New Direction
the foundation for european reform

CYBERSECURITY EXPENDITURE IN THE EU MEMBER STATES

JOANNA ANTCZAK, KRZYSZTOF KAMIŃSKI

www.europeanreform.org @europeanreform

www.europeanreform.org @europeanreform

New Direction

Established by Margaret Thatcher,
New Direction is Europe's leading free market political foundation & publisher with offices in Brussels, London, Rome & Warsaw.

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
REGISTERED OFFICE: Rue du Trône, 4, 1000 Brussels, Belgium. **EXECUTIVE DIRECTOR:** Naweed Khan.
The European Parliament and New Direction assume no responsibility for the opinions expressed in this publication. Sole liability rests with the author.

AUTHORS

Joanna Antczak

Joanna Antczak holds a PhD degree in economic sciences. She is an assistant professor at the War Studies University in Warsaw, Poland as well as she works as a lecturer at the Vistula Academy of Finance and Business.
Her research and publications pertain to accounting, controlling and financial analysis and bankruptcy risk assessing. She is also interested in economic and defense security of the state, with particular regard to cybersecurity.

Krzysztof Kamiński

Krzysztof Kamiński graduated from the University of Warsaw (Internal Security) and completed the course in The Institute of World Politics in Washington, DC.
He gained his professional experience in energy sector. Currently he serves as President of the Board of the Warsaw Institute. His areas of interest are geopolitics, energy security and public affairs.

TABLE OF CONTENTS

1

INTRODUCTION

Cyberspace is today one of the fastest evolving domains and the ever-changing area of threats that bring increasing losses to national economies, private enterprises and individual citizens. Cyber threats have taken on a strategic character, encompassing the entirety of the state's activities, together with its security and defense system. Both access to the Internet and an opportunity to take advantage of its resources have become a daily routine while bringing about a number of consequences.

Cyber methods are used to influence democratic elections in individual countries. On the other hand, armed forces do their utmost to protect against attacks while developing offensive abilities on the other. Cyber methods are seen as an effective deterrent when making political or military decisions; also, they can be used as a means of a retaliation or response to such actions undertaken by other countries, an example of which are recent changes by the U.S. President Donald Trump who took the decision to give even more freedom when it comes to offensive actions[1].

"Cybersecurity is a classic example of a matter that can neither be analyzed nor solved within one sector exclusively. In order to ensure digital security of the state, institutions and citizens, it is vital to establish both dialogue and partnership among many entities. First of all, a common strategy should be developed in cooperation between representatives of the administration responsible for action plans and entrepreneurs experienced in eliminating online threats. Second, it concerns operational activities undertaken by network administrators of public administration offices and their counterparts in private firms. Therefore such a dialogue cannot be simulated. The European Union and its Member States need to devise a coherent protection system be based on standards that apply to the entities affected by cybersecurity, which are in fact all of us. Cybersecurity is a matter which cannot be considered in isolation."

For example, the cooperation among some Member States was illustrated by the Three Seas Initiative, a group that was inaugurated in August 2016 by presidents of twelve countries. It is an economic and political project aimed at deepening integration processes in region's states while strengthening their position in the European Union and North Atlantic Alliance. The initiative is chiefly to enable collaboration on many levels, guaranteeing common economic, infrastructure and security undertakings.

The European Union is to play a considerable role in the field of cybersecurity. This applies to a regulatory domain as well as financial aid to the Community's scientific and technological potential, with particular regard to innovation, scientific cooperation, strengthening cybersecurity and any actions within the framework of common security and defense policy and counteracting Russian and radical Muslim disinformation online. Therefore it will be vital to plan the EU's Multiannual Financial Framework (MFF) to be properly implemented after 2020.

The following publication will be devoted to the analysis of cybersecurity expenses at the macroeconomic level. Expenditure calculated at the state level is dispersed in various areas, including digital technologies, digitization, development,

1 See also: https://www.whitehouse.gov (National-Cyber-Strategy of the United States of America, p. 21).

economy, science, security and defense, all of which makes it difficult to determine the exact values. There are no comprehensive statistics that would include spending on cybersecurity at various levels, though. Only such rankings and lists are published that partially take into account the use of digital technologies.

Such small countries with limited resources as Estonia and Lithuania are both highly ranked and listed as top states in the field of cybersecurity, which comes as a result of their strategic choices to invest in this domain and their subsequent consequences.

A brief description of the EU countries was made first, followed by a review of international cybersecurity strategies that were quoted in order to analyze the actual cybersecurity situation while the next part of the paper is an attempt to estimate cybersecurity spending in EU Member States. The final chapters contain conclusions and recommendations.

The study was based on such research methods as reports, document analysis, National Cyber Security Strategies and statistical data related to both defense and security.

The following analysis also points to the need to conduct and develop research of both purpose and task-oriented structure of public spending on all cybersecurity-related objectives. The report has a practical character and serves as a reference for discussion on cybersecurity expenditure in the state budget.

Figure 1. European Union

2

CHARACTERISTICS OF THE EU MEMBER STATES

The European Union was founded on November 1, 1993 under the Maastricht Treaty signed on February 7, 1992 while its origins date back to 1951, when Belgium, France, the Netherlands, Luxembourg, Germany, and Italy started economic cooperation.

At present, the European Union is a group of 28 Member States. On June 23, 2016, the EU referendum took place and the people of the United Kingdom voted to leave the community. On March 29, 2017, British Prime Minister officially notified the European Council of the UK's intention to withdraw from the EU and launched the withdrawal process under Article 50 of the Treaty on European Union. For the time being, the United Kingdom remains a full member of the EU and rights and obligations continue to apply in and to the UK.Table 1 presents a brief description of the EU Member States (following the chronological order). Such countries as Denmark, the United Kingdom, Sweden, Poland, the Czech Republic, Hungary, Bulgaria, Romania, and Croatia are EU members but have not adopted the euro as their currency. The Schengen Area includes all European Union countries with the exception of Ireland, the United Kingdom, Cyprus, Bulgaria, Romania, and Croatia. The following EU Member States are part of the North Atlantic Treaty Organization (NATO): Belgium, Denmark, France, the Netherlands, Luxembourg, Portugal, the United Kingdom, Italy, Greece, Germany, Spain, the Czech Republic, Poland, Hungary, Bulgaria, Estonia, Lithuania, Latvia, Romania, Slovakia Slovenia, and Croatia.

If to consider the standard of living, measured as GDP per capita expressed in PPS, the highest results among all country analyzed was recorded by Luxembourg (266) while the lowest by Bulgaria (47). It should be noted that Ireland was ranked second (134). By terms of area, France is the largest country while Malta is the smallest. The most populous member state is Germany while Malta is the least. The EU covers a total of 4,463,600,000 square kilometres.

Table 1. Characteristics of EU countries

Country	Capital city	Currency	Schengen area	Total area (in thousands of square kilometres)	Population	GDP per capita in PPS*
EU accession date: January 1, 1958						
Belgium	Brussels	Euro	Yes	30.5	11,258,434	119
France	Paris	Euro	Yes	632.8	66,415,161	107
Netherlands	Amsterdam	Euro	Yes	41.5	16,900,726	131
Luxembourg	Luxembourg	Euro	Yes	2.6	562,958	266
Germany	Berlin	Euro	Yes	357.3	81,197,537	124
Italy	Rome	Euro	Yes	302.1	60,795,612	96
EU accession date: January 1, 1973						
Denmark	Copenhagen	Danish krone (DKK)	Yes	42.9	5,659,715	125
Ireland	Dublin	Euro	No	69.8	4,628,949	134
United Kingdom	London	Pound sterling (GBP)	No	248.5	64,875,165	109
EU accession date: January 1, 1981						
Greece	Athens	Euro	Yes	132.0	10,858,018	73
EU accession date: January 1, 1986						
Spain	Madrid	Euro	Yes	506.0	46,449,565	91
Portugal	Lisbon	Euro	Yes	92.2	10,374,822	78
EU accession date: January 1, 1995						
Austria	Vienna	Euro	Yes	83.9	8,576,261	130
Finland	Helsinki	Euro	Yes	338.4	5,471,753	110
Sweden	Stockholm	Swedish krona (SEK)	Yes	438.6	9,747,355	123
EU accession date: May 1, 2004						
Cyprus	Nicosia	Euro	No	9.3	847,008	82
Czech Republic	Prague	Czech koruna (CZK)	Yes	78.9	10,538,275	85
Estonia	Tallinn	Euro	Yes	45.2	1,313,271	76
Lithuania	Vilnius	Euro	Yes	65.3	2,921,262	75
Latvia	Riga	Euro	Yes	64.6	1,986,096	64
Malta	Valletta	Euro	Yes	0.3	429,344	84
Poland	Warsaw	Polish zloty (PLN)	Yes	312.7	38,005,614	68
Slovakia	Bratislava	Euro	Yes	49.0	5,421,349	77
Slovenia	Ljubljana	Euro	Yes	20.3	2,062,874	83
Hungary	Budapest	Hungarian forint (HUF)	Yes	93	9,855,571	68
EU accession date: January 1, 2007						
Bulgaria	Sofia	Bulgarian lev (BGN)	No	111.0	7,202,198	47
Romania	Bucharest	Romanian leu (RON)	No	238.4	19,870,647	55
EU accession date: July 1, 2013						
Croatia	Zagreb	Croatian kuna (HRK)	No	56.5	4,225,316	59

* measurement of prices of many goods and services in each country in relation to average income, using a common, contractual currency, referred to as „purchasing power standard" (PPS)

Source: author's own study based on https://europa.eu/european-union/index_pl (DOA: July 19, 2018)

3

CYBERSECURITY STRATEGY OF THE EU MEMBER STATES

EU legal regulation on cybersecurity constitutes important prerequisites for both public and private sectors as well as for citizens of EU Member States.

In 2013, the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, has published a cybersecurity strategy – "An Open, Safe and Secure Cyberspace[2]" – alongside a Commission proposed directive on network and information security. Figure 2 presents the five strategic priorities of the EU Cybersecurity Strategy.

On May 6, 2015, the European Commission presented A Digital Single Market Strategy for Europe.

On September 13, 2017, both the EU Commission and the EU High Representative for Foreign Affairs and Security Policy announced the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[3]".

The first EU-wide act on cybersecurity is Directive (EU) 2016/1148 of the European Parliament and[4] of the Council of 6 July 2016 concerning measures

Figure 2. Strategic priorities for EU cybersecurity strategy

Source: author's own study based on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

2 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, Brussels, May 6, 2015, COM/2015/192 final.

3 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EUJOIN/2017/0450 final.

4 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union L 194/1 of 19 July 2016).

for a high common level of security of network and information systems across the European Union (referred to as The Network and Information Security Directive NIS Directive). The NIS Directive entered into force in August 2016 while EU Member States committed themselves to transpose the regulation into domestic legislation by May 9, 2018.

The Network and Information Security Directive comes as a response to ever-increasing threats in cyberspace. The scope of the NIS Directive seems to cover all issues related to information security, business continuity, system auditing, penetration testing and incident response. All requirements introduced by the Directive show the synergy of solutions with those incorporated by global ISO/IEC 27001 and ISO/IEC 27002 standards that defined the framework of the Information Security Management System.

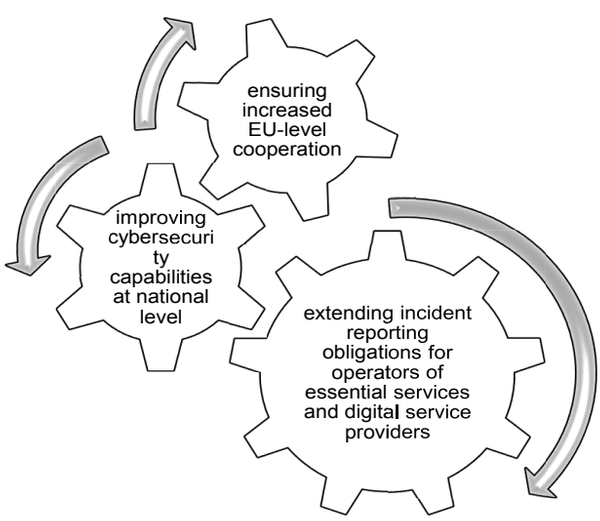
The objectives and core principles of the NIS Directive are set out in Figures 3 and 4.

According to data published by the European Commission on its official website[5], only 15 countries managed to successfully implement the NIS Directive. Such countries as Austria, Belgium, Bulgaria, France, Greece, the Netherlands, Ireland, Lithuania, Luxembourg, Latvia, Romania, and Hungary did not fully transpose the regulation into their local legislation. Figure 5 shows current status of implementation of the NIS Directive in individual EU countries.

In the EU Commission's information note released on September 13, 2017, "the Commission and the High Representative are therefore proposing to reinforce the EU's resilience, deterrence and response to cyber attacks by:

– Establishing a stronger European Union. Cybersecurity Agency built on the Agency for Information and Network Security (ENISA), to assist Member States in dealing with cyber attacks.

Figure 3. Main objectives of the NIS directive



Source: author's own study.

Figure 4. The core of the NIS Directive

Source: author's own study.

Figure 5. Transposition of the NIS Directive

Source: author's own study based on https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

– Creating a EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world.

– A blueprint for how to respond quickly, operationally and in unison when a large- scale cyber attack strikes.

– A network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.

– A new Directive on the counterfeiting of cybercrime.

– A Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.

– The EU aims at driving high-end skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a cyber defense training and education platform[6]".

The EU Commission's information note on cybersecurity identified the following three key areas of cybersecurity:

1. Building EU resilience to cyber attacks and stepping up the EU's cybersecurity capacity.

2. Creating an effective criminal law response.

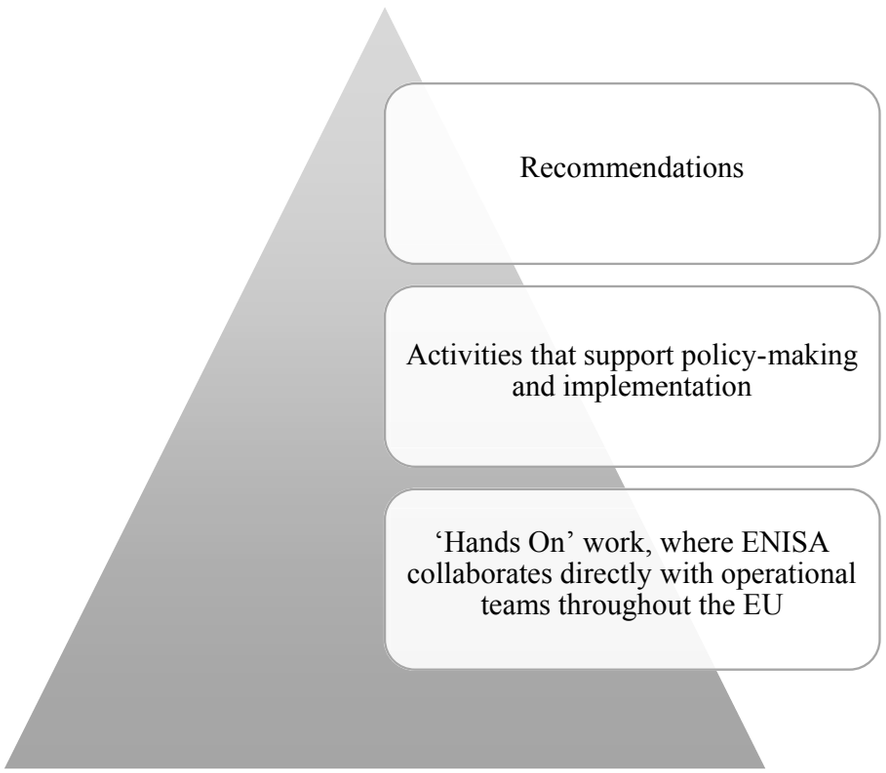
3. Strengthening global stability through international cooperation.

In 2004 the European Union Agency for Network and Information Security (ENISA) was established. It is a center of expertise for cybersecurity in Europe. The Agency is located in Greece with its seat in Athens and a branch office in Heraklion, Crete.

"The Agency works closely with the Member States and the private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National

5 https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.
6 https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf.

Figure 6. ENISA's mission and objectives:



Source: author's own study based on:https://www.enisa.europa.eu/about-enisa

Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS"[7].

Figure 6 illustrates ENISA's approach by presenting its activities in three areas: recommendations, policy implementation and "Hands On" work.

In 2018, ENISA held the fifth Cyber Europe pan-European cyber crisis exercise. Last year's edition was attended by around 900 specialists, from the public authorities and private companies from all EU Member States as well as Norway and Switzerland. The exercise confirmed the effective technical-level cooperation between EU countries. As indicated in an executive summary, this is mainly due to the introduction of the CSIRTs Network in all EU Member States. The main findings of the report[8]:

1. The EU-level technical cooperation has been undoubtedly improved and thus proved efficient. Regular exercises, trainings and communication checks are important in order to keep the knowledge of procedures and usability of cooperation tools at an adequate level.

2. EU-level cooperation at operational-level shall be further developed and tested. This also applies to the interaction between operational and technical levels, and the strategic guidance of higher political management.

3. Countries shall develop national-level procedures and tools for coordinated response, including structured cooperation and information exchange between private actorsand public authorities.

7 https://www.enisa.europa.eu/about-enisa

8 CYBER EUROPE 2018: AFTER ACTION REPORT EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY Findings from a cyber crisis exercise in Europe, ENISA 2018.

Table 2. National Cyber Security Strategy

Country	Strategy status	Implementation date	Number of objectives implemented
Austria	Complete	03/20/2013	12
Belgium	Complete	11/23/2012	11
Bulgaria	Complete	07/18/2016	8
Croatia	Complete	07/10/2015	7
Cyprus	Complete	04/23/2012	10
Czech Republic	Complete	02/16/2015	9
Denmark	Complete	05/01/2018 (past versions: 2015)	11
Estonia	Complete	09/01/2014 (past versions: 2009)	13
Finland	Complete	01/24/2013	14
France	Complete	10/10/2015	13
Germany	Complete	11/07/2016 (past versions: 2011)	9
Greece	Complete	09/21/2017	6
Hungary	Complete	03/21/2013	9
Ireland	Complete	07/20/2015	5
Italy	Complete	41610	15
Latvia	Complete	41645	9
Lithuania	Complete	40544	8
Luxembourg	Complete	01/26/2018	12
Malta	Complete	09/26/2016	6
Netherlands	Complete	04/21/2018 (past versions: 2014 and 2011)	7
Poland	Complete	11/30/2017 (past versions: 2013)	13
Portugal	Complete	05/28/2015	11
Romania	Complete	05/23/2013	11
Slovakia	Complete	06/01/2015 (past versions: 2009)	11
Slovenia	Complete	02/01/2016	10
Spain	Complete	01/03/2013	15
Sweden	Complete	06/22/2017	9
United Kingdom	Complete	11/29/2016 (past versions: 2011)	12

Source: author's own study based on https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

4. IT security shall be identified by the private sector as a priority while firms shall committed to investing in resources and expertise, especially when the services they are providing is essential for the society.

5. Both public and private entities must ensure that they have crisis communication protocols in place and that employees in sensitive positions are aware of these protocols.

6. Cyber Europe has been established as the main EU cyber crisis management exercise. The participants unanimously agreed that the exercise has proven both mature and helpful while shaping cybersecurity levels and it will be continued to keep standards at the highest level.

The NIS Directive was the main legislative proposal under the 2013 EU Cybersecurity Strategy and it lays down - amongst other measures - obligations for all

Table 3. Thematic scope of the National Cyber Security Strategy

Country	Addressing cybercrime	Keeping balance between security and privacy	Citizen's awareness	Critical Information Infrastructure Protection	Developing national cyber contingency plans	Engaging in international cooperation	Establishing a public-private partnership
Austria	X			X	X	X	X
Belgium	X		X	X		X	X
Bulgaria	X	X	X			X	
Croatia	X	X				X	
Cyprus	X		X	X	X	X	X
Czech Republic		X	X	X		X	X
Denmark	X		X	X	X	X	
Estonia	X	X	X	X	X	X	
Finland	X	X	X	X	X	X	X
France	X	X	X	X	X	X	
Germany	X		X	X	X	X	
Greece	X		X			X	
Hungary				X	X	X	
Ireland					X	X	
Italy	X	X	X	X	X	X	X
Latvia	X	X	X	X	X	X	
Lithuania	X		X	X	X	X	
Luxembourg	X		X	X	X	X	X
Malta	X		X			X	
Netherlands	X			X		X	X
Poland	X		X	X	X	X	X
Portugal	X	X	X	X		X	
Romania	X		X	X	X	X	X
Slovakia			X	X		X	X
Slovenia	X	X	X	X		X	
Spain	X	X	X	X	X	X	X
Sweden	X	X		X	X	X	X
United Kingdom	X		X	X		X	X

Establishing an incident response capability	Establishing an institutionalized form of cooperation between public agencies	Establishing baseline security requirements	Establishing incident reporting mechanisms	Fostering R&D strategies	Holding cybersecurity exercises	Providing incentives for the private sector to invest in security measures	Strengthening training and educational programs
X	X	X	X	X	X		X
X	X			X	X		
X			X	X			X
X		X	X	X			
X	X				X		X
X	X			X	X		
X		X	X	X	X		X
X	X	X	X	X	X		X
X		X	X	X	X	X	X
X	X	X	X	X	X		X
X	X	X		X			
X			X		X		
X	X	X	X		X		X
X			X		X		
X	X	X	X	X	X	X	X
X		X					X
X		X					X
X	X	X	X		X		X
X			X				X
X		X					X
X	X	X	X	X	X		X
X		X	X	X	X		X
X		X	X	X			X
X	X	X	X	X	X		X
X	X		X		X		X
X	X	X	X	X	X	X	X
				X	X		
X	X	X	X	X	X		X

Source: author's own study based on https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

EU Member States to adopt a national strategy on the security of network and information systems. ENISA is supporting the EU. Member States since 2012 to develop, implement and evaluate their National Cyber Security Strategies (NCSS). All Member States have developed their own NCSS[9].

Table 2 presents when individual EU countries implemented cybersecurity strategies along with issues they were related to. Table 3 illustrates a thematic scope.

It shall be noticed that all EU Member States dispose of their own cybersecurity strategies. In some countries, including Denmark, the United Kingdom, Poland, Slovakia, Germany and Estonia, they have been accordingly amended over the years. Among the countries that have introduced most issues to their regulations are Spain (15), Italy (15), Finland (14), Poland (13), France (13), and Estonia (13). The lowest number of amendments was implemented by Ireland (5), Greece (6), Netherlands (7), and Croatia (7).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) entered into force on May 25, 2018. The Regulation covers all public and private entities that process personal data and most of the data processing processes.

It is worth to note the following two cybersecurity initiatives:

- Back in July 2017, the European Commission and the European Cyber Security Organisation (ECSO) signed a joint agreement on implementing the EU's Horizon 2020 initiative in the form of public-private partnership.

- In June 2018, the European Commission proposed the "Digital Europe" program, aimed at increasing and maximizing the benefits of digital transformation for EU citizens and businesses in all relevant EU policy areas, mainly by strengthening policies and fostering the ambitions of a digital single market.

9 https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

4

MAIN GOALS OF NATIONAL CYBERSECURITY STRATEGIES IN THE EU MEMBER STATES

In the framework of its Cyber Security Strategy, **Austria** pursues "the following strategic goals:

- Availability, reliability and confidentiality of data exchange as well as the integrity of data themselves are guaranteed only in a secure, resilient and reliable cyber space. Therefore, the virtual space must be capable of resisting risks, absorbing shocks and adjusting to a changed environment. The design of crucial ICT systems should be as redundant as possible.

- Based on the national approach of the competent federal ministries, Austria will ensure that its ICT infrastructures are secure and resilient to threats. The governmental bodies will cooperate closely and as partners with the private sector.

- The legal asset "cybersecurity" is protected by the Austrian authorities – in cooperation with non-governmental partners – by taking effective and proportionate measures in the field of political-strategic control, recognition and response as well as limitation of effects and restoration.

- By taking a number of awareness measures, Austria is building a "culture of cyber security".

- In the framework of a national dialogue on cybersecurity, existing cooperation is strengthened and new initiatives are supported and interlinked by building knowledge, capabilities and capacities. Thanks to this approach, Austria is acting as a pioneer in implementing measures to secure the digital society. Offering high levels of availability, integrity and confidentiality of required ICT infrastructures, Austria's attractiveness as a business location is also enhanced.

- Austria will play an active role in international cooperation at European and global level, particularly by exchanging information, formulating international strategies, developing voluntary schemes and legally binding regulations, prosecuting criminal cases, holding transnational exercises and conducting cooperation projects.

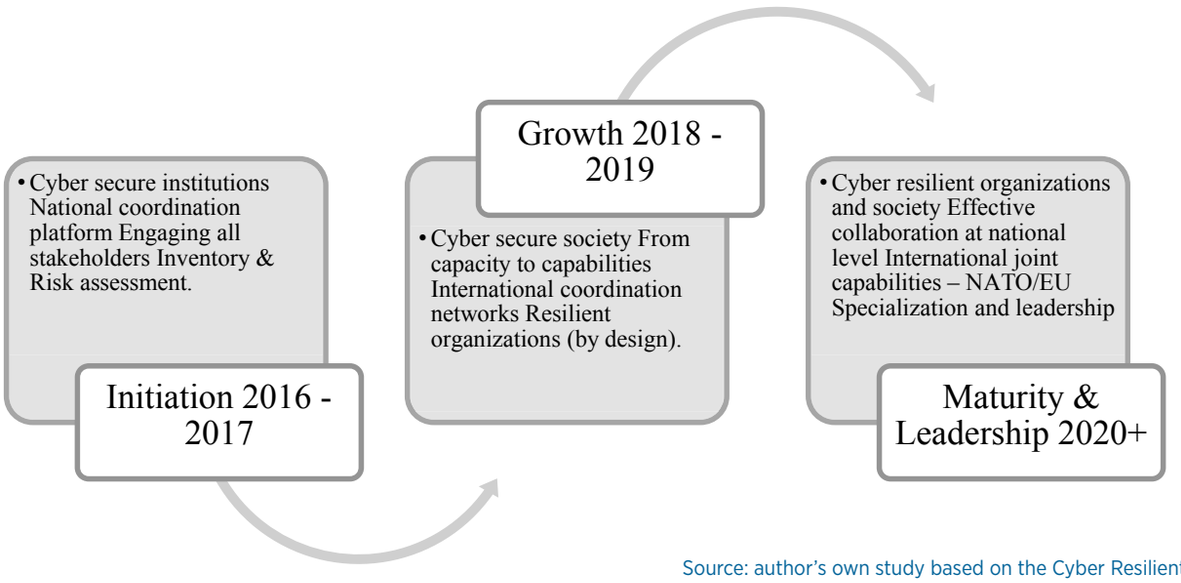
- The Austrian administration's e-government is secure and continuously further developed; the security measures of the Federal Republic of Austria, the federal provinces, cities and municipalities will be strengthened.

- All Austrian enterprises will protect the integrity of their own applications as well as the identity and privacy of their customers. The close and systematic cooperation among enterprises plays a crucial role in this process.

- The Austrian population should be aware of the individual's personal responsibility in cyberspace. All citizens should ensure adequate protection of their online activities and have the necessary capabilities for electronic authentication and signature"[10].

10 Austrian Cyber Security Strategy, Vienna, 2013, pp. 9-10.

Figure 7. Bulgarian National Cyber Security Strategy



Source: author's own study based on the Cyber Resilient Bulgaria 2020 National Cyber Security Strategy.

Bulgarian National Cyber Security Strategy presents three stages to be implemented within five years (Figure 7).

On February 16, 2015, the **Czech** government approved the new National Strategy for Cybersecurity for 2015-2020, a document which consists of a comprehensive set of measures aimed at achieving the highest possible cybersecurity level in the Czech Republic.

The main goals to be achieved within five years are a key part of the strategy. "They are divided into the following priority areas:

1. Ensuring efficiency and strengthening of all structures, processes and cooperation in the field of cybersecurity.
2. Active international co-operation.
3. Protection of the national Critical Information Infrastructure and Important Information Systems.
4. Co-operation with private sector.
5. R&D/Consumer's trust.
6. Support to the education, awareness and the development of the information society
7. Support for the development of police's capabilities to investigate and prosecute information crime.
8. Cybersecurity legislation (development of legislative framework). Participation in the creation and implementation of European and international regulations"[11].

The National Agency for Cybersecurity and Information was formed in August 2017.

Croatian National Cyber Security Strategy's "fundamental role is to connect and bring mutual understanding of complex issue cybersecurity in various sectors of the society and among various bodies and legal entities as the stakeholders of Strategy with different competences, responsibilities, tasks, needs, expectations and interests. This is particularly important for ensuring the required level of understanding of the complex operational and technical issues of cyber security, which is necessary for the central public authorities and decision makers in all the sectors of the society, as it is for the security of the citizens, prosperity of the entire society, and thus for the end goal of the Strategy: implementing the law and respecting all the fundamental human rights in the new, virtual dimension of the society.[12]"

11 https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/czech-republic-national-cyber-security-strategy-2015-2020, (DOA: August 19, 2018).
12 The National Cyber Security Strategy of Croatia, Zagreb, October 7, 2015 (Official Gazette No 108/2015) - p. 4.

The structure and contents of **Cyprian** National Cyber Security Strategy are based on the following guiding principles:

- "the development of strategy and policy within a framework of cooperation between all competent authorities, taking into account the competences of each governmental stakeholder, the development of a holistic approach to face threats in cyberspace,

– the recognition that a valid strategy must offer multiple levels of security (layered security, defence in depth, etc.),

– the use of open processes in all stages of implementation of the Strategy,

– and setting out ambitious goals with the will for the Strategy and its actions to contribute tangibly to the improvement of the levels of electronic security in Cyprus.

– development of the necessary skills, training and awareness in security topics, for those that are directly involved and also for the public,

– creation or adaptation of the necessary structures and instruments within the competent authorities and the more generally the Cyprus Government, to secure the demands and capabilities of immediate incident response.[13]"

– productive collaboration between the public and private sector, on both the national and international level,

In **Danish** National Cyber Security Strategy and "information security strategy, published along with a series of sub-strategies targeting the most critical sectors in society, the Danish government has set out an ambitious plan for the coming years' work of ensuring that Denmark is digitally secure. In the coming years, the Danish central government together with sectors that are of vital importance to society, such as the energy, transport, telecommunications, finance, healthcare and maritime sectors must increase their efforts to ensure the necessary level of cyber and information security throughout Denmark. This work must build on the national efforts of recent years which have helped increase the level of cyber and information security, but the government now intends to accelerate this process. Threats are developing at a rapid pace, and this necessitates a significant strengthening of efforts such that these challenges are met"[14].

Goal of **Estonian** National Cyber Security Strategy is to increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace[15].

Figure 8 shows the subgoals of the Estonian National Cyber Security Strategy

13 Cybersecurity Strategy of the Republic of Cyprus, April 23, 2012, pp. 14-15.
14 Danish Cyber and Information Security Strategy 2018-2021, May 2018, pp. 6-8.
15 Estonian Cyber Security Strategy 2014 - 2017, p. 7

Figure 8. Subgoals of Estonian National Cyber Security Strategy

Ensuring the information protection systems that underly important services

- Ensuring alternative solutions for important services
- Managing cross-dependency between important services
- Ensuring the security of ICT infrastructure and services
- Managing cyber threats to the public and private sector
- Introducing a national monitoring system for cybersecurity
- Ensuring digital continuity of the state
- Promoting international cooperation in the critical information infrastructure

Enhancing the fight against cybercrime

- Enhancing cybercrime detection
- Raising public awareness of cyber risks
- Promoting international cooperation against cybercrime

Development of national cyber defense capabilities

- Synchronizing military planning and preparation for civil emergencies
- Developing collective cyber defense and international collaboration
- Developing military cyber defense capabilities
- Ensuring a high level of awareness about the role of cybersecurity in national defense

Estonia manages evolving cyber security threats

- Ensuring the next generation of cybersecurity professionals
- Developing smart contracting for cybersecurity solutions
- Supporting development of enterprises providing cybersecurity and national cyber security solutions
- Preventing security risks in new solutions

Estonia develops cross-sectoral activities

- Development of a legal framework to support cyber security
- Promoting international cyber security policy
- Closer cooperation with allies and partners
- Enhancing the capability of the European Union

Source: author's own study based on: Estonian Cyber Security Strategy 2014 - 2017.

The main purpose of **Finland's** Cyber Security Strategy is to enhance public-private cooperation, which is considered the strength of the Finnish security community.

"The objective is to maintain the uninterrupted and safe flow of different functions in everyday life and during disturbances. The strategy includes the following guidelines:

1. Create an efficient collaborative model between the authorities and other actors for the purpose of advancing national cybersecurity and cyber defence.

2. Improve comprehensive cybersecurity situation awareness among the key actors that participate in securing the vital functions of society.

3. Maintain and improve the abilities of businesses and organizations critical to the vital functions of society as regardsdetecting and repelling cyber threats and disturbances that jeopardies any vital function and their recovery capabilities as part of the continuity management of the business community.

4. Make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime.

5. The Finnish Defence Forces will create a comprehensive cyber defence capability for their statutory tasks.

6. Strengthen national cybersecurity through active and efficient participation in the activities of international organizations and collaborative fora that are critical to cybersecurity.

7. Improve the cyber expertise and awareness of all societal actors.

8. Secure the preconditions for the implementation of cybersecurity measures through national legislation.

9. Assign cybersecurity-related tasks, service models and common cybersecurity management standards to the authorities and actors in the business community.

10. The implementation of the Strategy and its achievement will be monitored.[16]"

The main part of the **French** National Digital Security Strategy consists of five objectives. "The role of the state in cyberspace is to ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyber attack (objective 1), to protect the digital lives of citizens and businesses and combat cybercriminality (objective 2), to ensure the education and training required for digital security (objective 3), to contribute to the development of an environment that is conducive to trust in digital technology (objective 4) and to promote cooperation between EU Member States in a manner favourable to the emergence of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values (objective 5).[17]"

With the present Cyber Security Strategy for **Germany** the Federal Government adapts measures to the current threats on the basis of the structures established by the CIP implementation plan and the implementation plan for the federal administration. "The Federal Government will specifically focus on ten strategic areas:

1. Protecting critical information infrastructure.

2. Securing IT systems in Germany.

3. Strengthening IT security in the public administration.

4. National Cyber Response Centre.

5. National Cyber Security Council.

6. Effective crime control, also in cyberspace.

7. Effective coordinated action to ensure cybersecurity in Europe and worldwide.

8. Using reliable and trustworthy information technology.

9. Personnel development in federal authorities.

10. Tools to respond to cyber attacks.[18]"

16 Finland's Cyber Security Strategy, Government Resolution January 24, 2013, pp. 6-8.
17 French National Digital Security Strategy, p. 9.
18 Cyber Security Strategy for Germany, pp. 6 - 12.

The main principles of the **Greek** National Cyber Security Strategy are:

1. "The development and establishment of a secure and resilient cyberspace which will be regulated in accordance with national, EU and international rules, standards and good practices and in which citizens, and public and private sector stakeholders can be active and interact securely, as per the values that govern the rule of law such as, indicatively, those of freedom, justice and transparency.

2. The continuous improvement of our capabilities for protection against cyber attacks, with emphasis on critical infrastructure and the safeguarding of operational continuity.

3. The institutional shielding of the national cybersecurity framework, for effective handling of cyberattack incidents and the minimization of impact by cyberspace threats.

4. The development of a strong culture of security in citizens and the public and private sectors, by utilizing the relevant capabilities of the academic community and of other public and private sector stakeholders.[19]"

On March 21, 2013, the **Hungarian** government made a decision on the national cybersecurity strategy (No. 1139/2013).

"The purpose of Strategy is to determine national objectives and strategic directions, tasks and comprehensive government tools which enable Hungary to enforce its national interests in the Hungarian cyberspace, within the context of the global cyberspace.[20]"

Irish National Cyber Security Strategy pursues the following strategic objectives:

1. "To improve the resilience and robustness of critical information infrastructure in crucial economic sectors, and particularly in the public sector.

2. To continue to engage with international partners and international organisations to ensure that cyberspace remains open, secure, unitary and free and able to facilitate economic and social development.

3. To raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice.

4. To ensure that the State has a comprehensive and flexible legal and regulatory framework to combat cybercrime by An Garda Síochána that is robust, proportionate and fair, and that accords due regard to the protection of sensitive or personal data.

5. To ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is robust, proportionate and fair.

6. To build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.[21]"

Cyber Security Strategy of **Latvia** 2014–2017 sets five priority areas of action:

1. "Governance and Resources of Cyber Security.

2. Rule of law in cyberspace and reduction of cybercrime.

3. Crisis management.

4. Awareness raising, education and research.

5. International cooperation.[22]"

19 Greek National Cyber Security Strategy Version 3.0, p. 5.
20 National Cyber Security Strategy of Hungary, p. 2.
21 Irish National Cyber Security Strategy 2015-2017, p. 11.
22 Cyber Security Strategy of Latvia 2014-2018, p. 4.

The purpose of the Programme for **Lithuanian** Development of Electronic Information Security (CyberSecurity) for 2011–2019 is to determine the objectives and tasks for the development of electronic information in order to ensure the confidentiality, integrity and accessibility of electronic information and services provided in cyberspace, safeguarding of electronic communication networks, information systems and critical information infrastructure against incidents and cyber attacks, protection of personal data and privacy, as well as to set the tasks, implementation of which would allow total security of cyberspace and entities operating in this medium. The strategic objective of the Programme is the development of the security of electronic information in Lithuania, ensuring cybersecurity in order to achieve, in 2019, a 98-percent level of compliance of state-owned information resources with legislative requirements on electronic information security (cybersecurity), reduction (to 30 minutes) of the average time of response to critical information infrastructure incidents and a 60-percent level of the Lithuanian residents who feel secure in cyberspace[23]."

Luxembourgish National Cyber Security Strategy, which covers the 2018-2020 period, is structured around the following three guidelines:

1. "The strengthening of public trust in the digital environment in order to allow Luxembourg's digital transition towards a "smart nation" model, which will be sustainable from an economic, social, environmental and political point of view, particularly in respect of the UN sustainable development programme targets for 2030;

2. The protection of digital infrastructure, in order to ensure the availability of essential services, as well as information integrity and confidentiality, and finally

3. The promotion of the economy, particularly by creating an environment that is conducive to the establishment and development of companies which are digitally active.[24]"

Maltese National Cyber Security Strategy includes the following goals:

1. "Establish a Governance Framework that is based upon the premise that a cybersecurity strategy needs to be established, and more importantly, be effectively implemented and maintained on a continuous basis. Hence the need to ensure the key coordination structures, processes, roles and practice with particular focus on cyber risk management within the public and private sector.

2. Combat Cybercrime that aims to ensure and consolidate capabilities to tackle cybercrime.

3. Strengthen National Cyber Defence which aims to foster sharing of cyber security knowledge and intelligence, review current legislation and regulations in line with cyberspace developments and ensure digital resilience on a national and organisation wide scale of particular consideration are recent legal developments at EU level, notably legislation pertaining to data protection and that related to Network and Information Security.

4. Secure cyberspace that aims to foster self-regulation and voluntary self-commitment, bearing in mind that legislation is not a panacea to cybersecurity commitments. It also aims to stimulate use of standards and best practices that guarantee security whilst allowing for interoperability. Special focus is also given to promote security and trust of online public services and to consolidate support to the private sector.

5. Cybersecurity Awareness and Education aimed at targeting academia, the public and private sector and citizens as a mean to sensitize awareness, knowledge as well as capabilities and expertise in cybersecurity. A national strategic approach towards an ongoing educational and awareness campaign is especially recommended.

6. National and International Cooperation which aims to ensure effective consultation, cooperation and collaboration on a national level, on a European and on a global basis, enabled by EU and international institutions and activities, based on the understanding that cybersecurity has no bounds.[25]"

23 Government of The Republic of Lithuania Resolution no. 796 of 29 June 2011, On the Approval of the Program for the Development of Electronic Information Security (Cyber-Security) for 2011-2019, p. 1.
24 Luxembourgish National Cyber Security Strategy III. Approved and made enforceable by the Government Council on January 26, 2018, p. 7
25 Malta Cyber Security Strategy 2016, pp. 4-5..

Table 4 outlines thematic areas implemented within the Dutch National Cyber Security Agenda.

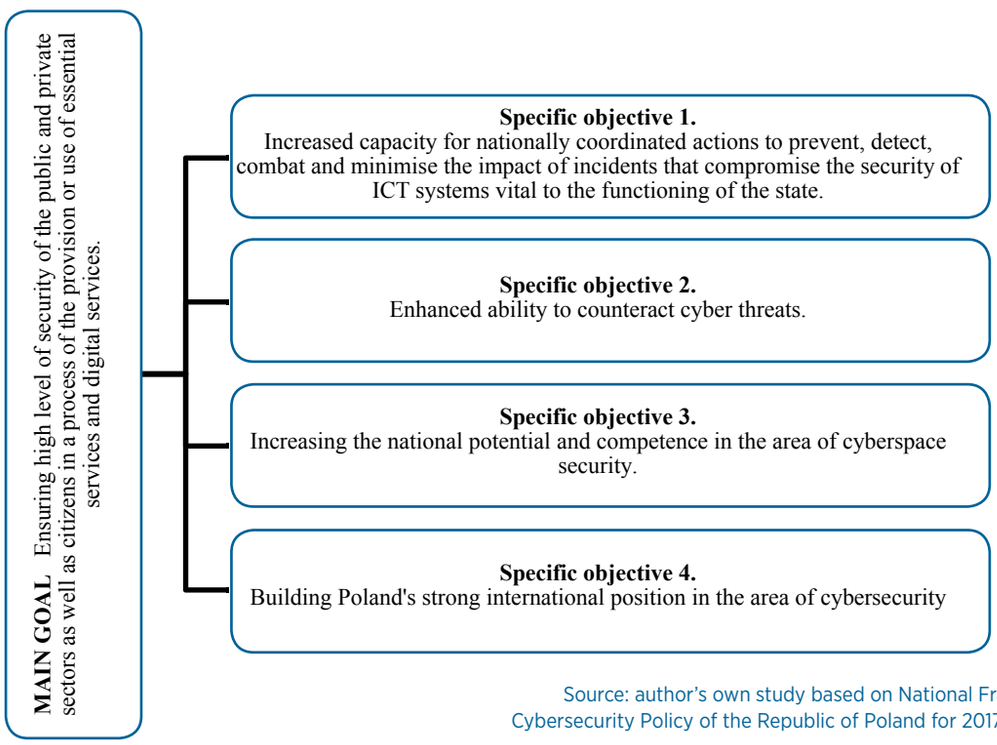
Table 4. Dutch National Cyber Security Agenda

Objectives	Characteristics
Addressing cybercrime	**The Netherlands has successful barriers to cybercrime** Criminals develop their activities on a large scale via the Internet: one in nine people were victims of cybercrime in 2017. The term cybercrime covers a broad range of criminal actions, from classic crime in digital form to new crime. This involves, for instance, hacking computers to transfer money to criminal bank accounts or turning on cameras and microphones undetected to be able to spy on people in their own surroundings. Professional criminals primarily target private organizations and citizens to steal data which can then be sold-on or published. The cybersecurity policy is intended to keep the Netherlands digitally secure and focuses on the entirely of measures to prevent or repair damage caused by disruption, failure or misuse of IT, with particular attention to vital national interests. The approach to cybercrime focuses on the prevention and combating of crimes and on limiting the numbers of victims, perpetrators and recidivism rates. This concerns both hightech crime and common crime. The efforts to strengthen cybersecurity and tackle cybercrime are conceived in conjunction with each other, and nowhere more explicitly so than in the field of preventive measures.
Critical Information Infrastructure Protection	**The Netherlands has resilient digital processes and a robust infrastructure** IT is becoming increasingly interwoven with Dutch society. One consequence of this is that the operations of businesses and public authorities are becoming increasingly data-driven through intelligent applications. This is not without risk. The business process can be disrupted if data is not exchanged with other organizations in a secure and reliable manner. When this occurs in the chains of vital providers, it can lead to major system failure, damage to physical security and social disruption. Because the availability (or continuity) of data communications networks is important, specific requirements are set for the providers of such networks, including those under the Telecommunications Act [Telecommunicatiewet] and the proposed legislation for the Cybersecurity Act [Cybersecuritywet] (CSW). The objective of those requirements is that providers make their systems resilient to various threats and incidents, including those that could lead to failure of the physical infrastructure. The software and protocols for worldwide exchange of data also require attention and maintenance to ensure effective and fault-free data exchange. This often involves what is known as open source software, which is usually developed by communities of volunteers. As a result, they often lack the capacities or resources for maintenance and/or professional investigation of the quality of the software. Other software developers also use open source software as building blocks for their work, further increasing the dependence on this software. The Dutch government is therefore calling for all organizations to be able to respond appropriately when the continuity of their provision of services is at risk. In consultation with the NCSC parties, including SMBs, the Digital Trust Centre, which is being set up, aims to help by raising awareness and offering action frameworks.
Engaging in international cooperation	**The Netherlands is contributing to international peace and security in the digital domain** More and more frequently, state actors are employing digital resources for espionage, influencing and sabotage objectives as an integral part of their range of instruments to exert power, or in concrete conflict situations. There has also been a rise in the number of countries that are setting up offensive military cyber capabilities. This threat has grown significantly in recent years and is a serious threat to international security. There have been strong divisions at an international level between various countries in the approach to the cyber domain. Distinct opinions have arisen on the application of international law, standards (of behaviour) in cyberspace, and dependence on access to digital resources. Moreover, the decentralized nature of the Internet and the opportunities the Internet provides for anonymous action are hampering the enforcement and monitoring of agreements that have been made. Due in part to the fact that attribution is difficult in the cyber domain, such cyber operations can threaten international legal order. The Netherlands should also have its own capabilities and instruments to be able to resolutely avert digital attacks on our national interests and – in extremis – also to retaliate proportionately.

Objectives	Characteristics
Establishing a public-private partnership	**The Netherlands has an integrated and strong public private approach to cybersecurity** In recent years, the public, private and public-private sectors have taken various initiatives to improve cybersecurity in the Netherlands. As the coordinator, the NCTV takes the lead in promoting and ensuring the improvement of cybersecurity in a cohesive manner, in conjunction with all the parties involved (public authorities, business community, science, civil society). However, the government cannot do this on its own. All parties may and must be expected to accept their responsibilities and contribute to make and keep the Netherlands digitally secure as part of a concerted effort. The approach can only be successful if it is shaped, further developed and evaluated in close public-private cooperation. The increasing complexity and breadth of the cyber domain require continuous clarification of the roles and responsibilities of the various parties involved. This should also help to identify successful market initiatives and link them to this Agenda. And on the private side too, there is a need for more cohesive efforts in the integrated Dutch approach to cybersecurity. To optimize the digital services provided to citizens and businesses by the government and to be able to guarantee high-quality services, it is essential for public authorities to keep investing in information protection and cybersecurity and to prioritize the availability and continuity of services.
Establishing an incident response capability	**The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats** Government bodies and private organizations in the Netherlands must cooperate and have appropriate capacities and resources to respond effectively to the growing digital threat. Sufficient capabilities also include those of security organisations which must be able to fulfil their national security tasks in both digital and physical domains. The information exchange between organizations and businesses in the Netherlands has improved greatly in recent years as a result of cooperation on incidents or because parties have come to know each other and started expressing mutual trust. Although this is a step in the right direction, it still does not provide sufficient guarantees that we can address digital threats now and in the future. The next step is to structurally guarantee the information exchange and while setting it up in a wider manner, for instance by promoting cross-sector analyses. There is a need to improve the detection and response capacities of government bodies and vital providers. By doing so, we will increase the digital capabilities of these parties. We must adopt a practice in which customers and suppliers encourage each other to organise their digital security. In this way, we will work towards a cyber ecosystem in which all parties build up capacities and share information, from the business community to public authorities and from individual citizens to information security officers.
Establishing baseline security requirements	**The Netherlands is at the forefront of digitally secure hardware and software** As a result of the rise of the Internet of Things, more and more devices are Internet-connected. It is important that everyone is able to use these products with confidence in a digitally secure manner, not only for their own digital security, but also for that of society as a whole. Malicious parties can easily gain access through vulnerabilities in hardware and software in a device, and through this device to the network it is part of. Users and providers of digital products often take little to no account of the potential harmful effects of their actions on others. This can bring about serious consequences, such as the misuse of the device for DDoS attacks, manipulation of the device or the theft of information stored on it. Digital security of hardware and software does not come about of its own accord. Hardware and software providers do not always resolve the digital security risks that are associated with their processes and production. Users have hardly any means of making a reliable estimate of the digital security level of a device that is connected to the Internet - and even if they do have this knowledge, it is difficult to make this estimate. Users therefore need to be empowered to be able to establish the digital security of hardware and software through the provision of instruments that respond to user behaviour. Research into the effectiveness of information campaigns on secure user behaviour plays an important role in this regard.
Strengthening training and educational programs	**The Netherlands leads the way in the field of cybersecurity knowledge development** Knowledge is an extremely important asset in the Netherlands. Dutch society, and digital security in particular, depends on the development and use of knowledge, which is why ambitions in the field of knowledge development are essential in the NCSA. Urgency is called for to maintain and deepen high-quality cybersecurity knowledge development in the Netherlands. It is thus crucial to boost intensifying sufficient and high-quality development of both fundamental and applied cybersecurity research. Cybersecurity knowledge development is needed to be able to implement measures to avert existing and new digital threats. Moreover, high-quality autonomous knowledge helps to avoid over-reliance on cybersecurity expertise and cybersecurity solutions from other countries. Cybersecurity knowledge development does not only apply to the natural sciences, but also to arts, humanities and social sciences. It concerns both targeted and interdisciplinary research that are aimed at investigating both short and long-term solutions. When doing so, it is extremely important for such research to cover the entire knowledge chain.

Source: author's own study based on: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Figure 9. Main goals and specific objectives of cybersecurity of the Republic of Poland for 2017 – 2022



Source: author's own study based on National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022, p. 8.

National Framework of Cybersecurity Policy of the Republic of **Poland** for 2017-2022 in accordance with the Point 4: "In 2022, Poland will be more resilient to attacks and threats from cyberspace. Thanks to a combination of both domestic and international activities, Poland's cyberspace will provide (constitute) a secure environment enabling the state to carry out their functions and allowing Poland to fully utilize the potential of the digital economy, while at the same time respecting the rights and freedoms of the citizens." Main and specific objectives of the strategy are listed in Figure 9.

Table 5 outlines the following principles implemented by the **Portuguese** National Cyber Security Strategy.

Table 5. Portuguese National Cyber Security Strategy

Objectives	Characteristics
Addressing cybercrime	Cyberspace has created new legal interests that deserve to be protected, new types of crimes and innovative ways to commit old crimes. The challenges posed by cybercrime mean that laws need to be constantly updated in order to ensure their maximum effectiveness. Similarly, institutions concerned with the investigation of cybercrime must be fully equipped to carry out their mission while the judicial system in general must adapt to the new technologies.
Keeping balance between security and privacy	The Strategy will develop the following objectives: To promote awareness, free, safe and efficient use of cyberspace. To protect fundamental rights, freedom of expression, personal data and the privacy of citizens.
Citizen's awareness	The success of cyberspace security results from promoting a security culture that supplies necessary knowledge, awareness and trust to use information systems while reducing exposure to the cyberspace risks. It is important to inform, educate and raise the awareness of public bodies and critical infrastructures as well as that of businesses and civil society in general.
Critical Information Infrastructure Protection	Guarantee and protect critical information infrastructures via National Information Infrastructure Protection System.

➥

Objectives	Characteristics
Engaging in international cooperation	The security and cyberspace defense require close cooperation and collaboration between national and international allies and partners. Responding to the challenges of cyberspace security and defense requires a network approach, where national and international cooperation in the various fields is of great importance.
Establishing an incident response capability	In a context of the distributed management of cyberspace, information sharing between interested parties is a critical success factor in ensuring improvements in detecting, preventing and responding to failures and breaches of cyberspace security. The role of Computer Security Incident Response Team (CSIRT) communities must be strengthened as a platform of excellence for sharing good practices and information on cyber incidents, for operational response services to incidents in Portugal and abroad, in this case when they represent a threat to national sovereignty. The various CSIRTs need to employ a common taxonomy and automatic mechanisms for sharing operational information among themselves and with the security forces and services.
Establishing baseline security requirements	Include cyberspace security measures in national critical infrastructures' protection plans, following a risk management based approach.
Establishing incident reporting mechanisms	In order to achieve operational effectiveness and improved situational assessment, cybersecurity incident report mechanisms must be developed for public bodies and critical infrastructure operators. The desired situational assessment results from the establishment of conditions for the identification of a national alert level in matters of cyberspace security, which is then shared with all of the bodies involved.
Fostering R&D strategies	Taking into account strategic importance of cyberspace security, it is important to support, develop and enhance technological capabilities in order to create certifiable national secure and trustworthy solutions that will improve the protection of systems that need to face a number of threats. It is essential to develop and support all research and development activities and initiatives involving businesses and industry, research bodies and academy.
Holding cybersecurity exercises	National crisis management exercises in cyberspace must be organized and held to enable the assessment of the level of preparation and maturity of the various bodies to cope with large-scale incidents, which should, whenever possible, leverage synergies resulting from the integration with other exercises in this field, organized and conducted at the national level.
Strengthening training and educational programs	Improve cyberspace security training. Improve and extend instruction and training in primary, secondary and higher education as a means of improving skills and knowledge on the safe use of ICT.

Source: author's own study based on https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

The purpose of Romania's cybersecurity strategy is to "define and maintain an secure virtual environment, with a high degree of resilience and confidence, based on national cyber infrastructures, which would constitute an important support for national security and good government, to maximize the benefits for citizens, businesses and the Romanian society as a whole. The strategy sets the following objectives for ensuring Romania's cybersecurity:

- adapting the regulatory and institutional framework to the cyberspace threats dynamics;
- establishing and implementing security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures;
- ensuring security through understanding, preventing and fighting vulnerabilities, risks and threats to cybersecurity of Romania;
- ensuring the resilience of cyber infrastructure;
- taking advantage of opportunities to promote the national interests, values and objectives in the cyberspace;
- promoting and developing cooperation between the public and private sectors at national and international level in the field of cybersecurity;
- developing a security culture by raising population's awareness of the vulnerabilities, risks and threats originating from cyberspace and the need to ensure protection of their information systems;
- active participation in the initiatives held by international organizations, which Romania is part of, in defining and establishing a set of international confidence-building measures concerning use of cyberspace.[26]"

26 Cyber Security Strategy of Romania, p. 2.

The cybernetic security concept of **Slovakia** (2015-2020) was implemented on June 1, 2015.

"The Concept is based on a statement and a description of the basic terms and principles, characteristics of the current situation of the strategic, legal and institutional frameworks in the area of cybersecurity in the Slovak Republic and on a strategic and methodological framework formed by NATO and European Union documents; subsequently, the Concept formulates principles, goals and proposed solutions.[27]"

In June 2015, the Slovak government established the National Cyber Security Organisation. Among domestic bodies in charge of cybersecurity control is also the National Agency for Networks and Electronic Systems.

The objective set in Slovenian Cyber Security Strategy is "establishing a comprehensive cyber security system as an important integral factor of national security, which will contribute to ensuring an open, safe and secure cyberspace, that will make the basis for smooth functioning of infrastructure, important for state bodies' operations as well as for the life of each individual. By 2020, Slovenia will establish an effective cyber security assurance system, which will prevent and also eliminate the consequences of security incidents. This objective comprises eight sub-objectives:

1) strengthening and systemic regulation of the national cybersecurity assurance system;

2) ensuring safety of citizens in cyberspace;

3) using cybersecurity in the economy;

4) ensuring the operation of critical infrastructure in the ICT support sector;

5) implementing cybersecurity to ensure public security and combat cybercrime;

6) developing of cyber defense capabilities;

7) ensuring the safe operation and availability of key IC systems in the event of major natural and other disasters;

8) strengthening national cybersecurity through international cooperation.[28]"

Table 6 presents thematic areas implemented within the **Spanish** National Cyber Security Strategy.

Table 6. Spanish National Cyber Security Strategy

Objectives	Characteristics
Addressing cybercrime	New legislation and LEAs coordination mechanisms: – As regards legislation, incorporate into the Spanish legal framework solutions to problems that arise in connection with cybersecurity, in order to establish types of criminal offences and define the work of the departments with responsibilities in this area. – Expand and improve the capacities of the bodies responsible for investigating and prosecuting cyberterrorism and cybercrime; ensure coordination of these capacities with activities in the field of cybersecurity by exchanging information and intelligence through the appropriate communication channels; – Ensure that legal professionals have access to the information and technical knowledge needed to ensure that the legal framework is implemented as effectively as possible. – A new cybersecurity structure has been set up for improving coordination between LEAs. – Spain has developed tailor-made training for law enforcement. The State Prosecution Office and the Council for the Judiciary have included specific cybercrime training for prosecutors and judges respectively. – The national priorities are linked to the strategic goals and operational action plans drawn up for the EU cybercrime priority.

➥

27 Cyber Security Concept of the Slovak Republic for 2015 - 2020, p. 6.
28 Slovenian Cyber Security Strategy Establishing a system to ensure a high level of cyber security, p. 6

Objectives	Characteristics
Keeping balance between security and privacy	– The National Security Scheme (ENS) includes measures to balance security and privacy. – The Spanish Agency of Data Protection is an independent public authority to ensure privacy and data protection of citizens. It has a flexible tool that allows the regulatory compliance.
Citizen's awareness	– Make It Safe worldwide campaign to make the Internet safer for children and adolescents. – National Cryptologic Centre: specific awareness campaigns and workshops for public administration. – The Ministry of Interior collaborates in all institutional prevention campaigns aimed at raising cybercrime awareness via annual cybersecurity conferences and monthly talks among those population groups that are considered most at risk: senior citizens, secondary school pupils and vocational training students, and university students.
Critical Information Infrastructure Protection	The National Centre for Critical Infrastructure Protection (CNPIC) is a body in charge of promoting, coordinating and supervising all critical infrastructure protection (CIP)-related activities for which the Secretariat of State for Security is competent at the national level. The main objective of the Centre is the promotion and coordination of the mechanisms needed to guarantee the security of all infrastructures that supply services of great importance to our society, encouraging all the agents of the system to take part in their respective fields of competence. By means of all these efforts, the CNPIC promotes both a security model based on mutual trust and an idea of establishing a public-private partnership that will allow minimizing any vulnerabilities of Spain's critical infrastructure. Operators – designated as being critical by the National CIP Commission – will be part of the CIP System and will be responsible for optimizing the protection of the critical infrastructure they manage.
Developing national cyber contingency plans	A national cybersecurity crisis management procedure has been developed and driven by the National Cybersecurity Council.
Engaging in international cooperation	– Appointing Ambassador for Cybersecurity – Enhancing Spanish presence in international and regional organizations and forums on cybersecurity by actively supporting and participating in the various initiatives and coordinating the position of national actors involved – Promoting the role of Spain in supporting the ratification of the 2001 Convention on Cybercrime (Budapest Convention) by other countries and projecting the efforts carried out by Spain. – Favoring the signing of non-normative agreements within international organizations and with the main partners and allies.
Establishing a public-private partnership	– Several measures regarding cooperation between the public and private sectors have been adopted: – Promoting information exchange related to vulnerabilities, cyberthreats and their possible consequences, especially in relation to protecting systems of national interest. – Hosting various meetings between public and private CSIRTs and creating a workgroup tasked with sharing information. – Conducting several cyber exercises with participation of representatives of both public and private sectors. – Defining and implementing cooperation model between public and private cybersecurity teams.
Establishing an incident response capability	An incident response capability has been set up at the national level. The following three types of national CERTs can be distinguished: – ESPCERTDEF in the Ministry of Defense as a body focused on military fields. – CCN-CERT focused on public administration. – CERTSI used for all purposes of Critical Infrastructures, citizens, companies, and investigation and national-level academy network. The above-mentioned CERTs are represented in the National Cyber Security Council. Besides, there are several regional CERTs.
Establishing an institutionalized form of cooperation between public agencies	– Incident response teams have signed various agreements. – The National Cybersecurity Council strengthens coordination, collaboration and cooperation relations among different public authorities with responsibilities in cybersecurity matters as well as between the public and private sectors. – The composition of the Specialised Cyber Security Committee reflects the spectrum of areas covered by the departments, bodies, and agencies of the public authorities with responsibilities in cybersecurity matters, all of which coordinate actions that need to be addressed jointly with the aim of raising security levels. Other relevant private-sector actors and specialists, whose contribution is deemed necessary, may take part in the Committee.

➥

Objectives	Characteristics
Establishing baseline security requirements	The National Security Scheme (ENS) contains basic principles and minimum requirements for adequate protection of information, aimed at establishing the security policy in the use of electronic media for public administrations. Adaptation to the ENS involves addressing the following issues: – Drafting and approving security policy, including a definition of roles and allocation of responsibilities. – Introducing system classification according to the importance of the information handled and the services provided. – Conducting risk analysis, including the assessment of existing security measures. – Drafting and approving Statement of Applicability of the ENS measures. – Drafting an adaptation plan for the security improvement, based on the failures identified, including estimated development schedule. – Implementing, executing and monitoring security measures through ongoing security management. – Assuring a security audit to be held in two years' time, whose results shall later be translated into relevant improvement actions.
Establishing incident reporting mechanisms	Depending on the type of organization (public, private, critical infrastructure, citizens or companies), they have a CSIRT for managing the incidents according to a specific procedure.
Fostering R&D strategies	– Network of excellence on cybersecurity R&D+i: In the context of the Trust in the Digital Domain Plan (derived from the Digital Agenda for Spain), INCIBE, in cooperation with the cybersecurity research ecosystem, is promoting the creation of a network of centres of excellence on cybersecurity research and innovation. – Grants for advanced cybersecurity research team excellence. The initiative to launch these grants for advanced cybersecurity research team excellence has emerged to meet the current need for retain and attract cybersecurity-research talent.
Holding cybersecurity exercises	The main organisms and big companies – Several national cybersecurity exercises have been conducted in both public and private sector. – Taking part in international exercise, including NATO CMX, Cyber Europe EU, NATO Cyber Shield
Providing incentives for the private sector to invest in security measures	– In the area of financing of innovative and technological companies, the Centre for the Development of Industrial Technology (CDTI) disposes of instruments for setting up and consolidating technology-basis companies and those for enhancing their growth and development. In order to accomplish these objectives, CDTI also performs supporting activities. – The Strategic Action of Economy and Digital Society (AEESD) has launched two programs – Technological Impulse and EUREKA – both of which are devoted to financing cybersecurity and digital trust projects. – Despite costly evaluation of checking the security level of ICT products (in accordance with the Common Criteria), as performed by the laboratory, the Certification Process, as an administrative process between the applicant and the National Cryptologic Centre, is free for companies.
Strengthening training and educational programs	According to the Line of Action 7 "Cyber Security Culture", an action plan has been developed to raise awareness of citizens, professionals and companies about the cybersecurity importance. It includes a set of specific projects and actions to be developed (some of them already done or ongoing). Some examples of these actions: – Under the Digital Agenda for Spain, the Spanish state has launched the Digital Trust Plan that contains both prevention and awareness-raising actions. As part of the Digital Trust Plan a pilot program is being examined, the role of which would be to assess the appropriateness and feasibility of incorporating a digital trust component in educational curricula. – Cybercamp (INCIBE-hosted cybersecurity event aimed at identifying, attracting, managing, and, in short, helping to generate cybersecurity talent that can be transferred to the private sector, in line with its demands). – Various Masters in Cybersecurity delivered by Universities. – Public administration: specific cybersecurity training courses dedicated for civil servants and delivered by the National Cryptologic Center.

Source: author's own study based on https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map

Sweden 's National Cyber Security Strategy is "based on the overall IT policy objective – for Sweden to become the world leader in harnessing the opportunities of digital transformation. To promote Sweden's security and IT policy objectives, the government believes there are six primary areas in society's cyber security that must be given priority:

1. Securing a systematic and comprehensive approach in cybersecurity efforts.
2. Enhancing network, product and system security.
3. Enhancing capability to prevent, detect and manage cyberattacks and other IT incidents.

4. Increasing the possibility of preventing and combating cybercrime.

5. Increasing knowledge and promoting expertise.

6. Enhancing international cooperation[29]" .

Under the National Cyber Security Strategy for 2021, the **United Kingdom** is secure and resilient to cyber threats as well as prosperous and confident in the digital world.

The following goals have been set to implement this vision:

– "DEFEND - country has the means to defend the UK against evolving cyber threats, to respond effectively to incidents, and to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have knowledge and ability to defend themselves.

– DETER - the UK will be a hard target for all forms of aggression in cyberspace. Will be detect, understand, investigate and disrupt hostile action taken against UK, pursuing and prosecuting offenders.

– DEVELOP – country has an innovative, growing cyber security industry, underpinned by worldleading scientific research and development. UK has a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.[30]"

29 Sweden National Cyber Security Strategy, Stockholm, June 22, 2017.
30 NATIONAL CYBER SECURITY STRATEGY 2016-2021

5

CONCLUSIONS

The following main conclusions can be drawn upon the aforementioned domestic strategies of individual EU Members States:

- Emphasis is shifted on the importance of cybersecurity of an individual country and the European Union as a whole, especially in the context of defense against cyberattacks and their immediate repercussions.
- Growing threats are identified, with particular regard to those resulting from evolving and boundary-free cyberspace.
- While defining assumptions related to cybersecurity matters states need to take into account a period of a few days, which comes as a positive sign.
- Aforementioned strategies are subject to change, making it necessary to update them in line with all developing and evolving cyber threats.
- There emerges a visible need for cooperation at various levels, both domestic and external ones; between the government and key social sectors, including transport, energy industry, healthcare, telecommunications, finances; between public and private sectors and citizens of the country.
- Promoting international cooperation on critical infrastructure protection
- A coherent and comprehensive approach to all issues related to ensuring the most appropriate use of advanced technologies while properly combining human capabilities for the purposes of digital transformation.
- Indicating that computerization, apart from providing the contemporary society with a number of undeniable benefits, may introduce some security gaps, which is why cyberspace security shall be considered the main concern of all interested parties, in particular at institutional level, where responsibility for developing and implementing coherent policies focuses at different levels.

6

CYBERSECURITY EXPENDITURE IN THE EU MEMBER STATES

Cybersecurity expenditure calculated at the state level is difficult to estimate, which is mostly due to its dispersion in various areas, including digital technologies, digitization, development, economy, science, security and defense, all of which makes it difficult to determine exact values. There are no comprehensive statistics that would include cybersecurity spending on various levels. There are various indexes/ranks in which countries are assessed in terms of many cybersecurity areas, e.g.: digital competitiveness, economic flexibility and capacity to adapt to technological changes, digital economy, and digital community.

When defining expenditure in terms of a purely economic category, it is vital to understand such factors as depreciation of workforce and assets of an economic unit, both of which are expressed in natural units. Expenditure applies to the entire enterprise while only a part of it may be referred to as a cost incurred by a previous established business activity.

Analyzes of cybersecurity spending of the EU countries were conducted on the basis of selected indicators:

- defense spending;
- defense spending as % of GDP
- R&D spending as % of defense expenditure
- ICT sector, as % of GDP
- ICT employment
- gross domestic expenditure on R&D (as % of GDP)
- number of ISO/IEC 27001 system certificates issued;
- ITU ICT development index;
- IMD World Digital Competitiveness (WDC);
- National Cyber Security Index (NCI);
- The difference shows the relationship between the NCSI score and DDL.
- The Digital Economy and Society Index (DESI)

Selected indicators indirectly point that the state is ready to incur cybersecurity expenses.

Table 7 presents defense expenditure while Table 8 defines defense-spending level as a percentage of GDP in 2010-2017.

Table 7. Defense expenditure 2010 – 2017 (in millions of euro)

Country	2010	2011	2012	2013	2014	2015	2016	2017, estimated
Austria	2,43	2,453	2,481	2,432	2,491	2,403	2,734	2,647
Belgium	3,951	3,986	4,094	3,939	3,913	3,789	3,901	3,965
Bulgaria	629	545	562	611	563	571	606	771
Croatia	no data available	no data available	no data available	639	606	602	563	615
Cyprus	361	345	323	290	270	296	287	352
Czech Republic	2,016	1,82	1,651	1,597	1,493	1,736	1,69	1,944
Denmark	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Estonia	249	280	340	361	386	418	450	478
Finland	2,707	2,654	2,857	2,862	2,714	3,183	3,208	2,879
France	39,237	38,45	39,105	39,391	39,198	39,199	39,95	40,852
Germany	33,492	33,781	32,49	33,784	34,749	33,899	37,598	40,447
Greece	4,841	4,933	4,348	4	4,001	4,073	4,19	4,213
Hungary	1,022	1	1,029	912	912	1,02	1,165	1,197
Ireland	911	881	900	891	893	891	899	915
Italy	21,637	21,741	20,6	20,078	18,427	17,642	20,226	20,534
Latvia	194	210	201	214	223	254	364	470
Lithuania	246	252	256	267	322	425	575	724
Luxembourg	187	167	167	176	190	225	213	289
Malta	44	40	39	41	43	50	54	57
Netherlands	8,472	8,156	8,067	7,702	7,788	7,816	8,234	8,686
Poland	6,392	6,557	6,754	6,72	7,565	9,546	8,5	8,683
Portugal	2,782	2,669	2,366	2,591	2,501	2,384	2,364	2,422
Romania	1,575	1,713	1,636	1,847	2,029	2,325	2,402	3,627
Slovakia	853	763	790	726	749	889	907	993
Slovenia	583	478	422	381	366	361	406	422
Spain	11,132	10,059	10,828	9,495	9,508	10	9,014	10,739
Sweden	4,265	4,331	4,632	4,673	4,711	4,632	4,683	4,638
United Kingdom	45,603	45,266	45,349	43,814	48,172	53,649	50,379	50,592

*estimated

Source: author's own study based on https://www.eda.europa.eu/info-hub/defence-data-portal

An increase in defense expenditure in EU Member States can be noted when analyzing data collected over the past eight years. When comparing 2017 with 2010, the following countries recorded the most considerable increase:

- Lithuania – by 478 million euro. Taking into account the year-on-year analysis, the highest increase amounted to 20% in 2014, 32% in 2015, 35% in 2016 and 26% in 2017.

- Latvia – by 276 million euro. Taking into account the year-on-year analysis, the highest increase amounted to 44% in 2016 and 29% in 2017.

- Romania – by 2,052 million euro. Taking into account the year-on-year analysis, the highest increase amounted to 51% in 2017.

- Estonia – by 229 million euro. Taking into account the year-on-year analysis, the highest increase amounted to 21% in 2012. Since 2013, the upward trend at the 7-percent level has been noticed.

When comparing 2017 with 2010, defense expenditure dropped in the following countries:

- Cyprus – by 2%, while taking into account the country's result in 2017, defense spending increased by 23% as compared to 2016.

- Czech Republic – by 4%, while taking into account the country's result in 2017, defense spending increased by 15% as compared to 2016.

- Greece – by 23%, while taking into account the country's result in 2017, defense spending increased by 1% as compared to 2016.

- Italy – by 5%, while taking into account the country's result in 2017, defense spending increased by 2% as compared to 2016.

- Portugal – by 13%, while taking into account the country's result in 2017, defense spending increased by 2% as compared to 2016.

- Slovenia – by 28%, while taking into account the country's result in 2017, defense spending increased by 4% as compared to 2016.

- Spain – by 4%, while taking into account the country's result in 2017, defense spending increased by 19% as compared to 2016.

When comparing defense spending in 2017 to the previous year, the following six countries experienced growth above the 20-percent level: Bulgaria (27%), Latvia (29%), Lithuania (26%), Luxembourg (35%), Romania (51%), while the decrease was reported in Austria (3%), Finland (10%) and Sweden (1%).

Given defense expenditure as a share in country's GDP, only three states spend more than 2 percent on defense budget: Estonia (2.1%), Greece (2.4%) and United Kingdom (2.2%).

Table 8. Defense expenditure as % of GDP, 2010-2017

Country	2010	2011	2012	2013	2014	2015	2016	2017
Austria	0.8%	0.8%	0.8%	0.8%	0.7%	0.7%	0.8%	0.7%
Belgium	1.1%	1.1%	1.1%	1.0%	1.0%	0.9%	0.9%	0.9%
Bulgaria	1.6%	1.3%	1.3%	1.5%	1.3%	1.3%	1.3%	1.5%
Croatia	no data available	no data available	no data available	1.5%	1.4%	1.4%	1.2%	1.3%
Cyprus	1.9%	1.7%	1.7%	1.6%	1.5%	1.7%	1.6%	1.8%
Czech Republic	1.3%	1.1%	1.0%	1.0%	1.0%	1.0%	1.0%	1.0%
Denmark	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Estonia	1.7%	1.7%	1.9%	1.9%	2.0%	2.1%	2.1%	2.1%
Finland	1.4%	1.3%	1.4%	1.4%	1.3%	1.5%	1.5%	1.3%
France	2.0%	1.9%	1.9%	1.9%	1.8%	1.8%	1.8%	1.8%
Germany	1.3%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%	1.2%
Greece	2.1%	2.4%	2.3%	2.2%	2.2%	2.3%	2.4%	2.4%
Hungary	1.0%	1.0%	1.0%	0.9%	0.9%	0.9%	1.0%	1.0%
Ireland	0.5%	0.5%	0.5%	0.5%	0.5%	0.3%	0.3%	0.3%
Italy	1.3%	1.3%	1.3%	1.3%	1.1%	1.1%	1.2%	1.2%
Latvia	1.1%	1.0%	0.9%	0.9%	0.9%	1.0%	1.5%	1.8%
Lithuania	0.9%	0.8%	0.8%	0.8%	0.9%	1.1%	1.5%	1.7%
Luxembourg	0.5%	0.4%	0.4%	0.4%	0.4%	0.4%	0.4%	0.5%
Malta	0.7%	0.6%	0.5%	0.5%	0.5%	0.5%	0.5%	0.5%
Netherlands	1.3%	1.3%	1.3%	1.2%	1.2%	1.1%	1.2%	1.2%
Poland	1.8%	1.7%	1.7%	1.7%	1.8%	2.2%	2.0%	1.9%
Portugal	1.5%	1.5%	1.4%	1.5%	1.4%	1.3%	1.3%	1.3%
Romania	1.3%	1.3%	1.2%	1.3%	1.3%	1.5%	1.4%	1.9%
Slovakia	1.3%	1.1%	1.1%	1.0%	1.0%	1.1%	1.1%	1.2%
Slovenia	1.6%	1.3%	1.2%	1.1%	1.0%	0.9%	1.0%	1.0%
Spain	1.0%	0.9%	1.0%	0.9%	0.9%	0.9%	0.8%	0.9%
Sweden	1.2%	1.1%	1.1%	1.1%	1.1%	1.0%	1.0%	1.0%
United Kingdom	**2.5%**	**2.4%**	**2.2%**	**2.1%**	**2.1%**	**2.1%**	**2.1%**	**2.2%**

Source: author's own study based on https://www.eda.europa.eu/info-hub/defence-data-portal

Table 9 presents research and development (R&D) expenditure as a share of defense spending in 2010-2017.

Table 9. R&D expenditure as a share of defense spending (in % and millions of euro)

Country	2010		2011		2012		2013		2014		2015		2016		2017, estimated	
	amount	%	amount	%	Amount	%	Amount	%	amount	%	amount	%	amount	%	amount	%
Austria	1.0	0.04%	43466	0.04%	43467	0.08%	1.0	0.04%	43586	0.06%	43678	0.07%	2.0	0.07%	3.0	0.11%
Belgium	43505	0.23%	43563	0.21%	43684	0.19%	43684	0.20%	43473	0.21%	43622	0.17%	43591	0.17%	43472	0.18%
Bulgaria	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.1	0.02%	4.0	0.71%	43619	0.59%	43469	0.54%
Croatia	no data available	no data available	no data available	no data available	no data available	no data available	0.5	0.08%	0.3	0.06%	0.2	0.03%	0.2	0.03%	0.9	0.15%
Cyprus	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%
Czech Republic	43516	1.00%	43540	0.90%	43512	0.98%	43570	0.97%	43661	1.10%	43724	0.97%	43661	0.93%	43482	0.88%
Denmark	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Estonia	0.7	0.30%	0.2	0.07%	43466	0.32%	0.5	0.13%	43586	0.38%	43647	0.41%	43525	0.29%	0.7	0.15%
Finland	38.3	1.41%	18.0	0.68%	37.0	1.30%	33.5	1.17%	35.1	1.29%	56.7.	1.78%	58.2	1.81%	39.7	1.38%
France	**3580**	**9.12%**	**3300.0**	**8.58%**	**3500.0**	**8.95%**	**3280.0**	**8.33%**	**3563.0**	**9.09%**	**3639.0**	**9.28%**	**2194.0**	**5.49%**	**2811.5**	**6.88%**
Germany	1454.7	4.34%	1059.4	3.14%	918.1	2.83%	927.4	2.75%	845.9	2.43%	837.6	2.33%	822.1	2.19%	1150.9	2.85%
Greece	43565	0.22%	43715	0.16%	43684	0.18%	0.6	0.01%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%
Hungary	0.2	0.02%	0.4	0.04%	0.5	0.05%	0.1	0.01%	0.0	0.00%	0.8	0.08%	0.4	0.04%	0.6	0.05%
Ireland	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%
Italy	64.2	0.30%	178.2	0.82%	92.4	0.45%	149.4	0.74%	103.0	0.56%	78.4	0.44%	51.2	0.44%	59.9	0.29%
Latvia	0.03	0.01%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%	0.0	0.00%
Lithuania	0.0	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%
Luxembourg	0.2	0.10%	0.1	0.03%	0.0	0.00%	0.1	0.03%	0.1	0.03%	0.1	0.02%	0.1	0.04%	43586	0.50%
Malta	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%	0.00	0.00%
Netherlands	74.7	0.88%	69.4	0.85%	70.7	0.88%	59.2	0.77%	59.4	0.76%	61.6	0.79%	57.2	0.69%	61.7	0.71%
Poland	121.2	1.90%	167.6	2.56%	143.6	2.13%	94.3	1.40%	217.2	2.87%	156.7	1.64%	138.9	1.63%	259.9	2.99%
Portugal	7.0	0.25%	43473	0.30%	0.9	0.04%	0.9	0.03%	43557	0.10%	43557	0.10%	43557	0.10%	43587	0.10%
Romania	43467	0.13%	43709	0.11%	43467	0.13%	43647	0.09%	43466	0.06%	43557	0.10%	43556	0.06%	43557	0.07%
Slovakia	0.1	0.01%	0.6	0.08%	43470	0.64%	43558	0.46%	43467	0.28%	43556	0.16%	43525	0.15%	0.6	0.06%
Slovenia	43684	1.33%	0.9	0.18%	0.8	0.20%	0.8	0.22%	0.0	0.00%	0.1	0.02%	0.1	0.03%	0.3	0.08%
Spain	162.1	1.46%	148.5	1.48%	110.1	1.02%	90.8	0.96%	75.4	0.79%	98.8	0.99%	88.6	0.98%	93.6	0.87%
Sweden	106.8	2.50%	102.6	2.37%	85.6	1.85%	118.5	2.54%	105.5	2.24%	109.8	2.37%	112.5	2.40%	128.4	2.77%
United Kingdom	**2895.2**	**6.35%**	**2678.7**	**5.92%**	**2464.4**	**5.43%**	**2793.0**	**6.37%**	**3752.7**	**7.79%**	**4134.5**	**7.71%**	**3663.4**	**7.27%**	**3211.3**	**6.35%**

Source: author's own study based on: www.eda.europa.eu, (10/07/2018). https://www.eda.europa.eu/info-hub/defence-data-portal

As indicated by the analysis of R&D spending as a share in defense expenditure, France and the United Kingdom managed to achieve the highest level, despite a noticeable fall in 2017. Yet indicators remain at a relatively high level of 6.88% and 6.35% respectively as compared to the previous year. The list of countries whose R&D expenditure as a share in defense spending exceeded 2 percent in 2017 includes Sweden (2.77%), Poland (2.99%) and Germany (2.85%) while it amounts to 1.38% in Finland. In other EU countries, R&D expenditure as a share of defense spending is at or below 1%.

Table 10 presents ICT sector as a share in GDP in selected countries (2010 - 2016).

Table 10. Percentage of the ICT sector in GDP, 2010 - 2016

Country	2010	2011	2012	2013	2014	2015	2016
Austria	3.12	3.25	3.15	3.23	no data available	3.37	3.47
Belgium	4.48	4.09	4.11	4.03	3.85	3.84	3.83
Bulgaria	**4.83**	**4.64**	**4.58**	**4.71**	**4.89**	**5.08**	**5.43**
Croatia	4.61	4.05	3.89	4.1	4.06	4.19	4.22
Cyprus	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Czech Republic	4.43	4.38	4.38	4.4	4.31	4.27	4.29
Denmark	4.62	4.62	no data available	no data available	no data available	no data available	no data available
Estonia	4.79	5.04	4.69	4.59	4.82	4.74	4.91
Finland	5.2	4.35	3.65	4.34	no data available	4.59	no data available
France	4.04	4.06	4.01	no data available	3.83	3.89	4.01
Germany	3.88	4.02	3.98	4.05	4.15	4.19	4.09
Greece	2.13	2.06	2.04	1.98	1.83	2.17	2.13
Hungary	**5.68**	**5.96**	**5.79**	**5.84**	**5.66**	**5.86**	**5.79**
Ireland	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Italy	no data available	3.43	3.49	3.26	3.23	3.23	3.28
Latvia	3.54	3.3	3.47	3.74	3.76	4.2	4.61
Lithuania	2.41	2.43	2.49	2.39	2.58	2.92	2.96
Luxembourg	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Malta	**7.43**	**9.02**	**8.71**	**6.85**	**7.17**	**7.24**	**6.88**
Netherlands	no data available	no data available	no data available	4.9	no data available	no data available	no data available
Poland	3.19	3.27	3.12	3.01	3.05	3.14	3.22
Portugal	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Romania	3.12	3.1	3.18	3.13	3.31	3.35	3.55
Slovakia	4.67	4.48	4.73	no data available	4.17	4.38	3.99
Slovenia	3.51	3.49	3.57	3.59	3.59	3.6	3.6
Spain	3.42	3.39	3.35	3.3	3.18	no data available	no data available
Sweden	6.39	no data available	no data available	no data available	6.4	no data available	no data available
United Kingdom	**5.45**	**no data available**	**no data available**	**no data available**	**5.72**	**5.88**	**5.95**

Source: author's own development based on Eurostat data, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ag&lang=en

Data analysis contained in Table 10 shows Malta's high percentage of the ICT sector in GDP, which amounted to over 6% in 2010-2016. The share of the ICT sector in the GDP of the United Kingdom, Hungary and Bulgaria exceeds the 5-percent level. In 2016, percentage of the ICT sector in GDP of Lithuania and Greece remained at the lowest level of 2.96% and 2.13% respectively while attention shall be drawn to Lithuania's progressive growth year by year. Speaking of other countries, such result may stand around 3%, which may indicate great development potential.

Table 11 illustrates the percentage of the ICT personnel in total employment in 2010 - 2016.

Table 11 Percentage of the ICT personnel in total employment

Country	2010	2011	2012	2013	2014	2015	2016
Austria	2.27	2.31	2.38	2.43	no data available	2.48	2.55
Belgium	2.84	2.71	2.67	2.74	2.64	2.61	2.65
Bulgaria	1.79	1.89	2.02	2.13	2.19	2.37	2.59
Croatia	1.92	1.93	1.9	2.17	2.19	2.29	2.34
Cyprus	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Czech Republic	2.7	2.79	2.79	2.76	2.81	2.84	2.96
Denmark	3.21	4.15	no data available	no data available	no data available	no data available	no data available
Estonia	**3.09**	**3.33**	**3.41**	**3.48**	**3.58**	**3.6**	**3.69**
Finland	3.94	3.86	3.83	3.73	no data available	3.72	no data available
France	2.81	2.85	2.91	2.84	2.99	2.96	2.97
Germany	2.26	2.38	2.35	2.47	2.6	2.66	2.74
Greece	1.28	1.33	1.44	1.32	1.42	1.53	1.55
Hungary	**3.63**	**3.69**	**3.65**	**3.54**	**3.41**	**3.42**	**3.51**
Ireland	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Italy	no data available	2.36	2.37	2.38	2.32	2.36	2.42
Latvia	**2.05**	**2.15**	**2.47**	**2.62**	**3.03**	**3.28**	**3.59**
Lithuania	1.79	1.88	1.99	2.08	2.23	2.37	2.48
Luxembourg	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Malta	**4.08**	**4.4**	**4.06**	**4.01**	**4.21**	**4.5**	**4.74**
Netherlands	3.04	3.06	no data available	no data available	no data available	no data available	no data available
Poland	1.71	1.76	1.84	1.91	2	2.14	2.3
Portugal	no data available	no data available	no data available	no data available	no data available	no data available	no data available
Romania	1.45	1.56	1.71	1.84	1.95	2.1	2.27
Slovakia	**2.72**	**2.85**	**2.79**	**no data available**	**2.86**	**2.92**	**3.04**
Slovenia	2.32	2.34	2.41	2.52	2.52	2.61	2.64
Spain	2.02	2.1	2.2	2.19	2.2	no data available	no data available
Sweden	4.41	no data available	no data available	no data available	4.44	no data available	no data available
United Kingdom	**3.31**	**3.25**	**3.09**	**3.32**	**3.41**	**3.47**	**3.6**

Source: author's own study based on Eurostat data

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ap&lang=en

According to data contained in Table 11, it can be noticed that the level of ICT employment is characterized by annual growth. In 2016, the highest level of ICT employment was recorded in Malta, with a result above 4%, followed by the United Kingdom, Slovakia, Latvia, Hungary, Finland, and Estonia (above 3%). The lowest score was reported in Greece (below 2%).

Table 12 presents gross domestic expenditure on R&D in 2006 and 2016 (as % of GDP).

According to data contained in Table 11, it can be noticed that the level of ICT employment is characterized by annual growth. In 2016, the highest level of ICT employment was recorded in Malta, with a result above 4%, followed by the United Kingdom, Slovakia, Latvia, Hungary, Finland, and Estonia (above 3%). The lowest score was reported in Greece (below 2%).

Table 12 presents gross domestic expenditure on R&D in 2006 and 2016 (as % of GDP).

According to the analysis of domestic expenditure on research and development as a percentage of GDP, only Sweden and Austria

- managed to achieve the 3-percent level in 2016 while
- such countries as Slovenia, the Netherlands, Germany, France, Finland, Denmark, and Belgium secured the 2-percent level.

ISO/IEC 27000:2018 provides an overview of information security management systems (ISMS). It also sets out terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document:

- cover commonly used terms and definitions in the ISMS family of standards;
- do not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining new terms for use[31].

The PN EN ISO/IEC 27001:2017-06 standard "Information Security Management Systems" was published on January 10, 2018. Requirements that do not introduce any new prerequisites for the PN-ISO/IEC 27001:2014-12 standard while its update results from introducing amendments to the ISO/IEC 27001:2013: Cor 1:2014 to Annex 1 Point 8.1.1, as issued previously, and Cor. 2:2015 to Point 6.1.3.

ISO/IEC 27001 (PN-ISO/IEC 27001) Information security management systems — Requirements gives

Table 12 Gross domestic expenditure on R&D, in 2006 and 2016 (as % of GDP)

Country	2006	2016
Austria (1)	**2.36**	**3.09**
Belgium (1)	**1.81**	**2.49**
Bulgaria	0.45	0.78
Croatia	0.74	0.85
Cyprus (1)	0.38	0.50
Czech Republic (1)	1.23	1.68
Denmark (1) (3)	**2.40**	**2.87**
Estonia	1.12	1.28
Finland	**3.34**	**2.75**
France (1)	**2.05**	**2.25**
Germany (1) (3)	**2.46**	**2.94**
Greece (2)	0.56	1.01
Hungary	0.98	1.21
Ireland (3)	1.20	1.18
Italy (1)	1.09	1.29
Latvia	0.65	0.44
Lithuania	0.79	0.85
Luxembourg (1)	1.67	1.24
Malta (1)	0.58	0.61
Netherlands (1)	1.76	2.03
Poland (1)	0.55	0.97
Portugal (1)(2)	0.95	1.27
Romania	0.45	0.48
Slovakia	0.48	0.79
Slovenia (1)	1.53	2.00
Spain	**1.17**	**1.19**
Sweden (1)(2)	**3.50**	**3.25**
United Kingdom (1)	1.59	1.69

(1) 2016: provisional (2) 2006: estimate (3) 2016: estimate

https://ec.europa.eu/eurostat/statistics-explained/images/archive/9/9e/

31 https://www.iso.org/standard/73906.html

Figure 10. ISO/IEC 27000 family of standards for Information technology Information technology - Security techniques

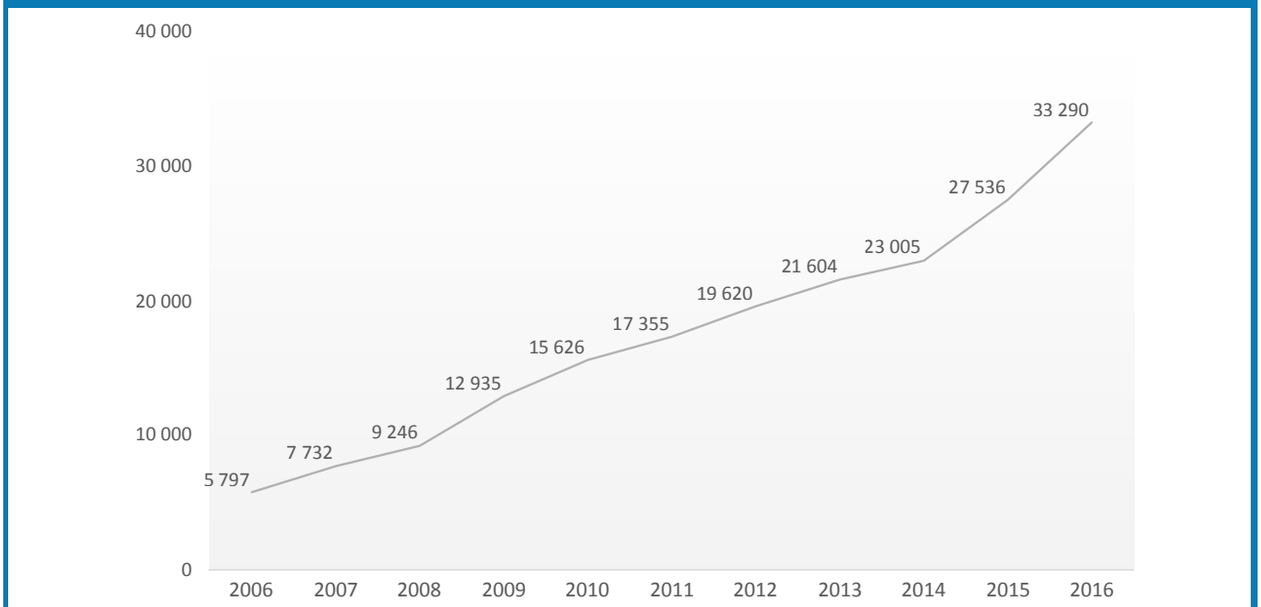
Source: author's own study based on https://www.iso.org/standard

basis for certification of the information security management system.

The ISO/IEC 27001 standard has international coverage while defining requirement and principles for initiating, implementing, maintaining and improving information contains best practices for applying security measures in the areas of information security management.

Back in 2016, the ISO 27001 global certification market rose by 25% compared to a year-by-year period. According to Przemyslaw Szczurek, Product Manager for Information

Chart 1. Number of ISO/IEC 27001 system certificates issued worldwide in 2006-2016



Source: author's own study based on https://www.iso.org.

32 Raport Analiza_rynku_ISO_27001.pdf, p. 3.

Security (TUV Nord Poland), the following reasons seem most motivating while awarding certifications for information security management systems:

- improving security of company's information and that entrusted to us by business partners,
- increasing the company's value,
- building competitive advantage[32]

Chart 1 illustrates the number of ISO/IEC 27001 system certificates issued worldwide in 2006-2016.

The number of ISO/IEC 27001 certificates awarded over the past eleven years has increased almost sixfold, which may be a sign of increasing awareness among information security managers. Back in 2016, the ISO 27001 global certification market rose by 25% compared to year-by-year period. According to Przemyslaw Szczurek, Product Manager for Information Security (TUV Nord Poland), the following reasons seem most motivating while providing certification for information security management systems:

- improving security of company's information and that entrusted to us by business partners,
- increasing the company's value,
- building competitive advantage [33]

Table 13. Top 10 industries with the highest number of ISO IEC 27001 system certificates issued

No.	COUNTRY YEAR	2010	2011	2012	2013	2014	2015	2016
1	Japan	6,237	6,914	7,199	7,140	7,171	8,240	8,945
2	United Kingdom	1,157	1,464	1,701	1,923	2,253	2,790	3,367
3	India	1,281	1,427	1,611	1,931	2,168	2,490	2,902
4	China	509	664	790	965	1,210	1,469	2,618
5	Germany	357	424	488	581	634	994	1,338
6	Italy	374	425	495	901	969	1,013	1,220
7	USA	247	315	415	566	654	1,247	1,115
8	Taiwan	1,028	791	855	918	781	939	1,087
9	Spain	711	642	805	799	698	676	752
10	Netherlands	97	125	190	316	335	455	670

Source: author's own study based on https://www.iso.org.

Table 14. Top 10 industries with the highest number of ISO/IEC 27001 system certificates issued

No.	INDUSTRY	2010	2011	2012	2013	2014	2015	2016
1	Information technology	3,217	3,588	4,558	5,059	4,933	5,573	6,578
2	Services	579	564	755	849	867	959	1,432
3	Transportation	184	241	288	322	327	301	401
4	Electrical and optical equipment	221	280	342	289	287	296	311
5	Financial intermediation	185	113	138	169	187	197	250
6	Engineering services	122	126	189	211	217	201	245
7	Public administration	79	106	155	192	191	212	235
8	Healthcare and social work	102	145	201	201	215	231	220
9	Construction services	266	350	409	396	454	186	216
10	Wholesale and retail trade, repair of motor vehicles, motorcycles and personal and household goods	164	214	215	224	206	198	202

Source: author's own study based on https://www.iso.org.

33 Raport Analiza_rynku_ISO_27001.pdf, p. 3.

Table 15. Number of ISO/IEC 27001 system certificates issued in EU Member States in 2010-2016

Country	2010	2011	2012	2013	2014	2015	2016
Austria	54	59	28	75	87	91	146
Belgium	26	29	31	47	43	53	98
Bulgaria	116	132	208	278	330	273	261
Croatia	24	32	58	69	96	55	110
Cyprus	4	5	9	16	9	13	11
Czech Republic	529	301	264	399	276	381	507
Denmark	6	5	7	8	13	29	68
Estonia	1	1	2	2	3	2	4
Finland	23	27	28	32	33	44	54
France	31	46	66	94	155	227	209
Germany	357	424	488	581	634	994	1,338
Greece	44	45	49	77	62	136	150
Hungary	151	178	199	280	295	323	421
Ireland	24	30	48	54	131	140	175
Italy	374	425	495	901	969	1,013	1,220
Latvia	6	9	9	18	24	24	30
Lithuania	11	14	19	23	25	35	43
Luxembourg	5	8	7	5	7	10	20
Malta	2	2	5	7	7	7	53
Netherlands	97	125	190	316	335	455	670
Poland	229	233	279	307	310	448	657
Portugal	17	20	34	58	55	56	96
Romania	350	575	866	840	893	1,078	513
Slovakia	70	111	127	159	162	232	212
Slovenia	33	31	13	49	58	50	57
Spain	711	642	805	799	698	676	752
Sweden	30	37	32	49	45	61	160
United Kingdom	1,157	1,464	1,701	1,923	2,253	2,790	3,367

Source: author's own study based on https://www.iso.org, (DOA: July 10, 2018).

Table 15 presents the number of ISO/EC 27001 system certificates issued in EU Member States in 2010-2016.

s of data collected over a seven-year period indicated that the highest number of certificates has been issued in the United Kingdom; in 2016, 3,367 certificates were awarded, which meant a 21-percent increase compared to 2015. Globally, the United Kingdom is ranked second in priority only to Japan where the number of certificates issued amounted to 8,945 in 2016.

An increase in the number of certificates issued has been visible over the past seven years. While taking into account the country's result in 2016, as compared to the previous year, the drop in the number of certificates issued is noticeable in the following countries:

- Bulgaria – by 4%;
- Cyprus – by 15%;
- France – by 8%;
- Romania – by 52%;
- Slovakia – by 9%.

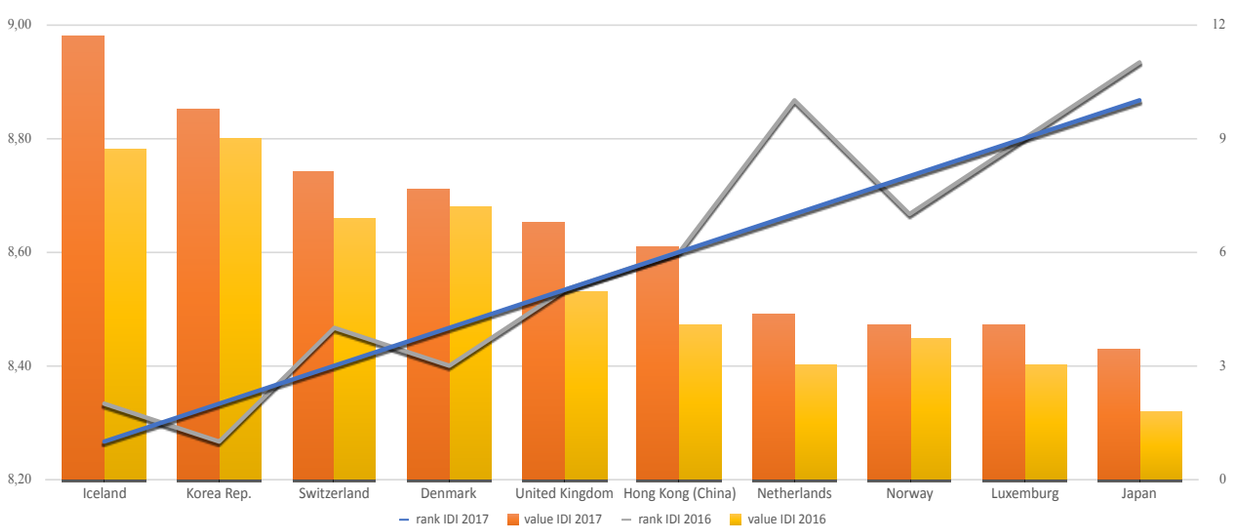
If to take into account particular industries, first place was given to information technologies (total number of certificates issued in 2016: 6,578). Public administration was ranked seventh, with a total of 235 certificates awarded.

Table 16. ITU ICT Development Index in 2017

Country	Index value		Position in ranking	
	2016	2017	2016	2017
Austria	7.70	8.02	24	21
Belgium	7.70	7.81	23	25
Bulgaria	6.86	6.66	53	50
Croatia	6.96	7.24	40	36
Cyprus	7.30	7.77	31	28
Czech Republic	7.06	7.16	39	43
Denmark	8.68	8.71	3	4
Estonia	8.16	8.14	14	17
Finland	7.83	7.88	21	22
France	8.05	8.24	17	15
Germany	8.20	8.39	13	12
Greece	7.23	7.08	38	38
Hungary	6.74	6.93	49	48
Ireland	7.90	8.02	19	20
Italy	6.84	7.04	46	47
Latvia	7.26	7.05	40	35
Lithuania	6.97	7.19	41	41
Luxembourg	8.47	8.40	9	9
Malta	7.86	7.65	25	24
Netherlands	8.49	8.40	10	7
Poland	6.73	6.89	50	49
Portugal	6.88	7.13	44	44
Romania	6.23	6.48	61	58
Slovakia	6.84	7.06	46	47
Slovenia	7.38	7.20	33	33
Spain	7.61	7.79	27	27
Sweden	8.41	8.41	8	11
United Kingdom	8.53	8.65	5	5

Source: author's own study based on www.itu.int.

Chart 2. Top 10 Countries Ranked by ITU ICT Development Index



Source: author's own study based on www.itu.int.

The ICT Development Index (IDI) is an index published by the United Nations International Telecommunication Union. It constitutes one of the world's leading indicators measuring developments in information and communication technology (ICT) of individual countries, their society and economy. It points indirectly to technological advancement of individual states, which in turn translates into a degree of awareness of cyber threats and thus readiness to participate in costs incurred for strengthening cybersecurity.

In 2017, the ITU published the second edition of the index while the first one had been released three years before. The indexes in both reports were based on the same pillars:

1) legal basis - with particular regard to forensics and combatting cybercrime;

2) operational capabilities - comparable to the EU index;

3) organizational measures, including "roadmaps", policies, procedures and assessment systems;

4) constructing state capacity, mostly though development standardization, certification and professional staff development;

5) cooperation between states, agencies, sectors and within interstate organizations.

According to data contained in Table 16 (2017), the following countries were awarded with a total value of 8 points and more in 2016-2017: the United Kingdom, Sweden, the Netherlands, Luxembourg, Germany, France, Estonia, Denmark, followed by Ireland and Austria in 2017. The following countries were granted the value of 7 points and more: Belgium, Cyprus, Czech Republic, Finland, Greece, Latvia, Malta, Slovenia, and Spain. In 2017, they were joined by Croatia, Italy, Lithuania, Portugal, and Slovakia.

Of the 178 countries analyzed in the Top 10 (2017, see Chart 2), the following four EU Member States were classified:

– Denmark was ranked fourth (8.71),

– United Kingdom was ranked fifth (8.65),

– The Netherlands was ranked seventh (8.49),

– Luxembourg was ranked ninth (8.47)

In 2017, the first three positions were held by Iceland (8.98), South Korea (8.85) and Switzerland (8.74). Denmak fell from third (2016) to fourth place (2017) while Sweden, which obtained the same index value of 8.41, fell from eighth (2016) to eleventh position (2017). Both the United Kingdom and Luxembourg managed to remain on the same position, ranked fifth and ninth respectively. In 2016, the Netherlands was ranked tenth, compared to its seventh position in 2017.

In 2018, International Institute for Management Development (IMD), based in Luzern, Switzerland, published the second edition of its annual world digital competitiveness ranking.

The IMD World Digital Competitiveness (WDC) ranking analyzes and ranks countries' ability to adopt and explore digital technologies leading to transformation in government practices, business models and society in general. Based on research, the methodology of the WDC ranking defines digital competitiveness into three main factors: knowledge, technology, future readiness[34].

Of the 63 countries analyzed in the digital competitiveness ranking (2018), the following five EU Member States were ranked among the world's top ten leaders (Chart 3):

– USA – ranked first (third in 2017), with the score of 100.000;

– Singapore – ranked second (first in 2017), with the score of 99.422;

– Sweden – ranked third (second in 2017), with the score of 97.453;

– Denmark – ranked fourth (fifth in 2017), with the score of 96.764;

– Switzerland – ranked fifth (eighth in 2017), with the score of 95.851;

34 IMD WORLD DIGITAL COMPETITIVENESS RANKING 2018, p. 28.

Table 17. IMD World Digital Competitiveness Ranking

Country	Overall			Knowledge		Technology		Future Readiness	
	2018		2017	2018		2018		2018	
	Ranking	Scores	Ranking	Ranking	Scores	Ranking	Scores	Ranking	Scores
Austria	15	86,770	16	13	83,202	26	73,987	14	87,544
Belgium	23	82,165	22	25	73,688	24	76,503	23	80,727
Bulgaria	43	59,032	45	41	58,072	42	57,869	55	45,578
Croatia	44	57,528	48	44	57,211	49	52,609	54	47,189
Cyprus	54	54,891	53	55	49,765	56	45,618	44	53,715
Czech Republic	33	71,488	32	38	60,959	31	73,064	34	64,864
Denmark	**4**	**96,764**	**5**	**8**	**89,447**	**10**	**87,571**	**1**	**97,700**
Estonia	25	80,845	26	29	70,736	20	79,794	26	76,428
Finland	**7**	**95,248**	**4**	**9**	**85,753**	**4**	**92,667**	**8**	**91,748**
France	26	80,753	25	20	75,005	19	79,795	27	71,882
Germany	18	85,405	17	14	81,413	21	77,708	20	81,518
Greece	53	56,287	50	51	51,071	51	50,747	46	51,467
Hungary	46	57,099	44	48	53,292	40	60,146	58	42,284
Ireland	20	84,285	21	22	74,711	29	73,188	13	89,380
Italy	41	64,958	39	42	57,368	41	58,366	36	63,563
Latvia	35	69,172	35	34	65,618	32	70,688	39	55,635
Lithuania	29	76,059	29	23	74,464	30	73,131	33	65,007
Luxembourg	24	81,490	20	32	65,957	15	81,797	21	81,140
Netherlands	**9**	**93,886**	**6**	**12**	**83,259**	**8**	**88,325**	**4**	**94,498**
Poland	36	68,557	37	33	65,629	37	63,838	37	60,627
Portugal	32	73,441	33	27	71,818	36	66,443	32	66,485
Romania	47	57,092	54	45	55,503	44	57,564	57	42,632
Slovakia	50	56,536	43	49	52,301	47	54,340	53	47,393
Slovenia	34	71,427	34	26	72,692	38	62,319	35	63,695
Spain	31	74,272	30	31	67,385	33	69,438	30	70,416
Sweden	**3**	**97,453**	**2**	**7**	**92,037**	**5**	**90,700**	**5**	**94,045**
United Kingdom	**10**	**93,239**	**11**	**10**	**84,946**	**13**	**83,362**	**3**	**95,832**

Source: author's own study based on IMD WORLD DIGITAL COMPETITIVENESS RANKING 2018

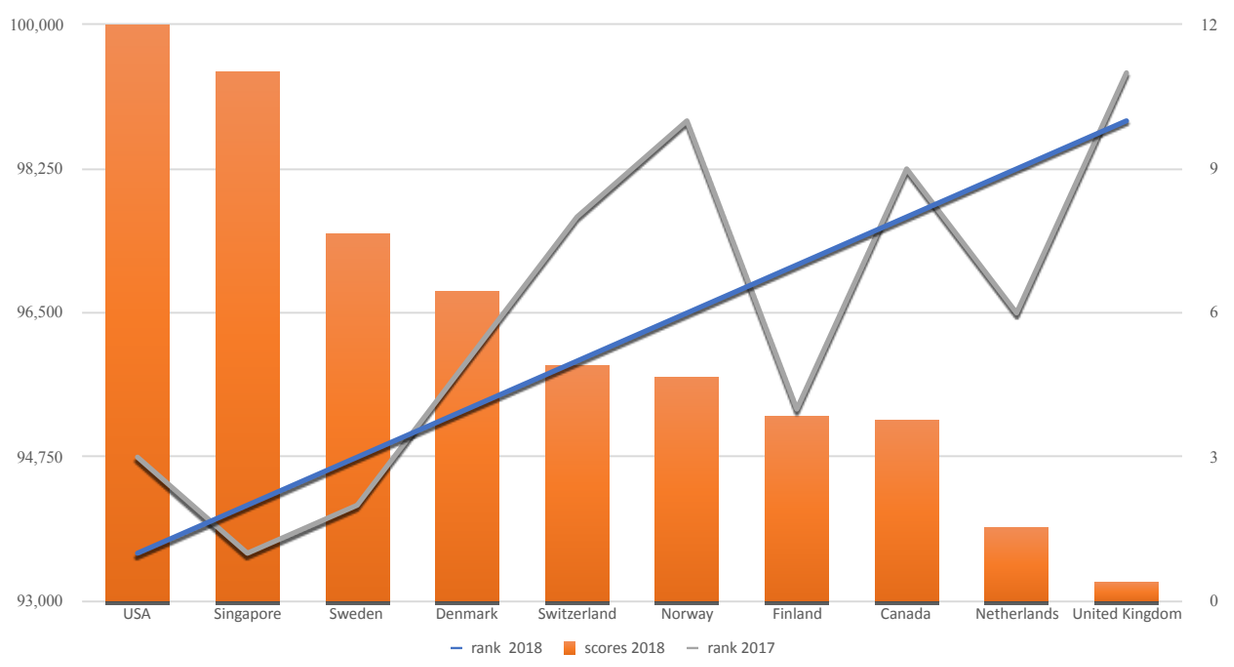
- Norway – ranked sixth (tenth in 2017), with the score of 95.724;
- Finland – ranked seventh (fourth in 2017), with the score of 95.248;
- Canada – ranked eighth (ninth in 2017), with the score of 95.201;
- Netherlands – ranked ninth (sixth in 2017), with the score of 93.886;
- United Kingdom – ranked tenth (eleventh in 2017), with the score of 93.239.

The National Cyber Security Index is a global index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for building national cybersecurity capacity. The indicators of the NCSI have been developed according to the national cybersecurity framework. The NCSI Score shows the percentage the country received from the maximum value of the indicators. The maximum NCSI Score is always 100 (100%) regardless of whether indicators are added or removed[35].

The indicators of the NCSI have been developed according to the national cybersecurity framework. The fundamental cyber threats are:

35 https://ncsi.ega.ee/methodology/, August 17, 2018.

Chart 3. Top 10 IMD World Digital Competitiveness Ranking



Source: author's own study based on IMD WORLD DIGITAL COMPETITIVENESS RANKING 2018

1. Denial of e-services - services are not available
2. Data integrity breach - unauthorized modification
3. Data confidentiality breach - secrecy is exposed

These threats directly affect normal functioning of national information and communication systems and, through the ICT systems, electronic services (including critical e-services).

In addition to the NCSI Score, the index table also shows the Digital Development Level (DDL). The DDL is calculated according to the ICT Development Index (IDI) and Networked Readiness Index (NRI). The DDL is the average percentage the country received from the maximum value of both indexes. The difference shows the relationship between the NCSI score and DDL. A positive result shows that the country's cybersecurity development is in accordance with, or ahead of, its digital development. A negative result shows that the country's digital society is more advanced than the national cybersecurity area[36].

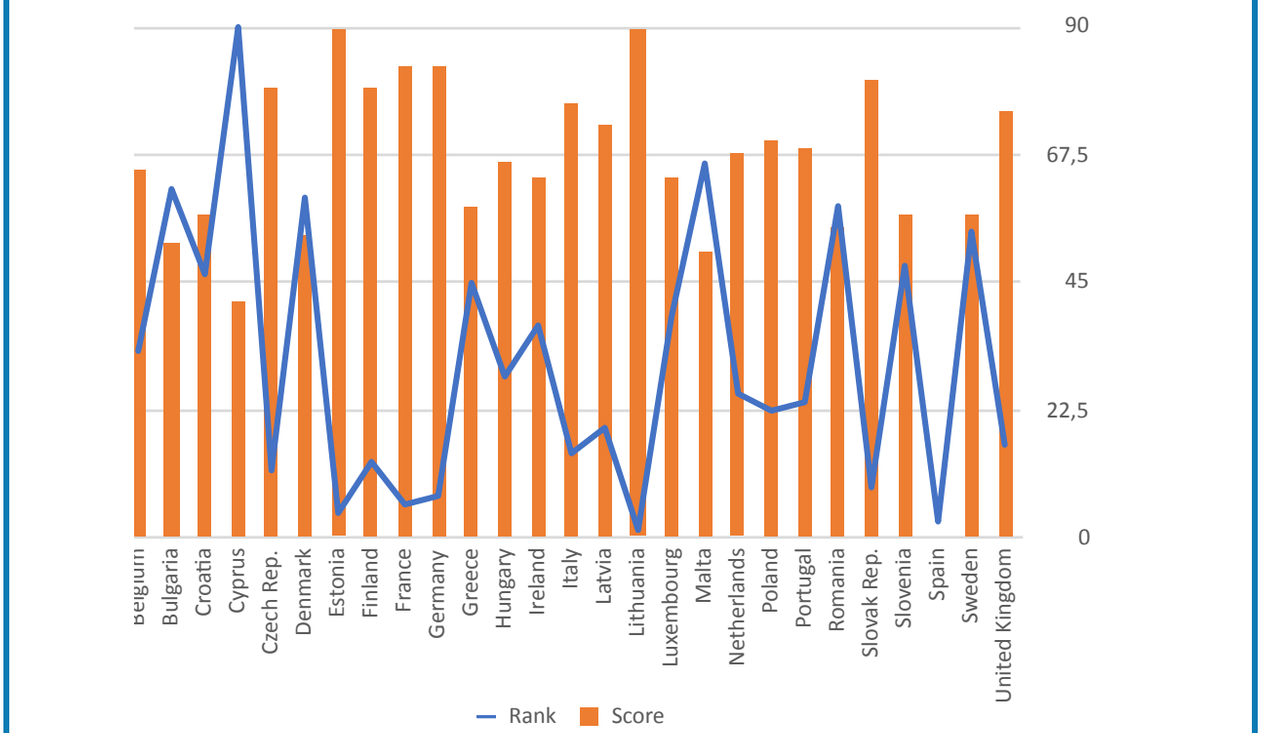
Chart 4 illustrates the current NCSI index while Table 18 shows the difference between the NCSI and DDL scores.

Of 124 countries taken into account in 2018, as many as nine EU Member States were classified in the world's top ten:

- Lithuania – ranked first with the score of 89.61%,
- Spain – ranked second with the score of 89.61%,
- Estonia – ranked third with the score of 89.61%,
- France – ranked fourth with the score of 83.12%,
- Germany – ranked fifth with the score of 83.12%,
- Slovakia – ranked sixth with the score of 80.52%,
- Czech Republic – ranked eighth with the score of 79.22%,
- Finland – ranked ninth with the score of 79.22%,
- Italy – ranked tenth with the score of 76.62%.

36 https://ncsi.ega.ee/methodology/, August 10, 2018.

Chart 4. National Cyber Security Index



Source: author's own study based on https://ncsi.ega.ee/ncsi-index/, (DOA: December 22, 2018).

Among non-EU states Singapore was classified as seventh, getting the score of 80.52.

When analyzing correlation between NCSI and DDL results, it can be said scores obtained by 15 countries are negative, which indicates that their digital society is more advanced than the national cybersecurity area. Among these countries are:

- Belgium (score: -12.68);
- Bulgaria (score: -11,64);
- Croatia (score: -9,77);
- Cyprus (score: -30.15);
- Denmark (score: -30.30);
- Finland (score: -3.04);
- Greece (score: -7.00);
- Ireland (score: -14.32);
- Luxembourg (score: -19.42);
- Malta (score: -22.94);
- Netherlands (score: -16.35);
- Portugal (score: -1.82),
- Romania (score: -7.14);
- Slovenia (score: -13.33);
- Sweden (score: -26.31);
- United Kingdom (score: -8.64).

Other EU Member States (except for Austria that has not been included in the NCSI index) achieved positive scores, which means that the cybersecurity development is in line with each country's digital development.

The European Commission publishes every year the Digital Economy and Society Index (DESI) that summarizes Europe's digital performance.

The Digital Economy and Society Index (DESI) is a composite index measuring progress in digital through five components:

1. Connectivity Fixed broadband, mobile broadband and prices.

Table 16. ITU ICT Development Index in 2017

Country	NCSI		DDL	Difference
	Rank	score		
Austria	no data available	no data available	no data available	no data available
Belgium	22	64.94	77.62	-12.68
Bulgaria	41	51.95	63.59	-11.64
Croatia	31	57.14	66.91	-9.77
Cyprus	60	41.56	71.71	-30.15
Czech Republic	**8**	**79.22**	**69.37**	**9.85**
Denmark	40	53.25	83.55	-30.30
Estonia	**3**	**89.61**	**79.27**	**10.34**
Finland	**9**	**79.22**	**82.26**	**-3.04**
France	**4**	**83.12**	**79.06**	**4.06**
Germany	**5**	**83.12**	**81.95**	**1.17**
Greece	30	58.44	65.44	-7.00
Hungary	19	66.23	66.08	0.15
Ireland	25	63.64	77.96	-14.32
Italy	10	76.62	66.63	9.99
Latvia	13	72.73	70.59	2.14
Lithuania	**1**	**89.61**	**70.95**	**18.66**
Luxembourg	26	63.64	83.06	-19.42
Malta	44	50.65	73.59	-22.94
Netherlands	17	67.53	83.88	-16.35
Poland	15	70.13	66.59	3.54
Portugal	16	68.83	70.65	-1.82
Romania	39	54.55	61.69	-7.14
Slovakia	**6**	**80.52**	**66.73**	**13.79**
Slovenia	32	57.14	70.47	-13.33
Spain	**2**	**89.61**	**73.24**	**16.37**
Sweden	36	57.14	83.48	-26.34
United Kingdom	11	75.32	83.96	-8.64

Source: author's own study based on https://ncsi.ega.ee/ncsi-index/, (DOA: December 22, 2018).

2. Human Capital Internet use, basic and advanced digital skills.

3. Use of Internet Services Citizens' use of content, communication and online transactions.

4. Integration of Digital Technology Business digitization and e-commerce.

5. Digital Public Services: eGovernment and eHealth.

Chart 5 and Table 19 illustrate the DESI Index in 2017-2018.

EU countries can be divided into the following three groups based on the results of the DESI Index in 2017-2018:

1. High-performing countries are Denmark, Sweden, Finland, the Netherlands, Luxembourg, Ireland, the UK, Belgium and Estonia (the first nine, bold in the table).

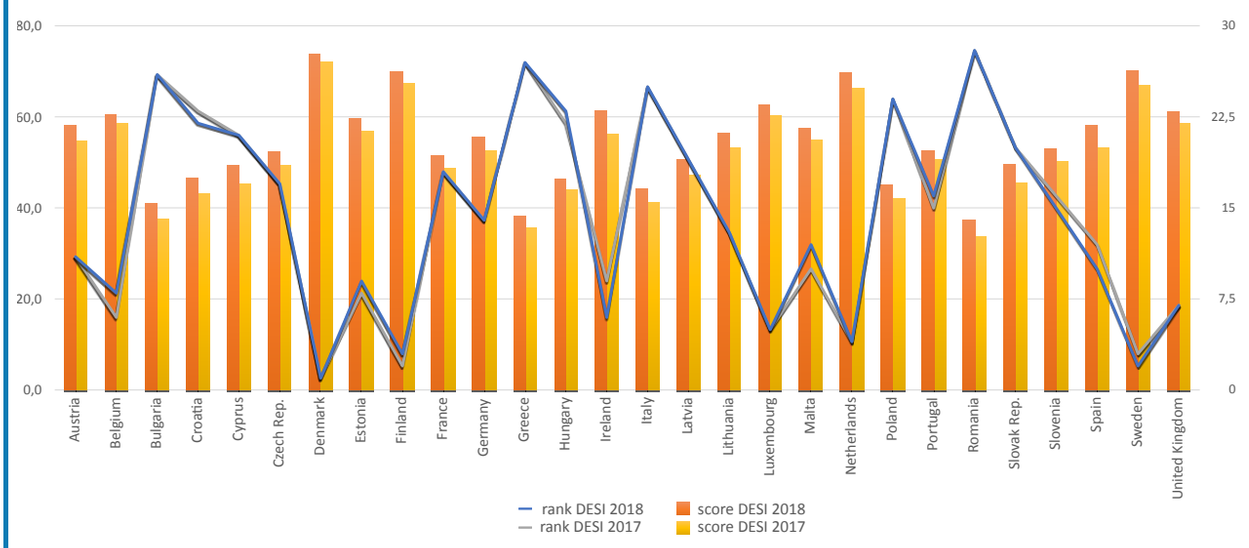
2. Medium-performing countries are Latvia, the Czech Republic, Slovenia, France, Portugal, Spain, Lithuania, Malta, Germany and Austria (next ten, italics in the table).

3. Low-performing countries are Romania, Greece, Bulgaria, Italy, Poland, Hungary, Croatia, Cyprus and Slovakia (last nine).

The Top 10 of The Digital Economy and Society Index (2018):

– Denmark – ranked first with the score of 73.7 (as compared to the first place with the score of 72.1 in 2017);

Chart 5. DESI Index for EU Member States, 2017-2018



Source: author's study based on 2018 reports on digital economy and society index in the EU Member States.

- Sweden – ranked second with the score of 70.4 (as compared to the third place with the score of 67.0 in 2017);
- Finland – ranked third with the score of 70.1 (as compared to the second place with the score of 67.2 in 2017);
- Netherlands – ranked fourth with the score of 69.9 (it remained on the same position yet in 2017 its score amounted to 66.5);
- Netherlands – ranked fifth with the score of 62.8 (it remained on the same position yet in 2017 its score amounted to 60.4);
- Ireland – ranked sixth with the score of 61.3 (as compared to the ninth place with the score of 56.3 in 2017);
- United Kingdom – ranked seventh with the score of 61.2 (managed to retain its position with the score of 58.6 in 2017);
- Belgium – ranked eighth with the score of 60.7 (as compared to the sixth place with the score of 58.6 in 2017);
- Estonia – ranked ninth with the score of 59.7 (as compared to the eighth place with the score of 57.0 in 2017);
- Spain – ranked tenth with the score of 58.0 (as compared to the twelfth place with the score of 53.3 in 2017);

"**Denmark** ranks first out of the 28 EU Member States in DESI 2018. Denmark made progress in most dimensions, with the exception of Integration of Digital Technology. As a leader in digitization, Denmark performed very well in connectivity, thanks to the widest 4G coverage in Europe, and the increase in coverage and take-up of fast and ultrafast fixed broadband connections. Almost all Danes are online, and they make good use of a variety of online services, particularly for banking, shopping and accessing online entertainment. The percentage of ICT specialists is slowly increasing, and a high percentage of Danes have at least basic digital skills. However, some gaps still exist, as evidenced by the fact that more than a quarter of Danes do not have basic digital skills. Denmark also made outstanding progress in the use of digital technologies by enterprises, leading the EU and the world rankings. However, some indicators show areas for potential improvement. Denmark is strong in the delivery of online public services thanks to a consistent long-term national strategy"[37].

37 Digital Economy and Society Index 2018, Country Report Denmark, p. 2.

"In DESI 2018, **Sweden** now ranks second after Denmark. Overall progress is in line with the EU average as well as the countries in the high-performance cluster. Sweden is well connected, ranking fourth in the EU. However, it is a challenge to reach the remaining regions, considered as remote ones. 95% of Swedes are online and make good use of a variety of services. In human capital, Sweden ranks third and shows progress in all DESI dimensions. Despite having the second highest number of ICT specialists in the workforce, demand exceeds supply and the relatively low numbers of STEM graduates are not expected to increase in the coming years. Swedish businesses actively use digital technologies to improve efficiency, productivity and sales, providing the country with the fourth position. In digital public services Sweden now ranks 5th, but open data is still an area where Sweden's performance is relatively weak[38]."

"**Finland** ranks third out of the 28 Member States, with a score that is virtually identical to both the second and fourth place. Its overall score regularly progresses more or less in line with the EU average, which is maintaining its outstanding position. In addition to its leadership position in digital skills, which Finland has already held for several years, it also became the top scorer in digital public services. Moreover, it improved its score in the integration of digital technologies, where it showed up as a frontrunner. While it remained steady in fifth place in terms of Internet services use, it went down two places in the connectivity dimension, which is partly due to the introduction of a new indicator on ultra-fast broadband, a category in which Finland does not score very well. Overall, Finland remains a world leader in digitization and one of EU's leading countries in this domain.[39]"

"The **Netherlands** ranks fourth out of the 28 Member States, only 0.02 score from second position. The country progressed at a faster pace than the EU average, outperforming the other Member States in all five DESI dimensions while improving its ranking in two of them compared to the previous year. The Netherlands continues to be the European leader in connectivity, a domain in which it may boast of high-quality ubiquitous digital infrastructure. These advanced digital networks boost the growth of the Dutch digital economy and society, support highly advanced business, education and science environment while attracting international investments. Almost all Dutch individuals (94%) make extensive use of Internet services, especially for banking (93%) and shopping (82%). Integration of Digital Technology (rank 6) has increased over the last year in most DESI categories. In Digital Public Services (rank 6), the Netherlands improved its scores in terms of all relevant parameters and remains way above the EU average."[40]

"**Luxembourg** ranks fifth out of the 28 EU Member States. Overall, it has maintained its rank and improved its score slightly since last year. Luxembourg performs well in connectivity (second rank in DESI 2018), both for coverage and subscription (take-up). It records very good results (fifth rank in DESI 2018) for human capital, especially in use or in digital skills as a top performer. It achieves very good results for Internet use by its residents (fourth rank in DESI 2018). On the other hand, it lags behind in the integration of digital technologies by companies (twenty-second rank in DESI 2018), for e-business and even more for e-commerce as well as in digital public services (seventeenth rank in DESI 2018)[41]."

"In DESI 2018 **Ireland** ranks sixth, up three places from DESI 2017. Whilst outstanding in some areas (with top rankings in Science, Technology, Engineering and Mathematics (STEM) graduates, the use of online trading by SMEs and Open Data), it lags well behind in others. With more than half of the adult population lacking at least basic digital skills, Ireland continues to suffer from ICT skills shortages. Access to fast broadband has improved, but 6% of rural homes still do not have access to even basic fixed broadband and ultrafast broadband coverage remains below the EU average. In Digital Public Services, Ireland ranks top for Open Data and is in second place for business services. However, it ranks comparatively when it comes to the use of eHealth services. Addressing the gaps in Human Capital and Connectivity would help improve Ireland's positioning in the remaining dimensions. These two aspects are also critical for

38 Digital Economy and Society Index 2018 Country Report - Sweden, p. 2.
39 Digital Economy and Society Index 2018, Country Report Finland, p. 2.
40 Digital Economy and Society Index 2018, Country Report the Netherlands, p. 2.
41 Digital Economy and Society Index 2018, Country Report Luxembourg, p. 2.

individuals, enterprises and public bodies to make the best use of digital technology.[42]"

"The **United Kingdom** ranks seventh out of the 28 EU Member States in DESI 2018. While its ranking remained unchanged over 2017, its score increased somewhat due to an improved performance in all DESI domains. UK citizens are well connected: broadband coverage and take-up (fixed and mobile), and NGA coverage are high. Furthermore, progress is being made with NGA take-up. Most UK citizens are now online and make good use of a variety of online services, particularly for shopping, accessing online entertainment and for social networking. Their digital skills are also improving. However, some gaps still exist. In particular, one-third of people still have no digital skills and computer science graduate numbers not increased, despite growing demand on the labor market. Use of digital technologies by businesses in the UK shows a mixed picture. While use of Social Media, Cloud and eCommerce is relatively high, use of Electronic Information Sharing, RFID and eInvoices is very low and showing little improvement. While the UK performs relatively well on a number of eGovernment indicators, online service completion and provision of prefilled forms is relatively low. To reap the full benefits of the digital transformation, the UK needs, in particular, to improve business integration of digital technologies, the level and availability of digital skills and some elements of its digital public service provision.[43]"

"**Belgium** ranks eighth out of the 28 EU Member States in DESI 2018. While its absolute performance improved in all DESI domains, its ranking slightly slipped compared with 2017, also due to the good performance of other countries in its peer group. Residents of Belgium are well connected: broadband coverage and take-up (fixed and mobile), and next generation access network (NGA) coverage are high. Furthermore, progress is being made with NGA take-up. Most people in Belgium are now online and make good use of a variety of online services, particularly for shopping, entertainment and social networking. Their digital skills are good but not improving. However, some gaps still exist. The country's key challenges in connectivity are to convince more people to use mobile broadband. Despite a lot of innovative projects being launched to boost digital skills, the impact of these initiatives on human capital is not yet reflected in the statistics. A key challenge in this area is to motivate more young people in Belgium to start a career in digital technology and more generally to attract more pupils to consider studying a subject related to science, technology or mathematics ('STEM'). When it comes to the integration of digital technology by companies, Belgium is doing well, and there are several complementary strategies in place to further digitize Belgian businesses. For digital public services, Belgium shows an overall mixed picture, and progress compared to past years has been lower.[44]"

"**Estonia** ranks ninth out of the 28 EU Member States. The country progressed over the last year but more slowly than the EU average. Estonia remains a leading country in Europe for digital public services, as it has been for many years. Its citizens are well skilled in the use of digital technologies and are keen users of a variety of internet services. Regarding connectivity, fixed broadband coverage is very low (partially compensated by mobile coverage), as is the take-up of ultrafast broadband. The key challenge in the Estonian economy remains the digitization of companies.[45]"

"**Spain** ranks tenth out of the 28 EU Member States in the European Commission Digital Economy and Society Index (DESI) 2018. Its score increased due to an improved performance in all of the DESI dimensions measured. Spain performs well in connectivity, thanks to the wide availability of fast and ultrafast fixed and mobile broadband networks and to the increasing take-up. Most Spanish people make good use of a variety of online services. Spain improved with regards to human capital, but still scores slightly below the average. In particular, one fifth of Spanish citizens are not yet online and close to half of them still do not have basic digital skills. Despite growing demand on the labour market, the supply of ICT specialists is still below the EU average. Spain made biggest progress when it came to the use of digital technologies by businesses. More Spanish businesses use social media, electronic invoices, cloud and e-commerce. Among all dimensions, Spain ranks highest in the eGovernment domain.[46]"

42 Digital Economy and Society Index 2018, Country Report Ireland, p. 2.
43 Digital Economy and Society Index 2018, Country Report United Kingdom, p. 2.
44 Digital Economy and Society Index 2018, Country Report Belgium, p. 2.
45 Digital Economy and Society index 2018, Country Report Estonia, p. 2.
46 Digital Economy and Society Index 2018, Country Report Spain, p. 2.

Table 3. Thematic scope of the National Cyber Security Strategy

Country	DESI 2018		DESI 2017		Connectivity				Human Capital			
					DESI 2018		DESI 2017		DESI 2018		DESI 2017	
	rank	Score	rank	score	rank	score	rank	score	rank	score	rank	score
EU		54.0		50.8		62.6		58.5		56.5		54.6
Austria	11	58.0	11	54.7	17	63.7	17	58.8	7	64.4	7	62.4
Belgium	8	60,7	6	58.6	5	75.1	4	72.7	12	57.5	11	57.3
Bulgaria	26	41.0	26	37.7	25	54.9	23	51.6	27	34.8	27	31.1
Croatia	22	46.7	23	43.2	27	49.4	27	44.2	18	49.8	19	45.9
Cyprus	21	49.3	21	45.2	19	60.6	20	55.5	24	43.0	25	37.5
Czech Republic	17	52.3	17	49.3	16	63.9	16	59.0	13	55.1	13	53.1
Denmark	1	73.7	1	72.1	3	78.5	3	74.5	6	70.4	6	69.0
Estonia	9	59.7	8	57.0	15	64.1	10	62.1	10	61.4	9	58.0
Finland	3	70.1	2	67.2	9	66.1	7	65.0	1	79.2	1	76.7
France	18	51.5	18	48.8	23	56.4	21	52.7	11	59.1	10	57.4
Germany	14	55.6	14	52.7	13	64.7	11	62.1	8	62.9	8	61.6
Greece	27	38.4	27	35.5	28	43.1	28	39.8	26	38.2	26	36.7
Hungary	23	46.5	22	44.2	18	61.7	18	57.7	21	48.0	18	49.2
Ireland	6	61.3	9	56.3	11	65.1	15	59.7	9	61.7	12	56.0
Italy	25	44.3	25	41.4	26	52.8	25	49.8	25	40.8	24	39.7
Latvia	19	50.8	19	47.2	10	65.9	12	61.7	23	43.8	22	44.1
Lithuania	13	56.6	13	53.2	12	64.8	13	61.4	19	48.5	20	45.7
Luxembourg	5	62.8	5	60.4	2	80.1	1	77.9	5	71.3	2	73.2
Malta	12	57.7	10	54.9	6	73.1	6	67.2	17	51.6	17	50.0
Netherlands	4	69.9	4	66.5	1	81.1	1	77.8	2	74.3	3	72.3
Poland	24	45.0	24	42.1	21	58.8	22	52.0	20	48.3	21	45.7
Portugal	16	52.6	15	50.7	8	67.4	9	63.8	22	45.8	23	42.9
Romania	28	37.5	28	33.7	22	58.1	26	49.5	28	32.1	28	30.9
Slovakia	20	49.5	20	45.5	24	55.1	24	50.8	16	51.9	15	50.5
Slovenia	15	53.0	16	50.4	20	60.3	19	56.9	15	52.0	14	52.4
Spain	10	58.0	12	53.3	14	64.7	14	60.2	14	54.6	16	50.2
Sweden	2	70.4	3	67.0	4	76.0	5	72.5	3	74.2	5	69.4
United Kingdom	7	61.2	7	58.6	7	68.8	8	64.0	4	71.6	4	71.3

"Over the last year, **Austria** progressed roughly in line with both the EU average and the average for the cluster of medium performing countries, keeping the eleventh place it had in 2017. Its main strengths remain Human Capital and Digital Public Services, but it improved its relative position regarding both the use of Internet services by citizens, where it is lagging behind, and the integration of digital technology by businesses, where it scores significantly above average. These improvements come despite a connectivity ranking is still in the lower half of EU countries, although Austria's score improved considerably. Austria's ranking has also been affected by the introduction of new indicators on ultra-fast broadband, where it performs less well than the majority of other Member States.[47]"

"**Malta** ranks twelfth out of the 28 EU Member States. Overall, it progressed at an average pace over the last few years. Malta performs above the EU average in broadband connectivity and the use of Internet services by citizens. Malta remains a European leader on the availability of fixed broadband (basic, fast and ultrafast), being the only Member State with full coverage of ultrafast networks. Malta scores also very well in the provision of digital public services. The key challenges are digital skills, especially the low number

47 Digital Economy and Society Index 2018, Country Report Austria, p. 2.

Use of Internet Services				Integration of Digital Technology				Digital Public Services			
017	DESI 2018	DESI 2017		DESI 2018		DESI 2017		DESI 2018		DESI 2017	
score	rank	score	rank	score	rank	score	rank	score	rank	score	rank	Score
54.6		50.5		47.5		40.1		36.7		57.5		53.7
62.4	19	47.6	20	43.9	10	44.1	12	39.4	8	66.5	7	66.3
57.3	13	53.3	11	51.9	5	54.6	5	52.4	15	57.9	15	52.3
31.1	26	41.7	26	38.6	26	24.4	26	22.5	23	49.7	22	45.2
45.9	11	54.1	14	50.2	21	35.4	17	34.6	25	44.4	25	41.4
37.5	17	51.1	13	50.9	17	37.7	18	34.2	18	54.8	17	50.0
53.1	20	46.4	21	43.0	13	40.4	11	40.8	22	50.2	23	44.7
69.0	1	75.1	1	73.9	1	61.3	1	62.4	3	73.2	3	71.3
58.0	8	61.6	6	60.0	19	37.1	20	31.6	2	78.1	1	77.4
76.7	5	65.4	6	61.8	2	60.9	3	55.7	1	78.6	2	75.8
57.4	24	42.2	25	40.3	16	37.8	16	34.7	13	58.4	13	55.6
61.6	14	52.7	18	47.3	12	41.3	14	38.8	21	50.2	21	46.2
36.7	22	45.2	22	42.0	24	26.9	23	24.4	28	39.2	27	35.0
49.2	12	53.6	12	51.7	25	25.1	24	23.5	27	40.4	28	33.6
56.0	15	52.3	16	47.8	3	60.0	2	55.7	10	64.7	9	60.6
39.7	27	37.4	27	36.1	20	36.8	19	33.0	19	52.5	19	47.0
44.1	10	54.8	10	54.5	23	27.0	25	22.7	9	65.2	14	53.7
45.7	9	56.8	9	55.6	9	47.5	8	44.1	7	68.2	8	61.6
73.2	4	65.9	3	63.9	22	33.2	22	29.9	17	56.2	20	47.0
50.0	6	63.3	8	59.0	15	38.9	13	38.8	11	61.3	10	60.0
72.3	3	66.5	4	62.2	6	52.3	6	48.0	6	70.5	6	67.2
45.7	25	42.1	24	40.4	27	23.5	27	21.6	24	48.2	18	48.5
42.9	21	46.3	19	43.9	11	41.9	9	42.9	12	59.6	11	59.0
30.9	28	35.0	28	29.0	28	17.8	28	18.6	26	41.4	26	44.2
50.5	16	51.3	15	49.4	18	37.4	21	30.2	20	50.4	24	44.6
52.4	23	44.9	23	41.4	8	47.9	7	46.0	16	57.3	16	51
50.2	18	49.4	17	47.5	7	49.8	10	41.7	4	72.4	4	68.5
69.4	2	73.4	2	71.4	4	56.4	4	53.8	5	70.8	5	67.4
71.3	7	62.4	7	59.4	14	40.0	15	36.9	14	58.2	12	56.2

Source: author's study based on "The Digital Economy and Society Index 2018".

of STEM (science, technology and mathematics) graduates and open data. The improvement of digital skills is also vital to enhance the integration of digital technologies in enterprises.[48]"

"**Lithuania** ranks thirteenth out of the 28 EU Member States in the Digital and Society Index (DESI) 2018. Lithuania's DESI score is above the EU average and the country has progressed at the same pace as the EU over the last year. Lithuania performs particularly well in terms of Connectivity and the Integration of Digital Technology. Lithuania has improved in Human Capital as well, but it is still below the EU average. This is largely due to the constant drop in the proportion of STEM graduates and the persisting low proportion of ICT specialists as a fraction of employed individuals, although a positive trend in the latter has been seen in the last couple of years. Lithuanian Internet users are very active online in using new services over mobile, e.g. payment instruments, mobile e-signature, car parking, banking services, etc. As concerns Digital Public Services, Lithuania is above the EU average and has significantly improved compared to last year and is making continuous progress towards increasing its uptake of eGovernment services.[49]"

48 Digital Economy and Society Index 2018, Country Profile Malta, p. 2.
49 Digital Economy and Society Index 2018, Country Profile Lithuania, p. 2.

"**Germany** ranks fourteenth out of the 28 EU Member States. Overall, it progressed over the last year. It is performing well as regards fixed broadband take-up and prices. However, there is an obvious urban-rural digital divide as regards fast Internet coverage and the share of fibre connections is very low throughout the country. Germans have good digital skills (seventh rank), although a shortage of ICT professionals may hamper the potential of Germany's economy. German Internet users are very active online shoppers and German enterprises are active in selling online. The country's greatest digital challenge is to improve the online interaction between public authorities and citizens. With only 39% of the population being eGovernment users, Germany ranks twenty-fifth among the Member States in this respect.[50]"

"**Slovenia** ranks fifteenth out of the 28 EU Member States in the European Commission's Digital Economy and Society Index (DESI). Slovenia made significant progress in the use of Internet services and the delivery of digital public services. Slovenia remains above the EU average in the integration of digital technology. Human capital levels are stable. However, connectivity remains below the EU average, and the rollout and take-up of fast and mobile broadband is progressing slower than planned. Promoting the use of the Internet and digital public services will improve take-up of and demand for digital services. Enhanced efforts to improve connectivity are a necessary precondition for a successful digital transformation in Slovenia.[51]"

"**Portugal** ranks sixteenth out of the 28 EU Member States. The country's overall score increased slightly, although in a smaller proportion than the EU average. Portugal's scores have gone up in all DESI dimensions except for integration of Digital Technologies. Noteworthy improvements relate to take-up of fixed and mobile broadband services as well as Internet usage by citizens, although there is still room for further improvement in all of these areas. Although Portugal progressed faster than the EU average in all components of the Human Capital dimension, low digital skills levels, particularly among the elderly and those with low levels of education or on low incomes, continue to entail risks of digital exclusion and hinder progress in most of the other dimensions of DESI.[52]"

"The **Czech Republic** ranks seventeenth out of the 28 EU Member States. Over the last year, the country progressed across all dimensions, with the exception of the Integration of Digital Technologies, where its score was slightly lower than in 2017. The Czech Republic is very well positioned in terms of 4G coverage (99%). However, take-up of mobile broadband is growing at a slower pace.[53]"

"**France** ranks eighteenth out of the 28 EU Member States. Overall, it retains its ranking with some slight improvements to its score, making overall some progress. France has achieved good results in digital skills, both basic and advanced, in particular because of a high proportion of scientific and technical graduates (ninth rank). France occupies an average position in terms of e-government (use and services offered online) and performs well in open data. However, France has a level of connectivity that is below the EU average, in particular because of a low degree of coverage for the 4G mobile band and for fast and ultra-fast broadband. Furthermore, companies in France have a below average degree of integration of digital technologies.[54]"

"**Latvia** ranks nineteenth in the DESI 2018, its position has remained unchanged for the last two years. The country has progressed in line with the EU average. Progress has been driven by improvements in connectivity — both coverage and take-up of ultrafast broadband are relatively high — and in digital public services — due to the launch of the national data portal as well as the life events approach being adopted in the provision of public services. More and more Latvians are using Internet banking and eGovernment services, but half of the population has no or low digital skills. Improving citizens' digital skills is necessary for Latvia to benefit from an inclusive labour market, as well as for improving the productivity of businesses, which make only limited use of digital.[55]"

50 Digital Economy and Society Index 2018, Country Report Germany, p. 2.
51 Digital Economy and Society Index 2018, Country Report Slovenia, p. 2.
52 Digital Economy and Society Index 2018, Country Report Portugal, p. 2.
53 Digital Economy and Society Index 2018, Country Report Czech Republic, p. 2.
54 Digital Economy and Society Index 2018, Country Report France, p. 2.
55 Digital Economy and Society Index 2018, Country Report Latvia, p. 2.

"**Slovakia** ranks twentieth out of the 28 EU Member States in the European Commission's Digital Economy and Society Index (DESI) 2018, having made progress on previous years. While its ranking remained unchanged from 2017, its score increased due to an improved performance in all of the DESI dimensions measured. Slovaks are average Internet users and made good use of a variety of online services. Availability of fixed broadband and 4G services are not as widespread as would be desirable, but ultrafast broadband coverage is well above the EU average. For human capital, the supply of ICT specialists is still below the EU average despite growing demand on the labour market. On eGovernment, Slovakia is progressing well and now ranks twentieth. However, the number of eGovernment users is below the EU average. Improving its broadband infrastructure will help the country reap the full benefits of digital transformation.[56]"

"**Cyprus** ranks twenty-first out of the 28 EU Member States. Overall, Cyprus is progressing slowly but steadily. It shows improvement in all aspects of DESI. Even though it is ranked twenty-first, Cyprus is relatively close to the EU average. Improvement in digital skills is crucial, since, although Internet users engage in a wide variety of online activities, low levels of digital skills could hold back its digital economy and society. Moreover, despite some progress in the past few years, Cyprus still lags behind the EU average in supply and demand for eGovernment services.[57]"

"**Croatia** ranks twenty-second out of the 28 EU Member States. Overall, it made good progress over the last year. Croatian citizens are above average Internet users and enterprises are also keen to employ digital technologies. Croatia's greatest challenge in digital remains its low performance in connectivity (ranked twenty-seventh). Rural broadband connectivity and fast broadband coverage are limited, while prices for fixed broadband remain the highest in Europe. The incumbent, altogether with its subsidiaries, has a very high market share. In terms of eGovernment, Croatia is progressing slowly and remains twenty-fifth. The number of eGovernment users is above the EU average but there has been no progress on the delivery of eGovernment services. Croatia performs well on Open Data and eHealth Services. In order to reap the full benefits of the digital transformation, Croatia needs to improve its broadband infrastructure.[58]"

"**Hungary** ranks twenty-third out of the 28 EU Member States. Overall, it has progressed at an average pace over the last few years. Hungary performs well on Connectivity, thanks to the wide availability and the high take-up of fast and ultrafast broadband. Hungary scores below the average on human capital, since half of the population does not have basic digital skills, and there is a low number of STEM (science, technology and mathematics) graduates. Although the use of ICTs by businesses and e-commerce has improved, Hungarian companies are still far from fully exploiting the opportunities offered by digital technology. The improvement of digital skills is also vital to enhance the integration of digital technologies within enterprises. As for Digital Public Services including eHealth, the situation has somewhat improved, but Hungary still ranks twenty-seventh, scoring below the EU average in all aspects.[59]"

"In the Digital Economy and Society Index **Poland** ranks twenty-fourth out of the 28 EU Member States, the same as in 2017. It has been making steady progress over time at a pace equal to the EU. In 2017, it improved its ranking in the Connectivity and Human Capital. It has also improved its performance on Use of Internet, Integration of Digital Technology and Digital Public Services. Poland has visibly improved in mobile broadband take-up, fast and ultra-fast broadband take-up and has moderately improved in all Human Capital indicators. Despite improvements in the usage of video calls, social networks and online shopping, Poland's ranking slipped in the use of Internet. It maintained its ranking on Integration of Digital Technology despite significant improvements in electronic information sharing, the use of cloud services and e-invoices.[60]"

"**Italy** ranks twenty-fifth out of the 28 Member States. It made progress in general over the last year, and its DESI ranking remained unchanged. Integration of Digital Techologies and Digital Public Services are the main drivers of digital progress in Italy. Another positive aspect is the NGA generation, which is now much better (from twenty-third in 2016 to thirteenth in 2017). As in previous years, the main challenge is

56 Digital Economy and Society Index 2018, Country Report Slovakia, p. 2.
57 Digital Economy and Society Index 2018, Country Report Cyprus, p. 2.
58 Digital Economy and Society Index 2018, Country Report Croatia, p. 2.
59 Digital Economy and Society Index 2018, Country Report Hungary, p. 2.
60 Digital Economy and Society Index 2018, Country Report Poland, p. 2.

still the low level of digital skills, for which the Italian government has taken some (but not enough) steps. This has a negative impact on the performance of DESI indicators across all five dimensions: take-up of broadband, Internet users, take-up of online services, SMEs selling online and eGovernment users.[61]"

"**Bulgaria** ranks twenty-sixth out of the 28 EU Member States in DESI 2018. Overall, Bulgaria has retained its ranking from last year with some slight improvements to its score. Compared to last year, Bulgaria made progress in connectivity and the availability of digital services. In particular digital public services improved, resulting in an increased number of egovernment users. Bulgaria's main challenges relate to the very low level of digital skills among its citizens — also among young people — and the low integration of digital technologies by businesses. In particular, the low level of digital skills combined with shortages of ICT specialists and underinvestment in digital infrastructures may be among the reasons why the digitisation process in Bulgaria is slow both in the public and private sector.[62]"

"**Greece** ranks twenty-seventh out of the 28 EU Member States. Overall, in recent years, Greece has not made much progress relative to other Member States. It progressed slightly slower than the EU average over the last year. In connectivity, the transition to fast broadband connections is slower than in other EU Member States. On the positive side, 4G coverage has increased in Greece and is now close to the EU average. Greeks are active users of Internet services, and company use of social media is in line with the EU average. But the integration of more sophisticated digital technologies remains low, though the use of e-invoices has progressed to some extent. Greece's performance in digital public services and digital skills remains low and can act as a brake on the further development of the digital economy and society.[63]"

"**Romania** ranks last of the EU-28 in the DESI 2018. While its ranking remained unchanged over 2017, its score increased thanks to an improved performance in four of the five DESI dimensions. However, overall progress last year was slow, and Romania did not manage to catch up. Digitization of the economy and digital skills in the population is low and hinders progress in most of the DESI dimensions. On the other hand, 44% of Romanian homes subscribe to ultrafast broadband (which is the second highest in the EU). ICT contributes 6-7% to Romania's GDP and the digital sector is growing, with two major hubs in Bucharest and Cluj as well as significant ICT investments in other cities.[64]"

61 Digital Economy and Society Index 2018 Country Report Italy, p. 2.
62 Digital Economy and Society Index 2018 Country Report Bulgaria, p. 2.
63 Digital Economy and Society Index 2018, Country Report Greece, p. 2.

6

CONCLUSIONS

The comparison of indicators for individual countries leads to the following conclusions:

- there is a need for constant expenditure analysis as compared to costs/threats at the national level, with particular regard to public and private sectors, critical infrastructure as well as support provided for science, ICT, cybersecurity and development of society/digital economy;

- expenditure analysis as compared to costs/threats shall be linked to one cybersecurity analytics and decision-making center that would be tasked with coordinating activities (and expenses) at the national level;

- both R&D spending and its share in defense expenditure and country's GDP shall be increased as only two countries (France and the United Kingdom) exceeded the 6-percent level while three (Sweden, Poland, and Germany) scored above 2 percent;

- EU Member States are characterized by relatively good cybersecurity potential;

- there is a difference between Europe's most digitally advanced countries and those that are considered less advanced. Further work and investment is required in order to take full advantage of all opportunities offered by the Digital Single Market.

The difference shall be observed based on observation of countries' rank in the indexes/rankings taken into account:

- Denmark is ranked fortieth in the NCSI, first in the DESI, fourth in the IMD World Digital Competitiveness Ranking and third in the ITU ICT Development Index 2017;

- Lithuania is ranked first in the NCSI, thirteenth in the DESI, twenty-ninth in the IMD World Digital Competitiveness Ranking and forty-first in the ITU ICT Development Index 2017;

- Estonia is ranked third in the NCSI, ninth in the DESI, twenty-sixth in the IMD World Digital Competitiveness Ranking and seventeenth in the ITU ICT Development Index 2017;

- The Netherlands is ranked seventeenth in the NCSI, fourth in the DESI, sixth in the IMD World Digital Competitiveness Ranking and seventh in the ITU ICT Development Index 2017;

- France is ranked fourth in the NCSI, eighteenth in the DESI, twenty-fifth in the IMD World Digital Competitiveness Ranking and fifteenth in the ITU ICT Development Index 2017;

- Germany is ranked fifth in the NCSI, fourteenth in the DESI, seventeenth in the IMD World Digital Competitiveness Ranking and twelfth in the ITU ICT Development Index 2017;

- Sweden is ranked thirty-sixth in the NCSI, second in the DESI, third in the IMD World Digital Competitiveness Ranking and eleventh in the ITU ICT Development Index 2017;

6

SUMMARY AND RECOMMENDATIONS

The following analysis indicated that defining appropriate ceilings for cybersecurity expenditure is not an easy task. This is to indicate that governments, public institutions and private entities lack such a tool as all these actors account for estimating short, medium and long-term risks and threats on the basis of which they are able to develop appropriate strategies and programs and allocate adequate financial resources.

It is vital to ensure national-level systemic coordination aimed at minimizing costs on a national scale while performing an efficient expenditure analysis. It is also essential to make national decision-makers aware of costs incurred by the private sector. Conclusions drawn from the following analysis shall affect the process of building the country's scientific, technical and industrial potential in terms of national cybersecurity.

A good decision-making structure is a key to a rational and thus more effective policy of cybersecurity expenditure on a national scale, which should be incurred both by the government (public sphere) and the private sector. It is necessary to define precise national-level competences in the following three areas: detection, protection and response to threats at all levels while initiating and coordinating such activities.

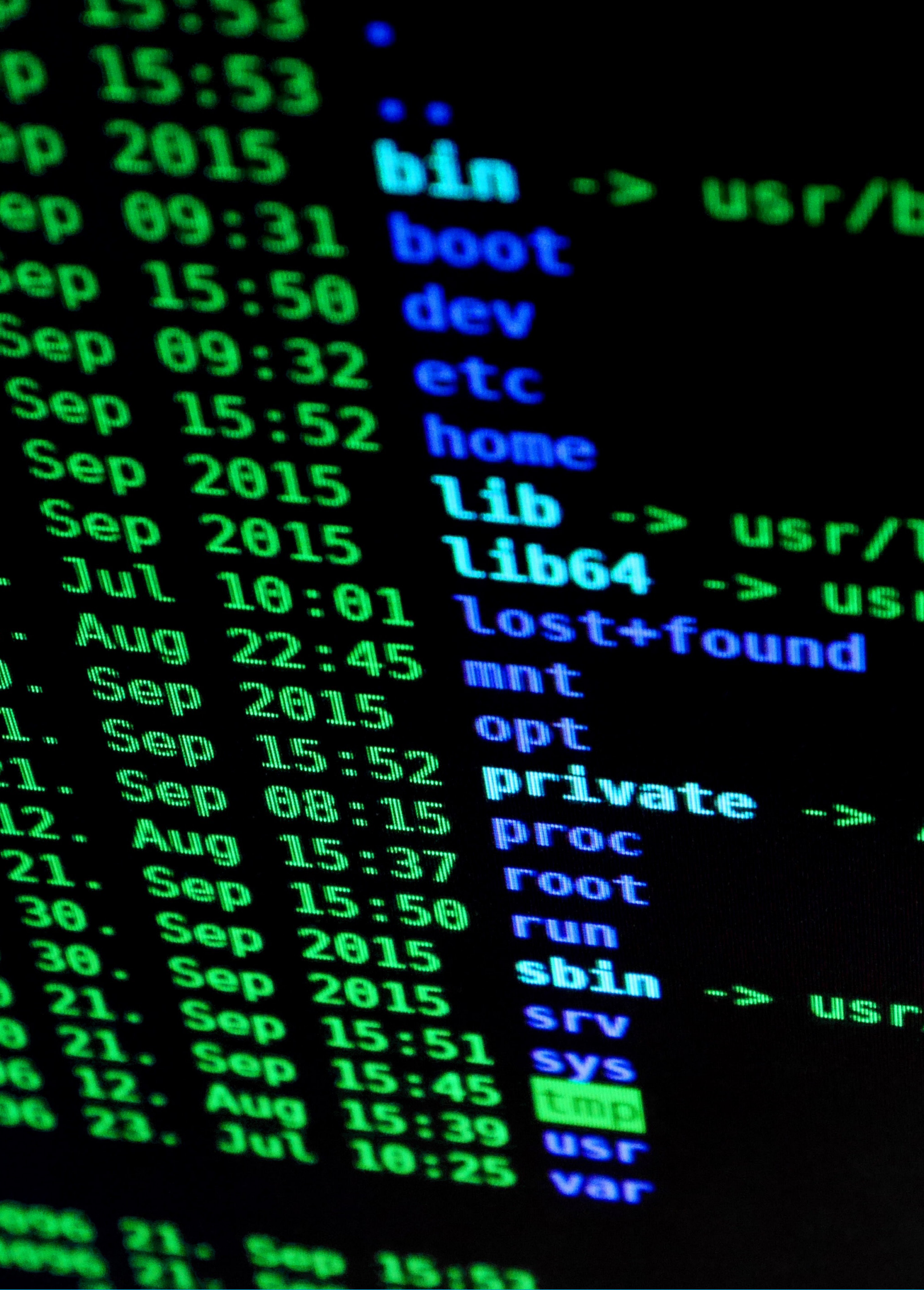
It can be noticed that such small countries with limited resources as Estonia and Lithuania are both highly ranked and listed as top states in the field of cybersecurity. This is a result of strategic choices to invest in cybersecurity and their consequences.

Actions undertaken by the Visegrad Group and the Three Seas Initiative eems to prove that their countries are searching for ways to increase their competitiveness in the domain of cybersecurity through regional cooperation, a solution that shall be considered both just and beneficial. They should allow for even better insight into the challenges while providing adequate allocation of funds and more efficient investment in cybersecurity matters. The Visegrad Group countries are ranked more or less at the EU average level. Good coordination both within and between the V4 states may result in developing their distinct specializations in the field of cybersecurity. It should however be taken into account that they need to struggle with competition from larger states, including France and Germany, countries such as the Netherlands and, last but not least, Estonia and Lithuania.

The European Union is to play a considerable role in the field of cybersecurity. This applies to the regulatory domain as well as its financial aid to the Community's scientific and technological potential with particular regard to innovation, scientific cooperation, strengthening cybersecurity and within the framework of common security and defense policy and counteracting Russian and radical Muslim disinformation online. Therefore it will be vital to plan the EU's Multiannual Financial Framework (MFF) to be properly implemented after 2020.

Developing European programs within the European Common Security and Defense Policy (including PESCO) will be of major importance in relation to constructing cybersecurity strategies. An important feature will include the implementation of decisions made during the NATO summit, held in Warsaw in 2016, in particular further development of EU-NATO cooperation, which will allow to plan expenses in a more efficient way so as not to duplicate actions and investments conducted by both organizations or those under their auspices in individual countries.

The following analysis also points to the need to conduct and develop research of both purpose and task-oriented structure of public spending on all cybersecurity-related objectives. The report has a practical character and serves as a reference for discussion on cybersecurity expenditure in the state budget.


15:53
15:53
2015
09:31
15:50
09:32
15:52
2015
2015
10:01
22:45
2015
15:52
08:15
15:37
15:50
2015
2015
15:51
15:45
15:39
10:25
.
..
bin -> usr/b
boot
dev
etc
home
lib -> usr/
lib64 -> usr
lost+found
mnt
opt
private ->
proc
root
run
sbin -> usr
srv
sys
tmp
usr
var

NOTES

www.europeanreform.org
Follow us @**europeanreform**