



THE DIGITAL 3 SEAS INITIATIVE

Mapping the challenges to overcome

Izabela Albrycht, Krševan Antun Dujmović, Anushka Kaushik, Agnieszka Konkelt,
Iulian Popa, Michał Pilc, Marta Przywała, Ildikó Voller Szenci, Barbara Sztokfisz

with *Geopolitics and the CEE Region*, by Edward Lucas

Editors: Agnieszka Konkelt, Marta Przywała

PARTNERS OF THE DIGITAL 3 SEAS INITIATIVE:



RAKETTAVÄEÜKSUSE KAITSEALAMSUUTLUSE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI - ESTONIA

Publisher: The Kosciuszko Institute
Editors: Agnieszka Konkul, Marta Przywała
Proofreading: Justyna Kruk, Adam Ładziński
Typesetting: Paweł Walkowiak | perceptika.pl

Copyright © 2018

Izabela Albrycht – The Kosciuszko Institute (Poland)
Krševan Antun Dujmović – Institute for Development and International Relations (Croatia)
Anushka Kaushik – GLOBSEC Policy Institute (Slovakia)
Agnieszka Konkul – International Policy Expert (Poland)
Iulian Popa – New Strategy Center (Romania)
Michał Pilc – Poznań Supercomputing and Networking Center (Poland)
Marta Przywała – The Kosciuszko Institute (Poland)
Ildikó Voller Szenci – Antal József Knowledge Centre (Hungary)
Barbara Sztokfisz – The Kosciuszko Institute (Poland)

with *Geopolitics and the CEE Region* by Edward Lucas – CEPA

The report takes into account the conclusions of the discussion entitled 'Civil Advocacy for the Digital 3 Seas Project', which took place during the 4th European Cybersecurity Forum – CYBERSEC 2018. The panellists were: Izabela Albrycht, Laurens Cerulus, Bartosz Cichocki, Anushka Kaushik, Piotr Marczuk, Piret Pernik, Iulian Popa, Tom Reeve, Ildikó Voller Szenci, Karolina Zbytniewska.

© The Kosciuszko Institute, 2018

Public task co-financed by the Ministry of Foreign Affairs of the Republic of Poland under the competition 'Support for the civil and municipal dimension of Poland's foreign policy 2018'.

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the position of the Polish Ministry of Foreign Affairs. Responsibility for the information and views set out in this publication lies entirely with the authors.

The publication is available under license Creative Commons Uznanie autorstwa 3.0 Polska. Some rights are restricted to Stowarzyszenie Instytut Kościuszki. The content was created under the competition 'Support for the civil and municipal dimension of Poland's foreign policy 2018'. It is allowed to use the content under condition of non-disclosure of the above-mentioned information, including information about the license, rights holders and the 'Support for the civil and municipal dimension of Poland's foreign policy 2018' competition.

Krakow, 2018

THE DIGITAL 3 SEAS INITIATIVE

MAPPING THE CHALLENGES TO OVERCOME

Izabela Albrycht, Krševan Antun Dujmović, Anushka Kaushik,
Agnieszka Konkel, Iulian Popa, Michał Pilc, Marta Przywała,
Ildikó Voller Szenci, Barbara Sztokfisz

with *Geopolitics and the CEE Region* by Edward Lucas

Editors: Agnieszka Konkel, Marta Przywała

TABLE OF ABBREVIATIONS

AI	– Artificial Intelligence
BBU	– Baseband Unit
CEE	– Central and Eastern Europe
CECSP	– Central European Cyber Security Platform
C-RAN	– Cloud Radio Access Network
EASME	– Executive Agency for Small and Medium-sized Enterprises
EU	– European Union
DESI	– Digital Economy and Society Index
DIH	– Digital Innovation Hubs
DoS	– Denial-of-Service
D3S	– Digital 3 Seas
EM (Radiation)	– Electromagnetic
GDP	– Gross Domestic Product
GCI	– Global Cybersecurity Index
GEI	– Global Entrepreneurship Index
GII	– Global Innovation Index
ICT	– Information and Communication Technologies
IOI	– International Olympiad in Informatics
IoT	– Internet of Things
ISO OSI Model	– International Organization for Standardization Open Systems Interconnection Reference Model
ITU	– International Communication Union
LAN	– Local Area Network
NCSI	– National Cyber Security Index
NIS Directive	– Directive on security of network and information systems
NIST	– National Institute for Standards and Technology
NFV	– Network Function Virtualization
R&D	– Research and Development
ROI	– Return on Investment
SDN	– Software Defined Network
SME	– Small and Medium Enterprise
STEM	– Science, Technology, Engineering and Mathematics
UN GEE	– UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
WIPS	– Wireless Intrusion Prevention Systems
3S(I)	– Three Seas (Initiative)
3SDH	– 3 Seas Digital Highway

THE DIGITAL 3 SEAS INITIATIVE

**MAPPING THE CHALLENGES
TO OVERCOME**

TABLE OF CONTENTS

THE THREE SEAS REGION – ON THE PATH TO BE A LEADER	6
THE 3 SEAS DIGITAL HIGHWAY	11
THE THREE SEAS REGION IN NUMBERS	17
Key takeaways	35
DIGITAL SKILLS	39
WOMEN IN ICT	49
EU APPROACH TO DIGITAL SKILLS	50
DIGITAL SKILLS PROJECTS	51
Recommendations for the 3S countries	54
DIGITAL INDUSTRY	61
INTEGRATION OF TECHNOLOGY	63
DIGITAL INNOVATION HUBS	69
A DIGITAL FRIENDLY REGULATORY FRAMEWORK	73
Recommendations for the 3S countries	75
ARTIFICIAL INTELLIGENCE AND ROBOTICS	81
SECTORAL APPLICATION OF AI	82
EU APPROACH TO AI	90
ETHICAL ASPECTS OF AI	93
Recommendations for the 3S countries	96

CYBERSECURITY	103
CYBERSECURITY READINESS IN THE 3S	104
CYBERSECURITY MARKET IN THE 3S REGION	107
EU APPROACH TO CYBERSECURITY	109
TRANSATLANTIC CYBERSECURITY COOPERATION	111
ATTACKS ON ELECTIONS AND INFORMATION WARFARE	112
INTERNATIONAL PROSPECTS FOR A COMMON AGREEMENT	114
Recommendations for the 3S countries	116
 5G	 123
BROADBAND COVERAGE IN THE 3S	124
ON THE WAY TO THE 5G TECHNOLOGY	127
5G-RELATED PROJECTS IN THE 3S	133
Recommendations for the 3S countries	134
 GEOPOLITICS AND THE CEE REGION	 139
Russian security policy: aims and means	146
The transatlantic relationship: the end of an affair?	148
Sixteen plus one: China's divide-and-rule strategy in Europe	153
Action points	155

THE THREE SEAS REGION

– ON THE PATH TO BE A LEADER

by Izabela Albrycht

– Chairperson, The Kosciuszko Institute

The Three Seas Initiative

Launched in 2016 by the countries bordering the Adriatic, the Baltic and the Black Seas, the **Three Seas Initiative (3SI)** has been set to deepen integration among 12 Member States of the European Union: Austria, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia, and to strengthen economic competitiveness, connectivity and cohesion of the Central and Eastern European region. The tools to achieve this, namely a new cross-border regional infrastructure, concentrate on increasing interconnectivity in the fields of energy, transport and telecommunication along the North-South axis of the region.

A digital upgrade

As soon as the region's significant and largely untapped potential was recognised, the concept of the 3SI started receiving

more attention, attracting new committed champions to support the cause. Consequently, in June 2018, a group of regional think tanks spearheaded by the Kosciuszko Institute introduced the **Digital 3 Seas Initiative (D3SI)**.

Resting upon an enhanced cybersecurity dimension, the D3SI embraces a disruptive technological change in the global economy. This disruption is powered by digital advancements in all production sectors and in all types of processes, irrespective of geographical location.

Drawing upon the 3SI, the D3SI proposes solutions to tackle this disruptive change within its international framework. Moreover, the D3SI highlights the fact that next to the two pillars of 3SI – energy and transportation, the third, digital pillar is now emerging and becoming increasingly prominent. To enable its development, we need to duly recognise the digital potential of the region and create a favourable and secure ecosystem for it to thrive.

The 3 Seas Digital Highway – a foundational project

On 17 September 2018, the leaders of the 3S countries gathered in Bucharest for the third Three Seas Summit, with the aim to make substantial progress in enhancing their collaboration efforts. One of the summit's outcomes was **a shortlist of main strategic projects in the energy, transport and digital domains**. Within the digital domain, the 3 Seas Digital Highway, an integral part of the D3SI, was identified as one of the priority interconnection projects of the 3SI that can enhance North–South secure digital connections in the region. It was acknowledged that the 3SDH could bridge the gaps in the communication infrastructure including fibre optics (both backbone and access layers) and 5G technology infrastructure. This cross-border digital infrastructure could be deployed along the already planned the 3S transport and energy routes (the Via Carpatia is especially promising one).

The 3SDH underpins the growth of the data economy in the region. It can set the foundations for projects that contribute to the development of modern digital economies and data-driven industries in the region, such as modern cloud-based services and data centres (the so-called 3S data islands), IoT projects, AI technology, e-commerce centres, DIHs and Competence Centres, and the autonomous vehicle industry.

The future ahead

This report provides an overview of strengths and weaknesses of the 3S countries in relation to their economic outlook, the ICT sector development (including cybersecurity) as well as their digital skills pool, digital industry, and emerging technologies, such as 5G and the most up and coming field of AI and robotics.

‘Technology in everything’ and global interconnectivity is now running the world. Therefore, secure digital transformation and systemic support for data-based economy and hi-tech innovations can serve not only as another engine of growth, but also as a lever for leapfrogging and gaining new economic momentum for the region.

Technological advancements also have their geopolitical implications. In the era of a strategic struggle between global powers, a continuous expansion of the Science, Technology, Engineering, Mathematics (STEM) talent pool will determine the outcome of the battle for technological supremacy and economic dominance. Additionally, the economic and digital potential of the 3S region can be unlocked and systematically supported to become a new driver of growth and modernisation, also for the EU.

Setting up strategic goals

The threat of economic stagnation, the so-called middle income trap, which could have prevented the CEE countries from catching up with more advanced economies, was identified and addressed by the Kosciuszko Institute and think tanks from the region in 2015.¹

Therefore, one of the region's strategic goals of the region's strategic goals should be to climb up the global supply chain ladder in IT and cybersecurity sectors and create more value-added products and services. It is up to the 3S countries to develop strategies for both the convergent and innovative growth. Providing systemic support for data-based education, reskilling and development of digitally advanced skilled workforce will help achieve the perfect balance between old-style investments in manufacturing and modern-style funding of cutting edge technologies that focuses on identifying emerging niches and competitive advantages in order to maintain the lead in the technological race and leveraging in the global value chain. The times of being a mere economic follower are over; now the time has come to become a leader.

It takes good projects, money, planning and collaboration...

Technological capacity and resources need to be pooled together in the cooperation with EU Member States and our transatlantic allies. This approach would significantly enhance our agility in identifying upcoming trends and opportunities but, most importantly, in addressing security challenges and threats. An innovation friendly ecosystem requires collaboration, mash-ups and link-ups of the region's most innovative growth engines, such as universities with R&D centres, Digital Innovation Hubs and Competence Centres. It also calls for defining the 3SI's value proposition to boost its domestic potential and attract foreign direct investments. For the ecosystem to be successful, it also requires ramping up cross-border investments as well as developing joint infrastructural projects and trade between 3S countries.

In time to come, we can design and successfully negotiate financial support for secure digital transformation within the next Multiannual Financial Framework (2021-2027), including Horizon Europe's next research and innovation framework programme to help the entire region to flourish. The investments would positively resonate across the EU, enhancing its economy and strengthening its cybersecurity posture.

In this context, the cooperation between the 3S region and the U.S. that concentrates on a transfer of technology, sharing of experiences and achievements of digital transformation as well as the means of addressing cyber threats would be highly beneficial.

... and an enhanced cybersecurity dimension

Without strengthening the resilience of national and regional infrastructures, the 3S will be exposed to cyberattacks and cyber disruptions. Therefore, cybersecurity needs to be properly recognised as an overarching dimension that permeates all the three pillars of the 3SI. It requires capacity building and collaboration within the framework of EU policies and strategies as well as within the international context, such as the Cyber Deterrence Initiative planned by the U.S. National Cyber Strategy. A stronger American bilateral and regional engagement in CEE with respect to cybersecurity has potential for synergy within the 3S.

The present report identifies a set of recommendations for the development and implementation of cutting-edge technologies to unlock economic potential of the region. However, its potential will not be achieved without enhanced cyber cooperation and capabilities within the 3S region, the EU and the transatlantic area.

All this can happen here in CEE, with the 3SI on the rise.

How to read the report?

The report should be considered as a continuation of the Kosciuszko Institute's White Paper *The Digital 3 Seas Initiative: A Call for a Cyber Upgrade of Regional Cooperation* released in June 2018. In order for the report to present as wide range of viewpoints as possible, the representatives of 5 out of 12 3S countries (Croatia, Hungary, Poland, Romania and Slovakia), including think tanks and experts, were asked to participate in the creation of the Roadmap. The chapters reflect the standpoints of several authors from these countries. In addition, the think tanks delegates were asked to take part in a survey with questions concerning all the key topics covered in this publication. Their responses have been woven into the final document in several different forms: main narration, a Case Study and a Success Story. The chapters also give an outline of the current state of play, seen from the perspective of both the 3S region and the EU. Each chapter ends with *Recommendations for the Digital 3 Seas countries* providing specific guidance for the 3S countries and their allies.



SOURCES:

1. Middle-Income Trap in V4 Countries?, The Kosciuszko Institute, 2015





THE 3 SEAS DIGITAL HIGHWAY

The 3 Seas Digital Highway (3SDH) is a concept developed by the Kosciuszko Institute. The project is now on the list of priority interconnection projects announced at the Three Seas Summit in Bucharest in September 2018.¹ The project was submitted by the Polish Ministry of Digital Affairs and the Chancellery of the President of the Republic of Poland and supported by the Polish Ministry of Entrepreneurship and Technology.

The empowering 5G is the nucleus of the idea of connecting the 3S region by means of the 3SDH, which would allow for better and more secure data transfer from the north to the south of the region. The 3SDH could bridge the gaps in the communication infrastructure including fibre optics (both backbone and access layers) and 5G technology infrastructure. This cross-border digital infrastructures could be deployed along the already planned 3S transport and

energy routes (the Via Carpatia is especially promising one).

The 3SDH underpins the growth of the data economy in the region. It can set the foundations for projects that contribute to the development of modern digital economies and data-driven industries in the region, such as modern cloud-based services and data centres (the so-called 3S data islands), IoT projects, AI technology, e-commerce centres, DIHs and Competence Centres, and the autonomous vehicle industry. Technical parameters of the 5G network can be customised to deliver endpoint services and are expected to revolutionise mobile telecommunications by providing access to new mobile technologies not only to citizens, but also, on a large scale, to companies, that will build upon it to maintain their competitive advantage.²

The construction of a modern, robust and secure technology infrastructure can incentivise strategic domestic and foreign investments, promote development and strengthen the position of the companies operating in the region.³ The 3SDH will also enable the creation of an enabling environment for industrial data to be exchanged in safe ecosystems in order to tap into the unexplored potential of the data-based economy of the 3S countries.⁴

The project description underlines its coherence with the EU's priorities and policies as 'it would further deepen digital

cooperation throughout Europe, contributing significantly to the competitiveness of the region and meeting the objectives of the Digital Single Market. At the same time, the 3SDH is coherent with a funding programme focused on transport, energy and digital infrastructure within the trans-European framework network – Connecting Europe Facility. To support infrastructure projects connecting regions within the EU for the period of 2021-2027, the European Commission proposed the allocation of a total budget of EUR 42.3 billion. The digital envelope for improving digital connectivity (very high capacity broadband networks that are crucial for modern digital services) was scheduled for EUR 3 billion. Financially eligible projects are: 5G networks along important transport routes, Gigabit and wireless connectivity to institutions and local communities. The aim of the new proposal is to speed up the digitalisation of the EU economy and deployment of new technologies. Moreover, strengthening digital infrastructure foundations for future EU competitiveness is proposed to be a more significant goal under the next cohesion policy objectives, which will allow 3SDH parties to leverage the European Regional and Development Fund and the Cohesion Fund resources towards mutual benefit in terms of common, high-speed and highly reliable connectivity.⁵

Although the calendar for the 3SDH implementation was preliminarily drafted and

included in the description of the priority interconnection projects, some significant political will be needed to operationalise it.

2018-2019: project design and development phase⁶

- Identification of core country stakeholders and designation of relevant private entities in the 3S region;
- Letter of intent signed by the country stakeholders and designated private partners;
- Development of good practices or criteria for the selection of subcontractors, including telecommunications service operators, cloud-based service providers, vertical and virtual private 5G networks;
- Development of common security models and good practices related to the construction of 5G networks (this is happening now in the U.S.);
- Identification of currently available funds: public (national, European, international) and private that can serve as the 'seed capital' for the project;
- Common advocacy of the letter signatories during the negotiations of the next EU Multiannual Financial Framework (2021-2027) in order to ensure that:
 - the 3S region will receive increased financial assistance from the European Cohesion Fund and the European Regional

Development Fund, and that a significant portion of the funds will be allocated for cyber-resilient digital infrastructure projects that are critical for a further development of the economy based on telecommunications networks and systems, and are fundamental for balancing growth opportunities;

- the Connecting Europe Facility digital envelop will get appropriate funds allocation that reflects the digital transformation needs of the 3S countries;
- trans-border digital projects will be intentionally considered eligible for the European Cohesion Fund and European Regional Development Fund.

2020 – Implementation phase

- Creation of the final proposal of the 3SDH Map;
- Signing of the consortium for the deployment of the 3SDH;
- Preparing and submitting relevant applications for the European/national funds;
- Building the 3SDH (only if sufficient funding is provided).



SOURCES:

1. The full list of projects may be found here:
<http://three-seas.eu/press-releases/>.
2. Three Seas Initiative (2018). The Three Seas Initiative – Priority Interconnection Projects [on-line]. Available at:
<http://three-seas.eu/press-releases/>.
3. Ibidem.
4. Ibidem.
5. Ibidem.
6. Ibidem.







THE THREE SEAS REGION IN NUMBERS

Over the last decades, all economies of the 3S countries except Austria have undergone huge transformation. Their transition from closed, centrally planned and very often ineffective economies to highly competitive markets was possible to a great extent due to political and structural reforms, democratisation, entrepreneurship and investment incentives as well as integration processes in the region. With over 100 million consumers (which is more than one fifth of the European population) and with the continuously increasing importance in the global value added, the 3S region is gaining strategic significance for the global economy as a whole. Yet, the development and growth indicators of the 3S countries very often lag behind the rest of Europe. However, the continuous strong growth and low unemployment rates prove the region is developing in a very dynamic way. Generally, more favourable investment environment than that of Western neighbours may help the 3S countries breach this development gap.

The aim of this chapter is to present the key economic indicators of the 3S countries and juxtapose them with those of the EU28 to reveal the genuine economic potential of the 3S countries.

POPULATION

In 2017, the population of the 3S region totalled over 111 million (1.), which represents almost 22 % of the total EU population (over 512 million).

Being the sixth largest EU country in terms of population, Poland is also the largest nation in the 3S region with almost 38 million citizens. Romania, the second biggest country in the region with 19.5 million citizens, is almost half as populous as Poland.

1. POPULATION BY COUNTRY IN 2017

Austria	8 809 212
Bulgaria	7 075 991
Croatia	4 125 700
Czech Republic	10 591 323
Estonia	1 315 480
Hungary	9 781 127
Latvia	1 940 740
Lithuania	2 827 721
Poland	37 975 841
Romania	19 586 539
Slovakia	5 439 892
Slovenia	2 066 748
EU	512 461 290
Three Seas Total	111 536 314
Share in the EU	21,76%

Source: World Bank, 2018, Population, total.

GROSS DOMESTIC PRODUCT

In 2017, the share of the 3S countries in the total GDP of the EU equalled 10.81 % (2.).

The GDP per capita (3.) was lower than the EU average in all 3S countries, except Austria. The lowest rates were observed in Bulgaria and Romania (less than one fourth and one third of the EU average respectively).

2. GDP (CURRENT BLN USD) IN 2017

Austria	416,60
Bulgaria	56,83
Croatia	54,85
Czech Republic	215,73
Estonia	25,92
Hungary	139,14
Latvia	30,26
Lithuania	47,17
Poland	524,51
Romania	211,80
Slovakia	95,77
Slovenia	48,77
EU	17 277,70
Three Seas Total	1 867,34
Share in the EU	10,81

Source: World Bank, 2018, GDP (current USD).

3. GDP PER CAPITA IN 2017

Austria	47 290 912,00
Bulgaria	8 031 598,00
Croatia	13 294 515,00
Czech Republic	20 368 139,00
Estonia	19 704 655,00
Hungary	14 224 846,00
Latvia	15 594 286,00
Lithuania	16 680 678,00
Poland	13 811 664,00
Romania	10 813 717,00
Slovakia	17 604 951,00
Slovenia	23 597 292,00
EU	33 715 127,00
Three Seas Average	19 362 332,27

Source: World Bank, 2018, GDP (current USD).

In 2017, the average GDP growth rate in the 3S countries (4.2 %) was a 1.8-percentage-point higher than the EU average (2.4 %). Romania (6.9 %), Slovenia (5 %), Estonia (4.9 %) and Poland (4.6 %) were the countries with the highest growth rates (4.).

4. GDP GROWTH (ANNUAL %)

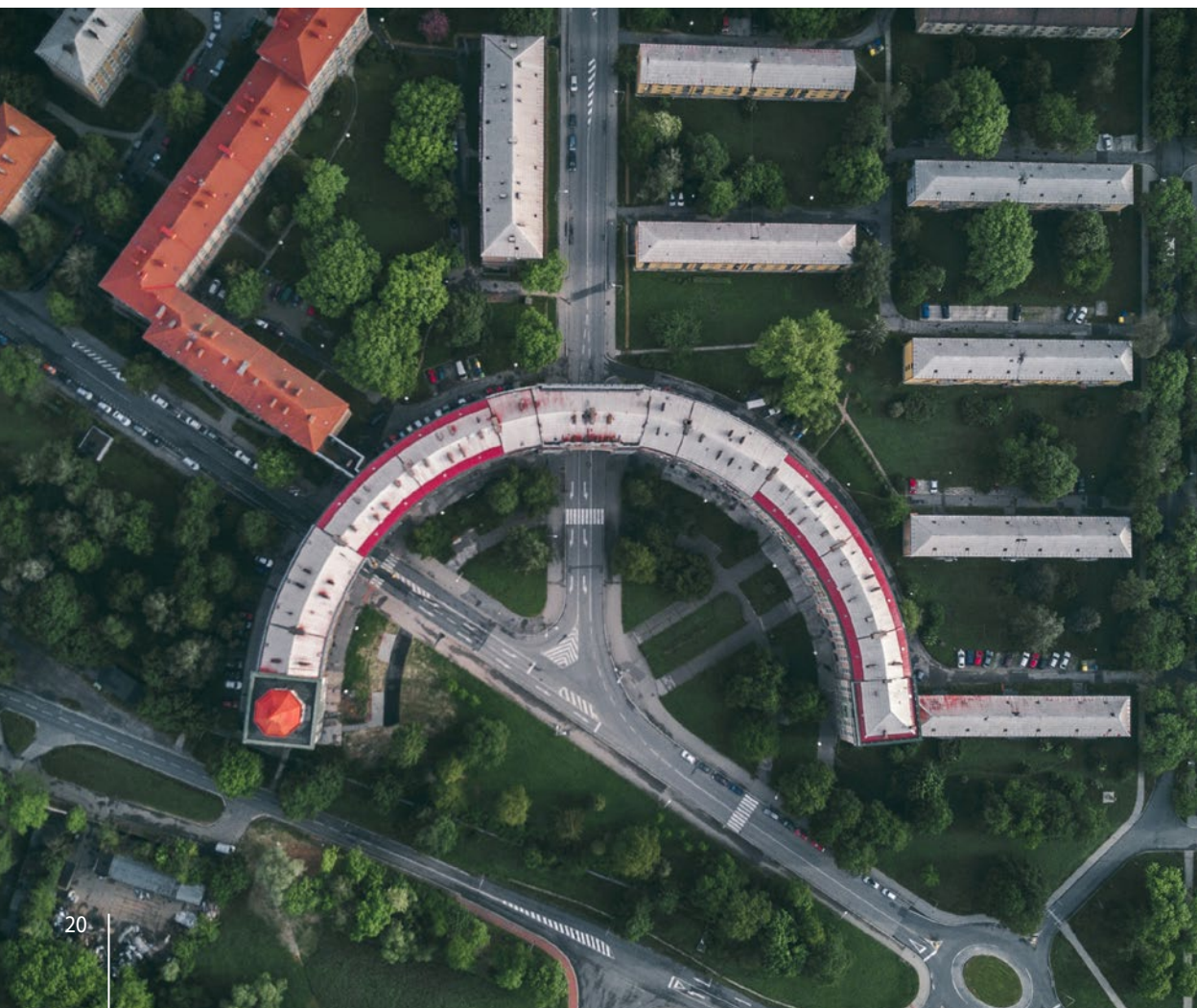
	2010	2011	2012	2013	2014	2015	2016	2017
Austria	1,80	2,90	0,70	0,00	0,80	1,10	1,50	3,00
Bulgaria	1,30	1,90	0,00	0,90	1,30	3,60	3,90	3,60
Croatia	-1,40	-0,30	-2,20	-0,60	-0,10	2,30	3,20	2,80
Czech Republic	2,30	1,80	-0,80	-0,50	2,70	5,30	2,60	4,30
Estonia	2,30	7,60	4,30	1,90	2,90	1,70	2,10	4,90
Hungary	0,70	1,70	-1,60	2,10	4,20	3,40	2,20	4,00
Latvia	-3,90	6,40	4,00	2,40	1,90	3,00	2,20	4,50
Lithuania	1,60	6,00	3,80	3,50	3,50	2,00	2,30	3,80
Poland	3,60	5,00	1,60	1,40	3,30	3,80	2,90	4,60
Romania	-2,80	2,00	1,20	3,50	3,10	4,00	4,80	6,90
Slovakia	5,00	2,80	1,70	1,50	2,80	3,90	3,30	3,40
Slovenia	1,20	0,60	-2,70	-1,10	3,00	2,30	3,10	5,00
EU	2,10	1,70	-0,40	0,30	1,70	2,30	2,00	2,40
Three Seas Average	0,98	3,20	0,83	1,25	2,45	3,03	2,84	4,23

Source: World Bank, 2018, GDP growth (annual %).

LABOUR MARKET

In 2017, the average unemployment rate for the 3S region was 6.3 % (5.), which in the analysed period of 2013-2017 was lower than the EU average.

In 2017, in the EU (and therefore the 3S region), the lowest unemployment rate was recorded in the Czech Republic (2.9 %). The highest rate in the region was observed in Croatia (11.1 %) and Latvia (8.7 %). To compare, among all EU countries, the biggest rate was recorded in Greece (21.5 %), Spain (17.2 %) and Italy (11.2 %) (5.).



5. UNEMPLOYMENT RATE (%)

	2013	2014	2015	2016	2017
Austria	5,4	5,6	5,7	6,0	5,5
Bulgaria	13,0	11,4	9,2	7,6	6,2
Croatia	17,4	17,2	16,1	13,4	11,1
Czech Republic	7,0	6,1	5,1	4,0	2,9
Estonia	8,6	7,4	6,2	6,8	5,8
Hungary	10,2	7,7	6,8	5,1	4,2
Latvia	11,9	10,8	9,9	9,6	8,7
Lithuania	11,8	10,7	9,1	7,9	7,1
Poland	10,3	9,0	7,5	6,2	4,9
Romania	7,1	6,8	6,8	5,9	4,9
Slovakia	14,2	13,2	11,5	9,7	8,1
Slovenia	10,1	9,7	9,0	8,0	6,6
EU	10,9	10,2	9,4	8,6	7,6
Three Seas Average	10,6	9,6	8,6	7,5	6,3

Source: Eurostat, 2018, Unemployment rate 2007-2017.

The sectoral employment distribution in 1997 and 2017 is presented below (6.). The rate of employment in the least advanced areas of the economy (category no 1: agriculture, forestry and fishing) has dropped significantly over the two decades in all 3S countries. However, as compared to the EU, this rate is still high in some countries, especially in Bulgaria (18.9 %) and Romania (despite an almost 18-percentage-point drop, it equalled 23.7 %).

6. EMPLOYMENT BY INDUSTRIAL BREAKDOWNS (% OF TOTAL).

	EU 1997	EU 2017	AT 1997	AT 2017	BG 1997	BG 2017	HR 1997	HR 2017	CZ 1997	CZ 2017	EE 1997
Agriculture, forestry and fishing	8,4	4,5	7,0	3,8	23,3	18,9	14,5	6,9	4,9	3,0	9,3
Industry (except construction)	20,5	15,3	19,5	15,8	25,6	20,1	23,6	19,7	31,7	29,1	25,5
Construction	6,9	6,3	7,8	6,7	4,2	5,0	7,5	6,6	9,3	7,5	7,4
Wholesale and retail trade, transport, accomodation and food service activities	23,1	24,8	27,2	27,0	18,9	25,2	25,1	28,7	22,9	23,7	24,0
Information and communication	2,3	3	2,0	2,6	1,5	2,7	2,2	2,7	1,9	2,8	1,9
Financial and insurance activities	2,7	2,5	3,5	2,8	0,7	1,8	1,9	2,8	1,7	1,7	1,2
Real estate activities	0,9	1,1	1,4	1,4	0,3	0,8	0,1	0,5	1,3	1,8	1,5
Professional, scientific and technical activities; administrative and support service activities	7,9	12,9	6,5	11,9	3,6	7,0	3,9	7,0	6,3	8,6	4,0
Public administration, defence, education, human health and social work activities	22	23,5	21,1	23,4	19,0	15,4	17,8	20,8	17,3	18,1	21,2
Arts, entertainment and recreation; other service activities; activities of household and extra-territorial organizations and bodies	5,3	6,1	3,9	4,5	2,9	3,2	3,3	4,3	2,6	3,6	3,8

Source: Eurostat, 2018, Which sector is the main employer in the EU Member States?

EE	HU	HU	LV	LV	LT	LT	PL	PL	RO	RO	SI	SI	SK	SK
2017	1997	2017	1997	2017	1997	2017	1997	2017	1997	2017	1997	2017	1997	2017
3,5	14,9	5,6	14,6	7,8	20,6	7,8	-	10,2	41,6	23,7	13,3	7,4	8,3	3,0
21,4	25,9	19,8	18,7	15,7	19,9	17,8	-	24,0	25,8	21,9	31,0	22,8	30,2	24,3
7,3	5,4	6,5	6,0	7,0	5,9	7,3	-	7,1	5,3	8,0	6,6	6,4	6,8	7,1
25,3	22,5	24,2	24,9	27,3	21,8	26,9	-	22,8	13,3	21,7	20,3	21,4	21,4	26,3
4,8	1,5	3,1	2,5	3,3	1,2	2,1	-	2,3	1,2	2,2	1,5	3,0	1,9	2,9
1,9	2,1	2,0	1,6	1,8	0,9	1,5	-	2,4	0,9	1,3	2,1	2,2	1,6	2,0
1,6	1,0	1,5	2,1	2,5	0,4	1,1	-	0,9	0,4	0,3	0,2	0,6	0,9	1,1
8,1	3,3	10,8	4,4	9,1	3,5	8,2	-	6,6	2,0	4,5	6,7	13,3	5,4	10,3
21,1	19,5	22,2	22,0	20,6	23,7	22,9	-	20,2	7,2	13,5	15,1	18,9	21,2	20,0
5,0	3,8	4,4	3,2	4,8	2,1	4,5	-	3,5	2,4	2,8	3,1	4,0	2,3	3,0

The category representing the information and communication sector (category no 5), which is the driving force of digital economy, is on the rise in each country. The biggest change, from 1.9 % to 4.8 % (almost 3 percentage points), was recorded in Estonia.

Minimum monthly wages in the 3S countries are considerably lower than in Western countries (7.). The highest minimum wage among the 3S countries in 2018 was recorded in Slovenia (EUR 842.79), Estonia (EUR 500) and Poland (EUR 480.20). These values are remarkably lower than in the three biggest EU economies of Germany, the UK and France. For example, the lowest minimum wage in the 3S countries that was recorded in Bulgaria (EUR 260.76) is almost six times lower than in France.

7. MONTHLY MINIMUM WAGES (IN EUR, 2018)

Austria	-
Bulgaria	260.76
Croatia	465.72
Czech Republic	468.87
Estonia	500.00
Hungary	418.47
Latvia	430.00
Lithuania	400.00
Poland	480.20
Romania	407.45
Slovakia	480.00
Slovenia	842.79
Three Seas Average	468.57
Germany	1498.00
UK	1463.80
France	1498.47

Source: Eurostat, 2018, *Unemployment rate 2007-2017*.

STANDARD OF LIVING

Since the minimum wage does not reflect the actual cost of living, it is worth highlighting the median equivalised net income (measured by Purchasing Power Parity¹) and comparing it with the three biggest EU economies – Germany, the UK and France (8.).

8. MEDIAN EQUIVALISED NET INCOME (PURCHASING POWER PARITY) IN 2006 AND 2016

	2006	2016
Austria	17 420	23 112
Bulgaria	3 200	6 746
Croatia	-	8 982
Czech Republic	8 261	12 476
Estonia	5 627	11 870
Hungary	6 077	8 271
Latvia	4 475	9 234
Lithuania	4 620	9 360
Poland	5 095	10 854
Romania	-	4 728
Slovakia	4 620	10 469
Slovenia	12 153	15 249
Three Seas Average	7 155	10 946
EU	-	16 452
Germany	15 167	21 179
UK	17 630	17 369
France	14 981	20 624

Source: Eurostat, 2018, Living standard statistics.

The average for the 3S region (10 946) is considerably lower than the EU average (16 452).

An amount higher than the EU average was recorded only in one 3S country – Austria (23 112). A strong increase, however, was achieved between 2006 and 2016 in the whole region. Some countries like Bulgaria, Estonia, Latvia, Lithuania, Poland and Slovakia even doubled the level of the median net income, which translates into a significant increase in the standard of living in these countries.

RESEARCH AND DEVELOPMENT

R&D expenditures are of fundamental importance for the development of economies as they contribute to both social and economic benefits. A well-developed R&D sector boosts innovation and a competitive advantage on the international arena. This correlation will only grow stronger as the global economy is undergoing change and transformation caused by digital technologies. It will require national economies to be agile in order to remain competitive in the global value chain.

When comparing the years 2006 and 2016, the average R&D expenditure (in EUR per capita) in the 3S region increased by 72.9 %, while the amount for the EU as a whole went up by 36.2 %. The largest growth was recorded in Bulgaria (230.2 %), Slovakia (193.1 %) and Poland (173.5 %) (9.).

In terms of R&D expenditure (as % of GDP), only Austria (3.09 %) has a bigger share than the EU average (2.03 %). However, as compared to 2006, this share increased in each country except Latvia (10.). The continued growth may eventually lead to the levelling of expenditures with Western economies.

9. R&D EXPENDITURE (EUR PER CAPITA)

	2006	2016	change
Austria	765.5	1 255	63.9 %
Bulgaria	15.9	52.5	230.2 %
Croatia	69	93.6	35.7 %
Czech Republic	149.3	280.8	88.1 %
Estonia	111.8	205.4	83.7 %
Hungary	89.4	139.5	56.0 %
Latvia	50.4	56.1	11.3 %
Lithuania	57.9	113.4	95.9 %
Poland	39.6	108.3	173.5 %
Romania	20.9	41.4	98.1 %
Slovakia	40.3	118.1	193.1 %
Slovenia	241.5	392	62.3 %
Three Seas Average	137.6	238	72.9 %
EU	435.8	593.7	36.2 %

Source: Eurostat, 2018, Science, technology, digital society.

10. R&D EXPENDITURE (% OF GDP)

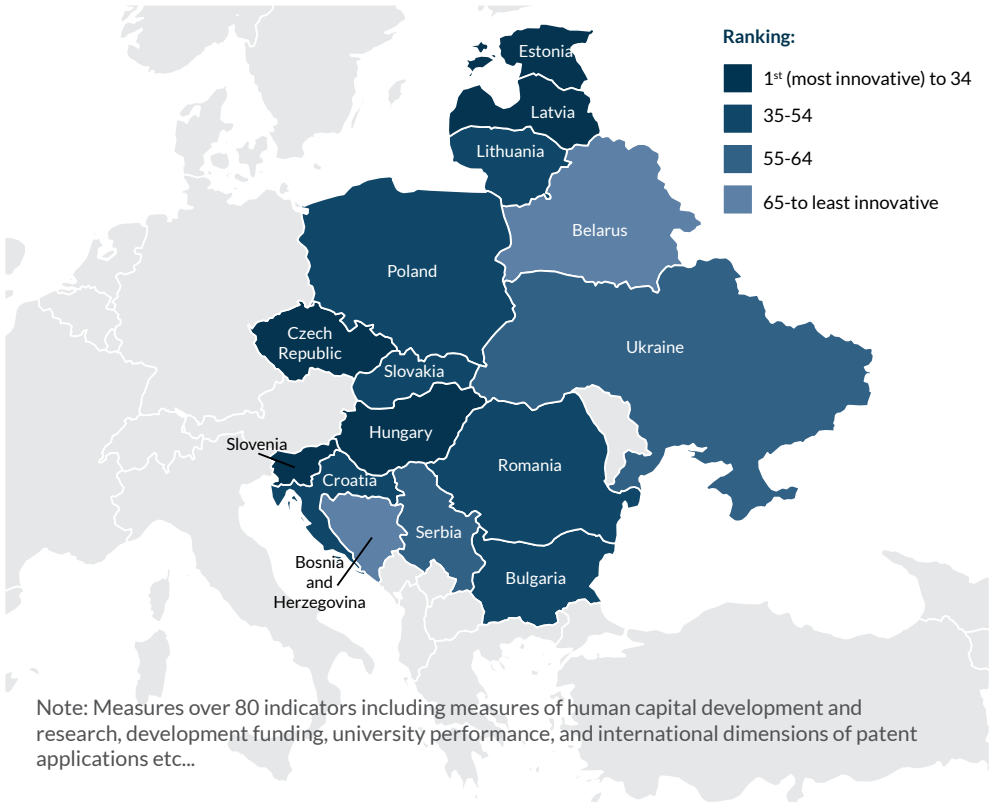
	2006	2016
Austria	2.36	3.09
Bulgaria	0.45	0.78
Croatia	0.74	0.85
Czech Republic	1.23	1.68
Estonia	1.12	1.28
Hungary	0.98	1.21
Latvia	0.65	0.44
Lithuania	0.79	0.85
Poland	0.55	0.97
Romania	0.45	0.48
Slovakia	0.48	0.79
Slovenia	1.53	2.00
Three Seas Average	0.94	1.20
EU	1.76	2.03

Source: Eurostat, 2018, Science, technology, digital society.

THE LEVEL OF INNOVATION IN THE REGION

In the Global Innovation Index 2018² (11.), Estonia, the Czech Republic, Hungary and Latvia top the list in the 3S region and the first tier of the world's most innovative economies. However, the GII index highlights persistent differences in performance across the continent, a so-called 'EU paradox' both in the EU and the 3S region. Despite having high quality education systems, good research infrastructure and significant scientific results, some countries struggle to translate these assets into tangible innovation, as there is room for improvement regarding the quality of entrepreneurship skills.

11. RANKING IN THE GLOBAL INNOVATION INDEX 2018



Source: Insead, WIPO, Cornell SC Johnson College of Business, 2018.

According to the Global Entrepreneurship Index 2018,³ Northern European countries rank highly among all the EU nations while the 3S region finds itself in the bottom of the ranking. Nonetheless, it was the United Kingdom, Bulgaria, Italy, Poland and Ireland which were top fliers as compared to 2017 GEI scores, placing themselves among the top 10 highest gains worldwide.

The region would see quickest gains by improving networking, i.e. supporting geographic and social networks to connect entrepreneurs.

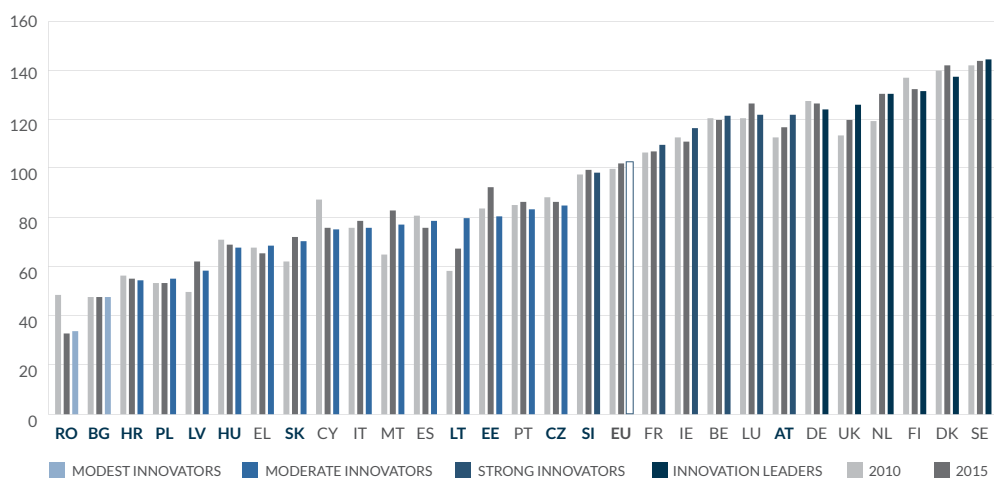
The European Innovation Scoreboard⁴ divides EU countries into modest innovators, moderate innovators, strong innovators and innovation leaders (12.). The scoreboard takes into account different dimensions related to investment (both R&D and venture capital), human resources, research systems, intellectual property, etc.

The majority of the 3S countries are moderate innovators.

Less innovative countries tend to improve their scores faster than more innovative ones. Between 2010 and 2017, Lithuania and Latvia recorded the highest growth among the 3S countries, improving their performance by 20.1 % and 11.6 % respectively. The performance of six countries declined: Romania (-14 %), Estonia (-3.2 %),

the Czech Republic (-2.9 %), Croatia (-2 %), Bulgaria (-1.5 %) and Hungary (-0.1 %). In 2017, the lowest innovation indicator was observed in Romania and Bulgaria (these two countries are in the group of modest innovators). There are only two 3S countries among strong innovators: Austria and Slovenia.

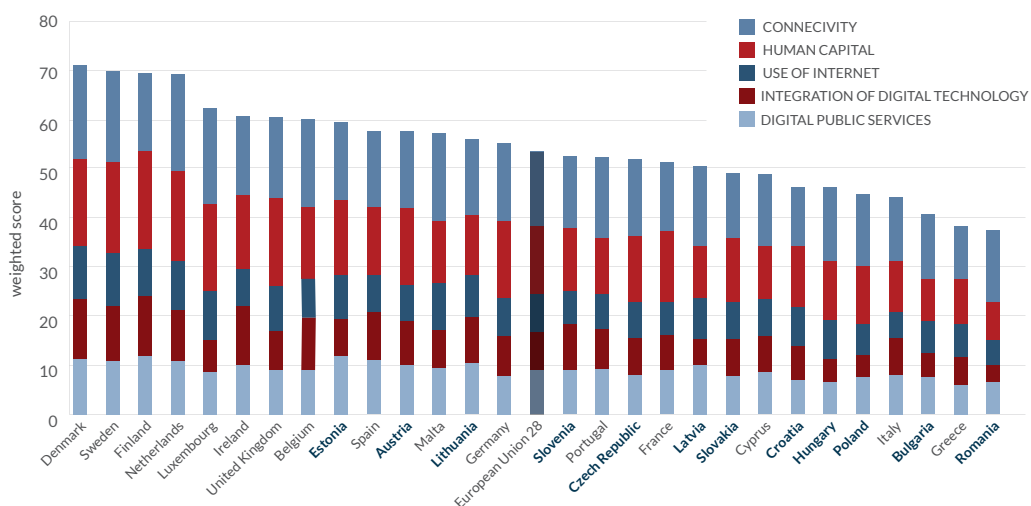
12. EUROPEAN INNOVATION SCOREBOARD. PERFORMANCE OF EU MEMBER STATES' INNOVATION SYSTEMS IN 2016



Source: European Commission, 2017, European Innovation Scoreboard.

The Digital Economy and Society Index⁵ aims to track the evolution of the EU countries in digital competitiveness (13.). The DESI takes into account factors such as connectivity (broadband market development), human capital (digital inclusion and skills), the use of Internet services, the integration of digital technology by business, digital public services and R&D in ICT. Over the past year, the gap between the most and the least digitised countries has been reduced (from 36 to 34 points). However, the majority of the 3S countries are still among the less advanced digital economies. In the 3S region, three countries – Estonia, Austria and Lithuania scored higher than the EU average, being ranked 9th, 11th and 13th respectively, with Slovenia and the Czech Republic following suit. Romania, Bulgaria, Poland, Hungary and Croatia are the lowest performing countries both in the EU28 (along with Greece and Italy) and the 3S region.

13. DIGITAL ECONOMY AND SOCIETY INDEX, 2018 RANKING



Source: European Commission, 2018, DESI composite.

The analysis of DESI results demonstrates how critical it is to further invest in the ICT sector and digital skills. Their homogenous level among the EU countries will translate into a robust digital single market and will boost competitiveness of the 3S region, both within the EU and the global market.

INFORMATION AND COMMUNICATION TECHNOLOGY SECTOR

ICT SHARE IN NATIONAL GDP

The ICT industry has a pivotal role to play in the growth of modern-day economies, being the main driving force behind boosting countries' competitive advantage in the global markets. The ability to leverage the potential of the ICT sector leads to the emergence of new opportunities and the reduction of development barriers. Year by year, the share of the ICT sector in GDP in the majority of the EU Member States is increasing. The same can be observed in the 3S countries.

In a five-year period, from 2010 and 2015, the change in percentage points varied from 0.02 in Estonia to 0.66 in Latvia, with four countries recording a decline: Croatia (-0.43), Slovakia (-0.28), the Czech Republic (-0.16) and Poland (-0.05). In 2015, the highest share of the ICT sector in GDP among the 3S countries was observed in Hungary (5.87 %), while the lowest share was noted in Lithuania (2.92 %). Conversely, Lithuania was a country with the second biggest change between 2010 and 2015 (0.51 percentage points) (14.).

14. PERCENTAGE OF THE ICT SECTOR IN NATIONAL GDP

	2010	2015	change (% points)
Austria	3.12	3.37	0.25
Bulgaria	4.83	5.08	0.25
Croatia	4.61	4.18	-0.43
Czech Republic	4.43	4.27	-0.16
Estonia	4.79	4.81	0.02
Hungary	5.68	5.87	0.19
Latvia	3.54	4.20	0.66
Lithuania	2.41	2.92	0.51
Poland	3.19	3.14	-0.05
Romania	3.13	3.35	0.22
Slovakia	4.67	4.39	-0.28
Slovenia	3.51	3.60	0.09
Three Seas Average	3.97	4.09	0.11

Source: Eurostat, 2018, ICT specialists in employment.

EMPLOYMENT OF ICT SPECIALISTS

The digitalisation of economies has strong impact on production processes and the way people work. Human capital in the ICT industry is a key factor in the development of innovation-driven economies. In 2017, the highest number of individuals working as ICT specialists was recorded in the UK (1.6 million), which accounts for almost one fifth (19.4 %) of the total EU ICT workforce. The double-digit percentage was also observed in Germany (18.6 %) and France (11.8 %).

In 2017, ICT specialists accounted for 3.7 % of the total workforce in the EU, while in the 3S region this share was 3.3 % (a 0.7-percentage-point increase compared to 2007). The share of ICT specialists from the 3S region in the total number of ICT specialists in the EU was 21.1 % in 2007 and 17.8 % in 2017 (15.).

The highest number of ICT specialists in 2017 was recorded in Poland (452 000), which is more than twice as much as in the second-ranked country – Austria (187 800) (16.).

Between 2007 and 2017, the number of ICT specialists in the EU grew by 36.1 % (16.). While the increase of this indicator was mainly driven by the rise in the EU15 (in the 3S countries the increase was only 15.1 %), some 3S economies also recorded strong growth, i.e. Bulgaria (96.1 %), Estonia (76.6 %), Croatia (60.7 %) and Latvia (60.5 %). The drop was observed only in Slovakia (-13.4 %) and Hungary (-2.3 %).

15. PERCENTAGE OF TOTAL EMPLOYMENT

	2007	2017
Austria	3.1	4.4
Bulgaria	1.1	2.3
Croatia	1.9	3.3
Czech Republic	3.8	3.6
Estonia	3.2	5.6
Hungary	4.1	3.6
Latvia	1.2	2.3
Lithuania	1.7	2.7
Poland	2.7	2.8
Romania	1.8	2.1
Slovakia	3.5	2.8
Slovenia	3.3	3.8
Three Seas Average	2.6	3.3
EU	2.8	3.7

Source: Eurostat, 2018, ICT specialists in employment.

16. EMPLOYED ICT SPECIALISTS (TOTAL IN THOUSAND)

	2007	2017	change
Austria	121.9	187.8	54.1 %
Bulgaria	36.2	71.0	96.1 %
Croatia	33.3	53.5	60.7 %
Czech Republic	184.5	184.9	0.2 %
Estonia	20.9	36.9	76.6 %
Hungary	161.4	157.7	-2.3 %
Latvia	12.9	20.7	60.5 %
Lithuania	24.8	36.9	48.8 %
Poland	416.4	452.0	8.5 %
Romania	171.4	185.4	8.2 %
Slovakia	81.4	70.5	-13.4 %
Slovenia	32.1	36.1	12.5 %
Three Seas Total	1 297.2	1 493.4	15.1 %
EU	6 162.0	8 385.1	36.1 %
<i>Share in the EU(%)</i>	<i>21.1</i>	<i>17.8</i>	

Source: Eurostat, 2018, ICT specialists in employment.

However, in the whole EU, only one fifth of businesses (20 %) employ ICT specialists. There are stark differences between SMEs and large enterprises. In 2016, only 19 % of SMEs had ICT specialist on board as compared to 75 % of companies with more than 250 employees. In 2016, among the EU Member States, Finland had the highest proportion (6.6 %) of its total workforce employed in the ICT sector as compared to 3.8 % in the EU28.

It is estimated that the IT workforce in the EU will grow from 8.5 million in 2016 to 9.5 million in 2020. The excess demand or shortage would amount to approximately 750 000 vacancies in 2020. By 2020, there will be around one million ICT graduates in the job market.⁶ Yet, in the EU, around 41 % of employers struggle to recruit ICT specialist. In the 3S region, the problem was most widespread in the Czech Republic (66 %) and Slovenia (63 %).⁷

ICT COMPANIES

Between 2011 and 2015, the total number of ICT companies in the region increased by 30.4 % (17.). The strongest growth was recorded in Lithuania (107.2 %), Latvia (80.1 %) and Estonia (42.7 %). Austria, which is the most innovative country of the 3S region (see LEVEL OF INNOVATION IN THE REGION), recorded the lowest growth (7.6 %). In 2015, the biggest number of ICT companies was recorded in Poland (81 357), the Czech Republic (35 182) and Hungary (31 157). The highest number of ICT specialists in 2017 was recorded in Poland (452 000), which is more than twice as much as in the second-ranked country – Austria (187 800) (16.).

17. NUMBER OF ICT COMPANIES

	2011	2013	2015	change between 2011 and 2015
Austria	14 798	15 388	15 916	7.6 %
Bulgaria	7 685	8 836	10 268	33.6 %
Croatia	5 134	5 438	5 878	14.5 %
Czech Republic	32 705	32 876	35 182	7.6 %
Estonia	2 731	3 364	3 897	42.7 %
Hungary	28 742	26 956	31 157	8.4 %
Latvia	3 405	5 064	6 133	80.1 %
Lithuania	2 779	3 818	5 758	107.2 %
Poland	57 887	69 169	81 357	40.5 %
Romania	16 127	18 188	20 564	27.5 %
Slovakia	11 719	-	16 231	38.5 %
Slovenia	5 422	6 091	7 210	33.0 %
Three Seas Total	183 712	189 097	239 551	30.4 %

Source: Eurostat, 2018, ICT specialists in employment.

KEY TAKEAWAYS:

- Considering the percentage of the 3S's population (which is 21.76 % of the total EU population), its share in the total EU's GDP is small, signalling a lower level of economic development of the region compared to the rest of Europe.
- Even though the GDP per capita is lower than the EU average in almost the entire 3S region, the GDP growth rates demonstrate that the 3S countries account for a large part of the EU's growth as a whole.
- The strong growth of the ICT sector in the 3S region is clearly visible in data regarding the number of ICT companies. This indicates that the growth tends to be quicker among less innovative countries. A further increase in the number of ICT professionals will boost the development of the sector, enhancing its share in national GDPs. This fact will translate into more innovative economies and a wider implementation of new technologies, both regionally and globally.
- Low unemployment rates are advantageous for the economy, guaranteeing an optimal level of production (effective use of resources), higher consumer buying power and a lesser need for the government indebtedness. Low

unemployment in the 3S countries is undoubtedly beneficial for their economic outlook, being a promising step towards closing the gap between them and the most developed Western economies.



SOURCES:

1. Purchasing power parities are indicators of price level differences across countries. PPPs tell us how many currency units a given quantity of goods and services costs in different countries. Using PPPs to convert expenditure expressed in national currencies into an artificial common currency, the purchasing power standard (PPS), eliminates the effect of price level differences across countries created by fluctuations in currency exchange rates (Eurostat (2018). Glossary: Purchasing Power Parities [on-line]. Available at: [https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Purchasing_power_parities_\(PPPs\)](https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Purchasing_power_parities_(PPPs)))
2. Insead, WIPO, Cornell SC Johnson College of Business (2018). Global Innovation Index [on-line]. Available at: <https://www.globalinnovationindex.org/Home>.
3. Global Entrepreneurship and Development Institute (2018). Global Entrepreneurship Index [on-line]. Available at: <https://thegedi.org/global-entrepreneurship-and-development-index/>.
4. European Commission (2017). European Innovation Scoreboard [on-line]. Available at: https://ec.europa.eu/growth/industry/innovation/facts-figures/scoreboards_en.
5. European Commission, (2018). DESI composite [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/desi>.
6. Capgemini, Empirica, IDC (2018). Digital Organisational Frameworks and IT professionalism [on-line]. Available at: <https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2015/12/digital-organisational-frameworks-and-it-professionalism.pdf>.
7. Eurostat (2017). Digital economy and society in the EU [on-line]. Available at: <https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-1c.html>.







DIGITAL SKILLS

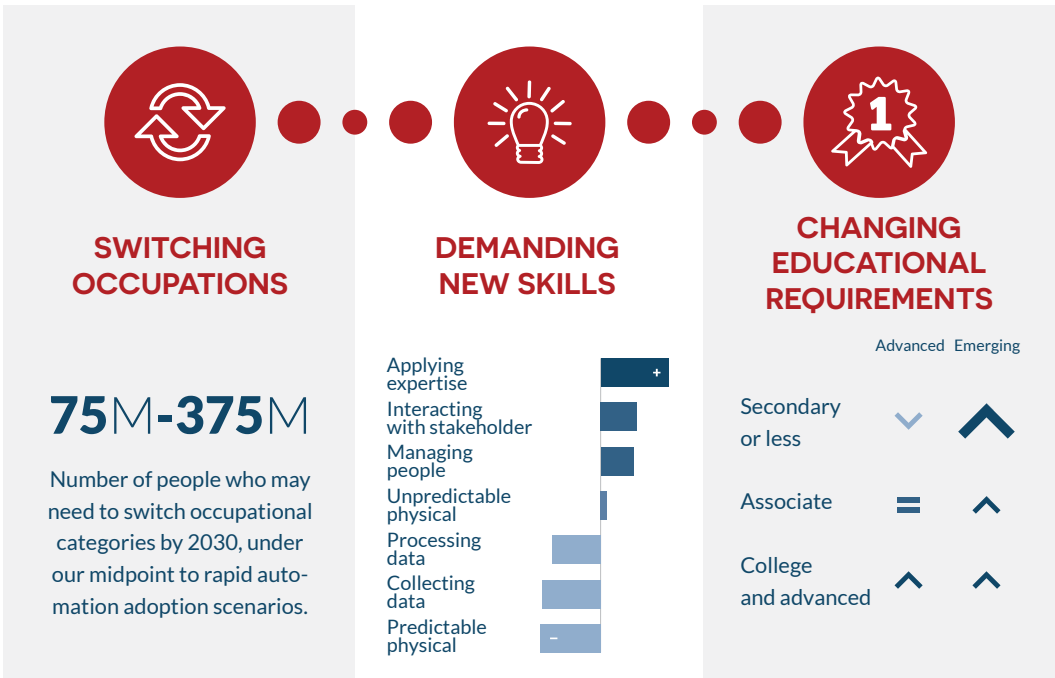
Given the importance of the ICT sector in today's economies and the growing demand for ICT specialists, digital skills are crucial for the inclusive development of societies. The 3S region alone may experience more profound changes due to its historical legacy.

There is a plethora of research on the implications of technology for the job market. A number of misconceptions have grown around the destructive power new technological advancements exert on workforce. In fact, it is expected that both machines and humans will work hand in hand. Although in the short run technological progress is likely to cause significant labour displacements, in the long run it will create a multitude of new jobs and professions, thus offsetting job losses (see ARTIFICIAL INTELLIGENCE AND ROBOTICS). Recent research indicates that by 2025, developments in machine learning and digital automation will cut 75 million jobs (1.), but at the same time generate roughly 133 million new roles.¹ It is a common view that automation will have lesser impact on jobs that consist in managing people, applying expertise or involving social skills.

By 2025, the ongoing changes will create demand for jobs which are today at their infancy, i.e. digital cultural commentator,

ethical technology advocate, human body designer, IoT data creative, personal content creator, space tour guide, sustainable power innovator, freelance biohacker or virtual habitat designer.² While – at this point – such professions might sound quite bizarre and futuristic, their potential is yet to be untapped.

1. WORKFORCE TRANSITION. MCKINSEY'S SCENARIOS FOR AUTOMATION AND LABOUR DEMAND HIGHLIGHT CHALLENGES FOR WORKERS



Source: McKinsey, 2017, *Jobs lost, jobs created. Workforce transitions in time of automation.*³

The emerging jobs will require a wide range of competences spanning science, technology, engineering and mathematics along with problem solving, creativity, argumentation, intellectual curiosity, flexibility,

data-driven decision-making, collaboration, holistic thinking, emotional intelligence, effective oral and written communication, entrepreneurial skills and collaboration across the networks.^{4,5,6} However, STEM

skills should be taught together with arts to produce multi-literate citizens and workforce ready for whatever future holds. IT leaders should add 'A' for fine arts to science and create a new acronym – STEAM, as designing engaging solutions requires creative talent.⁷

To some extent, all jobs will require digital skills, including the sectors not traditionally associated with technology but most susceptible to automation and therefore job loss, such as farming, healthcare, vocational training and construction. At least a basic level of digital skills will be required by 90 % of workers, clerks, technicians or agricultural workers.⁸ A general reduction in physical tasks and increase in jobs requiring a new approach will heighten demand for both basic and advanced digital skills. For people who have not yet entered the job market, specific training (i.e. computer skills, basics of coding, computational knowledge, even in AI if feasible) should ideally begin early in their educational career. For people already in employment, re-skilling will be essential; for those transitioning between jobs, vocational and adult education programs should be offered. Such programs work best when they are short, affordable, industry-specific and closely linked to the requirements of the job market.

However, there is a justified concern that current educational system might not be ready for the challenges of the future. Fur-

thermore, even present day instruction no longer provides adequate skills for the jobs of today, leading to a mismatch of skills.⁹ The mismatch will have profound impact on productivity, for instance in the manufacturing sector. If this skills mismatch is not addressed early enough, it will undermine the professional future of many people, particularly those who might find themselves at disadvantage, e.g. women, young people, underserved and living outside urban areas.¹⁰ Undoubtedly, automation will have a two-fold impact: citizens will have to be prepared for lifelong learning while education systems themselves will need to undergo transformation.¹¹

The digital skills gap, which will occur as a result of the upcoming changes, will need to be addressed at all levels of society, from engineers to ordinary citizens.

In 2017, the average share of population with basic or above basic digital skills for the 3S region (50 %) was lower than the EU average (57 %). However, in four 3S countries – Austria (67 %), the Czech Republic (60 %), Estonia (60 %) and Slovakia (59 %) – the indicator was higher than the EU average. Both in the EU and in the 3S region, the lowest level of digital skills was reported in Bulgaria, Romania, Croatia and Poland (2.).

2. DIGITAL SKILLS OF THE 35 POPULATION. % OF INDIVIDUALS WITH BASIC OR ABOVE BASIC OVERALL DIGITAL SKILLS, 2016 AND 2017

	2016	2017
Austria	65	67
Bulgaria	26	29
Croatia	-	41
Czech Republic	54	60
Estonia	60	60
Hungary	51	50
Latvia	-	48
Lithuania	52	55
Poland	44	46
Romania	28	29
Slovakia	55	59
Slovenia	53	54
Three Seas Average	49	50
EU	56	57

Source: Eurostat, 2018, Science, technology, digital society.

As compared to 2016, the share for the majority of countries remained at a similar level – the biggest change was recorded in the Czech Republic (6 percentage points) and Slovakia (4 percentage points).

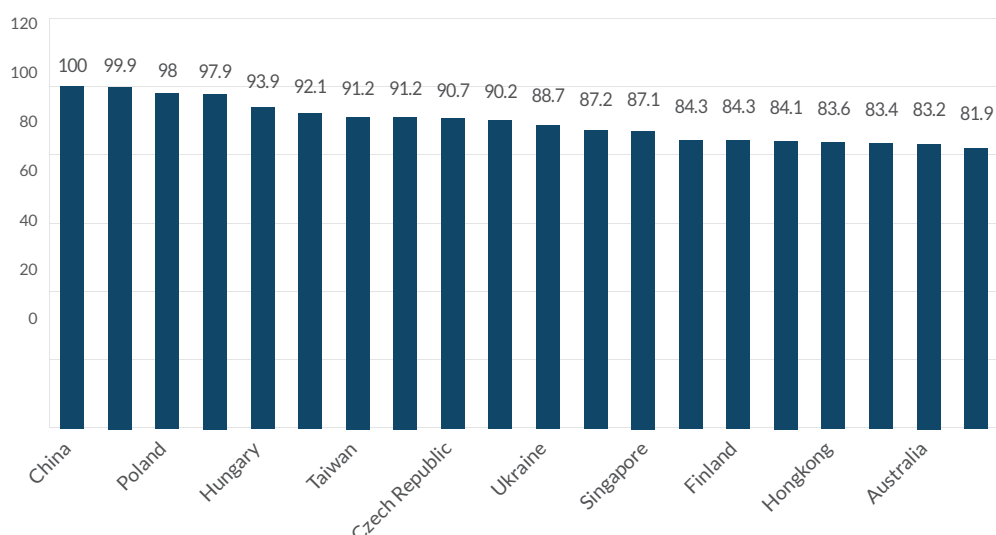
CASE STUDY – SLOVAKIA

The Digital Coalition (Digitálna Koalícia) was launched in late 2017 in Slovakia by bringing together partners from the state, private, non-profit and academic sectors to prepare Slovaks of all ages for work and life in the emerging digital economy. The project is seen as a way to initiate a wide range of processes, such as the enhancement of digital skills of the Slovak citizen, the strengthening of the excellence of ICT experts and overall preparedness for Industry 4.0.¹² However, there is a noticeable scepticism towards high level of automation and Slovakia's ability to override the digital skills gap. Currently, about 24 % of the labour force works in the industry sector, with the ICT industry employing about 3 % (see EMPLOYMENT OF ICT SPECIALISTS) of the labour force.¹³

According to the research held across 32 countries, almost one in two jobs is likely to be largely affected by automation (3). Roughly 14 % of jobs are highly automatable, another 32 % of jobs run a risk of significant change regarding the way they are carried out (between 50 % and 70 %). The difference in automation potential varies across the board.

In general terms, jobs in Anglo-Saxon and Nordic countries are less prone to automation than jobs in the 3S region, Southern Europe, Germany, Chile, or Japan.¹⁴

3. CROSS-COUNTRY VARIATION IN JOB AUTOMATION



Source: Nedelkoska N. and Quintini G., 2018, drawing on Survey of Adult Skills (PIAAC) 2012, 2015.

The highest risk of automation will be observed in Slovakia and Lithuania.

In general terms, the most profound impact and spill-over effect will be observed in small and medium enterprises, which constitute a backbone of the EU economy (99 out of every 100 EU companies are de facto SMEs) and are the main drivers of innovation (4.). However, only 54 % of large companies are classified as highly digitised versus only 17 % of SMEs. The majority of digitised companies can be found in the telecommunications sector, while only roughly 10 % of companies in construction, metal manufacturing and food processing can be described as highly automated.¹⁵

4. SMES AS A BACKBONE OF THE EUROPEAN ECONOMY

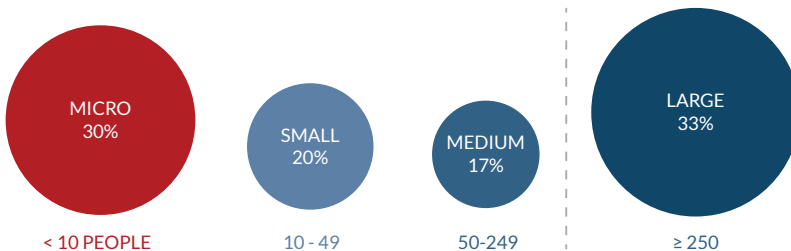


SMEs EMPLOY
2 OUT OF EVERY **3** EMPLOYEES
AND **PRODUCE 57 CENTS OF**
EVERY EURO OF VALUE ADDED



9 OUT OF **10** EU SMEs ARE MICROS
(less than 10 employees)

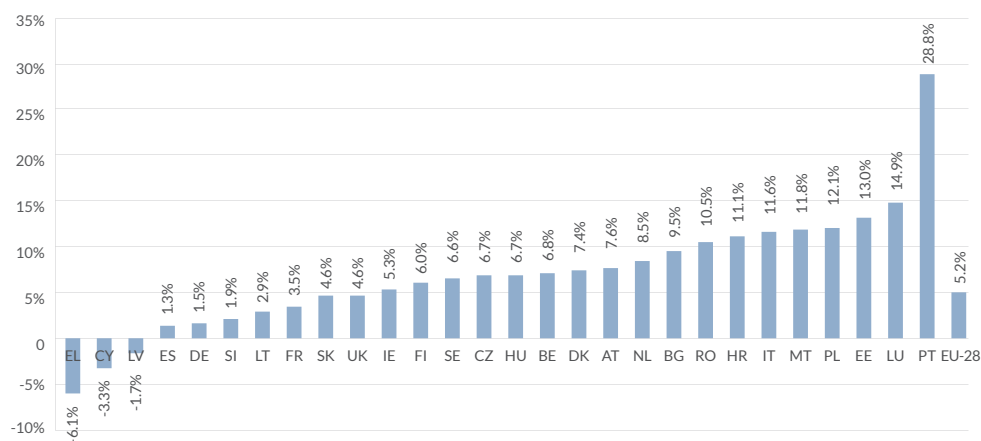
EMPLOYMENT SHARE PER SIZE CLASS



Source: European Commission, 2017, *Setting up a network of Digital Innovation Hubs*.

It becomes obvious that at present both engineering and software development skills are the most important competencies for the European industry. While software and application developers and analysts from EU constituted only 5.2 % of to the overall workforce between 2011 and 2016, Portugal contributed almost six times as many (5.). In the 3S region, Estonia, Poland and Hungary followed suit, taking the top places in the EU.¹⁶

5. ANNUAL GROWTH (CAGR) IN THE NUMBER OF SOFTWARE AND APPLICATIONS DEVELOPERS AND ANALYSTS IN THE EU BETWEEN 2011 AND 2016

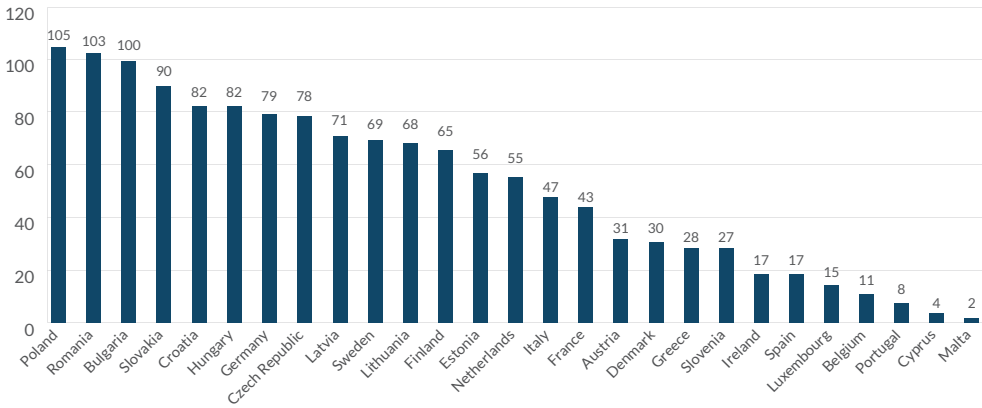


Source: EASME/COSME, 2018, *Digital Organisational Frameworks and IT Professionalism. Interim Report.*

In this respect, the 3S region has considerable programming and software development potential. For many years, representatives of 3S nations have dominated the ranking of the International Olympiad in Informatics, which is an annual programming competition for secondary school students (6.). Poland, Romania,

Bulgaria, Slovakia and Croatia are absolute front runners not only in the EU but also worldwide, with Poland (105) and Romania (103) being only second to China (115) and leaving behind the United States (95).¹⁷ This supremacy is not mirrored in the DESI, where the countries have been assessed moderate innovators.

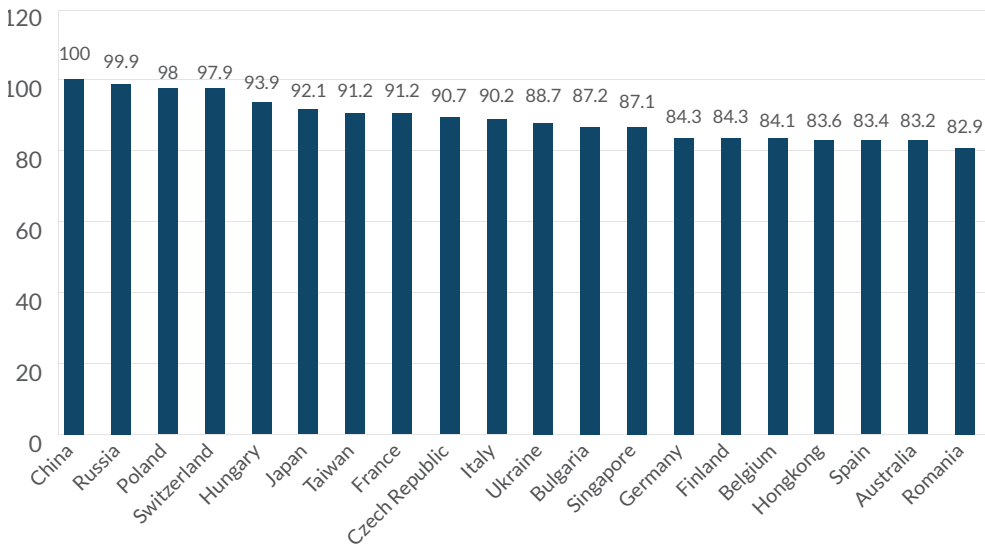
6. GLOBAL RANKING OF IOI CONTESTANT EU STATES



Source: Own elaboration based on the statistics of the International Olympiad in Informatics.

On top of that, many countries of the 3S region score as having the most talented developers worldwide, with Poland and Hungary being in the top five (7.).

7. BEST DEVELOPERS BY COUNTRY



Source: Hackers Rank, 2018, Developer Skills Report ¹⁸

Poles outscore others in Java, coming second worldwide in algorithms and Python. Hungary is best at developing tutorials, comes third in Java, C++ and Shell. The Czech Republic dominates in Shell and is second best in mathematics. However, the top contestants in the IOI ranking are DESI laggards, almost without an exception.

Romania and Hungary are among the top 10 countries when it comes to the number of hackers.

When it comes to the countries with the highest share of developers coding between 5 and 10, it is Poland (7.7 %) and Romania (7.0 %), both of which lead the pack, ranking fourth and sixth worldwide, respectively.¹⁹

CASE STUDY – POLAND

Many global tech giants set up their R&D and IT centres in Poland, which is an indication that Polish scientific talent is top quality. At the beginning of 2017, 748 business service centres, owned by 524 foreign companies, were operating in Poland.²⁰ One third of them focus on IT, including those belonging to firms such as Volvo (developing new solutions and technologies and providing IT support to the entire company), Opera Software (R&D centre in Wroclaw) and IBM (IT R&D centre in Wroclaw). Global companies such as Samsung²¹ have chosen Poland mainly because of the availability of high-quality IT talent. Similarly to Samsung (R&D Institute in Krakow working on software in a number of areas, including natural language processing), Intel and TomTom (Intel's Compiler Center of Excellence in Gdansk and TomTom's engineering centre in Łódź are partly working in the field of AI)²²,

other centres may follow their footsteps and become focused on carrying out R&D for AI, given the growing importance of this technology in many fields (see ARTIFICIAL INTELLIGENCE AND ROBOTICS).

Looking at the numbers in the 3S region, there are more than one million developers, which amounts to 6 % of the total number worldwide. A relatively high number of developers are based in capital cities – ranging from 93 % in Riga to 70 % in Sofia and just 29 % in Warsaw. On top of that, there are nearly 200 000 STEM graduates each year.²³ As noted above, new emerging jobs will require STEM skills.

Regarding STEM graduates per 1,000, in the 20-29 age group, the average for the EU was 19.1, noting increase of 0.8 % compared to 2013. The share of STEM graduates was particularly high in Malta



and the United Kingdom (17 %), Ireland (14.6 %) and Germany (14.4 %), while in the 3S region, the number was the highest in Estonia (12 %), Romania (11.2 %) and Slovenia (9.5 %).²⁴

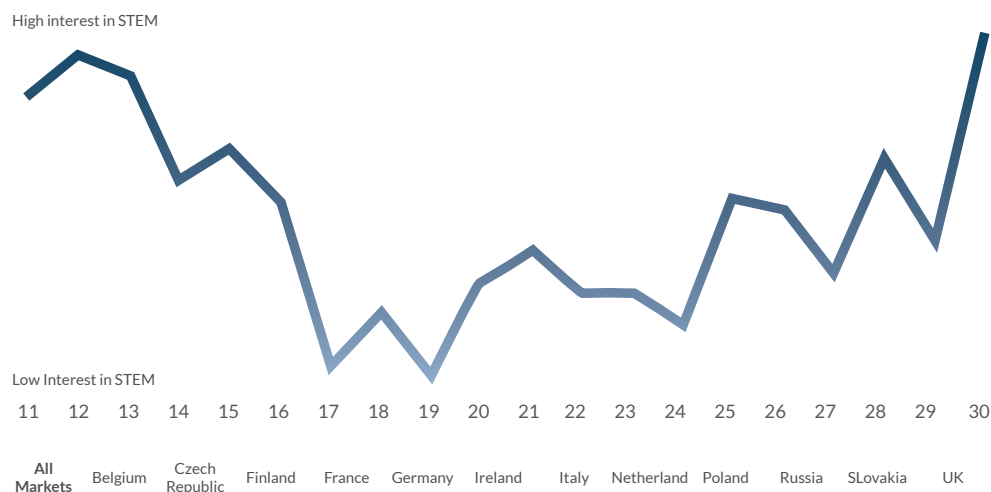
SUCCESS STORY – CROATIA

A Croatian NGO, the Institute for Youth Development and Innovativeness (IRIM), has initiated the Croatian Makers movement, one of the largest extracurricular STEM and digital transformation programs in the EU operating in Croatia, but also in the non-EU countries in the region like Bosnia and Herzegovina, Kosovo and Serbia, and including over 100 000 children in the program. The NGO has launched the Croatian Makers league within which 1800 robots have been donated to 360 schools. IRIM's project called STEM Revolution has helped introduce coding to the Croatian educational system and communities at an unprecedented level using a physical-computing controller – micro:bit. Previously, there was no coding in Croatian schools, apart from patchy optional subjects. IRIM's unique approach is combining grassroots (movement) with institutionalisation. In cooperation with the Ministry of Science and Education of Croatia, the NGO has implemented a number of initiatives to provide students in Croatian schools with computers and tablets. Also the government of Croatia supports universities and vocational study programs in STEM fields through scholarships.

WOMEN IN ICT

Failing to bring the minds and perspectives of half of the population to STEM and computer science stifles innovation and makes it less likely to solve today's social challenges at scale. In a research study conducted among 11 500 women aged 11-30 years in 12 EU Member States it has been noticed that young women have limited opportunities to gain practical, hands-on experience in STEM areas; only 42 % of them would consider pursuing STEM-related career whereas 60 % would tend to choose a STEM job, knowing that men and women have equal conditions of employment.²⁵

8. AGE AT WHICH GIRLS START TO LOSE INTEREST IN STEM



Source: Microsoft, 2017, *Why don't European girls like science or technology?*

The male-female ratio among ICT specialists in the EU is 83 % to 17 % in favour of men,²⁶ which stands in stark contrast to the overall gender distribution in total workforce, where genders are more balanced (54 % for men and 46 % for women). Despite sharp differences between the Member States, female ICT specialists are under-represented in all of them. The largest differences can be observed in Slovakia and the Czech Republic, wherein 91 % and 89 %

of ICT specialists are men. The highest presence of female ICT workforce was recorded in Bulgaria (26.5 %), Romania and Lithuania (both 25.7 %). However, the overall trend is worrying – only 24 out of every 1,000 women graduate in STEM-related subjects, of which only as few as six choose a job in the digital sector, which is a drop compared to 2011. Despite the growing demand for ICT-related jobs, there are fewer women than men who start their career in technology professions. The analysis shows that if more women entered ICT-related jobs, it could generate a EUR 16 billion GDP boost to Europe's economy.²⁷

EU APPROACH TO DIGITAL SKILLS

At the EU level, each Member State is responsible for its own training and education policy, while the objective of the overall European policy is to address common challenges, such as technological development and workforce skills deficit.

As a means to address the above-mentioned challenges, in January 2018, the European Commission adopted a Digital Education Action Plan,²⁸ which attempts to develop digital competencies in education through a set of 11 actions. These initiatives focus on making a better use of digital technology for teaching and learning, developing digital competencies and skills,

and improving education through better data analysis and foresight.

In order to do this, the European Commission has introduced, among other actions, the Digital Europe programme²⁹ for the years 2021-2027. Recognising the weakness of its predecessors (non-binding legal status), this strategic document is introduced by means of a regulation supported by a considerable budget. The budget for the implementation of the Digital Europe will be roughly EUR 9 billion, out of which up to EUR 700 million is to be spent on the development of advanced digital skills. The European Commission attempts to boost Europe's capacity in high performance computing, artificial intelligence, cybersecurity and advanced digital skills to provide for a widespread adoption of these technologies both by the economy and the society. By the end of 2027, the budget will be assigned to:

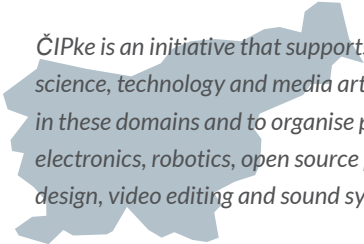
- 'support the design and delivery of long-term trainings and courses for students, IT professionals and the workforce;
- support the design and delivery of short-term trainings and courses for entrepreneurs, small business leaders and the workforce;
- support on-the-job trainings and traineeships for students, young entrepreneurs and graduates'.³⁰

The Programme will focus, among others, on assisting SMEs to accommodate digital disruption. In parallel, the Executive Agency for Small and Medium-sized Enterprises has started developing an integrated digital capability reference framework for enterprises to strengthen their capabilities to digitally transform businesses.³¹ The above-mentioned advanced skills will be implemented primarily through the DIHs (see DIGITAL INNOVATION HUBS).³²

The European Commission has also launched two other initiatives: the Erasmus for Young Entrepreneurs Initiative and the Mobilise SME Initiative, both of which are aimed at developing skills to cater for upcoming challenges. Such mechanisms and training schemes that intend to mitigate unemployment rates, at a domestic and a regional level, are the need of the hour for the 3S region.


DIGITAL SKILLS PROJECTS

CASE STUDY – SLOVENIA



ČIPke is an initiative that supports research into the situation of women employed in the fields of science, technology and media art. The goal is to create a space for dialogue about women working in these domains and to organise practical educational programme including various workshops on electronics, robotics, open source programming, and the use of open source programs for graphical design, video editing and sound synthesis.³³

CASE STUDY – ROMANIA



Coding for Kids in Libraries (CODE Kids) aims to popularise programming by setting up coding clubs in rural libraries across Romania to help equip youngsters with better IT skills and empower their communities. Since January 2017, CODE Kids has established 29 coding clubs in local libraries in Argeş, Vâlcea, Gorj, Timiş, Arad, Bihor, and Sălaj counties. With over 450 members aged between 10 and 14, the clubs offer coding classes during which youngsters are challenged to solve practical creative tasks with the support of qualified librarians and experienced project Ambassadors.³⁴

CASE STUDY - LITHUANIA

The initiative 'Digital skills for the engineering industry' is being implemented by LINPRA, the Engineering Industries Association of Lithuania. The project includes two main activities: competition ArTech 2k17 and the mobile STEAM laboratory InfoBus. The latter is a small laboratory with bespoke equipment, such as adapted CNC metalworking machines, information stands, TV screens, computers, printers, specific task tools and devices. It aims to give insight into a variety of mechanical engineering and metalworking occupations and enhance interest in the field and understanding of the professions. More importantly, the mobile STEAM laboratory InfoBus provides young people with an opportunity to see and learn about technological advances and the impact of digitalisation on the engineering industry.³⁵

CASE STUDY - HUNGARY

e-Tanoda is an e-mentoring network of secondary school students who volunteer to mentor underprivileged primary and secondary school students from underserved communities. The programme consists of a kick-off camp, weekly Skype lessons and regular supervision. e-Tanoda's short-term goals are to help underprivileged children to perform better in school by using modern technologies and tailored learning methods as well as to improve their digital skills and ensure better access to information. The long-term goal is to build a digital volunteer-driven mentoring network which efficiently applies the tools and methods of the 21st-century pedagogy and brings together school students from different socio-cultural backgrounds.³⁶

CASE STUDY - ESTONIA

The Estonian NGO Robotika has been performing 'Robotics Theatre' in schools since 2008 and it has managed to visit over 300 schools in Estonia and Latvia. The first part of each 'Robotics Theatre' is a seminar-based discussion on robotics showcasing different robots, talking about the role of robots in our daily lives and their usage.³⁷

Demand for computer science education goes hand in hand with the competitiveness, prosperity and maturity of the digital economy. Boosting demand generation for computer science education heavily relies on how mature a digital economy is. These determinants co-exist as there is a strong interdependency among them. It is certainly the case with developing digital economies like those of the 3S region. Thus boosting the digital economy is likely to advance demand for computer science knowledge and education.

The shift to data-driven education is challenging and time-consuming for policy-makers, professionals and teachers/trainers, although the long-term benefits are unquestionable. The data-driven education is, in fact, an evidence-based education. The readiness of the 3S region's educational systems for data-driven education is poor. Yet, the 3S educational systems are quite attached to the traditional approach mainly due to historical, societal, cultural (poor data culture), institutional and technological factors. Moreover, the potential of data-driven education is rather poorly recognised by policy-makers, teachers, parents and even students themselves.

Many factors contribute to such a state of play. First, although teachers may have broad and valuable classroom experience, they are less likely to keep pace with latest computer science developments. Second, we should bear in mind that any ICT- or

computer science-related training is costly. Third, there is little consensus on what the most appropriate curriculum for every grade is, with the curricula for computer science being prone to ongoing changes as technology advances. The incentives for teachers and students alike should be both material and immaterial to stimulate them to understand the need for training. Continuous certification and recurrent validation of lessons learned by teachers should be mandatory in computer science. Last but not the least, the teaching and learning environment is of the utmost importance for both teachers and students. The learning content should, therefore, be interactive and easy for them to absorb. It is very unlikely that high quality training could be delivered in the absence of simulated and dynamic content (i.e. e-learning platforms), non-formal education or hands-on experience, which can deliver a proper balance between the students' acquired skills and knowledge.

RECOMMENDATIONS FOR THE 3S COUNTRIES:

1. Continue **building the capacity of ICT teachers and trainers** (including AI disciplines), not only by means of tools (i.e. equipment and software), but mainly by training and supporting them, particularly in rural and low income schools. This would entail **establishing adequate budgets for teacher training and curricula to be taught**.
2. Better use of data shall be addressed by means of strategic deployment of appropriate data infrastructures and information systems boosting data quality and its usage and establishment of best practices for data-driven education curricula/activities.
3. Introduction of such strategies should be preceded by **mapping studies** on how and where new technologies are employed with the aim of identifying and analysing opportunities, assessing demand and supply for particular skills required by the industry.³⁸
4. Industry transformation maps shall represent the expectations of each industry sector regarding future trends and in-demand skills in order to better match skills with the existing and future requirements, as well as to identify sectors with the highest re-skilling needs. **Equality benchmarks** should be introduced to diminish unfairness in computer science education and to enable anyone to pass a minimal threshold of computer science education.
5. Other specific measures should focus on reducing disparities in computer science and provide, among others, adequate and tailored curricula for vulnerable students, financial support and scholarships, training for parents on the benefits of digital skills, admission privileges for vulnerable students,³⁹ incentives to attract talented teachers,⁴⁰ adequate mentoring for parents, students and teachers, interactive educational content and instructional materials,⁴¹ computer science after-school opportunities.⁴²
6. Governmental programmes supporting **the development of new technologies** departments at universities (for instance AI and cybersecurity) shall be established through cooperation with the private sector.

7. **Cross-national competence centres** with a dynamic sustainable funding model shall be established to focus on introducing coding and computing at an early educational level across the D3S region.
8. A set of tailored actions shall be introduced by means of government-industry cooperation to address shortages of skilled workers, provide for more inclusive workforce and eliminate gender bias in data and development of algorithms, i.e. target **women in tech and girls in STEM**.
9. The industry shall be encouraged to assist in the establishment of **national retraining schemes** to address the mismatch of skills and prepare current and future workforce for challenges stemming from technological advancements.
10. Moreover, a network of **vocational schools, secondary schools and technical colleges** shall benefit from partnerships with the private sector active in the field of new technologies. An increased number of **tailored industrial traineeships and bursaries** shall be offered to further tailor skills to market demand.
11. An increased number of **industry-sponsored MSc and PhD programmes** shall be established to enhance the adequacy of qualifications required by the industry. Such programmes shall introduce topics such as AI ethics, cybersecurity, privacy and data protection into their curricula.
12. Establishment of **STEM platforms as part of the EU STEM coalition** would channel concerted efforts to increase numbers of STEM graduates and reduce skills mismatch, particularly in the regional dimension. These could be formed as partnerships of national and regional governments, industry and EU institutions. The Hungarian STEM platform and Estonian Research and Technology Pact serve as examples of the activity in the region.
13. Given a relatively low level of **soft skills and entrepreneurship skills**, as indicated by the Global Entrepreneurship Index for the 3S region (see LEVEL OF INNOVATION IN THE REGION), both startups and SMEs shall benefit from **targeted training addressing these aspects**.

14. SMEs workforce shall employ new technologies to upgrade their **skills depending on the opportunities created by new solutions**. Data analytics, machine learning and deep learning shall be part of a tailored strategy under the Digital Europe programme.
15. The concept of **Digital Innovation Hubs**, as introduced by the European Commission and further supported under the Digital Europe programme and the H2020, as well as their dedicated budgets, shall be further enhanced.
16. Centres for Foreigners and its counterparts in the region shall organise tailored workshops and training sessions as part of a local-level response to the refugee crisis. **Quantitative research analysing the qualifications and competences of the asylum seekers** who are likely to receive international protection would be of great value in order to assess their work opportunities, tap into their skills and introduce workforce diversity. The results of such surveys could provide a valuable input into the process of designing workshops for this group to improve their knowledge and qualifications.







SOURCES:

1. Technology Review (2018), Machines will do more work than humans by 2025, says the WEF [on-line]. Available at: <https://www.technologyreview.com/the-download/612121/machines-will-do-more-work-than-humans-by-2025-says-the-wef/>.
2. Microsoft (2018a). Future proof yourself. Tomorrow's jobs [on-line]. Available at: https://enterprise.blob.core.windows.net/whitepapers/futureproof_tomorrows_jobs.pdf.
3. McKinsey (2018), Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages [on-line]. Available at: <https://www.mckinsey.com/featured-insights/future-of-organizations-and-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages>.
4. Adams C. (2017). The 7 most important STEM skills we should be teaching our kids [on-line]. Available at: <https://www.weareteachers.com/important-stem-skills-teaching-kids/>.
5. Garman K. (2017). In the era of artificial intelligence, STEM is not enough [on-line]. Available at: <https://www.forbes.com/sites/sap/2017/03/29/in-the-era-of-artificial-intelligence-stem-is-not-enough/#253912a06324>.
6. Singularity Hub (2017). 7 critical skills for the jobs of the future [on-line]. Available at: <https://singularityhub.com/2017/07/04/7-critical-skills-for-the-jobs-of-the-future/#sm.00h7ym4612ijcyg102s2byqfu6cbf>.
7. Deloitte (2015), Tech Trends 2015 The fusion of business and IT A public sector perspective [on-line]. Available at: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-fed-2015-ps-tech-trends-04212015.pdf>
8. European Commission (2017). ICT for work: digital skills in workplace [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/ict-work-digital-skills-workplace>.
9. World Economic Forum (2017). 4 predictions for the future of work [on-line]. Available at: <https://www.weforum.org/agenda/2017/12/predictions-for-freelance-work-education>.
10. Microsoft (2018b). Preparing people for the new world of work [on-line]. Available at: <https://news.microsoft.com/cloudforgood/policy/briefing-papers/inclusive-cloud/preparing-people-new-world-work.html>
11. European Parliament (2018). Education in the digital era: challenges, opportunities and lessons for EU policy design [on-line]. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-623.921&format=PDF&language=EN&secondRef=01>.
12. European Commission (2017, November 28). Digital Coalition launched in Slovakia [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/digital-coalition-launched-slovakia>.
13. Gubalova, V. (2017, December 1). Tackling Unemployment by Upgrading People's Skills: New Skills for New Jobs and the EU Support. GLOBSEC Policy Institute [on-line]. Available at: <https://www.globsec.org/tackling-unemployment-upgrading-peoples-skills-new-skills-new-jobs-eu-support/>.
14. Nedelkoska L. and Quintini G. (2018). Automation, skills use and training. OECD social, employment and migration
15. European Commission (2017). Setting up a network of Digital Innovation Hubs.
16. European Commission (2017). Talent for Europe. Towards an agenda for 2020 and beyond [on-line]. Available at: http://eskills-scale.eu/fileadmin/eskills_scale/all_final_deliverables/scale_e-leadership_agenda_final.pdf.
17. International Olympiad in Informatics (2018). Statistics [on-line]. Available at: <http://stats.ioinformatics.org/countries/>.
18. Ranked by average score across all Hacker Rank challenges.
19. [on-line]. Available at: <https://research.hackerrank.com/developer-skills/2018/>.
20. Association of Business Service Leaders (2017). Business Services Sector in Poland 2017 [on-line]. Available at: <https://www.everestgrp.com/wp-content/uploads/2017/07/Business-Services-Sector-in-Poland-ABSL-2017-min.pdf>.
21. Maciejewski, A. (2011, March 1). Centrum R&D Samsunga w Polsce będzie głównym ośrodkiem rozwoju systemu Bada [on-line]. Available at: <https://www.computerworld.pl/news/>

Centrum-R-D-Samsunga-w-Polsce-bedzie-glownym-osrodkiem-rozwoju-systemu-Bada,367633.html.

22. McKinsey & Company (2017). The AI revolution. How artificial intelligence will change business in Poland [on-line]. Available at: http://mckinsey.pl/wp-content/uploads/2017/09/AI-revolution_McKinsey_Forbes_EN.pdf.
23. Infoshare (2017). Central & Eastern Europe Developer Landscape [on-line]. Available at: <https://infoshare.pl/news/one,66,248,1,central-eastern-europe-developer-landscape-2017-a-report-by-stack-overflow.html>.
24. Eurostat (2017). Tertiary education statistics [on-line]. Available at https://ec.europa.eu/eurostat/statistics-explained/index.php/Tertiary_education_statistics.
25. Microsoft (2017). Why don't European girls like science or technology? [on-line]. Available at: <https://news.microsoft.com/europe/features/dont-european-girls-like-science-technology/>.
26. European Commission (2017). ICT specialist in employment. Statistics explained [on-line]. Available at: <https://ec.europa.eu/eurostat/statistics-explained/pdfscache/47162.pdf>.
27. European Commission (2018). Increase in gender gap in digital sector. Study on women in digital age [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/increase-gender-gap-digital-sector-study-women-digital-age>.
28. European Commission (2018). Digital competences and technology in education [on-line]. Available at: <https://ec.europa.eu/education/policy/strategic-framework/education-technology>.
29. The Programme will support, inter alia, the policy initiatives announced by the Commission on high performance computing under the Euro HPC initiative, FinTech Action Plan of March 2018, artificial intelligence under the Communication on AI, Regulation on promoting fairness and transparency for business users of on-line intermediation services and a Decision setting up an Observatory on the Online Platform Economy of April 2018, and the data package of April 2018, cybersecurity under the cybersecurity package of 15/9/2017, digital transformation of health and education, the New Industrial Policy Strategy of September 2017, the Digitisation of European Industry of April 2016 and the Skills Agenda for Europe.
30. European Commission (2018). Regulation of the European Parliament and of the Council establishing the Digital Europe
31. Capgemini, Empirica, IDC (2018). op. cit.
32. PWC (2018). 34 Digital Innovation Hubs that have qualified for the Smart Factories programme will receive support from PwC and Oxentia [on-line]. Available at: <https://www.pwc.pl/en/media/2018/2018-01-25-smart-factories-pwc.html>.
33. CIPKe [on-line]. Available at: <https://cipkeen.wordpress.com/>.
34. CODE Kids [on-line]. Available at: <http://www.codekids.ro/>.
35. LINPRA [on-line]. Available at: <http://www.infomobilis.it/>.
36. etanoda [on-line]. Available at: http://www.etanoda.hu/about_us.
37. Robotika [on-line]. Available at: <https://www.robotika.ee>.
38. See Vinnova (2018), Artificial intelligence in Swedish business and society [on-line]. Available at: <https://www.vinnova.se/en/publikationer/artificial-intelligence-in-swedish-business-and-society/>.
39. The University of Leeds (n/a). Policy on safeguarding children, young persons and adults in vulnerable circumstances [on-line]. Available at: https://www.leeds.ac.uk/secretariat/documents/safeguarding_policy.pdf.
40. OECD - Directorate for Education, Education and Training Policy Division, (2011). Teachers Matter: Attracting, Developing and Retaining Effective Teachers [on-line]. Available at: <http://www.oecd.org/education/school/48627229.pdf>.
41. Jamwal, G. (2012). Effective use of Interactive Learning Modules in Classroom Study for Computer Science Education [on-line]. Available at: <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1223&context=gradreports>.
42. The Afterschool Alliance (2016). Growing computer science education in afterschool: Opportunities and challenges [on-line]. Available at: http://afterschoolalliance.org/documents/Growing_Computer_Science_Education_2016.pdf.





DIGITAL INDUSTRY

The term 'Industry 4.0' stands for the fourth industrial revolution. While Industry 3.0 focused on the automation of single machines and processes, new approach focuses on the digitisation of physical assets and their integration into digital ecosystems. Nowadays, dependence on technology is the main driver of change, while previously traditional macro-economic policies or geopolitical changes were the main factors which influenced the process of transformation.¹

In general terms, digital industry is driven by: digitisation and integration of vertical and horizontal value chains (from product development and purchasing, through manufacturing, logistics and service), digitisation of product and service offerings (modernisation of existing products, e.g. by adding smart sensors or communication devices, as well as the creation of new digital products) and digital business models and customer access (provision of disruptive digital solutions such as complete, data-driven services and integrated platform solutions which generate additional digital revenues and optimise customer experience).²

CASE STUDY – SLOVAKIA

Slovakia's Smart Industry Initiative focuses on collaborative R&D cooperation with industry and the deployment of more advanced technologies like such as IoT. While there is no specific budget allocation for the Smart Industry Initiative, several innovative and new funding mechanisms are being considered, in addition to the existing industry funding pools and the European Structural and Investment Fund.³

One of the strong points of the initiative is that the representation of key stakeholders, in what started as the Smart Industry Platform, included various ministries of the Slovak government, as well as industry associations (IT Association, National Union of Employers, Federation of Employers' Associations, Automotive Industry association, Klub 500), R&D agencies (Slovak Innovation and Energy Agency), academic and educational institutions (Slovak University of Technology, Technical University of Kosice, Slovak Academy of Sciences), businesses (Embraco, Siemens, SOVA Digital, Matador, Microsoft, Volkswagen), and industry clusters (Cluster for Automation Technologies and Robotics AT+R). Despite lack of clear funding scheme, the creation of a coordinating body to implement the initiative and active cooperation with different stakeholders will prove to be extremely beneficial.

The digital maturity of the industry varies both across sectors, in particular between high-tech and more traditional ones, and

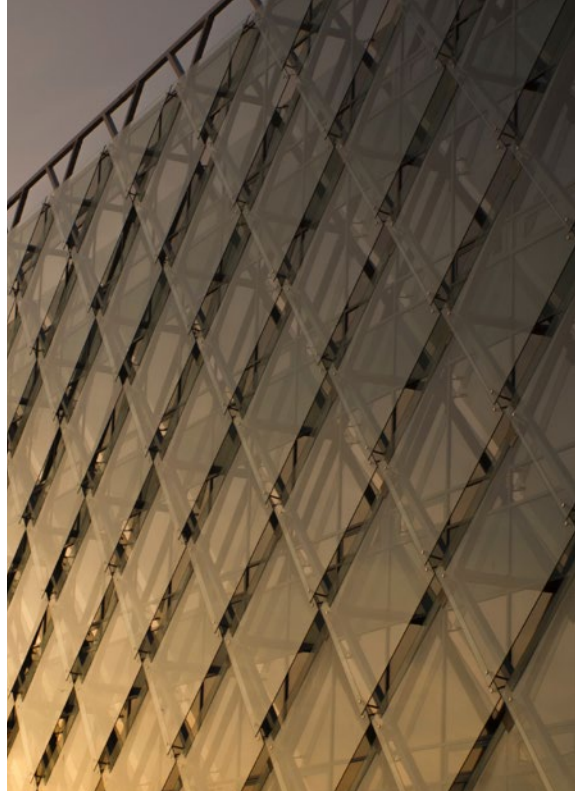
countries and regions. Disparities between large companies and SMEs only add to this diversity.⁴ Therefore, a number of challenges need to be tackled: boosting innovation and competitiveness potential of European regions, increasing interregional cooperation, strengthening the focus on the regions which are less developed regions or in industrial transition, improving and building on the results of implementing EU policies and innovation programmes.⁵ European leaders at the Tallinn Digital Summit of September 2017 stressed in a powerful joint message the need for Europe to invest in digitising our economies and enhance European competitiveness, our quality of life and social fabric.⁶

Since the first half of 2016, the EC, together with Member States and industry, has set up a governance framework to mobilise stakeholders, exchange best practices, and support the coordination of EU and national initiatives. The European Platform of national initiatives,⁷ launched in March 2017, is at the core of the coordination effort. Fifteen national initiatives for digitising industry have been launched across Europe in recent years. Seven more initiatives are under preparation. Among all of them, there are eight initiatives from the 3S countries.⁸

CASE STUDY – ROMANIA

The smart storage systems market is among the fastest growing ICT markets in Romania. A rather realistic evaluation reveals the potential of the smart storage market being currently around EUR 200-250 million. The demand for smart storage systems is surging. The annual growth is consistent with that of other EU states, as the use of the smart storage systems is expected to grow by 10-20 % each year by 2020. Therefore, Romania is likely among the top most attractive smart storage systems markets in Europe. The smart storage business in Romania comprises mainly data centres, cloud and document management solutions. To date no reliable data were identified to reveal the exact figures corresponding to the market share of each subsector.

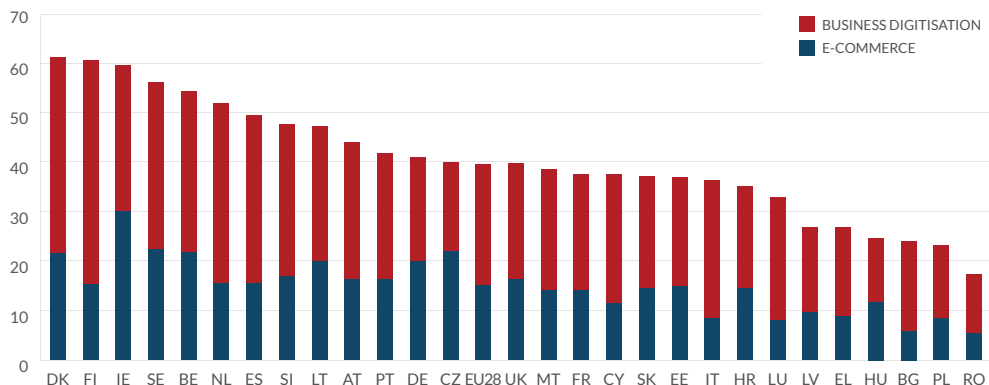
In 2016 the European Commission laid down a policy to develop the European digital industry in four strands: DIHs, enhanced leadership by means of partnerships and industrial platforms, regulatory framework and development of digital skills. While the last of these has been covered in detail in previous passages, this chapter will focus on a more elaborate description of DIHs, industrial public and private partnerships and relevant regulatory framework. However, a thorough analysis cannot be complete without a deep dive into the integration of digital technology, which measures the digitisation level in the case of businesses and e-commerce. An overview of digital industry initiatives in various states is presented below as well.



INTEGRATION OF TECHNOLOGY

Regarding technology integration, the most developed companies can be found in Denmark, Finland and Ireland (1.). In 3S region Slovenia, Lithuania and the Czech Republic have passed the EU average while the least developed companies can be found in Romania, Poland and Bulgaria. E-commerce is the main driver of digitisation in the Czech Republic. Generally speaking, only 20 % of companies in the EU are highly digitised but the situation differs between countries: in Bulgaria and Romania only 1 in 10 businesses is highly digitised while in Denmark and the Netherlands it is almost 40 %.⁹

1. INTEGRATION OF DIGITAL TECHNOLOGY



Source: European Commission, 2018, DESI Report 2019.

Companies in the 3S region are less digitalised than those from other countries of the EU. Generally speaking, only one in 10 companies in Bulgaria, Romania, Poland and Lithuania bought access to cloud-enabled services in 2016.¹⁰ In the EU development of cloud computing could lead to the growth of the market from EUR 9.5 billion in 2013 to EUR 44.8 billion by 2020, a five-fold increase as compared to 2013.¹¹ Increased adoption of cloud computing could offer 3S countries access to advanced computing capacity which in turn could reduce the need for heavy investment in data centres, hardware and software.

2. PURCHASE OF CLOUD COMPUTING SERVICE (AS A SERVICE) IN THE 3S REGION (2016)

Name of the country	Services (accounting software applications, CRM software, computing power)	Computing power to run the enterprise's own software	Cloud computing services used over the internet	E-mail	Office software (e.g. word processors, spreadsheets, etc.)	Customer Relationship Management software
Austria	8	4	17	12	3	4
Bulgaria	3	1	7	4	7	1
Croatia	13	5	23	17	8	3
Czech Republic	9	4	18	14	20	4
Estonia	15	6	23	15	17	4
Hungary	6	3	12	8	14	3

Latvia	4	2	8	6	6	2
Lithuania	10	6	17	12	9	4
Poland	4	2	8	6	8	2
Romania	4	2	7	5	11	1
Slovakia	10	4	18	15	29	3
Slovenia	12	5	22	13	9	5
Three Seas Average	8	4	15	11	12	3

Source: Lepore, D., 2018, *Descriptive Analysis on Security Perspectives Among EU Countries*, The Kosciuszko Institute.

The table 2. shows the current state of play regarding purchase of cloud computing as a service in different categories. In 2016, around 8 % of enterprises in the 3S region purchased advanced cloud computing as service related to financial and accounting software applications, customer relationship management or to the use of computing power to run business applications. The highest scores were noted in Estonia (15 %), Croatia (13 %) and Slovenia (11 %), only one in twenty companies buy services of such type in Bulgaria, Latvia, Poland and Romania.

CASE STUDY - HUNGARY

The primary sectors in the Hungarian digital revolution are the following:¹² 27.5 % automobile industry, 11.4 % ICT sector and SSC, 11.28 % food industry, 7.2 % green economy (e.g. in the construction industry), 6.7 % mechanical engineering, 4.62 % health economy (pharmaceutical industry, medical devices) and health tourism. The aim is to reduce the dependency of the automobile industry and put more efforts into, for example, the innovation of the healthcare industry. Unfortunately, there are still few innovator enterprises in Hungary.

Also in 2016, the EC, together with Member States and industry, has set up a governance framework to mobilise stakeholders, exchange best practices and support the coordination of the EU and national digital industry initiatives. Recent years have witnessed a boom as fifteen national initiatives for digitising industry have been launched across the EU, eight in 3S countries (3.). Seven more strategies and action plans are under preparation.

The European Platform of national initiatives¹³ launched in March 2017, is at the core of the coordination effort. Its goal is to build a critical mass of initiatives for digitising industry and to mobilise investment on side of Member States, regions and private sector to achieve the objectives set out for the EU.

3. DIGITAL INDUSTRY INITIATIVES IN 3S COUNTRIES

Name of the country	Description
Austria: 'Plattform Industrie 4.0'	Austria's national Plattform Industrie 4.0 (PI4.0) started in 2015 upon the initiative of the Austrian Ministry of Transport, Innovation and Technology. The platform acts as an observatory, network and strategic advisory body creating working groups, strategies, focus areas as well as case studies on industry 4.0 topics. At the end of 2016, after launching PI4.0, the Ministry adopted the Industry 4.0 package.
Czech Republic: 'Průmysl 4.0'	Průmysl 4.0 (Industry 4.0) is a national initiative aiming to maintain and enhance the competitiveness of the Czech Republic in the wake of the Fourth Industrial Revolution. The concept was firstly presented during the 57th International Engineering Fair in Brno, September 2015. The Ministry of Industry and Trade established a coordination platform – Alliance Society 4.0 – to prepare an action plan for the implementation of the initiative. It was finalised in 2017.
Hungary: 'IPAR 4.0 National Technology Platform'	'I4.0 NTP' (Industry 4.0 National Technology Platform) is a national initiative aspiring to boost manufacturing and industry transformation in Hungary in the wake of the Fourth Industrial Revolution. The strategy was adopted in May 2016. Both the Hungarian government and the scientific community of the country have established ties with flagship German and Austrian organisations.
Latvia: 'National Industrial Policy Guidelines 2014-2020'	The economic crisis proved that the Latvian economic model – mainly based on internal demand – was not sustainable. For that reason, action was taken to support the transition towards a more sustainable economy. In this context, the need to revise the different national policies arose, specifically regarding the national industry.

**Lithuania:
'Pramonė 4.0'**

The Pramonė 4.0 platform resulted from a bilateral German-Lithuanian Conference on 'Industry 4.0' held in Vilnius in May 2016. One year later, the Lithuanian Government officially launched Pramon3. Digital industry initiatives in 3S countries 4.0 aiming to increase and strengthen the competitiveness and productivity of the Lithuanian industry and to promote the integration of digital solutions and new technologies.

**Poland:
'Initiative for Polish Industry 4.0 – The Future Industry Platform'**

The Future Industry Platform was announced as part of the Responsible Development Plan ('Morawiecki Plan') by the Ministry of Finance and Development in 2016, and established in October 2018. The Platform will specifically focus on standards; specialisation; digital industry support; software and data processing; education and staffing; legal framework; and ICT sector activity. The Platform will also incorporate Industry 4.0 competence centres for vertical industries, established as joint ventures among industry, business, and science organisations.

**Slovakia:
Smart Industry Platform**

Inspired by similar initiatives implemented in Germany and the Netherlands, the Ministry of Economy first presented the Smart Industry concept for Slovakia at a high-level conference in March 2016. The government adopted the strategic direction of the paper on 29 October 2016, and with the decision to pursue the development of local smart industry. The Smart Industry Platform was established to act as a central authority coordinating the various efforts. The action plan with a defined timeframe and clear medium and long-term objectives was adopted in 2018.

**Slovenia:
Digital Partnership**

The Digital Partnership is aimed at linking the economy to encourage the digitalisation of the economy and wider recognition of Slovenia as a reference country. With a view to co-designing projects and implementing the Digital Slovenia 2020 strategy, through association with important Slovenian organisations.

Source: European Platform of national initiatives.


Another strand of the digital industry strategy touches upon strengthening leadership through partnership and industrial platforms. It supports both the development of digital industrial platforms and large-scale piloting and public-private partnerships in specific sectors. In the 2018-2020 period, the EC plans to invest more than EUR 3 billion, out of which roughly 2/3 will be spent on developing PPP and the rest on large-scale piloting, pilot lines and related actions. Such PPPs have a number of objectives: provide a legal structure to pool resources and to gather critical mass, make R&D funding across the EU more efficient, boosts creation of internal market for products and services, provides a framework for international companies to enhance their presence in the EU and last but not least, address critical social challenges. Ongoing PPPs include: cybersecurity, photonics, high performance computing, robotics, future internet, electronic components and embedded software and factories of the future. When a composition of PPP partners in cybersecurity is taken into consideration, a similar pattern of underrepresentation as in the case of DIHs becomes visible. Out of 255 members of the European Cybersecurity Organisation, less than 10 % come from the region of 3 Seas



DIGITAL INNOVATION HUBS

The digitising European industry strategy as one of the objectives set development of the DIHs. By 2020, each of the regions of the EU should have such a competence centre which acts as a one-stop shop where companies – especially SMEs, startups and mid-caps – can tap into such resources as the knowledge of business models, production processes, products or services by means of digital technology. Support of a strong network of DIHs is one of the key objectives of the DEI. Seeing the uneven distribution of the DIHs in the EU, the European Commission decided to enforce development of such facilities in underrepresented regions, by means of a dedicated action.

CASE STUDY – VISEGRAD GROUP



The main sector, where the Visegrad region is strong and competitive, is the automobile industry therefore developing high-end infrastructure, intelligent transportation systems, supporting the e-mobility, as well as connected and automated vehicles are in alignment with the V4's objectives. The main priorities are the followings: to create a 'Visegrad Good Practices Platform' dealing with autonomous vehicle manufacturing; to be an active participant in

Digitising European Industry initiative; to focus on the topic of analysing big data generated by sensors of fast-moving vehicles, and the necessary cooperation between autonomous vehicles (5G edge computing); to continue V4 coordination connected to EU policies and legislative packages, concerning especially the work on the new Electronic Communications Code, the free flow of data initiative, the mid-term review of the European Digital Single Market Strategy and the possibility to lower the value-added tax on internet access services.¹⁴

Under the H2020, ICT innovation for manufacturing SMEs initiative selected 29 DIHs which received support from the existing network of hubs on development of a business plan or identification of the industry needs in the region. Thanks to a similar action (Smart Factories in new EU Member States), with a budget of EUR 2 million, 34 new DIHs across the 3S region have been selected to participate in a training that attempts to enhance access to the latest knowledge, expertise and technology, to help connect users and suppliers of digital innovations across the value chain, enhance connections with investors and finance and foster synergies between technologies.¹⁵

Additionally, the European Commission envisages possible collaboration between selected 34 hubs and 31 other applicants, which touched upon similar domains and function in same geographical regions.

These efforts are to be enhanced in 2019 with EUR 8 million under Horizon 2020 in order to support new DIHs in underrepresented regions with strong industrial activity.¹⁶ In August 2018, the catalogue of 408 DIHs located in the European Union included 196 fully operational competence centres and 212 in preparation, out of which 25 and 30 in the 3S region respectively (4.). Roughly speaking, just 13 % of the European DIHs are located in the 3S region, which is roughly equal to a number of DIHs established in Germany solely (48).

4. A LIST OF DIGITAL INNOVATION HUBS (FULLY OPERATIONAL AND IN PREPARATION) IN THE THREE SEAS REGION

Name of the country	Fully operational		In preparation	
	No	Name	No	Name
Austria	4	<ul style="list-style-type: none"> • BioNanoNet ForschungsGmbH, BNN • CAMPUS 02 R&D Section • Know-Center GmbH • Virtual Vehicle Research Center 	4	<ul style="list-style-type: none"> • CDP – Center for Digital Production • Data Market Austria (DMA) • i.ku – Innovationsplattform Kufstein / Innovation Hub Kufstein, Tyrol • smart Fab Carinthia
Bulgaria			3	<ul style="list-style-type: none"> • Bulgarian Innovation and Technology Hub – DigiTech 4.0 • SmartFabLab • Sofia Tech Park
Croatia	2	<ul style="list-style-type: none"> • Algebra LAB • CROBOHUB Croatian Robotics Digital Innovation Hub 	4	<ul style="list-style-type: none"> • CroTechHub • Digital Innovation Hub for 3D printing (3DJPU) • DIH North • HUB385
Czech Republic	3	<ul style="list-style-type: none"> • DIGIMAT: South Moravian Digital Manufacturing Hub • IT4Innovations National Supercomputing Center • National Centre for Industry 4.0 		

Estonia			2	<ul style="list-style-type: none"> • e-Estonia Showroom • Software Technology and Applications Competence Centre (STACC)
Hungary	2	<ul style="list-style-type: none"> • am-LAB • Demola-Budapest 	2	<ul style="list-style-type: none"> • EIT Digital Budapest Node • Industry 4.0 National Technology Platform
Latvia	1	<ul style="list-style-type: none"> • Ventspils High Technology Park (VHTP) 	2	<ul style="list-style-type: none"> • Latvian IT Cluster • TechHub Riga
Lithuania	4	<ul style="list-style-type: none"> • Advanced Manufacturing Digital Innovation Hub • Laser Digital Innovation Hub (LaserLT DIH) • Lithuanian robotic DIH (LTroboticsDIH) • Sunrise Valley Digital Innovation Hub (SV DIH) 		
Poland	4	<ul style="list-style-type: none"> • Centre for Advanced Manufacturing Technologies, Wroclaw University of Science and Technology • CYBERSEC HUB • HPC4Poland • Institute of Electron Technology (ITE) 	7	<ul style="list-style-type: none"> • Emerging Transactional and Financial Technology Hub (ETFTH) • Industrial Research Institute for Automation and Measurements PIAP • IoT Poland Foundation Hub • IT and Expert Hub Supporting Biomedical Research, Technology and Education (BioMedHub) • Krakow Technology Park • Lublin Medicine Cluster • Regional Digital Innovation Hub related to Internet of Things (IoT North Poland HuB)

Member state	Fully operational		In preparation	
	No	Name	No	Name
Romania			3	<ul style="list-style-type: none"> • Cluj IT Cluster • Cluster for Innovation and Technology ALT Brasov, ALT Brasov • Transilvania Digital Innovation Hub – Transilvania DIH
Slovakia			2	<ul style="list-style-type: none"> • Institute of Informatics of SAS • TECHNICOM
Slovenia	6	<ul style="list-style-type: none"> • Digital Innovation Hub for Smart Manufacturing • Digital Innovation Hub of Eastern Slovenia (DIGITECH SI-East) • DIH AGRIFOOD – Digital Innovation Hub for Agriculture and Food production • HPC5 – High Performance and Cloud Computing Cross-border Competence Consortium • Jožef Stefan Institute • Styrian Technology Park, STP 	1	<ul style="list-style-type: none"> • Digital Innovation Hub Slovenia

Source: Catalogue of the Digital Innovation Hubs, own elaboration.

In order to create a strong pan-European network of DIHs, the EC plans to invest EUR 100 million per year, from 2016 to 2020. The implementation of draft regulation ‘Digital Europe 2021-2027’ will rest mainly on DIHs, which will serve as access points to latest digital capacities including high performance computing, artificial intelligence, cybersecurity as well as other existing technologies.

Presently, Slovakia has comparatively lower expenditures in R&D investment as a proportion of its GDP.¹⁷ The government recognises the need to increase the level of innovation within its economy and to do so it has invested in a number of digital research centres across the country. Slovakia has made advances in improving its innovative industries, and for several years had one of the highest growths in worker productivity across the EU.¹⁸ However, additional investments are necessary if Slovakia is to be better positioned to achieve growth in the digital age.

A DIGITAL FRIENDLY REGULATORY FRAMEWORK

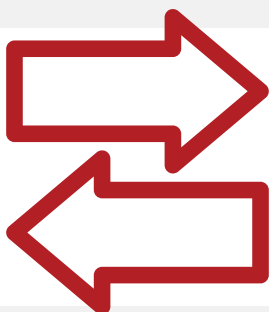
A digital-friendly regulatory framework is important for the EU's industry and economy to thrive. Within the Digital Single Market strategy, the EC has already proposed several measures to update regulations in key fields for industry such as cybersecurity and free flow of data. The list below shows (5.) the most relevant legislation which impacts the development of digital industry in the EU. As means of an introduction to artificial intelligence more in depth insight on data-related legislation and its impact on productivity will be provided (see ARTIFICIAL INTELLIGENCE AND ROBOTICS).



5. OVERVIEW OF THE MOST RELEVANT LEGISLATION IN THE FIELD OF THE EUROPEAN INDUSTRY

Cybersecurity Act (2017)

- Cybersecurity Agency ENISA
- European cybersecurity certification framework



Free flow of non-personal data (2017)

- Common European data space abolishment of unjustified and disproportionate localisation restrictions
- In combination with the General Data Protection Regulation

Towards a common European data space (2018)

- Review of the Directive on the re-use of public sector information



Proposal establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (2018)

Update

- Recommendation on access to / preservation of scientific information
- Guidance on sharing private sector data
- Revision of the EU directive concerning liability for defective products



6. EU FUNDS SUPPORTING THE DIGITAL INDUSTRY

The Horizon 2020 research program

The EU will provide 80 billion euro for research and innovation and fund transformation of research into prototypes and products. The funds are available for digital innovation centres and free flow data projects in six industries: automotive, space, defense, textiles, maritime technologies and tourism



Digital Europe

A new programme and part of the 'Single Market, Innovation and Digital' chapter of the EU's long-term budget proposal with the amount of EUR 9.2 billion. Building on the Digital Single Market strategy launched in May 2015 and its achievements over the past years, its main objective is to shape Europe's digital transformation to the benefit of citizens and businesses.

RECOMMENDATIONS FOR THE 3S COUNTRIES:

1. Strong and innovative IT sector serves not only as engine for domestic growth but also as an important export commodity. It can in particular become an important export commodity and **a smart specialisation** for region abundant in STEM talents like the 3 Seas region.
2. Smart specialisation policies depend on a frameworks of actions (e.g. competition, tax, trade policy, labour market policy and education and skills) therefore an intelligent policy approach should be sought by the countries of the 3S region to provide for **incentives for innovation** to stimulate private sector's investment in R&D.
3. Cross-regional cooperation between the DIHs both in the 3S region, in the EU and internationally would provide

for a critical mass and industry concentration. Therefore **policy support for linking regional strengths with international value chains** could take an interregional character as well as a European dimension.

4. Further **development of the European cluster policy**, with the aim of linking up and scaling up regional clusters into cross-European world class clusters, based on smart specialisation principles, in order to support the emergence of new value chains across Europe proves indispensable.
5. The DIHs should explore **liaisons with formal educational programs** to fill the gaps which exist in vocational schooling, undergraduate and graduate courses and to address potential mismatch of skills resulting from advancement in technologies.
6. Building **cross-border research partnerships with universities in the 3S region** to disseminate awareness among students and researchers as well as **custom made curricula** to educate companies would enhance commercialisation of knowledge.
7. The Digital Europe programme (2021-2027) should provide for a **balanced geographic distribution of the resources** directed at development of key strands of the programme, i.e.

cybersecurity, artificial intelligence, high-performance computing and digital skills. In this vein, the Smart Factories in new Member States programme serves as a good example.

8. Given that available financial resources for the development of DIHs are channelled through different programmes and policy instruments (training, infrastructure, entrepreneurship) what should be sought at the national level in #S countries is **the alignment of existing actions to support further development and expansion of the DIHs**.
9. There exists a **clear underrepresentation** of countries of the 3Seas region **in the public-private partnerships (PPP) and the European Technology Platforms** established by the European Commission. Therefore policy support to further strengthen linkages of both SMEs and large-companies needs to be introduced to eliminate such inequality.^{19, 20, 21}

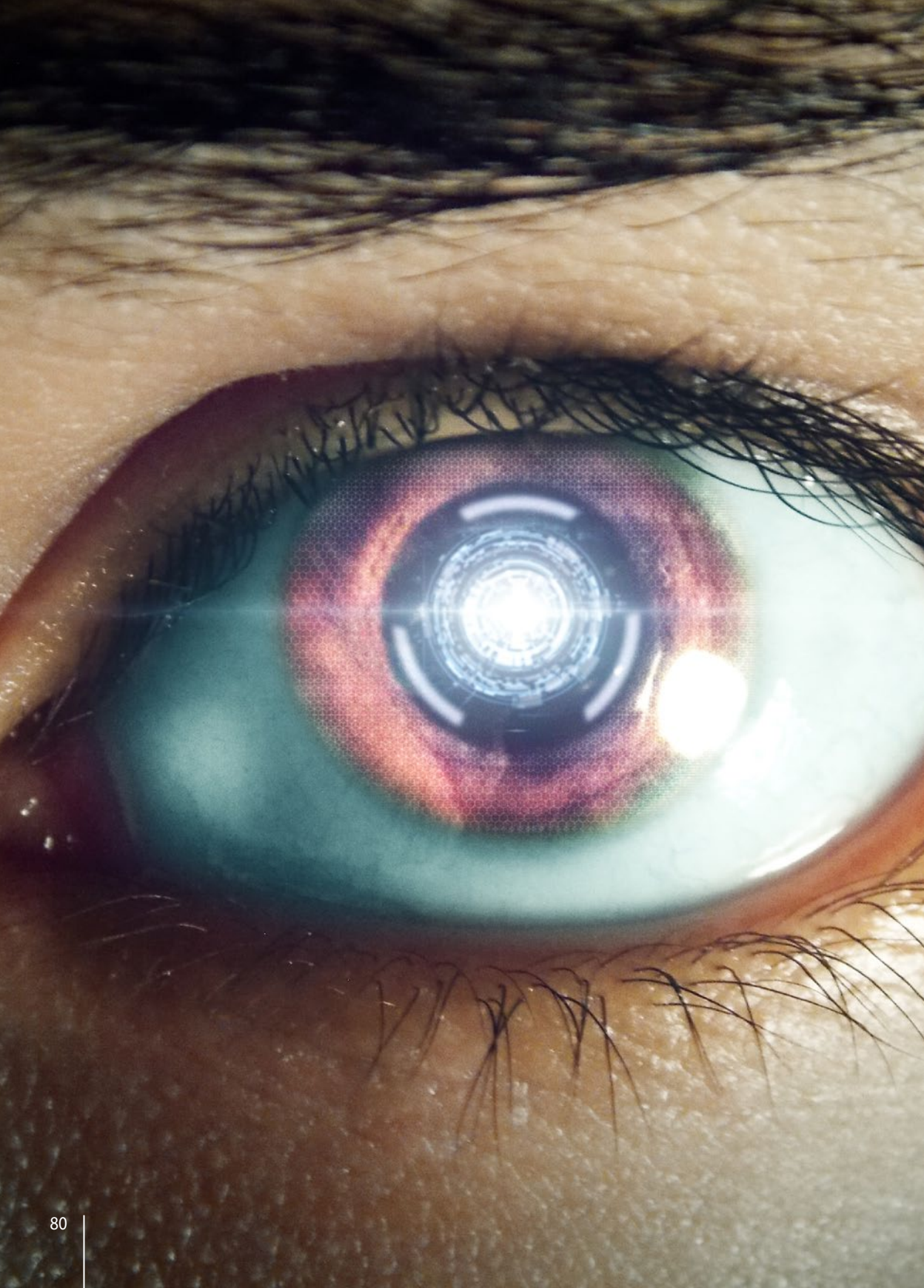




SOURCES:

1. Attal S. (2017, August 7). How Industry 4.0 and Industrial Analytics will disrupt the European manufacturing sector. Presenso [on-line]. Available at: <https://www.presenso.com/single-post/2017/08/07/how-industry-4-0-and-industrial-analytics-will-disrupt-the-european-manufacturing-sector/>.
2. PwC (2016). Industry 4.0: Building the digital enterprise [on-line] Available at: <https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf>
3. European Commission (2018). Digital Transformation Monitor: Slovakia [on-line] Available at: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Slovakia_FINAL.pdf
4. European Commission (2016). Communication from the Commission to the European Parliament, the Council, the European and the Social Committee and the Committee of the Regions. Digitising European Industry. Reaping the full benefits of a Digital Single Market [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0180>.
5. European Commission (2017). Strengthening Innovation in Europe's regions – Strategies for resilient, inclusive and sustainable growth [on-line]. Available at: http://ec.europa.eu/regional_policy/en/information/publications/communications/2017/strengthening-innovation-in-europe-s-regions-strategies-for-resilient-inclusive-and-sustainable-growth.
6. European Commission (2018), Digitising European Industry. Progress so far, 2 years after the launch [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/digitising-european-industry-2-years-brochure>.
7. European Platform of national initiatives [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/digitising-european-industry-digital-day>.
8. Digital Transformation Monitor (n/d). National initiatives [on-line]. Available at: <https://ec.europa.eu/growth/tools-databases/dem/monitor/category/national-initiatives>.
9. European Commission (2018), Digital Economy and Society Index Report 2018 – Integration of Digital Technology [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>.
10. Polityka Insight (2017). Artificial intelligence of the Polish economy [on-line] Available: <https://www.politykainsight.pl/reports/ai>.
11. European Commission (2018). Cloud computing [on-line]. Available: <https://ec.europa.eu/digital-single-market/en/cloud>.
12. According to a presentation of Mr Gyula Pomazi, former Deputy State Secretary, Ministry of Innovation and Technology of Hungary.
13. European Platform of national initiatives [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry>.
14. Hungarian Ministry of Foreign Affairs and Trade (2017). #V4 Connects: Presidency Programme. pp. 24-25.
15. PWC (2018). Smart Factories in new EU Member States General Presentation [on-line]. Available at: <http://www.kpk.gov.pl/wp-content/uploads/2017/09/Smart-Factories-in-new-EU-MS.pdf>.
16. European Commission (2018). Digitising European Industry, Progress so far ..., op. cit.
17. Eurostat (2018). R&D expenditure [on-line]. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/R_%26_D_expenditure.
18. OECD (2018). Highlights from the OECD Science, Technology and Industry Scoreboard 2017 – The Digital Transformation: Slovak Republic [on-line]. Available at <https://www.oecd.org/slovakia/sti-scoreboard-2017-slovak-republic.pdf>.
19. Council of the EU (2018). Conclusions on a future EU industrial policy strategy [on-line]. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2017/05/29/compet-conclusions-future-industrial-policy-strategy/>.
20. OECD (2013). Innovation-driven Growth in Regions: The Role of Smart Specialisation [on-line]. Available at: <http://www.oecd.org/sti/inno/smart-specialisation.pdf>.
21. AIOTI (2017). Digital Innovation Hubs: democratising digital technologies in agriculture [on-line]. Available at: https://aioti.eu/wp-content/uploads/2017/11/AIOTI_WG06_ADIHS_final.pdf.







ARTIFICIAL INTELLIGENCE AND ROBOTICS

In the overall discourse, common misconceptions, mistaken extrapolations or limited imagination hamper a constructive process of thinking about the future. These failed assumptions have already been summarised in the so-called Amara's law, in accordance with which the impact of new technologies is overestimated in the short run and underestimated in the long run. In fact, all innovations in robotics and artificial intelligence lead much further than one can imagine.¹ AI has arrived at the forefront of new technologies. However, on a methodological note, it poses challenges that stem from the lack of a sharp definition of what it really is, a nascent stage of its development and a difficulty in the assessment of where one industry or application ends and another begins.² What needs to be underlined is that the promise for AI is yet to be fulfilled, as today's AI applications tend to focus on a narrow scope of specific tasks – as opposed to general artificial intelligence, which attempts to perform intellectual tasks that a human can do. Nevertheless, taken together, they are starting to reshape the world that we know today.³

Without a doubt, AI will have deep implications for the socio-economic development and the competitiveness of the region. It is a common view that automation will have lesser effect on jobs that consist of managing people, apply expertise or involve social skills (see DIGITAL SKILLS). In such professions machines for the time being are not able to match human performance.⁴ More widespread deployment of machine learning, data analytics or robotics will result in augmenting the knowledge-intensive fields of both production and high-level decision-making processes. Adoption of AI so far has increased demand for human labour due to significant increases in productivity. More categories of jobs related to training AI systems, interpreting data and algorithms or ensuring that the solutions do not create ethical concerns are to emerge.⁵

67 % of executives say AI will help humans and machines work together to be stronger using both artificial and human intelligence.⁶

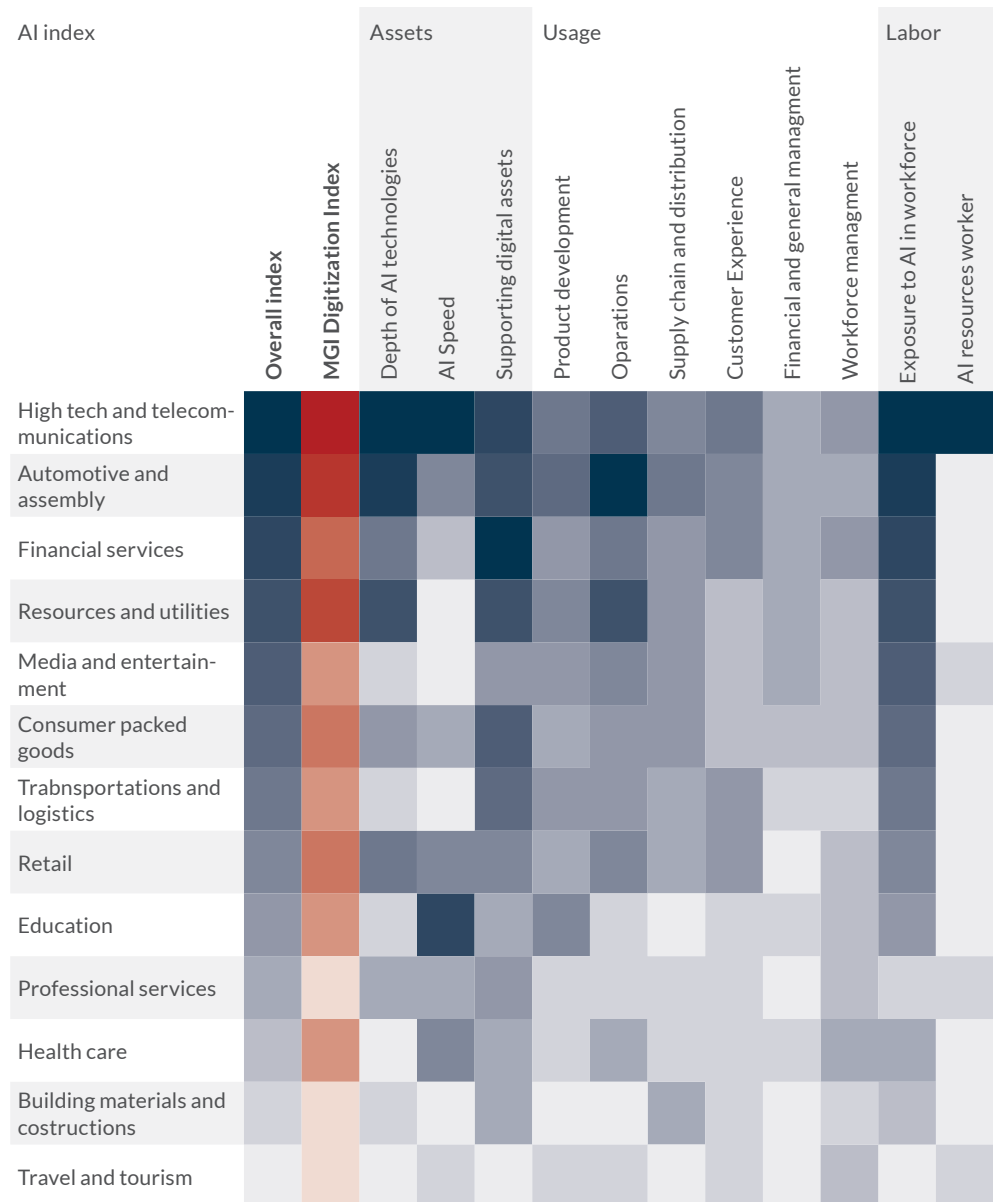
SECTORAL APPLICATION OF AI

The 3S region sees a growing level of spending on cognitive and AI technologies, with

a perspective to reach USD 83.9 million in 2018. This represents the annual growth of 41.2 % which is expected to continue in the future, reaching the compound annual growth rate of 44.2 % over the next five years.⁷ In the region, the industries which heavily invest into cognitive or AI systems are manufacturing, banking and retail. Behind heavy investments in financial sector stands a stringent compliance, where the innovation enhances a process of fraud and risk detection. It is, however, the health sector where solid investments are going to take place and reach the CAGR exceeding 55 %. Main areas of focus will be diagnosis and treatment system.

Globally, AI is being adopted faster in more digitised sectors, such as telecommunications, financial services and high tech (1.).⁸ Early AI adopters happen to be from the same sectors which have already invested in related technologies, such as cloud services and big data. Larger companies and industries that have already adopted other digital technologies are more likely to adopt AI. For them, AI is a kind of the next digitisation wave. This implies that, at least in the near future, AI deployment is likely to accelerate and may cause a widening of the gap between adopters and laggards.⁹ The traditionally less digital fields such as construction and healthcare have the most catching up to do in the area of AI.

1. AI ADOPTION IS OCCURRING FASTER IN MORE DIGITISED SECTORS AND ACROSS THE VALUE CHAIN



Source: McKinsey Global Institute analysis, 2017.¹⁰

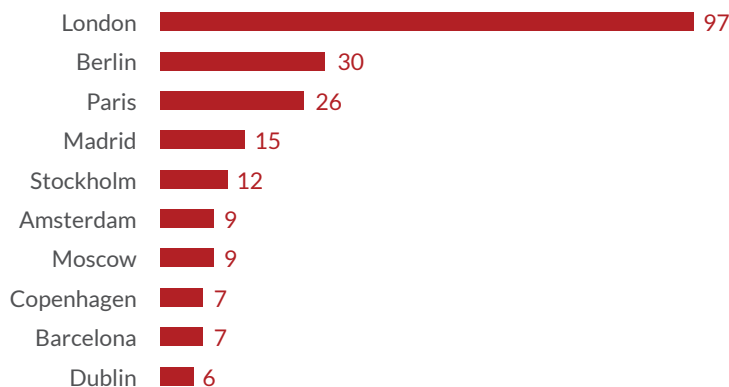
Also in the 3S region, the top three fields of AI application in terms of investment importance can be found in:

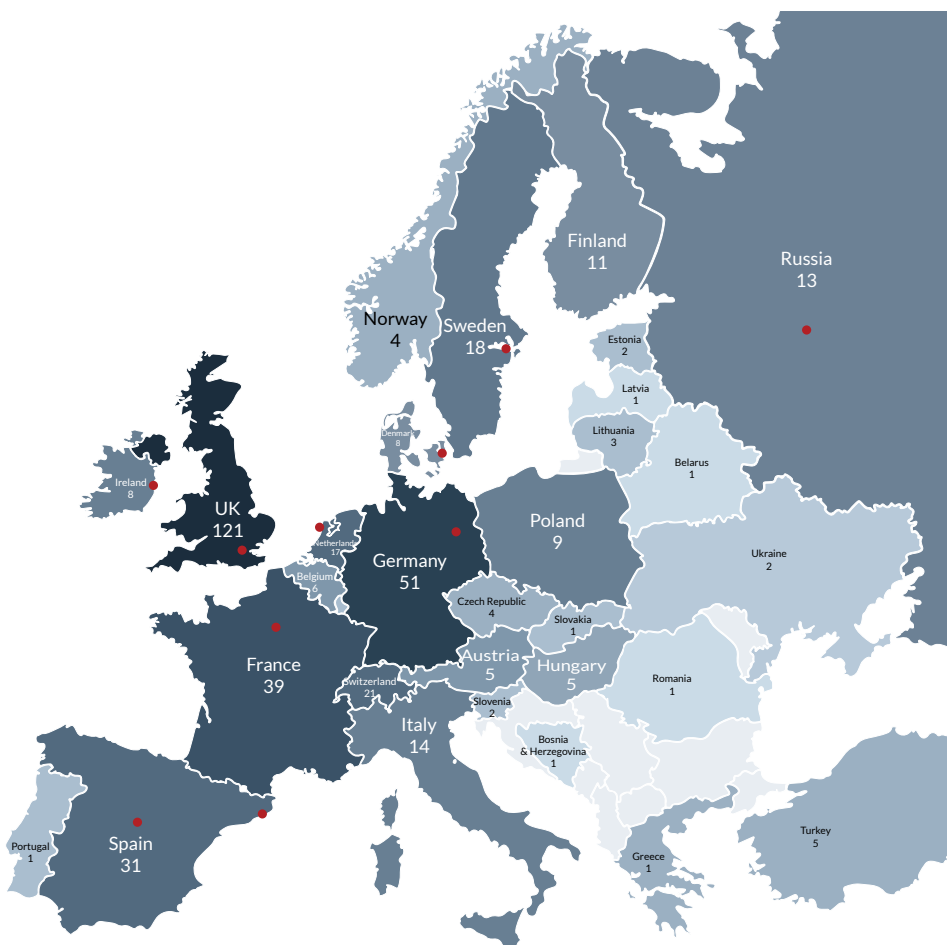
1. **threat intelligence and prevention systems** (USD 12.21 million) – for government, banking, utilities, telecommunications industries;
2. **fraud analysis and investigation** (USD 8.88 million) – for banking, securities, investment and investigation;
3. **supply and logistics** (USD 7.4 million) – for the manufacturing and retail sectors.¹¹

These three sectors constitute 81 % of the total venture capital inflows by value and 73 % by number of entities.¹² However, at the level of the EU as a whole, healthcare, finance, agriculture, advanced manufacturing, automated driving and fighting climate changes are perceived as key target sectors which should be addressed by means of coordinated actions. What should be borne in mind is that the impact of AI is cross-sectoral and the companies which create AI tools for business cannot be hemmed in one domain. This impact, through its interconnecting effect, is likely to be experienced by all sectors and consumers across the board.¹³

Regarding the AI startup hubs in Europe, one could observe that London (without parallel), Berlin and Paris dominated the landscape (2.). In the 3S region, Poland has the highest number of AI startup hubs (9), while Hungary and the Czech Republic (5 and 4 accordingly) achieve a better result if their numbers of inhabitants are taken into account.¹⁴

2. EUROPEAN AI STARTUP HUBS





Source: Asgard, 2018.

CASE STUDY – SLOVAKIA

Slovakia is seeing the development of many technology startups, including those that deal with using artificial intelligence tools for business. For example, AI startup *nettle.ai* joined forces with another one – Mazars, and established a strategic partnership to support

the exploration, development and delivery of AI-based conversational platforms to their customers in Slovakia and across the 3S region.¹⁵ Companies which specialise in predictive analysis, such as CaseCrunch, ESET, Sugic and Pixel Foundation, are established international market players.

As far as startups from 3S countries are concerned, they have developed their own signature domains, i.e. the Czech Republic – cybersecurity; Latvia – FinTech; Lithuania – e-commerce, gaming and laser technologies, Poland – software and life sciences; Romania – gaming and cybersecurity.

CASE STUDY – POLAND

Among Polish startups in the field of AI, over 80 % are developing machine-learning technology. Their work is mainly in the area of operational efficiency, fraud detection, customer forecasting and healthcare diagnostic applications based on image recognition. A number of startups specialise in robotics, building autonomous robots for specific industrial applications. A few are developing virtual assistants and language technologies for the Polish language.¹⁶


Despite the relatively small scale of investment from a global perspective, Poland is the birthplace of numerous companies that have become at least regionally recognisable as promising developers of AI. Some already have a significant international presence:

- IVONA produces high-quality text-to-speech technology, voice guides and explore-by-touch services. The company was acquired by Amazon in 2013, a move seen by many experts as a way to compete with Apple's Siri. IVONA is recognisable within the industry thanks to its natural voice quality, accuracy and ease of use. As of September 2017, it offers 47 voices in 24 languages.¹⁷
- Growbots was founded in 2014 and currently has offices in Warsaw, San Francisco and Cleveland. It provides a sales automation platform based on machine learning that, among other things, aims to find the right leads for sales teams and then conduct an automatic email campaign. Growbots has over 450 customers, most of them in the United States.¹⁸
- Nethone is a Warsaw-based startup specialising in AI solutions for fraud prevention. Founded in 2015 by a team of data scientists, risk managers and security specialists, it currently serves clients in Europe, North America and South America. Among its customers are a major American airline, an on-line travel agency and a leading video-streaming platform.¹⁹
- DeepSense.ai provides deep learning solutions for enterprises. It was founded and is now managed by CodiLime, a company established by Polish computer scientists and mathematicians. Neptune, DeepSense.ai's newest product, is a machine-learning platform designed to efficiently manage and monitor data-science experiments. The company lists Intel, IBM, Huawei and BZ WBK among its clients and partners.²⁰

- *Neurosoft is a Wroclaw-based startup that develops speech, language and image technologies. It specialises in intelligent transportation and road-safety systems, offering commercial solutions for the complex identification of vehicles in motion, including license plate, type of vehicle, manufacturer and model name recognition in real time (less than 120 milliseconds). The system has already been implemented in Ankara, Turkey.²¹*

The 3S region has AI-related potential (see DIGITAL SKILLS). Its countries, like Poland, have a large number of graduates in science and technology and a dynamic startup ecosystem, which enables them to train future AI specialists. Romania also has a relatively long tradition (more than 40 years) of R&D in AI and robotics. Currently, as parts of the Romanian ICT sector, both AI and robotics are growing economic sectors (NLP tools, cognitive systems, interfaces, decision support systems, 3D printing, biomechanics). Although Romania's general automation readiness is low,²² there is significant potential for development in the years to come, which results from human capital, investments and the commitment of the industry stakeholders to grow the domain. The Slovak government, for its part, prioritises creating an attractive business environment for companies that focus on AI and directing the economy towards higher added value enterprises.²³ The government will focus on three specific stakeholders to foster capacity-building and unlock the full potential of AI: universities and research organisations; businesses that must transfer expertise from labs to the market; and public administration that should follow best practices in decision-making.

CASE STUDY – POLAND



A great example of links and increased cooperation between the 3S countries was the CEE All Stars Event hosted by Google Campus Warsaw in June 2018,²⁴ organised by leading accelerators and hubs from the region. The event was held with a belief that conquering bigger markets can only be done by cooperating.

However, the scale of investment needed to develop AI technology is relatively small compared to, for example, industry, which requires major investments in plants and machinery. In recent years, AI has seen successful implementation in specific applications and uses. This opens the way for development of startups and SMEs.

There are, obviously, challenges that have been identified, i.e.:

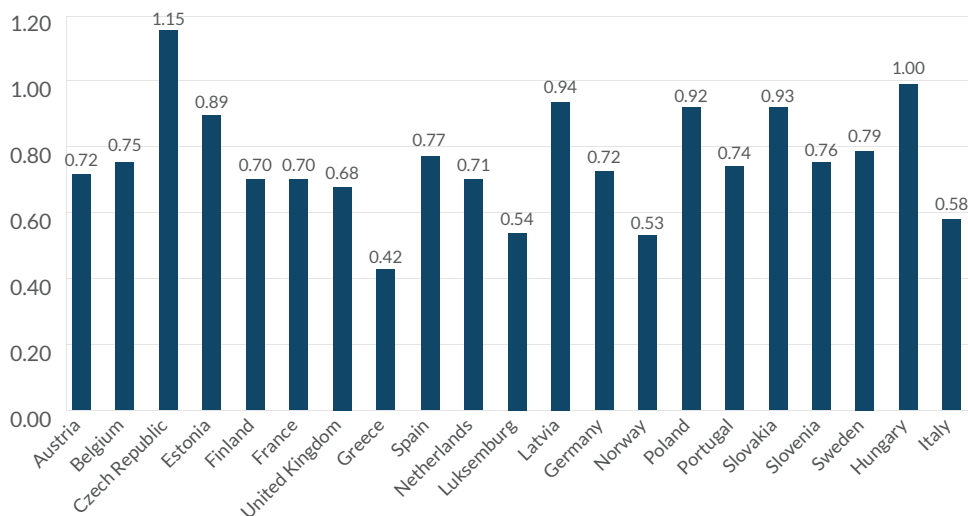
- As a nascent field, AI and robotics is not well established; therefore, researchers face a number of technical obstacles, such as problems related to finding premises for assembling their robotics systems. There is no equal treatment, some who are willing to work on new technologies have no conditions to do it properly.
- The commitment of the business sector to investing in AI and robotics is very clear and irreversible, however, the governments face challenges in defining the strategy and the approach towards AI and robotics.
- Now, the 3S region is more of an outsourcing centre. The private sector originating from the region does not have a unitary approach towards how the industry should be oriented in the future.
- Lack of high-quality data, limited AI capability and AI competence centres for dissemination of technology hamper the further development of AI.²⁵

Currently observed trends in the amount of data, its diversity and the multitude of possible applications do not find a historical precedent, which present both an opportunity and a threat. The chance is that recognising emerging trends enables accurate and early identification of the

strategic directions for development. On the other hand, the basic threat is that failure to participate in the process creates a kind of innovation debt, which will have to be repaid, although not today, but with a compound interest rate.²⁶ In June 2018, the EU negotiators reached an agreement on the regulation of a free flow of data, which will allow data to be both stored and processed without unjustified restrictions. These rules will allow for the free flow of data across borders thus creating a single European space for data; ensure data availability for regulatory control for public authorities and ensure creation of codes for cloud services to ease switching between providers.²⁷ While a rosy picture emerges from the potential of having seamless flows of data within the EU, this potential remains untapped.

In the 3S region, the ratio of the estimated level of data-driven productivity to the estimated level of the generic productivity is fairly high. As for the less developed economies, intensity of data usage by enterprises contributes to GDP in a significant way, relatively to other productivity-driving factors.²⁸

3. SIGNIFICANCE OF DATA-DRIVEN PRODUCTIVITY²⁹



Source: Ministry of Digital Affairs, 2018.

The significance of data-driven productivity (ratio between data-driven productivity and generic productivity) is depicted above (3.). Data-driven productivity would be highest in the Czech Republic (115 %), Hungary (100 %), Latvia (94 %), Slovakia (93 %) and Poland (92 %). Significance of data-driven productivity lines with the interests of various groups of the European countries, forming a field, in which joint undertakings can be mutually beneficial for all stakeholders.³⁰

CASE STUDY – POLAND

In the area of production automation, Poland continues to lag behind most developed nations and its neighbours. According to the International Federation of Robotics, the average number of installed robots worldwide was 74 in 2016, and in Europe the figure was

99 per 10,000 employees. With a value of 32, Poland is well behind Slovakia (135) and the Czech Republic (101). It is expected that this deficit will be compensated for in coming years: Poland recorded growth in robot density of 45 % within two years.³¹ This offers great prospects to providers of automation solutions; larger companies have already reac-

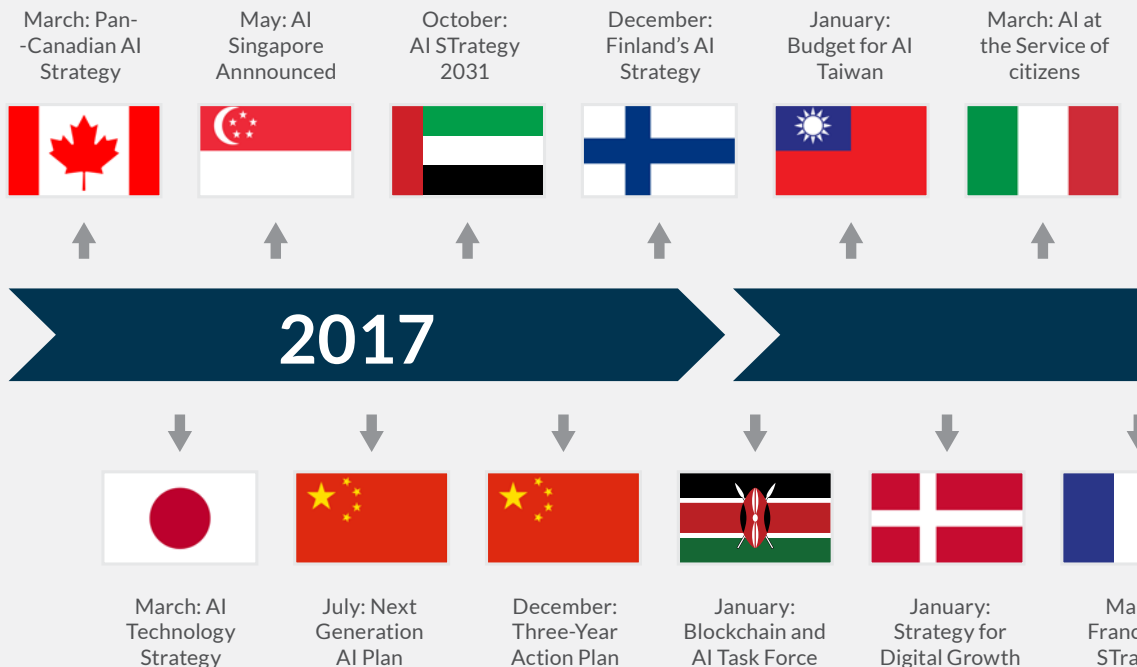
ted accordingly and expanded their presence in Poland. ABB is one example. Its robotics centre in Warsaw, which has been expanded

and was reopened at the end of January 2018, serves as a demonstration, training and test centre for customers throughout the region.³²

EU APPROACH TO AI

The EC recognises the need for strong AI ecosystems, which will unite AI developers, users and funding. In the time span of 2021-2027, the EC attempts to implement the Digital Europe Programme (see EU APPROACH TO DIGITAL SKILLS) by means of the DIHs in particular. By 2020, at least one DIH per region should be established (see DIGITAL INNOVATION HUBS). In one of the strands, the Digital Europe will address artificial intelligence.

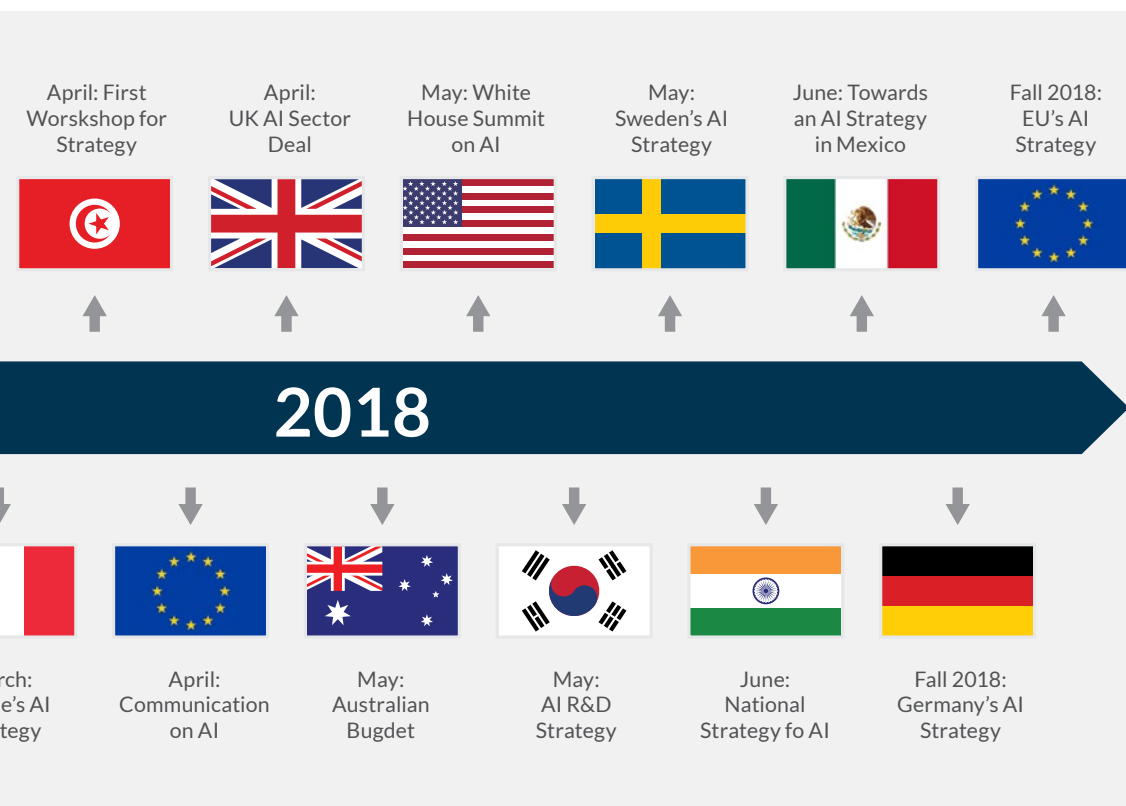
4. AI STRATEGIES




Source: Dutton T., 2018, Artificial intelligence strategies³⁴

In January 2018, the EC in cooperation with the European Association for Artificial Intelligence organised a workshop to take stock of the current state of the field in Europe and to identify opportunities for pan-European collaboration. In the workshop report, *The European AI Landscape*,³³ which constitutes a summary of the current state of play in AI in the EU, the input from the 3S comes only from Austria, the Czech Republic, Estonia and Romania. That clearly depicts an underrepresentation of information provided by the region, and thus the analysis might give a skewed picture of the actual activity taking place at the national level and would need to be supplemented.

Member States have also been encouraged to develop national AI strategies which are supposed to be supported by an investment plan. To date, a few Member States have published their strategies (Sweden, Denmark, France, Finland and the UK). By the end of 2018, Member States assisted by the EC will establish a coordinated action plan on the development of AI. The graph 4. shows an increased activity of countries over past few years, therefore a number of new strategies is to be expected.



CASE STUDY – ROMANIA



Romania does not have a specific AI strategy; however, in 2014 the government adopted the national strategy for R&D in which AI and robotics are deemed priority areas. AI and robotics are considered an opportunity that should be capitalised on according to the National Strategy on Digital Agenda for Romania.

The government supports R&D activities through the National Plan for R&D and Innovation. However, the amounts of research grants for the fields in question do not exceed 0.01 % of the GDP.

The main areas of focus are natural language processing, cognitive systems, advanced interfaces, decision support systems, cybersecurity and nanotechnology. Among examples of successful projects are: Romanian Spoken Language Processing (RSLP), CoRoLa – a reference electronic corpus of contemporary Romanian language, ReTeRom – Resources and Technologies for the development of human-machine interfaces in Romanian, Heimdallr – a tool for real time keyword spotting in phone conversations.

In April 2018, 24 Member States and Norway signed a Declaration on Cooperation on Artificial Intelligence³⁵ with the purpose of joining forces and engaging in a European approach to tackle the issue. The EU signatories of the declaration were Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France,

Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and the UK³⁶ – ten of which are 3S countries. Since then, Romania and Croatia have joined.

In addition, the EC calls for a boost of the EU's competitiveness and ensuring that the trust between the stakeholders is based on the European values. Three main goals can be named here: enhancing Europe's scientific base, technological know-how and industrial capacity; preparing for socio-economic changes brought about by AI; and ensuring an appropriate ethical and legal framework.³⁷

In view of the EC presenting a series of measures to put artificial intelligence at the service of Europeans and boost Europe's competitiveness in this field,³⁸ the Visegrad Group presented its joint position on AI in which the V4 identified 9 priorities for the EU.³⁹ Areas of importance include the 'pan-European initiative on establishing an ambitious framework for opening up the data for innovation in order to speed up research, development and implementation of ethically designed AI based systems'; uniform regulatory sandboxes at the EU level; education and research; and cybersecurity.

ETHICAL ASPECTS OF AI

It is worth noting that digital prosperity will not be achieved in countries that do not address issues related to citizens' well-being and fundamental principles.⁴⁰ Nimble policy-making and strong ethical guidelines are the key to ensure that AI does not threaten either equity or security. An important ethical question which arises is how machines are taught. In public discourse worldwide, there emerges a need for global regulatory norms that would ensure the ethical development of technology. The call for establishment of a common ethical and legal framework for the design, production, use and governance of AI, robotics and autonomous systems,⁴¹ as well as a framework for explaining processes, services and decision delivered by AI⁴² resonates well among a wider, international audience. There are voices to create an AI Charter,⁴³ a cross-sector AI Code⁴⁴ and the International Artificial Intelligence Organisation⁴⁵ in order to improve transparency and accountability.⁴⁶ Nevertheless, ethics in the AI context is still a nascent field.

Top ethical issues to be addressed are:

- changes to labour force,
- how the machines affect our behaviour and interactions,
- biases in machine-learning algorithms,
- how to keep AI safe from the adversaries,

- how to control a complex intelligent system, and
- robot rights – how to define the human treatment of AI.⁴⁷

Ethical and regulatory frameworks are a precondition for the widespread development of AI. By the end of 2018, the EC is to present ethical guidelines on AI. Nevertheless, the European Group on Ethics, Science and New Technologies has already proposed a set of recommendations related to the ethics of artificial intelligence and principles guiding its development.⁴⁸ They touch upon issues which require further attention: human dignity; autonomy translating into human responsibility and control over autonomous systems; responsibility with a regard to human values and rights; justice, equity and solidarity; democracy; rule of law and accountability; security, safety and integrity; data protection and privacy; or sustainability. In parallel, the EC keeps working on the revision of the EU directive concerning liability for defective products. A clarification is sought when it comes to legal understanding of certain concepts such as product, producer, defect, damage and burden of proof. The guidance on the directive will be issued with an accompanying report which covers potential gaps and future trends regarding liability and safety of AI.⁴⁹

CASE STUDY – FACIAL RECOGNITION TECHNOLOGY

New technologies can assist people but they could also be misused inadvertently or manipulate people on purpose by influencing their reasoning and judgement.⁵⁰ One of the challenging techniques is the Facial Recognition Technology which often happens to hit the headlines when misused by governments in times of unrest. Detection technologies show a considerable potential in recognising faces (even if partly covered by beards or glasses), determining emotions and reactions. Its commercial potential and impact on the public good is vast when it comes to security, detecting and deterring crimes, targeted advertising or authentication. FRT is an example of a troublemaker technology that goes to the heart of fundamental human rights and gives rise to legal concerns. At the EU level, under the General Data Protection Regulation, the digital images and outputs like reports and profiles will constitute personal data. As some types of FRT data will be categorised as sensitive, more stringent rules will apply. Roughly speaking, processing such data is – under the conditions of the GDPR – forbidden unless specified conditions are met. However, not all of FRT data will be personal data and fall under the GDPR scope. As a consequence, a number of regulatory issues – lawful basis, consent, transparency and information requirements, profiling and a right to object to processing – will still need to be dealt with.⁵¹ The recently established AI and Ethics in Engineering and Research Committee will address, among others, some form of compliance with the GDPR.

Despite the concerns, by 2022 the value of the market for FRT solutions is to reach USD 9.6 billion with a CAGR of 21.3 %. In parallel, general IT market will witness a growth of 3.3 % CAGR in the time span between 2015 and 2020.⁵²

The Council of Europe intends to map the concepts of legal and moral responsibility for AI decision-making systems within existing legal frameworks. It recognises that it is mostly private sector which has considerable knowledge and skills in the field; therefore, this expertise should be shared for the sake of all.⁵³ It is also the private sector that encourages governments to spearhead efforts on the establishment of best practices for AI to enable the technology to serve the public.⁵⁴

For example, the AI partnership, initially established by Apple, Amazon, Deep Mind and Google, Facebook, IBM and Microsoft, has grown into a multi-stakeholder organisation with more than 50 partners that call for, among others, AI tools which are safe, trustworthy and aligned with ethics or sensitive to potential biases and hidden assumption in the data. Quite unusual, but it is the private sector that makes an effort and asks governments to regulate the use of technologies, stating that ‘it seems more sensible to ask an elected government to regulate companies than to ask unelected companies to regulate such a government’.⁵⁵

Irrespective of definitions applied, development of the AI economy requires an ability to access, share, anonymise and protect data. Such an approach needs to be followed by the ability to develop algorithms, but also to explain their *modus operandi*.⁵⁶ Data reflects historical, social and political context in which it was created. Since AI applications learn from the data which seeds them, intelligent systems learn human prejudice. Use of such data might lead to biased, inaccurate or unfair outcomes.⁵⁷ This observation gains relevance in the critical fields, such as medicine or law. It is also stated that algorithmic bias is omnipresent in many other industries.⁵⁸

In this respect, the EU, while working on the ethical guidelines on AI, could establish its leading role by defining standards of data used to fuel machine learning.⁵⁹ Nonetheless, on the technical front, increasing diversity in order to remove bias in machine learning should be one of the cornerstones of policy-making. This means that more women and people of diverse backgrounds, including those with disabilities, need to take part in developing AI solutions. This would need to start with education and training through the interdisciplinarity of research. The ethical component of technology development should be addressed early on in the educational process.⁶⁰

The matters listed above – and there is no doubt that others will emerge – are to become important public policy problems

around the world, in the 3S region as well. Given the global nature of the technology itself, they will require an active engagement involving governments, academics, tech companies and civil society, regionally and internationally.⁶¹

The above-mentioned joint position on AI by the V4 also encompasses potential results of the AI development which involves industry, laws, society and ethics. It underlines the importance of fundamental human rights, which should not be compromised while creating AI solutions. The V4 expressed a concern regarding social engineering experiments with AI conducted by global leaders in the field. These four states also pointed out a need for defining AI, copyrighting products made by AI and discussing the responsibilities which lie on operators of AI machines.

However, when the approach of the whole 3S region is considered, the discussion on ethics of AI is still to gain momentum. Only a few academic debates addressed the topic and only tangentially. Until the present, no legislative initiatives have been registered, nor has a pedagogy of machine learning been introduced. Still, the ethical and legal challenges stemming from AI are a topic which has not commanded the due attention so far.

RECOMMENDATIONS FOR THE 3S COUNTRIES:

1. Establishing **AI strategies** supported by a concrete public-private funding/ investment plan will signal the importance of the domain in national and international policy. These strategies shall establish coordinating bodies (including the AI ethics councils) and a mechanism for legal enforcement of their implementation.
2. Such strategies should build an ethical and legal framework that adequately takes into consideration EU fundamental rights and values, including privacy and trust between users of data, and practices of accountability.
3. **Plans for international engagement** shall also be included in the strategies. By means of developing a list of AI fields for such engagement, an intraregional (3S countries) and multilateral cooperation with other technologically advanced regions and economies, including outside the EU, shall be undertaken.
4. In accordance with a common methodology (nomenclature, funding, AI sub-themes, sectors, accelerators, foreign branches, geographical expansion), **repositories of AI startups, SMEs, mid-caps and international companies** shall be established, with

a long-term objective to support a concept of national/regional domains and enhanced cooperation between startups, SMEs and established companies.

5. Given the scarcity of comparable data on the development of AI, its overall effects and future in the 3S region, **regional, cross-country AI think tanks/ centres of excellence** shall be established. They will serve for information sharing between countries on matters of AI regulatory frameworks, standards for securing privacy and safety of data, ethically designed AI systems, and for evidence-based policy-making in general.
6. Developing the 3S region as a centre for AI requires not only the involvement of businesses but also **decisive action by government** (voiced by means of AI strategy for instance), which shall: (1) **nurture local AI talent**, (2) support universities and more research projects in the AI area by opening new financial lines, which will **prepare the workforce**, (3) seek new products and solutions in public-private partnerships, in collaborating not only with companies but also with universities which lead the development of AI and robotics in the region, which will make **building local AI industry** possible, and (4) **deploy AI solutions also within public institutions**.

7. The private sector shall both **support R&D institutions** which educate their future employees, and create more interest in specific projects in collaboration with R&D institutions.
8. Despite a growing number of IT graduates and practitioners, there exists a scarcity in both the numbers and specific qualifications sought across the 3S region. To ease this strain, the governments in cooperation with a private sector could consider – drawing on international solutions – an introduction of **next-generation visas/talent passports** to attract AI practitioners from outside the EU to the domain where such scarcity can be observed.
9. An effective adoption of AI requires a solid foundation, including **access to large amounts of data**. Companies shall make sure that, together with governments, they **address all aspects of their digital transformation**: the identification of potential benefits and development of a business case, the setup of a right data ecosystem, the creation or acquisition of appropriate AI tools, as well as the adaptation of their processes, capabilities and culture.
10. Government policies shall aim at easing access to data, drawing on the UK example of **data trusts/warehouses**. Such policies should promote the principle of open data, in particular in the public sector, to provide a resource for wider sectoral applications of AI.
11. **Interoperable regional/bilateral data spaces** which aggregate public information across the region and become an input for AI regional solutions shall be created. Also, the development of **regional/bilateral AI facilities** including accessible data resources and repositories of accessible algorithms would strengthen capacity in the EU and the 3S region in particular.
12. More women and people of diverse backgrounds shall be involved in AI development. **Non-discriminatory and inclusive AI interdisciplinarity** shall also be supported (by encouraging joint degrees, for example in law or psychology and AI). The importance of ethics in the development and use of new technologies shall also be featured in programmes and courses.
13. **Awareness raising campaigns** shall be launched to raise awareness both on the importance of technologies and use of data for improved business performance and productivity, on the need of development of advanced digital skills, as well as on the need for cybersecurity solutions.



SOURCES:

1. Brooks R. (2018). The seven deadly sins of AI predictions. MIT technology review [on-line]. Available at: <https://www.technologyreview.com/s/609048/the-seven-deadly-sins-of-ai-predictions/>.
2. Fagella D. (2018). Artificial Intelligence Industry – An Overview by Segment [on-line]. Available at: <https://www.techemergence.com/artificial-intelligence-industry-an-overview-by-segment/>.
3. CBInsights (2018). Top AI Trends To Watch In 2018 [on-line]. Available at: <https://www.cbinsights.com/research/report/artificial-intelligence-trends-2018/>.
4. MC Kinsey (2017). Jobs lost, jobs created. Workforce transitions in time of automation [on-line]. Available at: <https://www.mckinsey.com/featured-insights/future-of-organizations-and-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages>
5. Hainfan G. (2018). New supply chain jobs are emerging as AI takes hold [on-line]. Available at: <https://hbr.org/2018/08/new-supply-chain-jobs-are-emerging-as-ai-takes-hold>.
6. PwC Consumer Intelligence Series (2017). Bot.me: How artificial intelligence is pushing man and machine closer together [on-line]. Available at: <https://www.pwc.com/CISAI>.
7. IDC (2018). Spending on Cognitive/AI Technologies in Central and Eastern Europe Reflects Organizations Growing Interest in Business Transformation, Says IDC [on-line]. Available at: <https://www.idc.com/getdoc.jsp?containerId=prCEMA43721618>.
8. Smart Insights (2017, August, 31). Artificial Intelligence adoption in different sectors [on-line]. Available at: <https://www.smartinsights.com/managing-digital-marketing/marketing-innovation/artificial-intelligence-adoption-different-sectors/>.
9. McKinsey & Company (2017). The AI revolution. How artificial intelligence will change business in Poland. op. cit.
10. MGI (2017). Artificial Intelligence: The Next Digital Frontier? [on-line]. Available at: <https://www.mckinsey.com/~media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx>.
11. Ibidem.
12. Invest Europe (2018). Central and Eastern Europe. Private equity statistics [on-line]. Available at: <https://www.investeurope.eu/media/727455/Invest-Europe-CEE-Activity-Report-2017-05072018.pdf>.
13. PWC (2018). The economic impact of artificial intelligence on the UK economy [on-line]. Available at: <https://www.pwc.co.uk/economic-services/assets/ai-uk-report-v2.pdf>.
14. Asgard (2018). The European Artificial Intelligence Landscape and largest AI hubs in Europe [on-line]. Available at: <https://asgard.vc/wp-content/uploads/2017/07/European-Artificial-Intelligence-Hubs-and-Landscape-2017-by-Asgard-VC.png>.
15. Mazars (n/d). Artificial Intelligence startup nettle.ai joins our Bratislava offices [on-line]. Available at: <https://www.mazars.sk/Home/News/News/AI-startup-nettle.ai-joins-our-Bratislava-offices>.
16. McKinsey & Company (2017). The AI revolution. How artificial intelligence will change business in Poland. op. cit.
17. Ivona website [on-line]. Available at: www.ivona.com.
18. Growbots website [on-line]. Available at: www.growbots.com.
19. Nethone website [on-line]. Available at: <https://nethone.com>.
20. Deepsense.ai website [on-line]. Available at: deepsense.ai.
21. Neurosoft website [on-line]. Available at: neurosoft.pl.
22. Automation readiness is greater within the private sector compared to the central and local administrations.
23. American Chamber of Commerce (n/d). AI-SK (Artificial Intelligence Platform in Slovakia) [on-line]. Available at: http://www.amcham.sk/events/2678_ai-sk-artificial-intelligence-platform-in-slovakia.
24. CEE All Stars website [on-line]. Available at: <http://www.ceeallstars.com>.
25. European Commission (2018). Commission staff working document. Impact Assessment accompanying the document: Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=SWD%3A2018%3A305%3AFIN>.

26. Ministry of Digital Affairs (2018). Data utilization intensity and economic performance – a diagnostic analysis [on-line]. Available at: <https://mc.bip.gov.pl/rok-2017/analiza-diagnostyczna-intensywnosc-wykorzystania-danych-w-gospodarce-a-jej-rozwoj.html>.
27. European Commission (2018). Digital Single Market: EU negotiators reach a political agreement on free flow of non-personal data [on-line]. Available at: http://europa.eu/rapid/press-release_IP-18-4227_en.htm.
28. Ministry of Digital Affairs (2018). op.cit.
29. Significance of data-driven productivity over studied countries – a ratio of estimated level of data-driven productivity to the estimated level of generic productivity.
30. Ministry of Digital Affairs (2018). op.cit.
31. Puszkiel R. (2018, February 28). Automation in Poland is Gaining Momentum and Presents Opportunities For Swiss SMEs [on-line]. Available at: <https://www.s-ge.com/en/article/news/20181-mem-poland-automation-making-progress>.
32. Ibidem.
33. European Commission (2018). The European Artificial Intelligence landscape [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/european-artificial-intelligence-landscape>.
34. [on-line]. Available at: <https://medium.com/for/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>
35. European Commission (2018, April 28). EU Declaration on Cooperation on Artificial Intelligence [on-line]. Available at: <https://ec.europa.eu/jrc/communities/community/digitranscope-digital-transformation-and-governance-human-society/document/eu-declaration>
36. European Commission (2018). Commission staff working document accompanying the document..., op. cit.
37. European Commission (2018). Artificial intelligence for Europe. Factsheet [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe>.
38. European Commission (2018, April 25). Artificial intelligence: Commission outlines a European approach to boost investment and set ethical guidelines [on-line]. Available at: http://europa.eu/rapid/press-release_IP-18-3362_en.htm.
39. Polish Ministry of Digital Affairs (2018). Visegrad 4 countries' thoughts on the Artificial Intelligence and maximising its benefits ahead of release of the European Commission's Communication on the topic [on-line]. Available at: <https://www.gov.pl/web/cyfryzacja/stanowisko-grupy-wyszehradzkiej-dotyczace-sztucznej-inteligencji>.
40. Kelly E. (2018). EU needs to balance data privacy with data sharing to drive artificial intelligence forward [on-line]. Available at: <https://sciencebusiness.net/news/eu-needs-balance-data-privacy-data-sharing-drive-artificial-intelligence-forward>.
41. European Commission (2018). Statement on artificial intelligence, robotics and autonomous systems. European Group on Ethics in Science and New Technologies [on-line]. Available at: https://ec.europa.eu/research/egs/pdf/egs_ai_statement_2018.pdf.
42. Wendy H. and Peseni J. (2017). Growing the artificial intelligence industry in the UK [on-line]. Available at: <https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk>.
43. European Political Strategy Centre (2018, March 27). The Age of Artificial Intelligence. Towards a European Strategy for Human-Centric Machines [on-line]. Available at: https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategicnote_ai.pdf.
44. UK Parliament (2018). UK can lead the way on ethical AI, says Lords Committee [on-line]. Available at: <https://www.parliament.uk/business/committees/committees-a-z/lords-select/ai-committee/news-parliament-2017/ai-report-published/>.
45. Erdelyi O. and Goldsmith J. (2018). Regulating Artificial Intelligence Proposal for a Global Solution [on-line]. Available at: http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_13.pdf.
46. Wendy H. and Peseni J. (2017). Growing the artificial intelligence industry in the UK, op.cit.
47. World Economic Forum (2016). Top 9 ethical issues in artificial intelligence [on-line]. Available at: <https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/>.
48. European Commission (2018). Statement of the EGE is released. European Group on Ethics of Artificial Intelligence [on-line]. Available at: https://ec.europa.eu/info/news/ethics-artificial-intelligence-statement-egs-released-2018-apr-24_en.
49. European Commission (2018). Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of the Council directive on approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) [on-line]. Available at: <https://ec.europa.eu/docsroom/documents/29233>.
50. Partnership on AI [on-line]. Available at: <https://www.partnershiponai.org/about/>.

51. Wessing T. (2018). Facial recognition technology in the EU: does GDPR spell the end [on-line]. Available at: <https://www.lexology.com/library/detail.aspx?g=104d7d1d-80c4-4674-9286-b3a9ca7ee181>.
52. MarketWatch (2016). Facial Recognition Market Is Expected to Reach \$9.6 Billion, Worldwide, by 2022 [on-line]. Available at: <https://www.marketwatch.com/press-release/facial-recognition-market-is-expected-to-reach-96-billion-worldwide-by-2022-2016-06-29-820323>.
53. Council of Europe (2018). Brief overview of the Council of Europe activities in the field of artificial intelligence [on-line]. Available at: <https://rm.coe.int/leaflet-artificial-intelligence-en/168089e571>.
54. Microsoft (2018). The future computed. Artificial intelligence and its role in society [on-line]. Available at: <https://news.microsoft.com/futurecomputed/>.
55. Microsoft (2018). Facial recognition technology: The need for public regulation and corporate responsibility [on-line]. Available at: <https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility>.
56. Impact (2017). Artificial Intelligence – Poland’s chance in the global race [on-line]. Available at: <https://impactcee.com/2018/06/11/artificial-intelligence-polands-chance-in-the-global-race/>.
57. Ainowinstiute (2018) [on-line]. Available at: <https://ainowinstitute.org/>.
58. Knight W. (2017). Forget Killer Robots—Bias Is the Real AI Danger. MIT Technology review [on-line]. Available at: <https://www.technologyreview.com/s/608986/forget-killer-robotsbias-is-the-real-ai-danger/>.
59. European Commission (2018). Digital Transformation Monitor. USA-China-EU plans for AI: where do we stand? [on-line]. Available at: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf.
60. European Commission (2018). Communication from the Commission. Artificial Intelligence for Europe [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>.
61. Microsoft (2018). Facial recognition technology... op. cit.





3



CYBERSECURITY

Cyberattacks are viewed as a global risk of the highest concern that is going to intensify. The growing dependence on technology as well as an increasing number of interconnected devices and a more pronounced use of artificial intelligence heighten our exposure to cyber threats. On top of that, the ever-increasing sophistication of cyberattacks adds to the complexity of the landscape where interruption of business processes, state and economic espionage, compromise of critical infrastructure, or reputational damage take their toll. Irrespective of the growing awareness, cybersecurity remains an under-resourced risk, given the potential scale and depth of a cyberattack.¹

It is important to ensure that providing cybersecurity should be a starting point for development of other projects within the 3SI. Sectors such as energy, transport and other critical infrastructures, therefore, the areas of the main focus for the 3SI, are prone to cyberattacks.

CASE STUDY – CROATIA



Gas supply is already part of the 3SI, with Croatia playing an important role in the initiative. However, the vulnerability of Croatia's energy sector along with Russia's persistent efforts to penetrate Croatian economy and Croatia's importance on the energy map of Southeast Europe make the country a likely target of cyberattacks. In terms of geopolitics, Croatia is an important bridge between three regions: the Mediterranean, Central Europe and Western Balkans, seeking to become an energy hub through projects like LNG in Krk and IAP-TAP pipelines.

This is a project not only of national interest, but also of particular importance for the 3SI, and on the list of Projects of Common Interest of the EU. The project is supported by the EU and the United States. The new supply route through LNG terminal to import American gas for Croatia and the Eastern European market could jeopardise Russia's supremacy. Croatia, like the rest of the EU, seeks to diversify its energy supply routes in order not to be dependent on one energy supplier. Gas coming through Croatia would not supply just the local market, but also many countries in the region, for example Ukraine. The other supply route could be the Adriatic Ionian Pipeline as a connection to the Trans Adriatic Pipeline to bring Caspian Sea Azeri gas along the Southern Gas Corridor to Europe. Currently, Croatia imports around 1 bcm of gas, with the remainder of 2 bcm being produced locally. Imports of Croatian gas could increase to 5 bcm if new

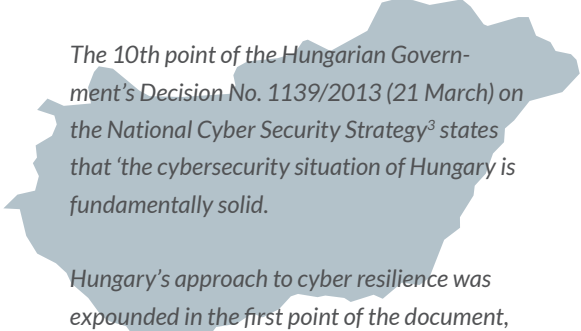
markets in Eastern Europe were accessed via the LNG terminal in the Krk island and IAP.

CYBERSECURITY READINESS IN THE 3S

According to the National Cyber Security Index, out of all countries in the 3S region, only Estonia (82), Slovakia (81) and Lithuania (80) fall into the category of the most advanced countries worldwide (1.).²

The Czech Republic and Latvia position themselves close to the most developed group, with the scores of 74 and 72 respectively. At the bottom of the ranking are Romania (55), Bulgaria (52) and Slovenia (44). In general terms, the preparedness of the 3S region as compared to the EU28 is rather moderate due to their historical legacy and different levels of innovation, which was presented in detail in the previous chapters.

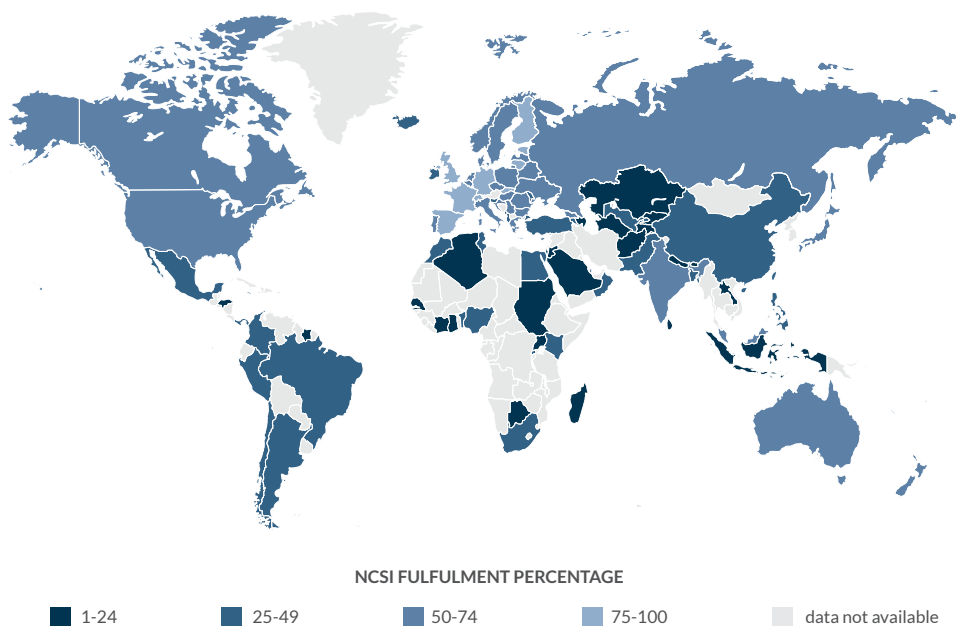
CASE STUDY – HUNGARY



The 10th point of the Hungarian Government's Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy³ states that 'the cybersecurity situation of Hungary is fundamentally solid.

Hungary's approach to cyber resilience was expounded in the first point of the document,

1. NCSI WORLD REACH



Source: EGA, 2018, National Cyber Security Index 2018.

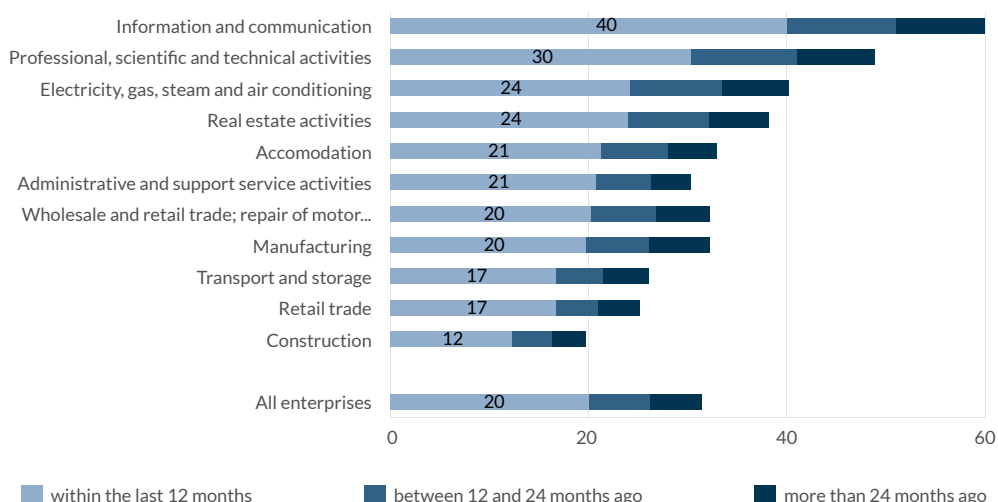
saying it is of ‘fundamental’ national interest to secure the Hungarian cyberspace.

However, the 2013 foundational document defined only the basics, missing out on detailed descriptions, explanations, and steps. Overall, the whole strategy is a description of the present state of play. This strategy belongs to the first generation of cyber strategies. The 2.0 cyber strategy is expected to be published in autumn 2018 and focus on the present day threats and challenges, fast reactions, and outcomes with a well-functioning hierarchy of decision-makers and responsive units.

The EU as a whole is not adequately prepared to face the mounting threats of cyberattacks, which stems from the fragmentation of the know-how and resources across the European Union. Only two Member States score the highest in the ITU Global Cybersecurity Index, while in a large majority of them, cybersecurity readiness ranges from average to weak.⁴ A varied level of preparedness of different sectors only makes the situation more complex.

The highest percentage of companies having a cybersecurity policy in place is observed among those conducting information and communication activities (60 %) as well as professional, scientific and technical activities (49 %) (2.). Conversely, the lowest percentage of companies with a cybersecurity policy can be found in construction (20 %), real estate (25 %), and transportation and storage (26 %) sectors.⁵ It must be noted, however, that the statistics come from a survey that was carried out in 2015. The next edition, which is expected in December 2019, should reflect progress made as a result of the implementation/transposition of the NIS directive into national legislation concerning critical sectors in particular.

2. ENTERPRISES HAVING A FORMALLY DEFINED ICT SECURITY POLICY, BY ECONOMIC ACTIVITY, 2015 (% ENTERPRISES)



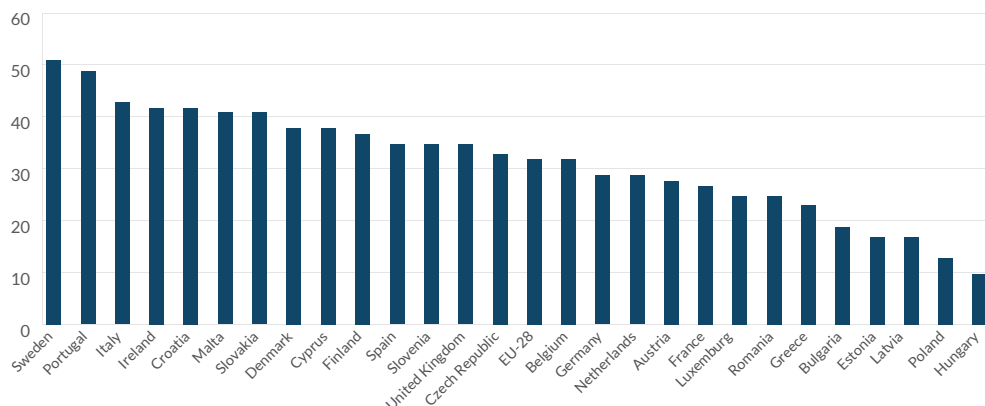
Source: Eurostat, 2015, ICT security in enterprises.

The analysis of enterprise cybersecurity in the EU, particularly in the 3S region, shows plenty of room for improvement. A staggering 69 % of companies have either none or limited understanding of their potential exposure to cybersecurity challenges. Only 32 % of businesses have a formally defined security policy.

In the case of large businesses, almost three-quarters of them have such a policy in place. In the case of SMEs, it is only one-third (31 %).⁶ Overall, contrary to what can be observed in the general DESI, companies in Croatia (42 %) and Slovakia (41 %) have a much higher level of

cybersecurity awareness than the EU28 (3.). With that said, Bulgaria (19 %), Estonia (17 %), Latvia (17 %), Poland (13 %) and Hungary (10 %) are in the lower echelons of the scores in the EU.

3. ECONOMIC ACTIVITY – ALL ENTERPRISES



Source: Eurostat, 2015, ICT security in enterprises.

CYBERSECURITY MARKET IN THE 3S REGION

As repeatedly voiced in debates on secure digital infrastructure, cybersecurity is not only about cost. With proactive and properly crafted policies, the cybersecurity sector can also generate revenue for the countries and the region. A strong and innovative cybersecurity sector not only helps to protect the public interest, but it can also be an important export commodity and an important driver of economic growth. This sector may especially become a smart specialisation for regions abundant in ICT talents – like the 3S region.

According to various reports, the worldwide spending on cybersecurity products and services has already reached more than USD 120 billion. In the last decade, the market grew by 8–10 % annually, with predictions for 2020 indicating a further steady growth amounting to USD 230 billion of the global market value at the end of that period. A research study conducted by CYBERSEC HUB in 2018 involving a set of selected 3S countries shows that the region has

tapped into that growth. The 3S already have growth rates exceeding the EU average with regard to the cybersecurity market, resulting, among others, from the growing security threats and new national and EU regulations. Multi-directional development of the IT security industry facilitates finding market niches and specialisations for the countries in the region, such as cybersecurity of industrial control systems, 'security by design' support products for software developers, Cyber Range Platforms – online training programmes for security specialists and Computer Security Incident Response services.

4. NUMBER OF ICT COMPANIES IN SELECTED 3S COUNTRIES IN 2010 AND 2015

	2010	2015	Change %	2010	2015	Change %
Poland	52 566	81 357	55 %	37 390	62 730	68 %
Bulgaria	7 279	10 268	41 %	4 763	7 645	61 %
Croatia	5 111	5 878	15 %	3 586	4 388	22 %
Czech Republic	32 315	35 182	9 %	24 506	27 525	12 %
Estonia	2 266	3 897	72 %	1 722	3 198	86 %
Lithuania	2 532	5 758	127 %	1 250	4 193	235 %
Latvia	3 152	6 133	95 %	1 932	4 442	130 %
Romania	17 157	20 564	20 %	10 486	13 763	31 %
Slovakia	9 847	16 231	65 %	7 319	14 126	93 %
Hungary	28 320	31 157	10 %	23 665	26 687	13 %
Total	160 545	216 425	35 %	116 619	168 697	45 %

Source: World Bank, 2018, GDP growth (annual %).

The region may be also particularly attractive for cybersecurity exporters – in 2016, in nine 3S countries⁷ imports amounted to almost EUR 2.2 billion (about 20 % of total EU imports), which means high demand for products and services cannot be satisfied only by domestic companies. Most of this import came from countries outside the EU; the EC calculates that the import volumes of IT security products in 2021 for those 9 3S region countries will raise up to EUR 3.3 billion (5.). Current low saturation of those markets by ICT products and services, combined with rapidly accelerating digitisation, makes them especially crucial in terms of long-term, strategic investments. Vendors who will take active part in the digitisation of the region in the coming years, will secure their lasting export presence on those markets.

4. NUMBER OF ICT COMPANIES IN SELECTED 35 COUNTRIES IN 2010 AND 2015

	2017	2018	2019	2020	2021	2017	2018	2019	2020	2021
Bulgaria	245	276	312	353	399	44	49	56	63	71
Croatia	29	33	37	42	48	6	7	7	8	9
Czech Republic	440	497	561	634	717	71	80	90	102	116
Estonia	113	127	144	163	184	26	29	33	37	42
Lithuania	97	110	124	140	159	26	29	33	38	43
Latvia	146	165	187	211	239	30	34	39	44	49
Romania	407	460	520	587	664	91	103	117	132	149
Slovakia	47	53	59	67	76	9	10	12	13	15
Hungary	490	553	625	707	799	89	101	114	129	146
Total	2013	2 275	2 571	2 905	3 283	392	443	501	566	639

Source: Own calculation based on Impact assessment accompanying the document: Proposal for a regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency, 2017.

The EU is now establishing regulatory and policy measures to support the development of European cybersecurity products.

EU APPROACH TO CYBERSECURITY

In recent years, the EC has intensified its efforts in a quest to enhance cyber resilience of the EU and tackle the fragmentation of capabilities between Member States and their economic sectors. The year 2016, when the NIS directive⁸ was adopted across the Union, marked a change in the European mind-set.

The NIS directive introduced cross-sectoral legislation to provide for a minimal level of protection in the critical sectors of the economy: energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution, and digital infrastructure. The NIS directive set a new standard for enhancing cybersecurity in the EU. In order to support its implementation that was carried out, among others, by the Cooperation Group and the CSIRT network, the EC issued an additional guidance to provide for an effective and harmonised approach.⁹ Member States were required to transpose the NIS directive by 9 May 2018. Howe-

ver, the assessment performed by the EC three months after the due date showed that only 11 Members States of the EU had complied; in the 3S region, these were the Czech Republic, Estonia, Slovakia and Slovenia.¹⁰

Subsequently, in 2017, the cybersecurity package was published. This wide-ranging measure attempts to improve the EU's capabilities in three key fields: building its resilience to cyberattacks and stepping up the EU's cybersecurity capacity; creating an effective criminal justice response; and strengthening global stability through international cooperation. In addition, the EC granted a permanent mandate for ENISA, transforming it into an EU Cybersecurity Agency, and set up a voluntary EU certification framework for ICT products and services.¹¹

As a next step, in September 2018, the EC proposed to strengthen cybersecurity capacity in the EU by means of a network of European Cybersecurity and Competence Centres.¹² According to a draft regulation, such a network of competence centres would be coordinated by a newly created European Cybersecurity Industrial, Technology and Research Competence Centre. In a long run, a large, open and diverse group of actors active in the field is planned to be established. Additionally, in September 2018, ENISA published a tool to evaluate national cybersecurity strategies to help Member States to assess their

priorities and reflect on the priorities of the next strategy.

In an attempt to set a long-term strategy for the development of digital policy in the EU, the EC has recently unveiled a draft version of the Digital Europe programme for 2021-2027.¹³ The programme builds on a set of measures previously outlined in the NIS directive, and focuses on the following areas to aid the implementation of the directive: support for the procurement of advanced cybersecurity equipment, tools and data infrastructures; the leveraging of Europe's accumulated knowledge, capacity and skills; deployment of the latest cybersecurity solutions; and reinforcement of capabilities within both the public and the private sector.

Given the fragmentation of approaches within the EU, Member States face an uneasy task to implement this wide-ranging legislation. In the overall discussion, the National Institute for Standards and Technology framework emerges as one of the standardised tools for the implementation of the NIS directive. This cybersecurity framework has been used by about 30 % of enterprises in the U.S. now and has been made binding for the U.S. government following 2017 executive order¹⁴ on strengthening the cybersecurity of federal networks and the critical infrastructure. In April 2018, the NIST released an updated version of the Framework 1.1 which modified the sections related to authentication

and identity, self-assessment of cybersecurity risks, management of cybersecurity within the supply chain and vulnerability disclosures.¹⁵

Competent national bodies often consider the NIST model as a tool to implement the requirements of the NIS Directive. Italy serves as an example in this respect. The National Cybersecurity Centre of the UK also followed suit and used the NIST framework as guidance for the implementation of the NIS directive. It referred to good practices and standards such as the ISO/IEC 27001/27002 standard series and the IEC 62443 series for OT.¹⁶ Recently, the U.S. government has announced plans to draw on the NIST framework in order to establish its equivalent to deal with privacy and assist companies in protecting personal data.

TRANSATLANTIC CYBERSECURITY COOPERATION

There is significant potential in transatlantic cybersecurity cooperation with the 3SI, and the D3SI format seems

particularly well suited for the advancement of this partnership.

The new National Cyber Strategy of the United States¹⁷ highlights the importance of cooperation with U.S. allies to preserve peace and security in cyberspace. It aims to build an international Cyber Deterrence Initiative, a coalition of responsible and like-minded partners: states, private companies, academia or the civil society in order to develop common strategies to combat malicious cyber threats.

A stronger American bilateral and regional engagement in Europe, including the 3S region is necessary. The eastern flank of NATO is usually on the frontline of state-orchestrated cyberattacks and sinister activity of cybercriminals. Following the attack on Estonia in 2007, the 3S countries are facing significant geopolitical tensions due to emerging security challenges, such as the hybrid and cyber threats. Even though this cooperation is increased at the operational level, it needs enhanced political incentives at the strategic level, and these so far have been largely unsatisfactory. A stronger engagement of the U.S., as well as the EU and NATO, is crucial to reinforce the strategic cooperation in the region and increase its resilience against cyberthreats. This partnership should consist of multifaceted tools, including the financial support of capacity building efforts, the creation of effective information sharing platforms,

public-private partnership mechanisms and the exchange of best practices.

There would be several significant benefits of the increased support of the EU, NATO and the U.S. The 3S region may be instrumental in enhancing NATO's and the EU's overall efforts to strengthen their defence capabilities against cyberattacks. Moreover, the region possesses a unique blend of experience that can be shared with the U.S. and other partners, thus contributing to building enhanced cybersecurity governance frameworks, response mechanisms and the norms of responsible behaviour of states in cyberspace.

ATTACKS ON ELECTIONS AND INFORMATION WARFARE

The velocity of change in technology and increasing attempts to misuse new advancements contribute to the complexity of regulatory approaches. Malicious activities of significant impact involve attacks targeting elections and electoral campaigns. They include direct interference with voting systems or attempts to influence voters' behaviour by means of hacks and leaks, fake news or targeted messaging.¹⁸ With regard to the security of voting systems, under a joint effort of Estonia and the Czech Republic, the NIS Cooperation Group came up with a set of guidelines on how to make the process of elections

resilient to a cyberattack. In the aftermath of electoral incidents worldwide and in the run-up to elections to the European Parliament, a number of initiatives surfaced at the EU level.¹⁹

CASE STUDY – SLOVAKIA

The latest edition of GLOBSEC Trends²⁰ indicates that 53 % of Slovaks believe that secret groups control world affairs and aim to establish a totalitarian world order. Only 27 % think that Russia tried to influence the outcome of several elections in Europe, making Slovakia the least aware of such attempts in CEE. Finally, 68 % of Slovaks aged 18-24 have encountered disinformation on social media. However, only 9 % of all Slovak social media users who come across inappropriate content actually report it. This illustrates that people are exposed to fake news and propaganda, which is likely to affect their opinions.

In July 2018, a code of practice on disinformation was published and its effectiveness will be assessed by December 2018.²¹ In September 2018, in a concerted effort, the industry submitted the code of practice which forms a set of self-regulatory standards to fight disinformation worldwide. Among others, the measures include commitment to transparency in political advertising, closure of fake accounts and demonetisation of the purveyors of disinformation. The code comes ahead of the European elections in spring 2019 and at-

tempts to make the campaign transparent and reliable.²² As a parallel measure, the EC issued a recommendation on election co-operation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns, guidance on the application of the General Data Protection Regulation and a legislative amendment, which tightens the rules applicable to funding of political parties.²³

CASE STUDY – SLOVAKIA

Russia's hybrid war includes disinformation campaigns in the CEE region, posing a significant security problem in Slovakia. The campaigns seemed to have had a negative impact on Slovakia's public opinion towards the EU as the public support for the EU decreased from 68 % in 2010 to 52 % in 2016.²⁴ In their 2017 annual report, the Slovak Information Service (SIS) highlighted their focus on selected hybrid warfare used by state actors. Under the sponsorship of the Office of the Security Council of the Slovak Republic, SIS also helped develop the strategy of the Slovak Republic's on countering hybrid threats.²⁵ One of their main tasks is to monitor Russian propaganda disseminated in Slovakia and other European countries. According to the Disinformation Resilience Index, the updated official documents 'Security Strategy of the Slovak Republic 2017' and 'Defence Strategy of the Slovak Republic 2017' are much better at addressing the issue, providing broad-spectrum countermeasures.²⁶ The Security Strategy classified disinformation

campaigns as a subtype of hybrid threats and suggested developing strategies to strengthen resilience against hybrid threats and increase strategic communications capacity. Lastly, in July 2017, the Slovak Ministry of Foreign and European Affairs established the Strategic Communication Unit.

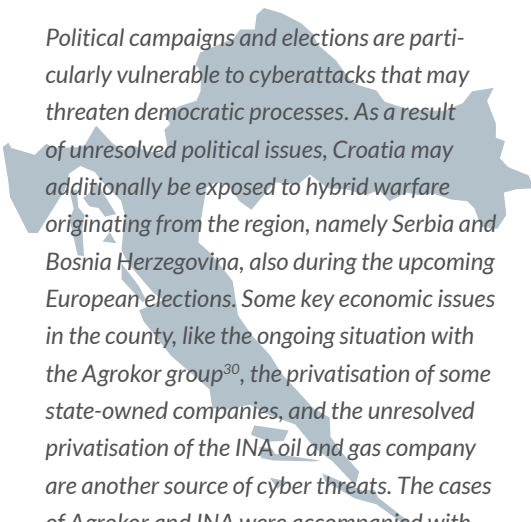
Since cyberattacks pose a significant threat to elections, campaigns or political parties, undermining trust into public institutions, the EC has proposed creating a network of cybersecurity competence centres located in Member States which, in cooperation with the new European competence centre, will better coordinate the activities against such attacks within the EU. The EC suggests Member States adopt technical and organisational measures to manage the risks related to the information systems employed for the organisation of elections.²⁷

CASE STUDY – ROMANIA

Information warfare is viewed as a growing issue and a very serious threat to national security. The Romanian law enforcement and intelligence agencies tackle the information warfare as a strategic threat. This approach focuses on building preventive mechanisms, such as better anticipation and intelligence gathering, while achieving an integrated, balanced, flexible and agile response capacity.²⁸ According to the National Defence Strategy, disinformation campaigns and

state-sponsored cyberattacks are threats that may obstruct Romania's strategic projects and objectives as well as negatively affect its decision-making processes.²⁹ In that sense, elections and decision-making as pillars of the democratic processes are commonly recognised as being most vulnerable to information warfare and cyber threats.

CASE STUDY – CROATIA



Political campaigns and elections are particularly vulnerable to cyberattacks that may threaten democratic processes. As a result of unresolved political issues, Croatia may additionally be exposed to hybrid warfare originating from the region, namely Serbia and Bosnia Herzegovina, also during the upcoming European elections. Some key economic issues in the country, like the ongoing situation with the Agrokor group³⁰, the privatisation of some state-owned companies, and the unresolved privatisation of the INA oil and gas company are another source of cyber threats. The cases of Agrokor and INA were accompanied with corruption scandals, disinformation campaigns, and involvement of foreign companies that used different methods to gain control over Croatia's key industries.

The common experience and high exposure to hybrid threats and disinformation within the 3S region should

result in closer security cooperation to counter information warfare at the EU level and between the 3S countries.

Together with the East StratCom Task Force and the Strategic Communications Centre of Excellence, the 3S countries should engage in combating disinformation campaigns by creating a platform to share experiences of their fight against disinformation and establishing a fund to support the development of expertise and analyses.³¹

INTERNATIONAL PROSPECTS FOR A COMMON AGREEMENT

Over the past years, state-led activities have created new capabilities that impact societies and economies. However, agreeing on international instruments to tackle cross-border threats proves challenging. Cybersecurity is discussed on multiple forums, for examples G7, G20, Shanghai Cooperation Organisation, the European Union, OSCE, FIRST, NATO, UNODC, UNIDIR, but only a few are doing this in a truly multi-stakeholder manner i.e. Global Conferences on Cyberspace (the London Process), Internet Governance Forum, Global Forum on Cyber Expertise or Global Commission for the Stability of Cyberspace.³²

In 2015, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security declared that international law also applies to cyberspace. It agreed on norms, rules and principles of responsible behaviour of states as well as confidence-building measures, international cooperation and capacity building saying that *existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms*.³³

The UN GGE has always been a forum for international discussion on the rules of behaviour for states in cyberspace. Two years later, despite making substantial progress, the UN GGE failed to arrive at a consensus on the outcome report. What proved to be a bone of contention was the manner in which international law (humanitarian law, law governing states' right to self-defence, law of state responsibility, including countermeasures) applies to the use of ICT by states.³⁴ The failure to reach an agreement on international law and its application left many issues unresolved, including norms, confidence-building measures and capacity building.

All V4 countries and most of the 3S countries are adopting European requirements for cybersecurity; they also participate in NATO's initiatives. Since 2017, Belgium, the Czech Republic, Estonia, France, Germany,

Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the United States have been sponsoring nations of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The Centre published the Tallinn Manual and its revised version on the application of international law to cyber warfare. The whole region is, however, not part of the UN GGE.

In the meantime, the EU continues to uphold that existing international law applies to cyberspace and that respecting international law is key to maintaining peace and stability. In this respect, the EU is willing to continue working on developing further, voluntary, non-binding norms, rules and principles drawing upon the UN GGE's 2010, 2013 and 2015 reports, both within the UN and other international forums.³⁵ In parallel, there are attempts to fill the vacuum created as a result of the recent failed proceeding of the UN GGE. A notion of a Digital Geneva Convention first emerged in February 2017. In a joint initiative spearheaded by Microsoft and Facebook, more than 30 companies introduced a set of principles to help governments fight against cyberattacks aimed at civilians and enterprises. Nevertheless, its lengthy list of signatories did not include some digital moguls like Google, Amazon, Apple, IBM or McAfee.³⁶ Despite receiving praise for applying a multi-stakeholder approach, the Digital Geneva Convention raised concerns of individual governments

with regard to the idea of creating the convention as such.³⁷

Given that the negotiations of the NIS directive lasted for seven presidencies of the EU Council, one should not expect that any international instrument will not encounter hurdles in the process that will not be easy and will take time. Some argue that the creation of such an agreement is impossible due to divergent interests around regulations, different expectations and concerns regarding cybersecurity.³⁸ Irrespective of the outcome, what counts is that the implementation of the above-mentioned legislative instruments will make the EU stronger and less fragmented, both politically and economically.

The above-mentioned lack of consensus within the UN GGE prompted the international community to seek an alternative space for discussion about the application of international law to cyber activities and the development of norms of responsible behaviour. During this process, it is necessary to enter into a dialogue on priorities with other partners, including non-state actors. Given its strong potential for influence, the 3S countries should now actively engage in that discussion, which can give it a new momentum. The D3SI is a project that aims to develop cybersecurity policies and strategic concepts to help build stability and increase trust in this domain. The place that regularly hosts the most prominent experts and policy-makers

in the field is Krakow, a city located in the heart of the region and a hometown of the annual European Cybersecurity Forum – CYBERSEC.³⁹

RECOMMENDATIONS FOR THE 3S COUNTRIES:

1. In most of the 3S countries, the regional cooperation in the digital domain is scarcely mentioned in the political discourse at a national level. The areas of focus are capability building and intelligence sharing, but its **enhancement within bilateral and multilateral diplomatic relations** is missed out. The NIS Directive, to some extent, can serve as an enabler in this respect.
2. In accordance with the Proposal for a European Cybersecurity Competence Network and Centre of the EC, the **collaboration of competence centres in the 3S countries** should be further pursued. Their joint capacities shall serve to respond to the needs of the public sector and the industry.
3. International/regional cooperation involving policy consensus, mutual technical assistance, sharing best lessons learned and even intelligence is not sufficient. Therefore, countering cyber threats that jeopardise democratic processes requires **states and relevant private-sector stakeholders**

to eventually engage in active defence to deny the posture of their enemies.

4. Public-private cooperation, including **capacity building, research and response coordination**, is critical. Increasing the use of **encryption, cyber exercises, establishing notification requirements, and enabling private entities and academia to assume a role in documenting and countering information warfare** are required to safeguard vulnerable mechanisms and processes against any hostile challenges.
5. **Increasing the number of cross-border exercises will contribute to better regional cooperation.** The Central European Cyber Security Platform,⁴⁰ which comprises the V4 Group and Austria, is an example of an entity that coordinates cross-border exercises organised by national cyber security centres.
6. **Enhanced preparedness, response (confinement) and rapid recover capacity at technical, economic, administrative, and social levels** are key elements to increase cyber resilience. The first step (1) is to secure the commitment of political stakeholders who shall **speed up decision-making**. Therefore, the second step (2) is to set up a policy model (strategy) and put in place a (continuity) plan for cyber resilience. The third step (3) is to ensure the deployment of the strategy and the plan into both national and local policies, and assign roles. The logic behind is to decentralise resilience building as much as possible.
7. There are some pillars and lines of action that normally shall be considered for increasing cyber resilience, namely infrastructure resilience, mandatory R&D, human skills for public services, public diplomacy, awareness and cooperation. The latter should be clearly defined to 'mitigate stakeholders' reluctance and to avoid ambiguity' when it comes to governments' duty to provide assistance.
8. It is important to have **highly qualified personnel** for screening, evaluation and compliance; therefore, high quality education is a must. The civil society must also be educated as **cybersecurity starts with its members**. Cybersecurity has to be part of the basic education.
9. There are sectors which are best prepared (i.e. financial and telecommunications) and worst prepared for cybersecurity challenges (i.e. health sector and local administration). **Sectoral CERTs/ CSIRTs and sector-specific cybersecurity readiness indicators** shall be introduced. **Cross-sectoral cooperation** is also needed to share best practices between the most successful actors and those who cope with the threats less effectively.

10. A stronger American bilateral and regional engagement in CEE with respect to cyber capacity building is necessary. The potential for synergy among the D3SI (and through that, the Three Seas Initiative), **the U.S. National Cyber Strategy** and the **Cyber Deterrence Initiative** is significant and should not be left unnoticed.
11. In the 3S region, it is possible to establish a **cybersecurity hub** that merges both international and regional resources and attracts the private and the public sector as well as academics to create innovative products and solutions for rapidly growing cyberthreats, mainly for the European market.
12. **The 3S region, the EU and the U.S. need to enhance their cybersecurity cooperation** by engaging with specialised agencies and task forces, such as ENISA, Europol, Interpol, future structures of the PESCO and the European Defence Fund, to jointly advance efforts to develop a comprehensive and transparent international framework for minimum standards for cybersecurity policies.⁴¹





SOURCES:

1. World Economic Forum (2018, January 17). Our exposure to cyberattacks is growing and we need to become cyber risk ready [on-line]. Available at: <https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/>
2. On a methodological note, the NCSI takes into account measures implemented by the central government (legislation in force, established units – organisations and departments, cooperation formats and outcomes/products).
3. Full text of the legislation can be read here: http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845
4. European Commission (2018). Proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period of 2021-2027. [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN>
5. Eurostat (2015). ICT security in enterprises. [on-line]. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises
6. Eurostat (2017). Digital economy & society in the EU. [on-line]. Available at: <https://ec.europa.eu/eurostat/cache/infographs/ict/images/pdf/pdf-digital-eurostat-2017.pdf>
7. Except Austria and Slovenia.
8. European Commission (2018). 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 [on-line]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG
9. European Commission (2018). Communication from the Commission to the European Parliament and the Council Making the most of the NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505297631636&uri=COM:2017:476:FIN>
10. European Commission (2018). July infringement package: key decisions. [on-line]. Available at: http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm
11. European Parliament (2017). Cybersecurity package. [on-line]. Available at: <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-cyber-security-package>
12. European Commission (2018). Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. [on-line]. Available at: <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research>
13. European Commission (2018). Proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period of 2021-2027 [on-line]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN>
14. White House (2017). Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [on-line]. Available at: <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>
15. NIST (2018). NIST Releases Version 1.1 of its Popular Cybersecurity Framework [on-line]. Available at: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework>
16. National Cybersecurity Centre (2018). The NIS Guidance Collection [on-line]. Available at: <https://www.ncsc.gov.uk/guidance/nis-guidance-collection>
17. White House (2018). National Cyber Strategy of the United States of America [on-line]. Available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
18. King J. (2018). Democracy is under threat from the malicious use of technology. The EU is fighting back [on-line]. Available at: <https://www.theguardian.com/commentisfree/2018/jul/28/democracy-threatened-malicious-technology-eu-fighting-back>
19. European Commission (2018). Latest NIS Cooperation Group's guidelines for implementing the NIS Directive and addressing wider cybersecurity policy issues [on-line]. Available at: <https://ec.europa.eu/digital-single-market/>

- en/news/latest-nis-cooperation-groups-guidelines-implementing-nis-directive-and-addressing-wider
20. GLOBSEC Policy Institute (2018). GLOBSEC Trends 2018 Central Europe: One Region, Different Perspectives [on-line]. Available at: <https://www.globsec.org/wp-content/uploads/2018/05/GLOBSEC-Trends-2018.pdf>
 21. European Commission (2018). Tackling online disinformation: Commission proposes an EU-wide Code of Practice [on-line]. Available at: http://europa.eu/rapid/press-release_IP-18-3370_en.htm
 22. European Commission (2018). Statement by Commissioner Gabriel on the Code of Practice on Online Disinformation [on-line]. Available at: http://europa.eu/rapid/press-release_STATEMENT-18-5914_en.htm
 23. European Commission (2018). Commission recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament [on-line]. Available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf
 24. MOSR (2016). White paper on the Defence of the Slovak Republic. p. 28 [on-line]. Available at: <https://www.mosr.sk/white-paper-on-defence-of-the-slovak-republic-2016/>
 25. SIS website (n/d) [on-line]. Available at: <http://www.sis.gov.sk/about-us/nsac.html>
 26. Ukrainian Prism (2018, July 31). Disinformation Resilience in Central and Eastern Europe [on-line]. Available at: <http://prismua.org/en/english-ukraine-disinformation-resilience-index/>
 27. European Commission (2018). State of the Union 2018. Free and fair European elections [on-line]. Available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf
 28. Administrația Prezidențială. (2015). Strategia națională de apărare a țării pentru perioada 2015-2019 [on-line]. Available at: http://www.presidency.ro/files/userfiles/Strategia_Nationala_de_Aparare_a_Tarii_1.pdf.
 29. Ibidem.
 30. Agrokor is a food producer, the biggest retailer in the country, and before 2017, the biggest privately owned company in the region, employing around 60 000 staff. Due to a large debt crisis that became evident in early January 2017, the Croatian government has imposed an administration run by the state which is still running the company. In July 2018, a deal to settle Agrokor's debt was approved by its creditors. The deal will enable Agrokor's creditors and bondholders to become its shareholders, thus effectively replacing the company's owner. Russian banks Sberbank and VTB will hold a 48 % stake.
 31. The Kosciuszko Institute Policy Brief (2018). The Digital 3 Seas Initiative: A Call for a Cyber Upgrade of Regional Cooperation [on-line]. Available at: <https://ik.org.pl/en/publications/white-paper-the-digital-3-seas-initiative-a-call-for-a-cyber-upgrade-of-regional-cooperation/>
 32. Neutze, J. (2017). The need for a Digital Geneva Convention in times of digital cyber(in)security [on-line]. Available at: <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=36025&no=4>
 33. UN (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [on-line]. Available at: <http://undocs.org/A/70/174>
 34. US Department of State (2017). Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security [on-line]. Available at: <https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm>
 35. Council of the EU (2018). Council conclusions on malicious cyberattacks [on-line]. Available at: <http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf>
 36. Sanger, D. (2018). Tech Firms Sign 'Digital Geneva Accord' Not to Aid Governments in Cyberwar [on-line]. Available at: <https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html>
 37. Ermert, M. (2018). A Digital Geneva Convention: Nobel Prize-Worthy Or Dangerous? [on-line]. Available at: <http://www.ip-watch.org/2017/12/19/digital-geneva-convention-nobel-prize-worthy-dangerous/>
 38. Holdorf, P. (2015). Prospects for an international cybersecurity regime. INSS Strategic Paper [on-line]. Available at: https://www.usafa.edu/app/uploads/Holdorf_Prospects_for_an_International_Cybersecurity_Regime9July2015.pdf
 39. The Kosciuszko Institute Policy Brief (2018). The Digital 3 Seas Initiative: A Call for a Cyber Upgrade of Regional Cooperation. op. cit.
 40. The CECSP was established in 2013 following the initiative of the Czech Republic and Austria. The aim of the CECSP can be summarised in the following way: 'through joint cyber security exercises, the enhancement of technical solutions and special training, the competent organisations of participating countries may elevate cyber security cooperation to an operative level in future. All this will lay the groundwork for shared future tasks in the fight against global-scale virus and hacker attacks.'
 41. European Parliament (2018). Report on the state of EU-US relations [on-line]. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP/TEXT+REPORT+A8-2018-0251+O+DOC+XML+V0//EN>.





5G

While 4G was designed to improve capacity, user data rates, spectrum usage and latency with respect to 3G, 5G is not only an evolution of mobile broadband. It will be a key enabler of the future digital world, the next generation of ultra-high broadband infrastructure that will support the transformation of processes in all economic sectors and the growing consumer market demand.¹

5G is going to bring new service capabilities for consumers and for new industrial stakeholders (e.g. vertical industries, novel forms of service providers or infrastructure owners and providers). Firstly, it will ensure user experience continuity in challenging situations. To give an example, in the best-case scenario, HD video or teleworking will be available anywhere, regardless of the user's location (be it a dense area like a city centre, a village, a high speed train or an airplane). 5G systems will provide access anywhere and will select transparently for the user the best performing 5G connection among heterogeneous technologies like Wi-Fi, 4G and new radio interfaces.

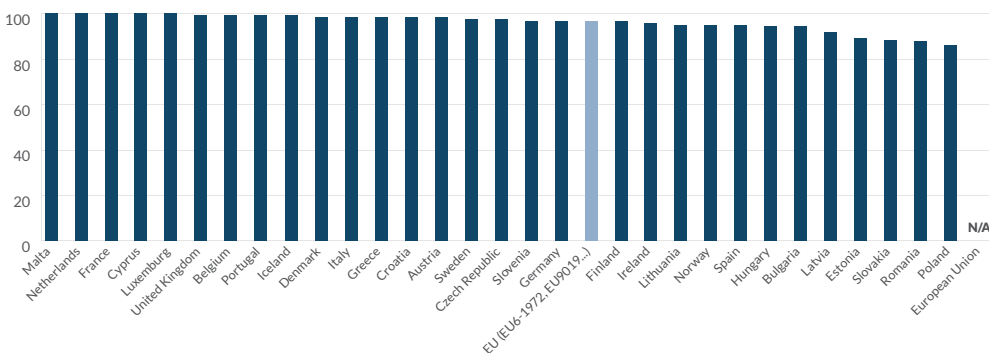
In addition, 5G will be a key enabler for the IoT by providing the platform to connect a massive number of objects to the Internet. Sensors and actuators will spread everywhere.

The empowering 5G is a kind of nucleus for the idea of linking the 3S region by the so-called 3 Seas Digital Highway. It would bridge the gaps in the communication infrastructure by implementing the 5G technology, above all, together with fibre optics, data islands, which would eventually complement energy and transport infrastructures built as part of the 3SI projects. The 3SDH would allow for better and more secure data transfer from the north to the south of the region.

BROADBAND COVERAGE IN THE 3S

First of all, a general image of the current state of play concerning the broadband coverage in the 3S region should be provided. The Broadband Coverage in Europe study is designed to monitor the progress of EU Member States towards their specific broadband coverage objectives.² The data presented below (1.) reflects the situation at the end of June 2017 compared to the situation at the end of June 2016.

1. OVERALL FIXED BROADBAND COVERAGE BY COUNTRY, 2017



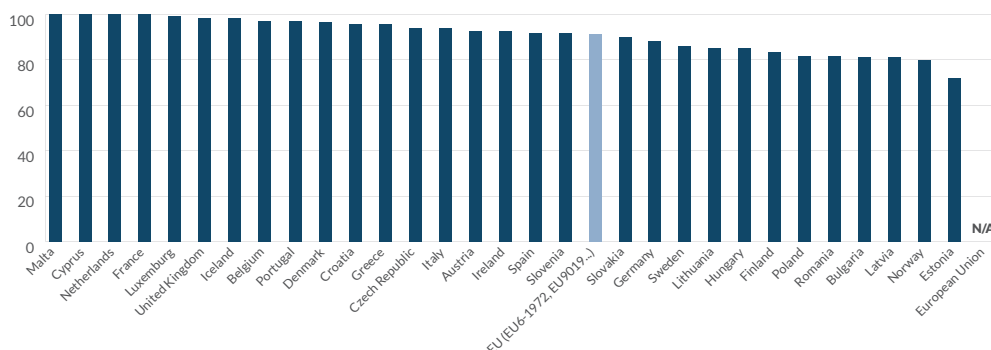
Source: European Commission, 2018, Broadband Coverage in Europe.

Out of the 31 study countries, 26 countries registered fixed broadband coverage of above 95.0 %, while 18 countries had fixed broadband coverage above the EU28 average (97.5 %). Several European countries recorded complete, or near complete, fixed broadband coverage including Malta, the Netherlands, France, Cyprus, Luxembourg and the UK. On the other side

of the classification, the majority of the 3S countries are at its very end. Only Croatia, Austria, the Czech Republic and Slovenia are above the EU average. Four countries (Estonia, Slovakia, Romania and Poland) reported coverage below 90 % in mid-2017. These countries face fixed broadband coverage challenges due to their sparsely populated and underserved rural areas.

Rural fixed coverage in most study countries is lower than national fixed coverage (2.). By mid-2017, rural fixed broadband coverage reached 92.4 % of rural households compared to national coverage of 97.4 %. However, the gap between total fixed coverage and rural fixed coverage continues to reduce. In mid-2017, the gap closed to 5.0 percentage points, compared with 5.3 percentage points in mid-2016.

2. OVERALL FIXED BROADBAND COVERAGE BY COUNTRY, RURAL AREAS, 2017



Source: European Commission, 2018, *Broadband Coverage in Europe*.

18 study countries reported rural fixed broadband coverage above the EU average (92.4 %). Above them are still only Croatia, the Czech Republic, Austria and Slovenia as representatives of the 3S region.

CASE STUDY – ROMANIA

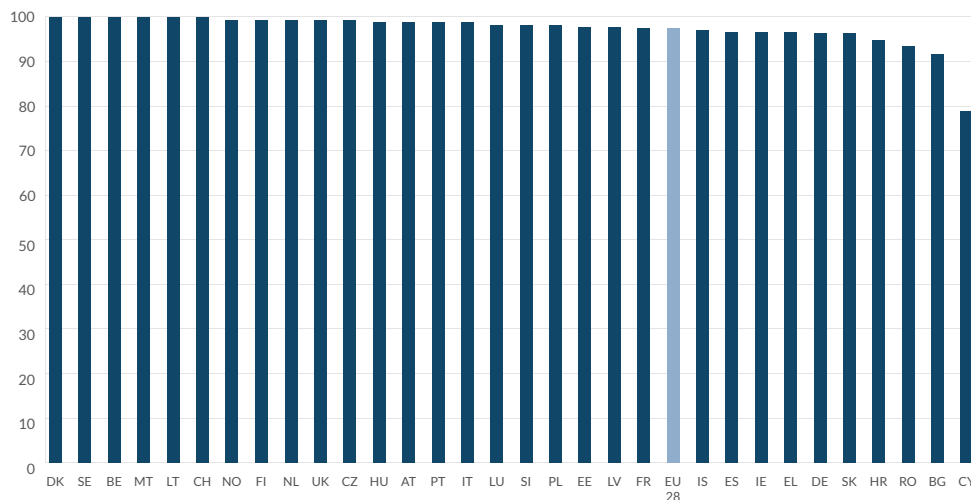
A public bidding for 5G frequencies is set to be organised no later than December 2019. The National Authority for Management and Regulation in Communications (ANCOM)

announced that the documentation concerning the bidding will be available no later than July 2019. ANCOM has adopted a plan and a timetable concerning the allocation of the 470-790 MHz spectrum and the associated regulatory framework in the form of a Natio-

nal Roadmap for the Allocation and Future Use of the 470-790 MHz band in June 2018.³ The 700 MHz band is not available at the moment for mobile use as the band is assigned to digital terrestrial television services. The assignment of the 790 MHz band for mobile services is expected by the end of 2018, when the legal framework concerning the use of the radio spectrum available in the 700 MHz, 800 MHz, 1500 MHz, 2600 MHz, 3400-3600 MHz and 26 GHz frequency bands will be ready. At the moment bilateral coordination negotiations concerning 5G are being initiated with neighbouring countries. There are no official technical trials yet. In July 2018, Orange Romania announced the first real-time testing of a fixed-point 5G multi-vendor network in Romania.⁴

The state of play reveals a good situation in terms of broadband access. During the past five years Romania demonstrated considerable growth and registered rapid improvements in broadband access. Depending on source, Romania ranks among top EU states in terms of fixed and mobile broadband speeds. The broadband coverage is universal. Fixed broadband availability is very good in urban areas, but overall below the EU average due to many sparsely populated and underserved areas. In 2017, Romania has had the largest increase in the EU in terms of mobile broadband coverage, over 93.6 % of households, while the average mobile broadband coverage is still below the overall EU average (3.). Concerning broadband coverage, it is likely that by 2022 Romania will get closer to EU averages, while the 5G is highly unlikely any time sooner than 2020.

3. LTE COVERAGE BY COUNTRY, 2017



Source: European Commission, 2018, Broadband Coverage in Europe.

ON THE WAY TO THE 5G TECHNOLOGY

To successfully launch 5G networks in the 3S region, many challenges must be addressed.

Firstly, legal frameworks for the 5G communication systems are needed. Conditions of launching new operator networks and their interoperability together with the existing 2G/3G/4G infrastructure must be defined. However, full functionality of 5G will only be possible in a few years. At the beginning it will be utilised only in the urban areas, mainly in the big city centres, while in rural and suburban areas, the legacy 2G/3G/4G networks will still be deployed. Thus, there must exist procedures of switching between new networks and the existing ones. They should be created with regard to not only technical aspects, like bandwidth occupation and inter-network interference, but also the economic ones. Responsible institutions should define the maximal tariffs for traffic between networks, both between the 5G operator network and its legacy counterpart and between different 5G operators.

CASE STUDY – CROATIA



The legal framework for the introduction of 5G network was created in December 2016 when the Croatian Parliament (Hrvatski Sabor) has adopted the 'Law on measures to reduce the cost of introduction of high-speed electronic communications networks'. With this law, Croatia has transposed the EU Directive 2014/61 of the European parliament and the EU Council, adopted in May of 2014 and also aligned with the European law in this area. This Croatian law is intended to lower the cost, facilitate and boost the construction of the high-speed electronic communications networks in order to accelerate the realisation of goals set by the Digital Agenda for Europe by 2020. With this implementation, the law also strives to abolish all obstacles to the introduction

of high-speed electronic communications networks in the whole of Croatia, including the high cost of construction works that in some case make up as much as 80 % of the total cost of introducing a new network. Croatia seeks to significantly lower these costs by introducing the model of integrated infrastructure construction, which includes simultaneous construction of different infrastructure levels, including the optical waveguide infrastructure. It also aims to avoid other obstacles like low effective use of the existing network of telecom operators, non-existence of a single database of existing fiscal infrastructure and a lack of coordination during the construction works.

The next challenge is connected with the bandwidth occupancy. Currently, several activities are carried out in order to fill in the TV white spaces that appeared after switching off the analogue TV in CEE. In Poland, for example, the analogue TV transmitters were switched off by July 2013. Thus, communication channels that had been occupied by analogue TV operators (i.e. 630 MHz, TVN) were released. These frequency bandwidths can be utilised for ad hoc communications in 5G networks.

CASE STUDY - CROATIA



The introduction of 5G network has started in mid-2018 and the process has been launched by the biggest telecom operator in the country, Croatian Telecom Inc. (Hrvatski Telekom d.d., owned by Deutsche Telekom), and in collaboration with another Croatian company Ericsson Nikola Tesla Group (Swedish company Ericsson owns 49.07 % of shares). Croatian Telecom and Ericsson Tesla have been long-time strategic partners in flagship projects in the country involving the modernisation of existing radio and access networks and the introduction of new ones, ever since both companies were privatised in the nineties. In early 2018 Croatian Telecom and Ericsson Nikola

Tesla have signed a long-term contract in order to introduce 5G network connectivity and to modernise the existing radio access network; this modernisation includes improving the existing infrastructure, transport capacities and the radio access equipment on the whole territory of the Republic of Croatia. The two companies plan to finalise the 5G network introduction process by the end of 2019. This new radio access equipment will be deployed in the new cableless, so-called feederless, mode that will abolish the need for long cable connections and the losses they produce. Optical antennas with radio amplifiers will be introduced and that will also significantly lower the consumption of electric energy.

The core infrastructure is another issue. So far, the new generation of mobile radio networks was built on the existing framework of previous generations. The new, at the time, 3G and 4G networks were launched on the existing core infrastructure of GSM which got upgraded to fulfil the new requirements. However, the current situation differs from that of from several years ago when 3G and 4G networks were to be launched. This is because 5G brings a new philosophy of communications, since it integrates cellular networks with home/office wireless LAN installations, industrial control systems and IoT networks that can be applied to remotely control devices at home, office, factory and city within the so called C-RAN architecture. Centralised architecture allows hundreds of remote radio heads to use one baseband unit.

This requires building many network items like IoT gateways, micro-cells and essential parts of the core network from scratch. However, the most prominent challenge lies deeper. Countries from the 3S will have to build an efficient, robust and secure core network that will support Network Function Virtualisation of necessary appliances. Governments will have to make decision about localisations of new data centres supporting 5G core functionalities or reuse the existing data centres that currently serve as nodes of the Internet backbone. As an example, in Poland it is most likely that the existing supercomputing and data centres located in the biggest cities across the country will be connected to each other (Warsaw, Krakow, the Silesia conurbation, Wroclaw, Poznan, Gdansk). However, the exact location of core 5G elements will be the result of negotiations between 5G operators, governmental institutions, regulatory bodies, existing data and supercomputing centres and local authorities.

The existing optical fibre trunks connecting different national networks will have to be upgraded. This may require signing bilateral agreements between different countries to define technical and economic aspects of cooperation, which was also underlined in relation to the 3SDH.

Regulatory institutions will have to disclose recommendations describing where new network components can be installed and where they are forbidden (i.e. in hospitals). Electromagnetic compatibility issues and the EM radiation originating from the growing number of devices which produce the so-called 'electromagnetic smog' that is often said to impact on the health of the population will have to be addressed and explained to the public. Different entities at the national level, such as ministries of healthcare and digital affairs will have to prepare recommendations in collaboration with institutions responsible for electronic communications. Technological growth cannot be enforced to the detriment of population health.



CASE STUDY – SLOVAKIA

Slovakia has set the long-term objective of achieving access to high-speed internet connection with at least 30 Mbps for all households by the end of 2020.⁵ On the private sector side, for example, telecom company Orange Slovensko is aiming to launch 5G between 2020 and 2022 as one of the first operators in Europe. The two main documents where this strategy has been elucidated are Slovakia's National Broadband Strategy and the Strategic Document for Digital Growth and Next Generation Access Infrastructure 2014-2020. In these strategic documents, what has been identified are Slovakia's regulatory measures needed to meet a target of 100 % coverage of 30 Mbps high-speed internet and the preparations for meeting the target concerning subscriptions of high-speed internet above 100 Mbps. These include legislative amendments to simplify the building of networks, auctions to facilitate innovation in mobile broadband access, and regulation of prices and access to completed networks to increase competition in the market and optimise the profitability of realised investment. More recently, a Memorandum of Cooperation was

signed between operators (Slovak Telekom, Orange Slovensko and O2 Slovakia) and the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization to give high-speed internet access to each municipality in Slovakia by 2020, recognising that in the digital economy it is a basic prerequisite for work and study.⁶ This is targeted specifically to eliminate 'white spots' or municipalities with no internet access, of which Slovak authorities counted 207 as of 2017.

In the 2007-2013 programming period, a plan to create conditions to provide internet services to everyone was prepared, under which steps were taken to commence procurement of backhaul networks to cover white areas. The steps taken included public procurement of projects for the building of national backhaul networks to cover white areas; a proposal for project documentation for the building of national backhaul networks; ensuring administrative capacities for the building of national backhaul networks.⁷ An auction for the allocation of frequencies of the digital dividend took place in 2013, enabling construction of fourth generation mobile networks.

Last but not least comes security. 5G networks, due to their ubiquitous character, demand upgrading requirements and procedures that will ensure information security and privacy is improved in comparison to the previous generations of radio systems. Since 5G networks will make it possible to remotely monitor home and office or to perform several activities, e.g. opening the door or increasing the temperature in the room, they have to prevent illegitimate parties from manipulating the commands sent remotely to devices and from disclosing sensitive data (such as the image of a bedroom from an IP camera connected to the Smart Home IoT

network). Therefore, complex approach to security that addresses both service availability and protection of the radio access is essential. The development of common security models and good practices such as selection of trustworthy contractors and providers related to the construction of 5G networks may take place not only on the designated international forums, but also as part of the D3SI, as the technology is now taking off around the globe and in the EU.⁸

Together with deployment of 5G and IoT networks, new types of threats and crimes will arise. Burglars willing to break into a house will try to bypass protection mechanisms of the Smart Home IoT network. Terrorist and organised crime groups will try to use 5G network in order to insert malware into industrial control systems of power grids, gas distribution networks or Smart Cities IoT networks that monitor traffic in big cities. Moreover, with rapid growth of computational power, the existing cryptographic mechanisms will not be sufficient to provide confidentiality and integrity of data transferred between mobile terminals and base stations. Since the 'weakest link' determines the overall security of any information system, there will be a necessity to strengthen the protection of the wireless traffic between all devices, from simple temperature sensors to sophisticated IoT gateways. Each subnetwork will have to be equipped with Wireless Intrusion Prevention Systems



to detect illegitimate traffic attempts, for instance caused by rogue access points, jammers and so on. In addition, procedures of detaching unwanted device and arresting suspected offenders who attempt to perform Denial-of-Service attacks or steal confidential data will have to be defined by relevant entities.

Due to the open nature of 5G architecture that exploits IP networks together with virtualisation mechanisms that rely on SDN and NFV and because of the diversity of access technologies possible to implement (6 Low PAN, Wi-Fi, etc.), a specific approach to data protection needs to be taken. The backbone or core part shall be protected with mechanisms known from decentralised networks, for instance Attribute-Based Access Control. However, the traffic within an Autonomous System or a subnetwork controlled by one entity should enforce a centralised approach, with one entity (i.e. access router) being responsible for authentication, authorisation and for detecting attempts of illegitimate operations.

In addition to protection mechanisms at the network and transport layer, operators will have to exploit radio channels for session key generation and mutual user authentication. Random fluctuations of radio channel characteristics are exploited to increase equivocation at the intruder's side. Thus, the increase in computational power by the enemy does not help them to discover the confidential message transfer-

red over the wireless medium by legitimate parties (i.e. wireless sensor and an IoT gateway).

These physical-layer security mechanisms have been attracting huge interest from academia and the industry for several years. Both theoretical analysis and experimental results performed in laboratory conditions have shown their usefulness in wireless sensor networks. Thanks to deployment of these mutual authentication and key generation mechanisms, the implementation of complicated key management mechanisms and storage of key repositories can be avoided. Moreover, sensors can still use lightweight hardware. Otherwise, all devices launched in a 5G network would have to be equipped with a very quick processor and a memory that supports complicated cryptographic operations performed in a reasonable time.

Two things should be especially noted. Firstly, launching the 5G network will require the holistic security approach comprising both virtualised and non-virtualised security functions to be put in place at all layers of the ISO OSI model. Secondly, an urgent need for automated security management solutions for 5G networking will be observed. Nowadays, every threat that may impact the network cannot be foreseen. However, technical tools to mitigate the impact of new threats and vulnerabilities that will come in the nearest 5 years exist already. It is the decision of governments

whether to enhance technical security requirements and put additional obligations for 5G operators. This will definitely require discussion between decision-makers, telecommunication industry and independent experts in academia.

5G-RELATED PROJECTS IN THE 3S

In recent years, we have been observing activities of mobile operators and decision-makers that aim to launch national 5G commercial instances.

1. The Slovenian and Hungarian telecommunication regulators have signed a cooperation agreement to support a pilot project for the implementation of 5G technology. The project is in the field of public security, protection and rescue technology. The cooperation agreement is part of a wider integration between the countries in this field, after the signing of a cross-border memorandum between Slovenia and Hungary for the 5G project. The pilot project thus gains an international dimension and, consequently, increased opportunities for obtaining European funding.⁹
2. It is likely that the results of EU-funded research projects will be applied directly. One of the projects that has been finished recently is CHARISMA.¹⁰

In spring 2018 the final presentation took place in the headquarters of Telekom Slovenije, which is one of the project partners.¹¹ The aim of the project was to design a hierarchical para-virtualised 5G access network architecture, which sets up the shortest network connection that supports end-to-end security. Hence, it is likely that Telekom Slovenije as a project participant will help to lead implementation of these features in other 3S countries. However, this will require inter-governmental agreements and cooperation between 5G operators in all the member countries.

CASE STUDY – HUNGARY

The Budapest based 5G Coalition already has 64 members. The Coalition was established on 19 June 2017 with the participation of governmental and market players, professional and interest groups, universities and scientific think tanks; it aims to put Hungary at the top of European 5G developers.

The other priority of the Hungarian government is to use the 5G technology in its Smart City development.

3. Hungary's telecommunications authority NMHH is planning to sell the frequencies needed for the launch of 5G services in the country in the third quarter of 2019. The draft legislation

required for 5G is supposed to be issued before the end of 2018. The authority already began preparing the new frequency trading planned for the third quarter of 2019. NMHH will sell licenses for the use of 700 MHz and 3400–3800 MHz bands as well as other currently available bands to service providers during the bidding.¹²

4. In July 2018, Magyar Telekom demonstrated a 5G test network in the 3.7 GHz spectrum band in Budapest under real-world, non-laboratory conditions. It was implemented with a pre-standard 5G system, using Huawei Technologies' 5G network devices, ready for commercial launch. The use cases shown included real-time remote diagnosis via the 5G network, rescue with drone using 5G and gaming in augmented reality. The technology could be available in 2–4 years. Although in Europe 5G are planned to already be generally available by 2020, in Hungary the target year is 2022.¹³
5. Telia Company, Ericsson and Tallinn University of Technology (TalTech) have joined forces to launch Estonia's first 5G pilot network at the university campus by year end. Companies and startups are invited to use the 5G network to develop future services and new business models. The network will provide mobile data for the whole TalTech campus, which makes the de-

velopment of innovative new services and solutions possible. TalTech has built a self-driving car named Iseauto, which will become one of the first co-operation projects within the 5G pilot network scope. The next milestone will come in 2019, when the project partners will showcase Iseauto driving around and communicating with the surrounding infrastructure with the help of 5G.¹⁴

RECOMMENDATIONS FOR THE 3S COUNTRIES:

1. **Harmonised approach** in the 3S region to the 5G development is needed due to potential regional application in projects such as D3SH.
2. Political will is needed to **operationalise the 3SDH project and implement its calendar** that was preliminary drafted and included in the description of the priority interconnection projects listed by the Three Seas Summit in Bucharest.
3. **Policy modernisation** is necessary to cater to the ubiquity of 5G technology without creating an overregulated system which stunts innovation and growth. Policy-makers have to enable firms to make long-term investments and R&D, facilitate public-private cooperation on 5G standards

and ensure adequate intellectual property protections for standardised technology.

4. A strong emphasis shall be placed on effective government frameworks which also have **clear and robust regulations on issues of data exchange, data privacy, security and well-being of the population.**
5. Providing an **encouraging regulatory environment for all stakeholders** which includes suitable spectrum available in the appropriate bands and with appropriate license conditions is necessary. Capability and technical standards and bands allocation are also areas that shall be prioritised.¹⁵
6. Building an **efficient, robust and secure, including cybersecure, core network that will support the 5G technology solutions** is a must. However, **end-to-end security** shall be addressed above all, as protection mechanisms for the core network are sufficient enough at the moment.
7. **Technical coordination of 5G frequency bands** on the backbone of the 3SI is required.
8. Development of 5G shall be **focused on specific sectors and thereafter monitored on that basis**; transport, energy, e-health, finances, water supplies and

other defined nationally critical infrastructures shall be taken into account. Other points of concern shall include automotive industry, M2M communications, agriculture.

9. Ensuring that a **broad range of stakeholders** is involved to discuss approaches and strategies for 5G is important for its development. It is crucial that all stakeholders have an equal voice in such discussions and debates. Different actors' involvement in established coalitions, working groups, etc., shall be beneficial, as will the clarification of what their possible responsibilities are.¹⁶
10. The role of academia and research institutes to contribute to creating an enabling environment for the 5G deployment is critical, also for R&D in the field of 5G. This can be done by **developing new educational and certification programs related to 5G technologies.** Universities can further bridge the gap between verticals and operators and aid in exploratory research.



SOURCES:

1. European Commission (2015). 5G Vision The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services [on-line]. Available at: <https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf>.
2. European Commission (2018). Broadband Coverage in Europe 2017 [on-line]. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52968.
3. ANCOM. (2018). Foia de parcurs națională privind alocarea și utilizarea viitoare a benzii de frecvențe 470-790 MHz [on-line]. Available at: http://www.ancom.org.ro/uploads/links_files/Foia_de_parcurs_pentru_banda_UHF_470-790_MHz.pdf.
4. Orange Romania. (2018). Orange, Samsung și Cisco anunță primul test din Europa de utilizare în condiții reale a unei rețele 5G multi-vendor de tip acces radio la punct fix [on-line]. Available at: <https://www.orange.ro/newsroom/comunicat/innovatii-1/orange-samsung-si-cisco-anun%C5%A3a-primul-test-din-europa-de-utilizare-in-condi%C5%A3ii-reale-a-unei-re%C5%A3ele-5g-multi-vendor-de-tip-acces-radio-la-punct-fix-1059>.
5. Deputy Prime Minister's Office for Investments and Informatization of the Slovak Republic (2018, February 6). Press release by Office of the Deputy Prime Minister of the Slovak Republic for Investment and Informatization [on-line]. Available at: <https://www.vicempremier.gov.sk/index.php/kazda-obec-na-slovensku-by-do-konca-2020-mala-mat-rychly-internet/index.html>.
6. Ibidem.
7. (n/d). Strategic Document for Digital Growth and Next Generation Access Infrastructure (2014 – 2020) [on-line]. Available at: informatizacia.sk/ext_dok-strategicky_dokument_2014_2020_en/16622c.
8. The Kosciuszko Institute Policy Brief (2018). The Digital 3 Seas Initiative: A Call for a Cyber Upgrade of Regional Cooperation [on-line]. Available at: <https://ik.org.pl/en/publications/white-paper-the-digital-3-seas-initiative-a-call-for-a-cyber-upgrade-of-regional-cooperation/>.
9. Telecompaper (2017, December 5). Slovenia and Hungary agree cooperation on 5G pilot project [on-line]. Available at: <https://www.telecompaper.com/news/slovenia-and-hungary-agree-cooperation-on-5g-pilot-project--1223221>.
10. [on-line]. Available at: <http://www.charisma5g.eu/>.
11. IDW (2018, July 17). Project completion of 5G-CHARISMA: Successful Development of new Network Architectures for the 5G [on-line]. Available at: <https://idw-online.de/de/news699257>.
12. Telecompaper (2018, September 27). Hungary plans 5G auction for Q3 2019 [on-line]. Available at: <https://www.telecompaper.com/news/hungary-to-sell-5g-licences-in-q3-2019--1262433>.
13. Telecompaper (2018, July 3). Magyar Telekom presents first 5G connection in 3.7 GHz band [on-line]. Available at: <https://www.telecompaper.com/news/magyar-telekom-presents-first-5g-connection-in-37-ghz-band--1251095>.
14. ITUUDISED.EE (2018, August, 24). TTÜ ja Telia loovad koos 5G lahendusid [on-line]. Available at: <http://www.ituudised.ee/uudised/2018/08/24/ttu-ja-telia-loovad-koos-5g-lahendusid>.
15. IHS Economics & IHS Technology (2017, January). The 5G economy: How 5G technology will contribute to the global economy [on-line]. Available at: <https://cdn.ihs.com/www/pdf/IHS-Technology-5G-Economic-Impact-Study.pdf>.
16. (2018, July 5). The International Telecommunication Union Report on the ITU-D Study Groups related Experts' Knowledge Exchange. 5G Implementation in Europe and CIS [on-line]. Available at: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5GHungary/FINAL_Budapest_Expert_Exchange_Report_5_July_2018.pdf.







GEOPOLITICS AND THE CEE REGION

by Edward Lucas¹

Define the term, and you define the problem. Geopolitics is about the influence of geographical relationships on political behaviour. A category constructed on the basis of proximity or history easily becomes an entity, which may then be overestimated as a subject or an object of international relations. China, for example, puts widely varying countries² into one category for its 16+1 format, examined later in this article. Some of these are in NATO; some are in the EU, some are in both and some in neither. Some are newly independent; others have centuries of sovereignty and statehood. So: why those sixteen, and not fifteen or seventeen?

These difficulties reflect the fact that defining 'Central and Eastern Europe' is getting harder: something which everyone living between the three seas – the Baltic, Black and Adriatic – should celebrate. Clarity in categories is a legacy of the brutal divides of the cold war, when 'eastern Europe' was crude but convenient shorthand for the countries of the Soviet empire. Now these shared memories of occupation, domination, and alien economic and

political structures, are fading. Underlying differences have emerged – between economically advanced and backward countries, between those with protestant, catholic or orthodox religious orientations, between a handful that historically regarded Russia as a liberator from other forms of oppression and a majority that did not. This variance increasingly outweighs the legacy of 1945-91. Despite their radically different experience during the cold war Sweden and Finland have much in common with the Baltic states and Poland when it comes to worries about Russia. More distinctions loom. Demography may play a role, for example: countries with ageing, fast-shrinking populations may in future display vulnerabilities and fix priorities not shared by those whose populations are stable or growing.

Any definition of 'Central and Eastern Europe' at the end of the second decade of the second millennium will therefore be a snapshot, and necessarily arbitrary and incomplete. We can do our best to draw definitions, but we should do so humbly, in the knowledge that even our best efforts will be out of date, and perhaps sooner than we think.

The use of 'central' as well as 'eastern' implies a difference that merits the separate adjectives. There must be some part of eastern Europe which is not central, and some of central Europe that is not eastern. Yet the two together must have enough

common characteristics to make it worth combining them.

This leads on to the second big point. Though 'central' and 'eastern' sound like geographical terms, physical location is only partially helpful in determining geopolitical significance. Even during the heyday of cold war 'eastern Europe', the term owed more to history than to topography.³ Prague, capital of the then 'eastern European' country of Czechoslovakia, is geographically west of Vienna, capital of neutral, but capitalist, democratic and therefore 'Western' Austria. Most of Finland lies to the east of most of 'eastern Europe'. Greece, a member of NATO since 1952, is also in the geographic east of the continent, Turkey even more so.

Nowadays, 'eastern Europe' is, if anything, shorthand for Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. These countries do have in common a shared past as former Soviet Socialist Republics, though why this should be of overwhelming relevance 27 years after the USSR collapsed is unclear. More importantly, they are not members of the main Western security and economic structures, the European Union and NATO, while being subject to severe economic, political and in some cases military pressure from the authorities in Moscow.

Reactions to this vary. In the case of Armenia and Belarus, relations with Russia are

sometimes tense but rarely overtly hostile. Azerbaijan pursues its own diplomatic path, often influenced by Turkey. Ukraine and Georgia are direct victims of Russian military aggression. They are ardent applicants for membership of the EU and NATO, and receive substantial military, economic and political bilateral support from Western countries.

The use of 'central' as well as 'eastern' implies a difference that merits the separate adjectives. There must be some part of eastern Europe which is not central, and some of central Europe that is not eastern. Yet the two together must have enough common characteristics to make it worth combining them.

If 'eastern' Europe is fuzzy, 'central' Europe is even harder to define. The geographical centre of Europe is disputed, because the continent's northern and eastern borders are not fixed. The term's historical and literary antecedents are questionable.⁴ Applying a degree of practical cynicism, 'central Europe' could nowadays be described as a catch-all phrase for countries ranging from Estonia southwards that a) were at some time under some sort of commu-

nist rule; and b) do not wish for whatever reason to be called 'eastern Europe'.⁵ The term 'central and eastern Europe' is indeed imperfect and should be used with caution and humility. But it carries two important messages.

One is that these countries are still recovering from the damage done in the decades following 1945. Backwardness, isolation and meanness survive, even when the tenets of Marxism-Leninism and self-managing socialism are long forgotten. Although a handful of countries, notably Slovenia, are now well into the middle-income category, the legacy of the past is mostly all too visible. Sometimes the shortcomings are most visible in infrastructure: pipelines, power lines, railways and roads built under communism in order to reinforce dependence on the east. Housing stock was built cheaply, with little regard for the human and environmental needs. Much has been done to bridge those gaps; much more remains. In other places the shortcomings are most apparent in public services such as health or education, or in the quality of criminal justice and public administration.

In particular the legacy of the secret police files and networks of informers, and of the expropriation of property and blighted lives which the totalitarian system enforced, is a moral Chernobyl. This will afflict social trust and cooperation, and the public's sense of justice and fairness, for decades to come. No country has fully engaged in the

truth and reconciliation which could heal these historical wounds. In the post-communist era, perpetrators mostly fared rather better than they deserved, while victims mostly have not received redress for the moral and physical damage they suffered. Yet these binary categories are misleading: some, and in some countries many, people can be viewed as both perpetrators and victims. This problem, toxic and unsolved, is unique in Europe. Dictatorships in Greece, Portugal and Spain were briefer and milder. They did not leave such deep scars. Just as it is hard for Britain to realise what it means never to have been under foreign occupation, it is hard for most countries in what we crudely term 'western' Europe to realise the true legacy of communist rule.

This is not just a moral burden. It is also a strategic vulnerability. Part of the legacy of the past is low levels of social trust, fragmentation and alienation. Resilient, cohesive countries are harder to attack than atomised, mistrustful ones. Moreover, Russia has human, commercial and physical ties to the former Soviet empire which it unhesitatingly exploits.

Though real differences exist, a related problem, paradoxically, is outsiders' exaggerated misperception of east-west differences. An 'orientalist' approach in countries that were never scarred by communist rule can lead to a patronising assumption of an 'eastern' Europe defined

by its otherness: less civilised, less important, less pleasant – a muddy, homogenous wasteland of crumbling concrete, populated by grim-faced barbarians in felt boots, with a history of ethnic hatred and superstition. In particular, the 'easterners' are seen as hot-headed, paranoid and resentful when it comes to geopolitics, dragging the rest of Europe into pointless and dangerous clashes with Russia.

The truth is the other way round. Much of 'old' Europe has been complacent about the rise of a revisionist Russia. The countries of what may be termed (with further compression) the 'CEE region' (and others outside it, notably Norway, Sweden and Finland) have a sober awareness of the danger. Sometimes they are threatened chiefly because of geographical proximity – the Baltic states, Georgia, Poland, Romania and Ukraine are the clearest examples. For countries farther away, the danger may stem more from political or economic vulnerabilities. The Czech Republic, Bulgaria and Slovakia fall into this category. Some countries are at risk because of their geopolitical choices: the coup attempt in Montenegro in 2016, on the eve of that country's accession to NATO, is a good example; so too are the shenanigans in Macedonia over attempts to solve the dispute with Greece over the former Yugoslav republic's constitutional name.

Of course the CEE region is not alone in experiencing these threats. Indeed, in



many respects the pressure from Russia is worse in countries that do not form part of the region even in its widest definition. The attack on the American electoral system in 2015-2016, involving the hacking-and-leaking of politically sensitive material, the use of polarising material on social media and questionable contacts with leading figures in Donald Trump's election campaign, far outstrips in ambition, scale and scope anything conducted in the CEE countries. The military pressure on non-NATO Sweden and Finland in some respects exceeds that on the Baltic states. Kremlin economic and political penetration of Germany and Austria is remarkable – probably only Ukraine in the Yanukovych era, Belarus and perhaps Serbia have experienced anything similar.

The threat perception within the CEE region is not uniform. It varies widely. For reasons ranging from arrogance and complacency to outright corruption, it can be hard to draw decision-makers' attention to the threat posed by Russia. In countries such as Serbia and Bulgaria, historical and cultural ties can distort the security culture. Countries such as Albania, Slovenia and Croatia have no lived experience of Soviet domination. Deep-rooted rivalries and historical issues (between Poles and Lithuanians, Poles and Ukrainians, Hungarians and Slovaks) can be exploited by the Kremlin to shift attention away from common external threats and towards neighbourhood disputes.

It is particularly important, therefore, to avoid using the CEE region as a synonym for 'front-line states'. Frontlines abound, and they do not all run through, or even include, this part of Europe. If we are worried about the Russian military threat, then we need to start in the Arctic and end in Syria. If we are interested in energy diplomacy, our field of vision must include Saudi Arabia and Venezuela. If we are worried about political penetration or influence operations, then geography has no limits at all. The CEE countries' common vulnerability does not make them shakier than their counterparts elsewhere in Europe. Knowledge of weakness is the beginning of strength. Russia finds it far easier to make mischief in countries which the term 'cold warrior' is a jocular term of abuse, than in societies where the Gulag is still in living memory.

Given these provisos and qualifications, where is the CEE region now as a subject and object of geopolitics?

The first and most important point is that the threat from Russia is real. The central organising principle of Vladimir Putin's regime is that stability at home requires revisionism abroad. Accommodating the Kremlin's interests, therefore, is not about changing outcomes within an existing set of rules. It would mean accepting new rules dictated by Russia. This is hard for many Westerners to understand, because we believe implicitly that the European

security order dating back to the Helsinki process in the mid-1970s is stable, because all sides regard it as fair.⁶ This assumption is profoundly mistaken. The Kremlin, citing the need for a buffer zone around its long and vulnerable borders, regards the Western-dominated security order as unfair, threatening and over-ripe for change. It believes that the rules were drawn up without regard to Russian interests and that the West is hypocritical in the way it implements them: dressing up self-interest with phony talk about human rights and the rule of law.

Russia also believes that conflict and competition are central to international relations; talk of win-win outcomes is naïve at best and mendacious at worst. As far as Russia is concerned, conflict with the West is inevitable; the only question is who wins. This has the advantage of strategic coherence. Russia's decision-makers share a broadly similar perception of the threat, at least as far as the West is concerned.⁷ They have common priorities, appetites for risk and assessments of our vulnerabilities. None of that is true on our side.

The stakes are particularly high for the CEE region. Russia does not believe that its neighbours should be fully sovereign, with the right to make their own decisions about their geopolitical future. In Russia, a former imperial power with a long history of invasion by (and of) its neighbours, such independent-minded behaviour is seen as

an affront to history and geography. In particular, many Russians see the CEE region as a war trophy, won through the sacrifice of the war against Nazi Germany and its allies. From this standpoint, any resistance to Russian influence in these countries now can therefore be dismissed as residual sympathy for fascism.

The Kremlin does not want to re-conquer its ex-colonies; even leaving aside the risk, restoring the empire would be prohibitively costly. Even accounting for differences in purchasing power, Russia's economy is only about one quarter of the size of the EU's.

Russia does not believe that its neighbours should be fully sovereign, with the right to make their own decisions about their geopolitical future. In Russia, a former imperial power with a long history of invasion by (and of) its neighbours, such independent-minded behaviour is seen as an affront to history and geography.

But it does want to constrain them. It particularly begrudges the former captive nations of the Soviet empire – which comprise most of the CEE region – their freedom, their prosperity, and their sovereignty. For countries already in the EU and NATO, the aim is to promote their marginalisation, pit them against each other, or to use them as Trojan Horses in order to gather intelligence or impede decision-making. For others, chiefly the poorer ex-Yugoslav republics such as Macedonia, the Russian priority is to prevent where possible their integration into Western structures.

This approach is economically perverse. Successful, stable prosperous neighbours would in almost all respects be good for Russia. But the success of former colonies poses an existential challenge to the stagnant and autocratic model of government pioneered by the Putin regime. If Estonians, under Soviet rule until 1991, can have European living standards, good public services and world-class digital infrastructure, why can people across the border in Russia not enjoy the same benefits? The answer is that the freedoms which Estonians exercise would, if spread to Russia, erode and challenge the Kremlin's grip on power. Despite much paranoid propaganda bombast to the contrary, neighbouring countries pose no military threat to Russia. But they do potentially challenge the Kremlin's political legitimacy.

The West has since 2008 substantially strengthened its security posture in CEE region. The Kremlin's reaction to this has been bombastic. Russia's defence minister, Sergei Shoigu, says Russia will continue to strengthen its forces in order to 'neutralise the security threat in the Black Sea region from NATO.' As with Kaliningrad⁸ in the Baltic region, Russia uses the mistaken (and, in truth, fictional) narrative of encirclement to justify an increasingly aggressive military posture. Having posited encirclement, Russia must have the capability to break it. Its security therefore depends on its neighbours' insecurity. Making Russia rethink its dangerous approach would require a combination of better deterrence (of which more later), a carefully calibrated defensive military build-up, and clear-spoken and united Western diplomacy. This is lacking now, and unlikely in the foreseeable future.

As a result of this weakness, Russia believes it has a realistic chance of changing the European security order, replacing the rules-based multilateral system with a bilateral one in which strong countries do the deals that they can, and weak countries accept the outcomes that they must.

Russian security policy: aims and means

In pursuit of that strategic aim, Mr Putin has intensified what is often called 'hybrid

warfare' against the West: a complex mixture of tactics, usually coordinated by the intelligence services, which are particularly potent against open societies.

This form of conflict uses money, bolstering self-interested commercial and financial lobbies which profit from doing business with Russia and fears any cooling in political ties. Energy, economic and financial ties constrain Western responses to Russian revisionism. Overt and covert payments buy influence in political parties, think tanks, media outlets and academic institutions.

Russia also practises information warfare (propaganda) with a level of sophistication and intensity not seen even during the Cold War. It uses the immediacy, anonymity and ubiquity of the internet to confuse and corrode Western decision-making and public life. It is prepared to threaten and apply force, ranging from physical and cyber-intimidation of opponents, including assassination, to military sabre-rattling. Where necessary – as in Georgia, Ukraine and Syria – it uses straightforward conventional warfare.

Money, propaganda and force are the most salient features of the Russian approach. But there are many more. A non-exhaustive inventory includes:

- the targeted use of corruption;

- covert information operations such as hacking and leaking attacks;
- cyber-warfare;
- diplomatic divide-and-rule games;
- the exploitation of economic, ethnic, linguistic, regional, social and other divisions;
- economic sanctions such as import curbs and restrictions on exports and transit; energy blackmail;
- the exploitation of religious sentiment, especially among Orthodox believers;
- stoking financial panics;
- lawfare (the abuse of local and international legal procedures, such as issuing Interpol Red Notices to critics, mounting libel actions and vexatious lawsuits);
- the use of organised crime networks to demoralise and intimidate;
- subversion of social norms, public confidence and state institutions;
- violent anti-social behaviour including sabotage and vandalism; and
- weaponising history to besmirch the reputation of a target country and hide Kremlin crimes.

To complicate matters further, these tactics are not applied in a static or even linear formation. Russia's spymasters are not stupid. They develop new approaches, especially new combinations and sequences of tactics, tweaking them based on results. We may think we are looking at a picture; our adversaries are writing a screenplay.

Human weakness means we find it is easier to admire problems than to solve them, to focus on the dangers we can see than worry about those that we can't, and to use the tools we have on hand rather than try to acquire the ones we actually need. Western policy-makers and analysts over-focus on easy-to-see Kremlin propaganda, especially in English and other Western languages. In fact, information warfare – meaning deliberately misleading 'fake news' plus the disorientating use of trolls and bots – is just one, albeit conspicuous, element of the arsenal outlined above.

We may think we are looking at a picture; our adversaries are writing a screenplay.

Many in the West still assume, annoyingly, that this problem is somehow recent. It is not. All the tactics above have been tried in the CEE region in previous years, in many cases since the early 1990s.

People in these countries warned the West of the decay of democratic life in Russia, of election-rigging, of the resurgence of the old KGB, and of the growth of kleptocracy. They could see from first-hand experience that Russia had not abandoned its arrogant, unrepentant imperialist attitudes, and used a toxic cocktail of force, money,

propaganda and subversion. Kremlin spy services were adept at finding targets and exploiting weaknesses. Though Russia was still economically weak back then, times would change. Trouble was on its way – not only for the CEE region, but for the rest of the world.

Western policy-makers did not just ignore those warnings. They patronised and belittled the people who delivered them. That arrogant complacency has been costly, and is now dangerous. Influence operations are far more pernicious than kinetic warfare. If they succeed, armed resistance is pointless. Russia's puny military struggles to operate outside its immediate neighbourhood, with Syria being for now the sole exception. But battle-honours for its influence operations include Berlin, Bratislava, Budapest, London, Prague, Rome – and, arguably, Washington, DC.

The transatlantic relationship: the end of an affair?

The nature and extent of Russian interference in the US political system in 2015-2016 is still unclear. The typical goal in Kremlin influence operations is to stoke controversy and division, rather than promote any particular cause or candidate. But regardless of putative Russian involvement in his campaign, President Donald Trump's rhetorical approach to transatlan-

tic security marks a sharp change from the past. Mr Trump has called the EU an enemy, threatened to withdraw from NATO, decried the idea that the alliance's Article 5 security guarantee applies to its newest member, Montenegro, and conducted highly unusual bilateral personal diplomacy with Vladimir Putin.

Rightly or wrongly, that has fuelled the belief in Europe that the US is an untrustworthy ally. In Germany, for example, opinion polls suggest that the public regards the US as a bigger threat to world peace than Russia. Mr Trump's anti-NATO rhetoric, including lines such as: 'Sometimes our worst enemies are our so-called friends or allies' has prompted an alarming drop in support for NATO among Republicans, long sceptical about multilateralism. In March 2016, Republicans wanted the US to remain in the alliance, by 48 per cent to 17 per cent. In a YouGov poll in July 2018, the party base split evenly, with 38 per cent opposing and backing continued membership.⁹

Though other countries also face threats from Russia, the CEE countries face a uniquely difficult mixture of economic, political and military threats. None of them is big or strong enough to manage its own defence, now or in the foreseeable future. The ability of a united West to constrain and deter Russia is a matter of the highest national security importance.

President Trump's behaviour on this front has, put mildly, been less than thoroughly helpful. The invasion of Ukraine and seizure of Crimea in 2014 made Mr Putin a diplomatic pariah. Now he is receiving a detox. After his friendly meeting in Helsinki in July 2018, the Russian president attended (ostensibly as a private guest) the wedding in August of the Austrian foreign minister, Karin Kneissl. It is hard for other European countries to complain about this, given the lead taken by the American president. Moreover, Mr Trump has invested his personal prestige in maintaining friendly relations with his Kremlin counterpart. That risks hampering his response to any future provocation by Russia, perhaps in Ukraine, the Western Balkans or Belarus.

Yet the picture is not as simple as the president's domestic critics would make out. Although the tone of Mr Trump's criticism of NATO is new, the substance is not. European allies have been spending too little on defence for decades. American officials have repeatedly warned of the dangers of this, both in diminished military capability, and in the strains this puts on the Atlantic alliance. Mr Trump may express himself with unprecedented acerbity on the issue, but Europeans cannot justly complain that they were taken unawares.

Secondly, American support for European defence in practical terms is rising not falling. The budget for the financial year starting in 2019 includes USD 6.5 billion

for the 'European Deterrence Initiative' (previously called the European Reassurance Initiative). The Pentagon requested USD 4.8 billion in the current financial year and received USD 3.4 billion in the previous one. The US Army presence in Europe, after years of decline, is now growing again.

Combined with the contributions of other European allies (not the least of which are significant contributions by vulnerable CEE states in enhanced NATO CEE security structures and formations it reduces the likelihood of a sudden Russian surprise attack on neighbouring states. But the reassurance is only partial. Territorial defence – and the doomsday thinking of the balance of terror which underpins it – is one part of 21st-century security, not the whole. Nuclear weapons are no answer to Russia's capacious and well-stocked hybrid-warfare arsenal. No local military solution, in either the Baltic region or the Black Sea, will be adequate on its own. The central component of collective defence is an effective deterrent that is not tied to any particular geographical theatre.

Other potential deterrents, such as rapid, punitive financial and visa sanctions, or the use of cyber and information weapons in response to aggression, are not yet part of our strategic planning. In response to a Russian non-military provocation, such as an economic blockade, targeted assassinations, cyber-attack, sabotage or subversion, NATO has few means of responding

in the right timeframe. Increasing the alliance's air policing presence in the Baltic states, bringing heavy armour from the United States, or holding a live-fire military exercise would be at best a symbolic (and probably belated) answer to such incidents.

Rebuilding resilience and developing next-generation deterrence requires a transformation in government and society, rethinking our silo-based approach to counter-intelligence, criminal justice, financial supervision, internet security and media regulation, while refashioning our threadbare security culture. This process will be costly and difficult, with some painful trade-offs. It will be particularly hard to do this at a time of increasing fragmentation and decreasing trust.

The second problem is decision-making. Russian penetration of some NATO European allies mean that it could be difficult to achieve a rapid consensus at the North Atlantic Council in response to a Russian provocation, in particular one with substantial non-military elements. That would put a particular emphasis on other countries' abilities to respond independently of NATO, in particular the US.

Here the question marks over Mr Trump's judgment (and in some eyes his integrity) become crucial. How would the commander-in-chief respond to Russian aggression? Would he really risk war, ordering the US military to deploy in force, and use live

ammunition? Or would he seek to sort the matter out with Mr Putin, doing a deal over the heads of the allies? We do not know. Leadership rests on credibility. Trust in the US has been ebbing for years, but under Mr Trump a rip tide is running. For the first time since the Berlin airlift seventy years ago, European allies no longer rely on decision-makers in Washington, DC to solve their problems.

Complete fragmentation, though, is not inevitable. Britain and other European countries are fighting a defensive battle to save the transatlantic alliance, making whatever efforts they can to placate the president, and shoring up support for NATO in Congress, with public opinion, and in other parts of the American system. The struggle is far from lost and could yet be won. A costly and risky new era of post-Atlantic defence is looming. The question is how Europe manages it.

Brexit both complicates and simplifies matters. It acts as a severe distraction in the short term, consuming scarce time and energy. But it also precipitates new thinking. In the past, Britain, along with Turkey, has acted as a brake on EU defence cooperation, now labelled PESCO (Permanent Structured Cooperation). It saw such efforts as a French-led attempt to undermine the Atlantic alliance, dangerous if it worked, and a distraction if it did not. Britain's looming departure from the EU means that policy-makers in London can

no longer hold back PESCO. Yet at the same time, Britain is aware that its clout in military, security and intelligence matters offers the best chance of keeping a role in post-Brexit European decision-making. Meanwhile, Turkey's autocratic leadership has marooned that country on the diplomatic margins.

In short, Britain is no longer blocking European defence cooperation. Instead, it hopes to shape it, along with France and in cooperation with Germany. EU-NATO ties, long blocked by Turkey, are flourishing too.

A particular priority here is promoting military mobility – a capability which has withered since the end of the cold war. Bureaucratic procedures for crossing borders, access to scarce rail-freight capacity and other infrastructure bottlenecks, strengthened bridges, and speedy permission for the transport of live ammunition are all inadequate, startlingly so in many respects. EU-NATO cooperation offers an ideal framework for dealing with these problems.

In short, the leadership vacuum created in Europe by the Trump presidency is already being filled. Old dividing lines are blurring. An Anglo-French expeditionary force aims to be operational by 2020. Mr Macron, who says that Europe can no longer rely on the US in security matters, has launched a French-led, nine-country European Intervention Initiative, which is independent of both NATO and the EU. The main

aim is to keep post-Brexit Britain involved in European collective security. Another, British-led, joint expeditionary force includes non-NATO Sweden and Finland, plus Norway (not an EU member), as well as Denmark, which opts out of EU defence policy.

Other bilateral and multilateral ties are strengthening too. Sweden and Finland have started unprecedented bilateral intelligence-sharing and military cooperation. The Northern Group, a twelve-country defence forum, comprises Denmark, Estonia, Finland, Germany, Iceland, Latvia, Lithuania, the Netherlands, Norway, Poland, Sweden and the UK. NORDEFCO brings the five Nordic countries together. The Bucharest-9 represents the countries of the alliance's eastern flank: Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania and Slovakia. The four Visegrád countries (the Czech Republic, Hungary, Poland and Slovakia) have pledged increased defence cooperation. The Three Seas Initiative brings together twelve EU member countries along a north-south axis from the Baltic Sea to the Adriatic Sea and the Black Sea: Austria, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia and Slovenia. All, except Austria, experienced some form of communist rule and have joined the EU since 1986. Though the initial focus was on infrastructure, the remit has broadened, as signalled by President Trump's presence at

the Three Seas Warsaw summit in 2017.

These new groupings are overlapping and untried. They cannot on their own substitute for the clout and credibility of structures with tried and tested formal decision-making, such as the EU and NATO. But in some circumstances they may offer greater speed and flexibility. Instead of the lumbering 29-country NATO bureaucracy, with its vulnerability to vetoes and delays, the new coalitions can bring together countries that are likely to share similar perceptions of the threat, and to trust each other to contribute speedily and effectively in dealing with it.

Many more such security arrangements are needed. Sometimes the US will be a conditional partner, other times it will be absent. Some of these groupings will be loose; others such as those dealing with counter-terrorism, will be tightly knit.

The trajectory of these efforts is encouraging. But so far the pace is too slow and the costs high – German-Dutch military integration efforts, for example, have at least initially constrained rather than boosted capability. The gap between Russia's ability to attack and the West's ability to defend is growing, not shrinking. And Europe's ramshackle security architecture is facing a wholly new challenge: China.

Sixteen plus one: China's divide-and-rule strategy in Europe

China's efforts in the CEE region first attracted attention with the inaugural 16+1 summit in April 2012. The format is striking in several respects. It lumps together sixteen CEE countries of widely varying background, size, economic heft and geopolitical outlook. It gives China an overwhelming diplomatic and tactical advantage: the sixteen countries do not form any kind of grouping. Instead, as the Czech analyst Martin Hála points out, the format packages sixteen separate bilateral relationships in a convenient diplomatic framework in which the countries are competing for Chinese favour:¹⁰

Czech President Miloš Zeman has publicly offered his country as an 'unsinkable aircraft carrier for China in Europe,' and Serbian politicians have mused about standing out as the best student in China's class in a way that would transform the '16+1' into a '15+1+1'.

The initial vague and grandiose rhetoric has given way to a sharp focus on infrastructure, in the form of President Xi Jinping's Belt and Road Initiative.¹¹ But the focus is deceptive. The reason for the Chinese focus is less that the sixteen countries are economically attractive – they make about one tenth of Chinese trade with Europe – than

that they are politically vulnerable. The sixteen countries' own economic involvement in China is minimal. They do not have domestic industries worried about loss of intellectual property to Chinese espionage. As open economies, they are not worried by cheap Chinese manufactured exports. And being mostly poorer than the European average, they find Chinese inducements especially attractive.

The reason for the Chinese focus is less that the sixteen countries are economically attractive – they make about one tenth of Chinese trade with Europe – than that they are politically vulnerable.

There are risks in these inducements. As the Slovak analysts Richard Turcsányi and Matej Šimalčík noted in a recent article,¹² China prefers construction projects based on direct agreements with national governments, involving credits with state-backed repayment guarantees, direct selection of Chinese contractors and the use Chinese materials and labour. This non-transparent process creates opportunities for cost-padding and corruption and is in clear violation of EU public contracting regulations. Second, these credits are costly. The

projects are not subsidised by the Chinese taxpayer; EU members would normally be able to borrow more cheaply elsewhere. The projects are attractive only if some other factors, such as personal gain or geopolitical posturing, are in play. Third, using Chinese labour and materials reduces the 'multiplier effect' which boosts the positive effect of conventional projects. Few if any extra jobs are created. The money paid for wages and other costs flows to China.

A leading example of Chinese 'construction politics' is the Belgrade-Budapest rail link, part of the Land-Sea Express Route between Hungary and the Greek port of Piraeus (owned by the Chinese company Cosco Pacific). First announced in 2013 at a 16+1 summit in Bucharest, this USD 2.89 billion, 350 km project has suffered repeated delays. The Hungarian side faces a European Commission inquiry into the evident breach of EU rules. Another example in the Western Balkans is the Bar-Boljare highway in Montenegro, which attracted criticism from the IMF because of its potential burden on public finances.

This model is in collision with the EU, for now chiefly over infrastructure projects. The Brussels rules stipulate clear public tenders for state-backed construction, ensuring open competition and minimising the scope for influence-peddling and bribery. China's model is secretive and ad hoc: construction projects are the result of political negotiation, not a response to an

objectively assessed public need. This, unfortunately, is increasingly attractive from the viewpoint of some European politicians, who regard the EU's rules as onerous and intrusive. As the EU tries to apply pressure to countries such as Hungary and Poland in response to their breaches of EU rules, China is an increasingly attractive alternative.

Rows over infrastructure projects are therefore just a harbinger of a deeper clash ahead. China's economic diplomacy and the 16+1 format have prompted severe criticism from some European leaders and attract increasing controversy. But the approach has already paid political dividends. The ex-communist countries used to be ardent supporters of human rights in Tibet: the Dalai Lama was one of the first foreign leaders to be invited to Prague Castle by Václav Havel after the 1989 Velvet Revolution in Czechoslovakia. Now the Tibet spiritual leader is lucky if he meets even a handful of parliamentary deputies and municipal politicians during his travels in the CEE region. In July 2016, Hungary and Greece tried to weaken the EU's stance on Chinese claims in the South China Sea. In March 2017, Hungary refused to sign an EU letter decrying the torture of jailed Chinese lawyers.

Beyond such diplomatic divide and rule games something deeper may be afoot. As Hála argues, the real purpose of 16+1 is the export of China's model of state capitalism,

in which market mechanisms are tools in the hands of the party-state.

The countries in the 16+1, he says, face a choice:

between open-tender requirements and contracts awarded via political deals; between economic competition and the collusion of economic and political interests; and finally, between democratic capitalism and a state capitalism dominated by shadowy oligarch networks.

Just the same could be said about Russian tactics. Geopolitics never really went away after 1989-91. But it is now back. Old structures are weakening and new threats rising. The 3S region is facing the eye of the storm, perilously short of friends, ideas and will-power.

ACTION POINTS:

1. Do not talk of 'fake news' or treat information operations as a discrete problem. We face influence operations in which propaganda is just one part and not necessarily the biggest or most important.
2. Nor is the problem new. The Soviet Union waged political warfare for decades.
3. Do not assume that Russia is the only adversary. China is trying to subvert, divide and dominate too.
4. Do not talk of 'frontline states'. Every country has vulnerabilities.
5. Do not assume that the Atlantic Alliance is doomed. Fight to preserve it.
6. Do not assume that the Atlantic Alliance will survive. Look for alternatives. Keep Britain involved in European security post-Brexit.
7. Old structures (EU, NATO) are increasingly irrelevant or insufficient: too big, too divided, too rigid, too slow, too sleepy. Instead, build coalitions of the willing, capable and threat-aware, domestically and internationally.
8. Corruption and the politicised use of money are the West's Achilles heel. Enforce laws, especially on rich and powerful people. Pass new ones if necessary, for example on corporate anonymity.
9. End the climate of impunity for influence operations. Catch Russian spies. Deport or jail them. Prosecute those they recruited.
10. Boost military resilience in the Baltic and Black Sea regions, but rethink deterrence, making it less dependent on nuclear and other military options.



SOURCES:

1. Edward Lucas is a London-based security-policy expert. He was a reporter for international media behind the Iron Curtain and in Yugoslavia during the cold war, witnessing the collapse of communism in Czechoslovakia, and the rebirth of independence in the Baltic states. After many years with *The Economist*, the London-based newsweekly, he is now a columnist for the *London Times* and other publications, and a senior vice-president at the Center for European Policy Analysis, a think-tank with offices in Warsaw and in Washington, DC.
2. Albania, Bosnia and Herzegovina, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Montenegro, Poland, Romania, Serbia, Slovakia, Slovenia, Macedonia. The answer seems to be that the initiative is for ex-communist countries outside the former Soviet border, with the exception for the Baltic states.
3. Nor was 'eastern Europe' ever a homogenous category. Romania's nationalist personality cult owed little to Marxism-Leninism, and pursued its own foreign policy orientation, recognising Israel and flirting with Western countries. Hungary liberalised its economy for small-scale private enterprise far more than other COMECON members, in a policy known as 'goulash communism'. The Baltic states, independent until 1940, were occupied and annexed by the Soviet Union; other countries in the Soviet empire retained at least nominal sovereignty. By contrast two Soviet Socialist Republics, Ukraine and what was then called Byelorussia (now Belarus) enjoyed no real independence but were members of the United Nations. These diplomatic puppets suddenly sprang to life as the Soviet Union began to disintegrate.
4. Among the rival locations claiming to be the continent's geographic centre are a Lithuanian village, an Estonian island, a small town in western Ukraine, and at least three places in Belarus. Attempts to elaborate the definition, such as 'East-Central Europe' (Oskar Halecki) and 'Middle Europe' (Michael Foucher) have largely fallen into disuse. The term 'Mitteleuropa', which has a nostalgic and at times fashionable ring, dates from an era in the 19th century when Germany sought geopolitical, cultural and economic domination of neighbouring regions. During the interwar years, 'central Europe' referred to the countries born out of the 1918 post-war settlement – Poland, Czechoslovakia, the republic of Hungary, Yugoslavia – with the addition, sometimes, of Romania. It was revived by Milan Kundera in his landmark article, 'The Tragedy of Central Europe' in the *New York Review of Books* in 1984, which highlighted the unwilling captivity of the Poles, Czechs, Slovaks and Hungarians in the Soviet empire, and the neglect and apathy they experienced from their cultural soul-mates in the continent's west. Yet that was at best a partial view: the same lament applied to Russian dissidents, or those yearning for independence in the Baltic states.
5. The shortcomings in this, however, are obvious: in what sense are Estonia or Albania part of 'central Europe' when the great Austro-Hungarian (and then Polish) city now called Lviv, is not? Why should Austria, the region's historic cultural hub for literature, art and music, and the former geopolitical hegemon, be arbitrarily divorced from its central European connections? Sub-categories such as 'Baltics', 'Western Balkans' or 'South-Eastern Europe' add some logical consistency but do solve the fundamental problems.
6. The Helsinki Final Act of 1975 established that borders in Europe would never again be changed by force. The Paris Charter of 1990 established common principles of political freedom, human rights and the rule of law. The Soviet Union signed both. The Russian Federation is its legal successor and is bound by the same undertakings, as well as the Budapest Memorandum of 1994, which guaranteed Ukraine's territorial integrity in exchange for its renunciation of its nuclear arsenal. Russia has flouted all these undertakings, and more besides.
7. Views on whether China is a partner or rival vary widely.
8. A geopolitical trophy carved out of the pre-war German territory of East Prussia.
9. Rakich N. and Mehta D., (2018, July 13). Is Trump Fueling Republicans' Concerns About NATO, Or Echoing Them?. *FiveThirtyEight* [on-line]. Available at: <https://fivethirtyeight.com/features/is-trump-fueling-republicans-concerns-about-nato-or-echoing-them/>.
10. Hála M. (2018, April 13). Europe's new 'Eastern bloc': Beijing's diplomatic masterstroke has put former Soviet countries on a collision course with Brussels. *Politico* [on-line]. Available at: <https://www.politico.eu/article/europes-new-eastern-bloc-china-economy-model-belt-road-initiative/>.
11. Originally called the New Silk Road, this project was renamed One Belt, One Road and is now known simply as Belt and Road.
12. Asia Research Institute (2018, August 28). Pitfalls of Slovakia's Chinese dreams [on-line]. Available at: <http://theasiadialogue.com/2018/08/28/pitfalls-of-slovakias-chinese-dreams/>.



Ministry
of Foreign Affairs
Republic of Poland

Public task co-financed by the Ministry of Foreign Affairs
of the Republic of Poland under the competition
'Support for the civil and municipal dimension
of Poland's foreign policy 2018'.

The publication presents the opinions of its authors
and cannot be equated with the official position
of the Ministry of Foreign Affairs of the Republic of Poland.

PARTNERS OF THE DIGITAL 3 SEAS INITIATIVE:



INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
RKK ICDS

IN COOPERATION WITH:

