Czech Republic	0.609	35	19
Luxembourg	0.602	36	20
Croatia	0.590	41	21
Romania	0.585	42	22
Turkey	0.581	43	23
Bulgaria	0.579	44	24
Hungary	0.534	51	25
TFYR of Macedonia	0.517	55	26
Portugal	0.508	56	27
Lithuania	0.504	57	28
Cyprus	0.487	61	29
Greece	0.475	64	30
Montenegro	0.422	71	31
Malta	0.399	76	32
Iceland	0.384	78	33
Slovakia	0.362	82	34
Slovenia	0.343	84	35
Albania	0.314	89	36
Serbia	0.311	90	37
Monaco	0.236	103	38
Liechtenstein	0.194	112	39
San Marino	0.174	118	40
Bosnia and Herzegovina	0.116	136	41
Andorra	0.057	154	42
Vatican	0.040	161	43

Annex 3: An illustration of all countries in the region and their score for each pillar is presented below.

Country	Legal score	Technical score	Organizational score	Capacity Building score	Cooperation score
Estonia	0.991	0.822	0.846	0.941	0.640
France	0.941	0.964	0.603	0.999	0.606
Norway	0.964	0.889	0.643	0.876	0.570
United Kingdom	0.819	0.964	0.787	0.883	0.492
Netherlands	0.937	0.848	0.632	0.575	0.789
Finland	0.764	0.756	0.629	0.669	0.871
Sweden	0.803	0.745	0.773	0.547	0.784
Switzerland	0.660	0.852	0.539	0.813	0.775
Spain	0.954	0.622	0.569	0.914	0.537
Israel	0.622	0.800	0.545	0.948	0.570
Latvia	0.681	0.730	0.496	0.745	0.784
Germany	0.670	0.964	0.566	0.636	0.575
Ireland	0.522	0.910	0.486	0.801	0.678
Belgium	0.968	0.688	0.445	0.605	0.632
Austria	0.800	0.898	0.470	0.612	0.430
Italy	0.423	0.822	0.500	0.724	0.678
Poland	0.670	0.613	0.581	0.531	0.700
Denmark	0.434	0.800	0.454	0.709	0.700
Czech Republic	0.754	0.822	0.512	0.678	0.303
Luxembourg	0.590	0.747	0.563	0.644	0.481
Croatia	0.781	0.593	0.404	0.635	0.532
Romania	0.677	0.658	0.413	0.443	0.712
Turkey	0.647	0.786	0.703	0.653	0.158
Bulgaria	0.716	0.551	0.495	0.597	0.532
Hungary	0.821	0.823	0.402	0.244	0.372
TFYR of Macedonia	0.439	0.268	0.334	0.777	0.755
Portugal	0.533	0.758	0.391	0.532	0.344
Lithuania	0.765	0.658	0.457	0.287	0.346
Cyprus	0.577	0.378	0.494	0.528	0.452
Greece	0.885	0.604	0.334	0.202	0.329
Montenegro	0.285	0.658	0.500	0.286	0.394

Malta	0.367	0.539	0.479	0.484	0.158
Iceland	0.558	0.376	0.458	0.044	0.452
Slovakia	0.285	0.632	0.416	0.276	0.223
Slovenia	0.411	0.452	0.460	0.242	0.158
Albania	0.310	0.343	0.247	0.155	0.495
Serbia	0.433	0.415	0.334	0.045	0.312
Monaco	0.472	0.038	0.334	0.160	0.158
Liechtenstein	0.571	0.142	0.000	0.000	0.223
San Marino	0.442	0.000	0.167	0.044	0.189
Bosnia and Herzegovina	0.285	0.126	0.070	0.000	0.086
Andorra	0.207	0.000	0.000	0.000	0.065
Vatican	0.096	0.000	0.000	0.000	0.094

Annex 4: Tables and figures

Tables

Table 4.2.1: A breakdown for GCI tiers for the Europe Region

Table 5.1: Top ten most committed countries

Table 7.1.1: Details of legal sub-index and its indicators per country

Table: 7.2.1: Details of Technical sub-index and its indicators per country

Table 7.3.1: Details of Organizational sub-index and its indicators per country

Table 7.4.1: Details of Capacity building sub-index and its indicators per country

Table 7.5.1: Details of Cooperation sub-index and its indicators per country

Figures

Figure 3.3.1: GCI pillars and sub-pillars

Figure 3.3.2: GCA tree structure illustrating all pillars (simplified)

Figure 3.3.3: GCI tree structure illustrating Legal pillar

Figure 4.1.1: GCI Heat Map of the Europe region

Figure 5.1.1: Global comparison of GCI and IDI

Figure 5.1.2 Comparison of the GCI and IDI in the Europe region

Figure 5.1.3: Europe region scorecard

Figure 6.1: Average pillar scores by region

Figure 7.1.1: Cybersecurity training

Figure: **7.2.1: National CIRT**

Figure: 7.2.2: Government CIRT

Figure: 7.2.3: Sectoral CIRT

Figure: 7.2.4: Standards implementation

Figure: 7.2.5 Standards implementation framework for professionals

Figure 7.3.1: Cybersecurity strategy and metrics

Figure 7.3.2: Responsible agency

Figure 7.4.1: Good practices

Figure 7.4.2: Standardization body

Figure 7.4.3: R & D programmes

Figure 7.4.4: Public awareness campaigns

Figure 7.4.5: Professional training courses

Figure 7.4.6: National education programmes

Figure 7.4.7: Incentive mechanisms

Figure 7.4.8: Home-grown industry

Figure 7.5.1: Participation of international FORA

Figure 7.5.2: Intra-state cooperation

Figure 7.5.3: Multilateral agreements

Figure 7.5.4: Public-private partnership

Figure 7.5.5: Inter-agency partnerships

DRAFT