European
Commission

October 2020

Advanced Technologies for Industry – Policy brief

Cybersecurity: more investment and better skills

This report was written by Kincsö Izsak and Palina Shauchuk from Technopolis Group.

EUROPEAN COMMISSION

Executive Agency for Small and Medium-sized Enterprises (EASME)
Unit A.1.2 — COSME
E-mail: EASME-COSME-ENQUIRIES@ec.europa.eu

Directorate General for Internal Market, Industry, Entrepreneurship and SMEs
Unit F.1 — Industrial Strategy and Value Chains
Unit F.2 — Social Economy
E-mail: GROW-ATI@ec.europa.eu

European Commission
B-1049 Brussels

LEGAL NOTICE

The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of EASME or of the Commission. Neither EASME, nor the Commission can guarantee the accuracy of the data included in this study. Neither EASME, nor the Commission or any person acting on their behalf may be held responsible for the use, which may be made of the information contained therein.

More information on the European Union is available on the Internet (http://www.europa.eu).

Print ISBN 978-92-9460-256-5 doi: 10.2826/639302 EA-02-20-820-EN-C
PDF ISBN 978-92-9460-255-8 doi: 10.2826/374793 EA-02-20-820-EN-N

October 2020

Table of contents

Section 1

1. Background

As digital transformation is accelerating around the world and an increasingly larger share of the interactions is hosted online, citizens, companies and governments are being more and more exposed to cyber threats and digital crimes. As a consequence of a network-enabled, interconnected economy and society, cybersecurity and privacy are areas of major policy concern. Hacked and breached data are becoming especially more common as a result of using connected devices powered by the Internet of Things. The COVID-19 pandemic also had an impact on cybercrime that has soared since the start of the outbreak.

According to Accenture, digital security breaches have increased by 11% since 2018[1]. Phishing has seen a spike in particular. The famous global Wannacry ransomware and NotPetya wiper malware attacks are some examples that affected more than 320 000 victims in around 150 countries. Effective protection against such cyber-attacks is the core objective of cybersecurity technologies.

Cybersecurity is defined as "*all the safeguards and measures adopted to defend information systems and their users against unauthorised access, attack and damage to ensure the confidentiality, integrity and availability of data*[2]". It includes the protection of networks, devices and data from cyber-attack through encryption, monitoring, identity management, authentication, network architecture, scheduled backups, firewalls and mobile device management.

Countries and businesses made significant efforts to strengthen their capabilities to respond to cyber-attacks, although the impact of cyber-crimes has been devastating[3]. Malware is the primary method to carry out malicious activity in the cyberspace by exploiting existing vulnerabilities. Ransomware encrypts data, preventing users from accessing their files until a ransom is paid, typically in cryptocurrency. Users can be also manipulated into disclosing confidential information.

The Council of the European Union in its conclusions on 'Shaping Europe's Digital Future'[4] underlined the importance of cybersecurity as "a key component for a digitalised Single Market, as it ensures trust in digital technology and the digital transformation process". The EU also supports the need for a coordinated approach to mitigate risks related to cybersecurity and to ensure a secure 5G deployment.

In this context, this policy brief has two main goals:

- first of all, it provides new evidence on EU strengths and weaknesses in cybersecurity technologies and about the potential of the European cybersecurity industry
- secondly it reviews EU- and national level policies and policy measures that can enhance cybersecurity capabilities and stimulate a stronger cybersecurity industry.

The full methodology behind the data calculations is available here: https://ati.ec.europa.eu/reports/eu-reports/advanced-technologies-industry-methodological-report .

[1] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[2] European Court of Auditors (2019). Challenges to effective EU cybersecurity policy, Briefing Paper

[3] ENISA

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

Section 2

2. Need for stronger investment and better skills in cybersecurity

The US boasts the highest average share of global patent applications in digital Security technologies in the 2013-2017 period (32%), followed by the **EU27 in the second place, owning 23% of the world patent applications** and China (18%).

The EU27 shows strengths at the level of producing cybersecurity technologies. It has unique expertise and a strong research community in **postquantum cryptography**, leading in secure implementations of **cryptographic algorithms** in both hardware and software.

Cybersecurity spending and investments in the EU27 are way behind the US. Total global cybersecurity spending of the EU as a percentage of GDP is estimated to be below US. The **investment gap in cybersecurity between the EU27 and US** is also confirmed by the analysis of venture capital data based on Crunchbase and Dealroom. The findings show that the EU27 is far behind the US and also behind China.

The share of professionals with cybersecurity skills and employed in selected industries has been compared in the case of the US and the EU27 based on LinkedIn data. The **US has relatively higher shares of cybersecurity professionals than the EU27 in all industries investigated including ICT, finance, electronics, medical devices, automotive, chemicals** and also stronger overall, which indicates not just an important skills gap in cybersecurity but also a lower uptake of these technologies in Europe than in the US.

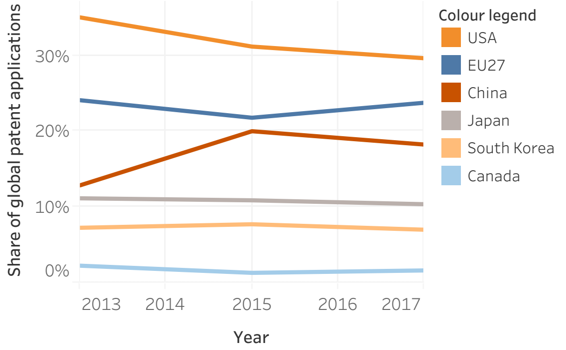
2.1 Strong research and development and relatively high digital security patent applications

The European Union has a strong base in cybersecurity in terms of academic research, industrial research and product development related activities. The EU is amongst the world leaders in quantum technologies research and innovation with a level of investment in R&D that is similar to the US[5].

Technological trends and development have been captured through patent analysis and the evolution of patents has been analysed specifically for digital Security[6] technologies. Figure 1 displays the share of global digital Security patent applications for EU27 relative to major competitors.

Leading economies with the highest share of total patent applications in Security is the US with an average share of approx. 32% of global patent applications in the 2013-2017 period, followed by **the EU27, owning 23% of the world patent applications in digital Security,** and China (18%). Over time declining trends can be observed in the share of global Security patent applications in the case of the US and China.

Figure 1: Share of global patent applications in digital security (2013-2017)



Source: Fraunhofer ISI calculations, 2019

The EU27 has the second highest share of international patent applications and shows strengths at the level of producing cybersecurity technologies.

Europe has unique expertise and a strong research community in postquantum cryptography, leading in secure implementations of cryptographic algorithms in both hardware and software. Also, in cryptography where there currently are almost 30 billion cryptographic devices, where around half uses public key cryptography; a significant part of this market is shaped by respectively

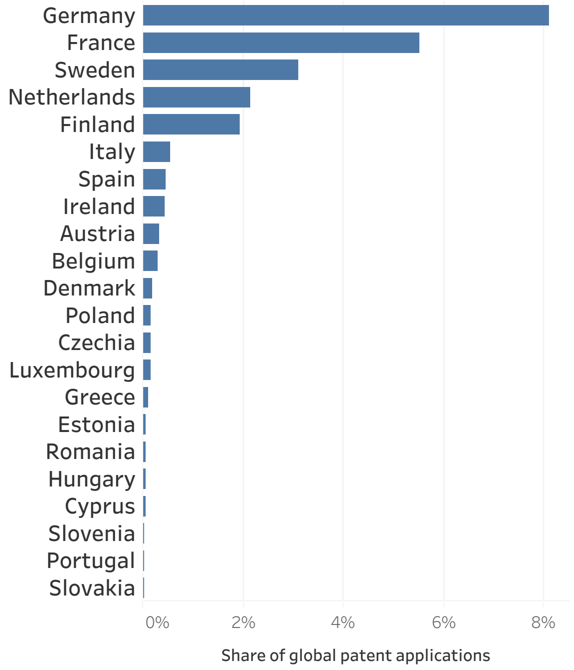
[5] European Commission, 2019

[6] Digital security has been defined through IPC codes in the patent analysis. The IPC codes are presented in the ATI methodological report.

secure integrated chips or system on a chip where Europe has a leading position[7].

Within the EU27, **especially France and Germany** contribute to EU strengths in cybersecurity patenting. They are followed up by **Sweden, Netherlands and Finland** as displayed in Figure 2.

Figure 2: Share of global patent applications in digital security (2013-2017)

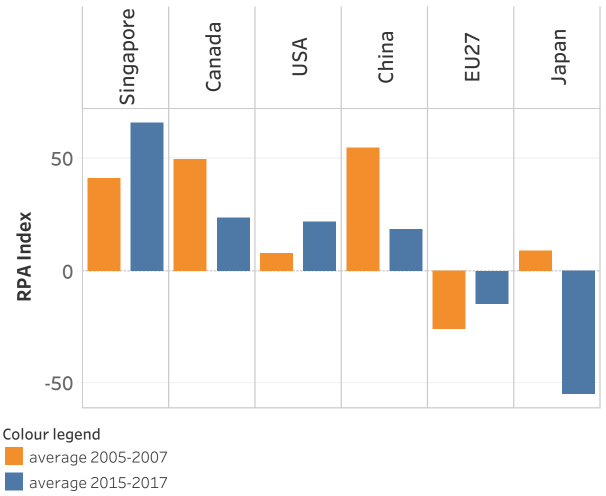


Source: Fraunhofer ISI calculations, 2019

The revealed patent advantage index (RPA)[8] – as presented in Figure 3 – displays the extent to which countries have specialised in digital Security. Among the most specialised countries at the global level are Canada, US and China. The **EU27 has relative weak specialisation, although its specialisation index has become stronger in the most recent period**.

Among the EU Member States that have also the highest share of global patents in security, Sweden and France are the most specialised. Germany is characterised as a country with a weak specialisation index. Based on the RPA analysis, most European countries are generally relatively unspecialised or have a rather weak specialisation in the field of digital security. Figure 4 presents the RPA index for all EU Member States that had filed transnational patent applications in Security. The results should be interpreted in the light of the total number of patent applications (countries with a low number of patents can be naturally more specialised).

Figure 3: Change in Revealed Patent Advantage (RPA) Index in Cybersecurity (2005-2007; 2015-2017), international comparison



Source: Fraunhofer calculations, 2019

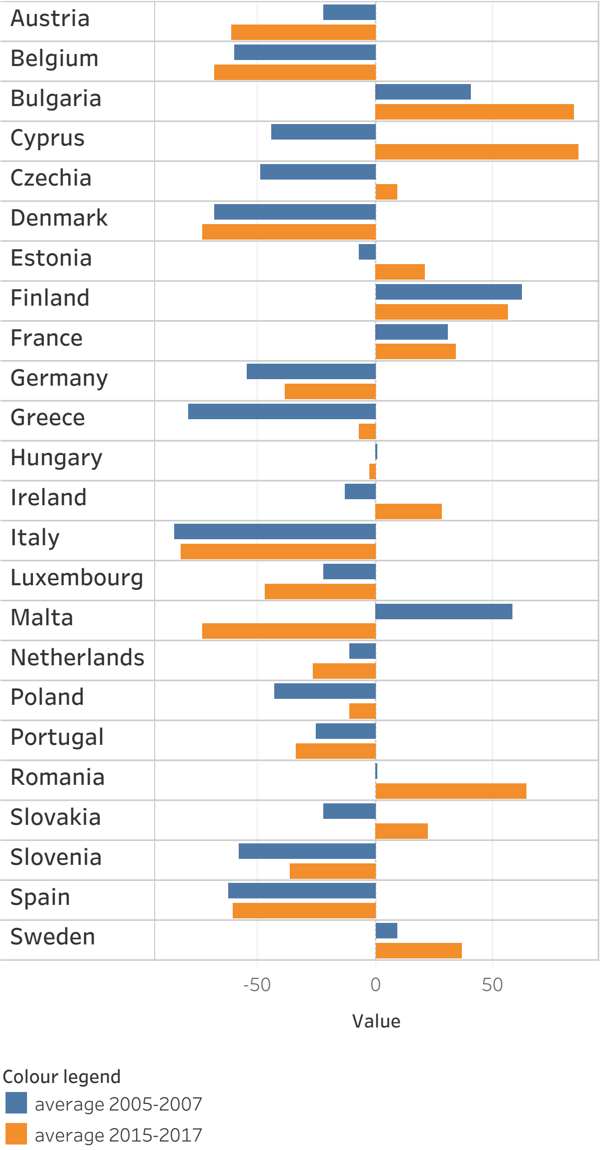
The above analysis of international patent applications shows European strengths in research and development in cybersecurity overall, but it also reveals a relative weakness compared to the US. With regard to the areas that would need more focus, the European Union Agency for Network and Information and Security pointed out especially the need for additional R&D activities in Artificial Intelligence related cybersecurity risks, quantum technologies, complexity of interconnectedness, cybercrime of digital identities and assets, as well as privacy[9].

[7] Capgemini (2019) Analytical report on cybersecurity

[8] The RPA indices between -100 and -60 indicate an absence of specialisation, whereas values between -60 and -20 points to a weak specialisation, between -20 and +20 to an average specialisation, between +20 and +60 to an above average specialisation and between +60 and +100 to a strong specialisation.

[9] ENISA, 2019

Figure 4: Change in Revealed Patent Advantage (RPA) Index in Cybersecurity (2005-2007; 2015-2017), EU Member States



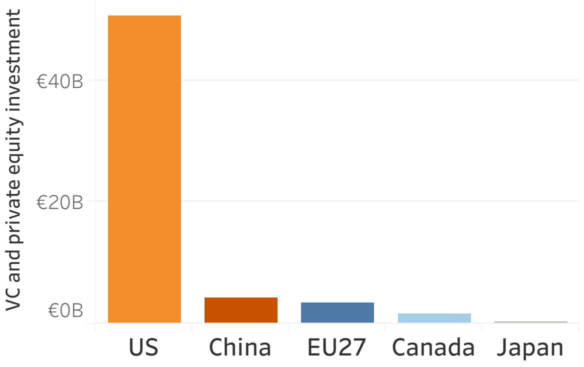
Source: Fraunhofer calculations, 2019

2.2 Still relatively low investment and startups in EU cybersecurity industry

Cybersecurity spending and investments in the EU27 are way behind the US. Total global cybersecurity spending as a percentage of GDP is estimated to be about 0.1%, while in the US, this rises to about 0.35% (including the private sector)[10]. Current public cybersecurity investments in the EU are estimated to be between €1-2 bn per year, which is far behind the US government investments (€13.3 bn per year) and China (€8.8 bn)[11].

The investment gap in cybersecurity between the EU27 and US is also confirmed by the analysis of venture capital data based on Crunchbase and Dealroom. Figure 5 presents the total amount invested in cybersecurity startups and companies since 2010. The findings show that the EU27 is far behind the US (even if data are less representative for the EU, the gap is evident) and also behind China.

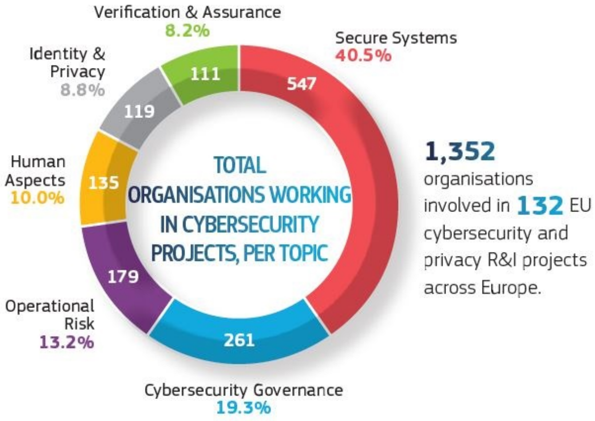
Figure 5: Venture capital and private equity investment in cybersecurity firms (2010-2019)



Source: Technopolis Group based on Crunchbase and Dealroom

Despite the weaknesses in VC, the European Union invests heavily in cybersecurity and for instance dedicated €160 m under the Horizon 2020 Research and Innovation Framework Programme (H2020) in cybersecurity research and innovation projects. Figure 6 shows the types of investments.

Figure 6: Type of investments in cybersecurity



Source: European Commission, 2020

The main challenge for the European cybersecurity industry is that the biggest players and service providers are non-European[12], as it has been highlighted in several studies. This is also indicated to some extent by

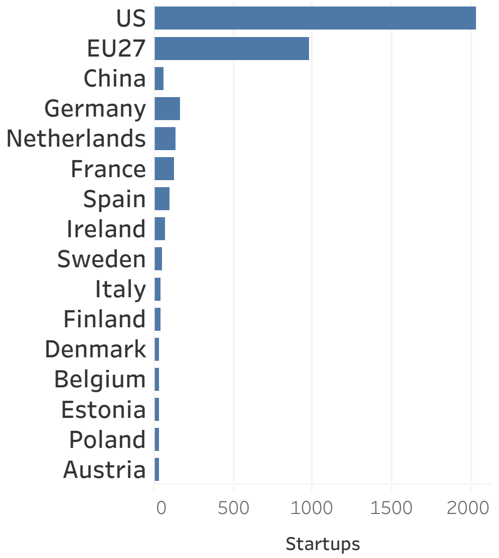
[10] European Court of Auditors (2019)

[11] Strategic Forum for Important Projects of Common European Interest

[12] Strategic Forum for Important Projects of Common European Interest

the analysis of startups in the area of cybersecurity based on Crunchbase and Dealroom data. The US startup landscape has been much more dynamic in cybersecurity related ventures than the EU27. EU Member States that are the most active in founding cybersecurity startups are **Germany, Netherlands, France, Spain and Ireland**. The numbers presented in Figure 7 should be interpreted with caution taking into account the overall size of the economy and IT sector in each country.

Figure 7: Startups in cybersecurity founded after 2010



Source: Technopolis Group based on Crunchbase and Dealroom

2.3 Professionals with cybersecurity skills lagging behind

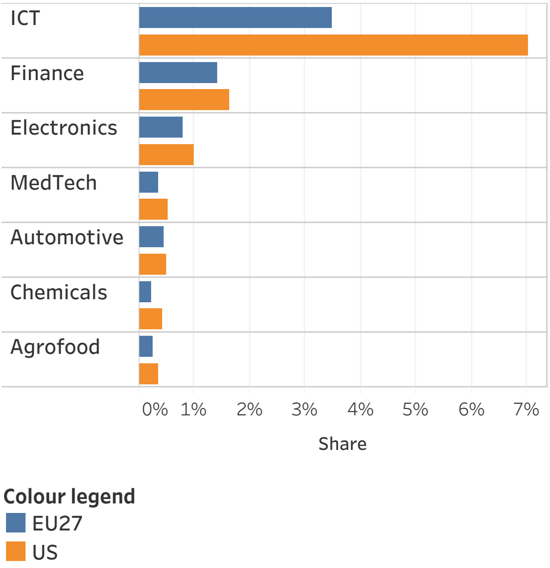
The need for increasing European efforts for better cybersecurity skills has been highlighted in various recent communication and studies[13]. According to the 2019 cybersecurity workforce study there is a shortage of approximately 291 000 cybersecurity professionals in Europe. On the one hand there is an insufficient supply of cybersecurity professionals, but there is also a mismatch in terms of the quality of cybersecurity skills to face current cyber challenges.

In order to reflect about the supply and demand of cybersecurity professionals, an analysis of LinkedIn data was conducted for the purposes of this report. To harvest the data from LinkedIn, keywords capturing skills by advanced technology have been defined and queries have subsequently been constructed to filter the database by location and industry. Data have been captured in the EU27 in three data points (November, December 2019 and January 2020).

The share of professionals with cybersecurity skills and employed in selected industries has been compared in the case of the US and the EU27. The representativeness of the LinkedIn sample has been assessed against several criteria including the level of education, gender and the share of registered users in information and communications technology compared to the actual active population in these fields in each individual country resulting in a corrective weighting.

As Figure 8 shows, **the US has relatively higher shares of cybersecurity professionals than the EU27** in all industries investigated including ICT, finance, electronics, medical devices, automotive, chemicals. The overall weighted score for cybersecurity professionals is also much higher in the case of the US than the EU27 and the gap is particularly high compared to other digital technologies such as Artificial Intelligence or Big Data.

Figure 8: Share of professionals with cybersecurity skills employed in different industries in the EU27 and US



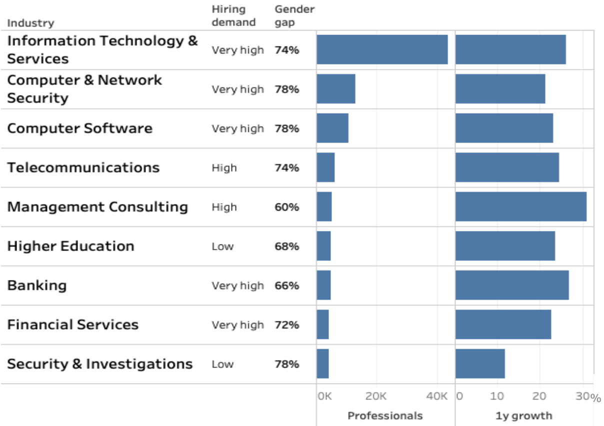
Source: Technopolis Group based on LinkedIn analysis

Among different industries that absorb cybersecurity skilled professionals, the most dominant one (see Figure 9) is the IT industry (Information technology and Services), followed by Telecommunications and Management Consulting. Especially in Information technology and Services as well as Banking and Financial

[13] eg. European Commission (2013). EU Cyber Security strategy: An open, safe and secure Cyberspace, Brussels, 7.2.2013; ENISA (2019). Cybersecurity skills development in the EU

Services there is a strong demand for professionals with cybersecurity skills. The highest growth of skills in cybersecurity from 2018 to 2019 in the top 10 industries is observed in the Management Consulting industry, followed by Information technology and Services and Banking industries.

Figure 9: Sectors employing the highest share of professionals with cybersecurity skills and their 1 year growth (in %) from 2018-2019 in the EU27



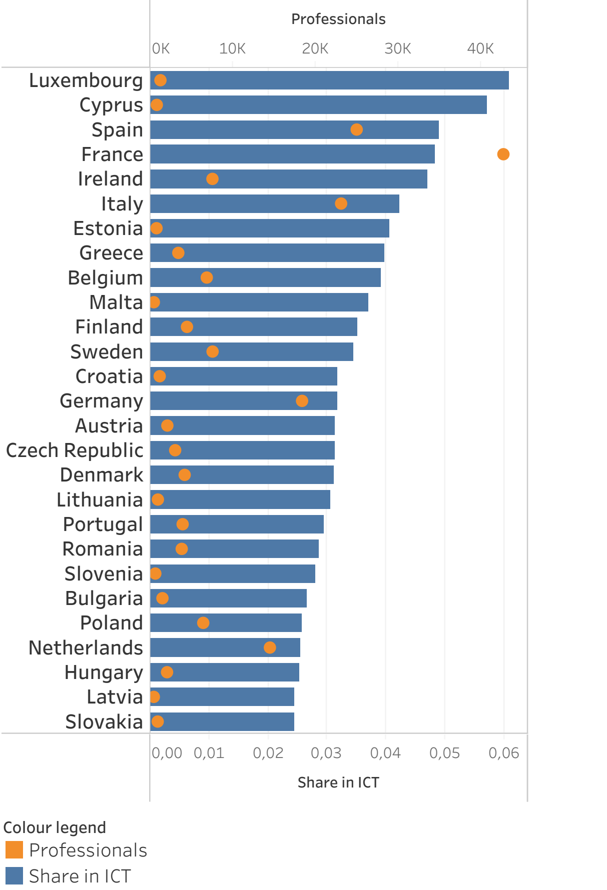
Source: Technopolis Group based on LinkedIn analysis

Within the EU the countries with the highest share of professionals with specific technological skills in cybersecurity include **Luxembourg, Cyprus, Spain, France, Ireland, Italy and Estonia**. Figure 10 visualises the graphical concentration of cybersecurity skills. 86% of professionals with cybersecurity skills are men that points at a **large gender gap** in the field. Countries where the gap is relatively smaller and employ more women in the area are Italy, Romania and Ireland.

The highest growth of skills in cybersecurity from 2018 to 2019 in the top 10 countries is observed in France (+34%), Poland, Spain and Italy (see Figure 11). The demand for specialists in cybersecurity is high in most of the European countries but especially relevant in France, Ireland, Germany, Romania, Poland, Belgium and the Netherlands where the most job ads related to cybersecurity specialists have been published in the past year.

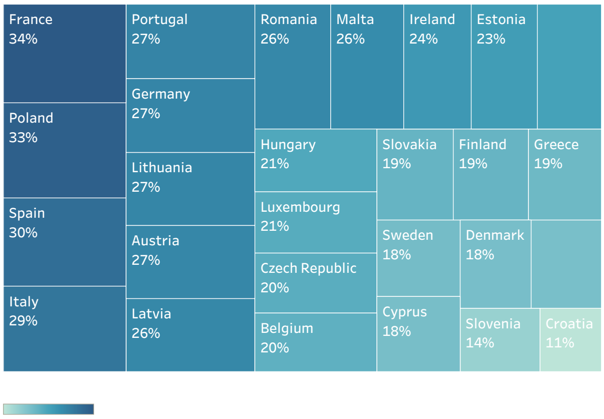
The hiring demand for cybersecurity professionals is in general very high across countries and industries and job advertisements remain unfilled for a longer time. Indeed, as the Information Systems Audit and Control Association also found in 2019, 58% of organisations have unfilled cybersecurity vacancies and that for 60% of them it takes a minimum of 3 months before a position is filled[14].

Figure 10: Share of professionals with cybersecurity skills within ICT, 2019



Source: Technopolis Group based on LinkedIn analysis

Figure 11: 1-year growth in the number of professionals with cybersecurity skills, 2018-2019



Source: Technopolis Group based on LinkedIn analysis

[14] ENISA (2019). Cybersecurity skills development in the EU

Section 3

3. Cybersecurity policies

The objective of the **new EU Cybersecurity Strategy** that has been put forward as part of the recovery plan in 2020 is to 1) further boost EU-level cooperation, knowledge and capacity, 2) strengthen EU industrial capabilities and partnerships, 3) encourage the emergence of SMEs in the field and 4) protect critical infrastructure.

The **European Cybersecurity Act** entered into force in June 2019 and established an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

The Strategic Forum for Important Projects of Common European Interest (IPCEI) developed a **common vision for "Cybersecurity in Europe by 2030**", serving as a guide for formulating, prioritising and coordinating recommendations for actions.

There are still various gaps in national and European level cybersecurity strategies such as lack of necessary capabilities to defend against new cyber challenges, skills shortages in cybersecurity, lack of entrepreneurship and funding gaps especially in the growth phase that prevent SMEs from expanding into new markets.

As presented in Section 2, while the EU27 has a strong research and technology base in cybersecurity technologies, it is lagging behind especially in terms of investment and skilled professionals with cybersecurity skills employed in European industry. In the light of this challenges, this section will review the existing policy measures at European and national level.

3.1 European cybersecurity policy

In the recovery plan published in May 2020 'Europe's moment: Repair and Prepare for the Next Generation', the European Commission put forward a proposal for **a new Cybersecurity Strategy.** The objective is to further boost EU-level cooperation, knowledge and capacity. The strategy is expected to strengthen EU industrial capabilities and partnerships, encourage the emergence of SMEs in the field and protect critical infrastructure. In the current strategy, the emphasis is on building greater strategic autonomy and boosting capabilities in terms of technology and skills, along with the building of a strong single market in the area of cybersecurity.

The **European Cybersecurity Act** entered into force in June 2019 and established an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices. It reinforced the mandate of the European Union Agency for Network and Information and Security, ENISA so as to better support Member States with tackling cybersecurity threats and attacks. ENISA is mandated to increase cybersecurity capabilities at EU level and support capacity building and preparedness working closely together with Members States.[15]

The European Commission and the European Cyber Security Organisation (ECSO) signed a **cybersecurity contractual public-private partnership cPPP** in 2016 with the objective to fostering cooperation between public and private actors at early stages of the research and innovation process. The cPPP aims to stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions. It includes a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes, brought together under the umbrella of ECSO. The EU will invest up to €450 m in this partnership, under its research and innovation programme Horizon 2020.

The European Commission has committed to setting up a **European Cybersecurity Industrial, Technology and Research Competence Centre**, a Network of National Coordination Centres and a Cybersecurity Competence Community.[16] The proposal aims to strengthen the Union's cybersecurity capacity by stimulating the European technological and industrial cybersecurity ecosystem as well as coordinating and pooling related resources.

Cybersecurity is a key pillar of the effective **EU Security Union**, which supports Member States in cyber defence, implementing the EU Cyber

[15] https://www.enisa.europa.eu/about-enisa

[16] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf

Defence Policy Framework[17]. Moreover, cybersecurity of 5G networks is also priority across Europe.

The European Commission and the European Investment Fund have launched the so-called **Digitalisation Pilot under the COSME Loan Guarantee Facility** in 2019 with the aim to providing support under the programme specifically for the purpose of digital transformation of SMEs including the area of cybersecurity.

Cybersecurity is one of the six key sectors selected under the **Blueprint for Sectoral Cooperation on Skills in the 2019** Work Programme for Erasmus+. The Sector Skills Alliances aim to tackle skills shortages in specific sectors. As it was also shown in the previous section, there are too few cybersecurity professionals available with the necessary skills on the evolving EU labour market[18].

Strategic Forum for IPCEI on Cybersecurity

The Strategic Forum for Important Projects of Common European Interest (IPCEI) developed a common vision for "Cybersecurity in Europe by 2030", serving as a guide for formulating, prioritising and coordinating recommendations for actions. This vision aims at ensuring the competitiveness of the EU cybersecurity industry on the global cybersecurity market and increasing levels of protection with appropriate cybersecurity solution. The EU shall also increase its autonomy and technological sovereignty in cybersecurity and achieve global industrial leadership.

Coordinated investments suggested are the following:

*1. Secure **5G for cybersecurity innovation** and services*

*2. **Sharing** and exploiting **information** on threats, vulnerability and incidents*

*3. Secure highly **critical applications** and essential services: electricity, gas, water, vehicles*

*4. Develop and deploy end-to-end data protection solutions using **advanced cryptography***

*5. European **Data Space**: create a framework and infrastructure for secure data communication, storage and handling*

3.2 National policies

Countries foster knowledge, raise awareness and build capacity to support better cybersecurity measures.

Several scoreboards exist that aim at measuring national preparedness against cyber-attacks. The Global Cybersecurity Index (GCI)[19] captures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars such as legal, technical, organisational measures, capacity building and cooperation. According to this index, there is a wide gap in cyber commitment around the world. Within **the most committed EU countries, we find France, Lithuania, Estonia and Spain**.

The National Cyber Security Index measures countries' cyber security ratings in the world. According to this different measurement, the top ten countries best prepared against cyber-attacks are **Greece, Czechia and Estonia, Lithuania, Spain, Croatia, France, Finland, Denmark and Netherlands**. To date, the NCSI includes cyber security data on 160 countries[20] and focuses on measurable aspects of cyber security implemented by the central government.

A ranking of countries in the field of cybersecurity has been also established by Comparitech that found Denmark to be the most cyber-secure country in the world in 2019[21]. Other top-performing countries include Sweden, Germany, Ireland and Japan. France, Canada and the United States were pushed out of the top five most cyber-secure countries into ninth, sixth and 17th place.

All EU Members States have their own national strategies for cybersecurity which are a collection of planned actions to improve the security and resilience of national infrastructures and services. An overview of examples of national cybersecurity strategies is presented in Table 1.

[17] EU Cyber Defence Policy Framework (2018 update) as adopted by the Council on 19 November 2018 (14413/18).

[18] https://ec.europa.eu/digital-single-market/en/news/sector-skills-alliance-cybersecurity-open-call-deadline-approaching

[19] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[20] 1. Legislation in force – legal acts, regulations, orders, etc.
2. Established units – existing organisations, departments, etc.
3. Cooperation formats – committees, working groups, etc.
4. Outcomes – policies, exercises, technologies, websites, programmes, etc.

[21] https://www.comparitech.com/

Table 1: Examples of national cybersecurity strategies

Country	***Title***	***Description***	***Budget***
Denmark	Danish Cyber and Information Security Strategy (2018)[22]	The national plan covers 25 concrete initiatives focussing on the enhancement of technological resilience of digital infrastructure; improving skills and know-how; and strengthen national coordination and co-operation on information security. It has a strong sectoral focus covering energy, healthcare, transport, telecommunication, maritime and financial sectors.	Government to invest up to €1.5 bn overall in cyber and security over next few years.
Estonia	New cybersecurity strategy 2019-2022 (in preparation)[23]	The strategy focusses on increasing technological and organisational capacities in the Estonian digital ecosystem, providing cross-sectoral priorities, including recognising cybersecurity as a wider priority for the Estonian society, and planning the resources necessary for the corresponding activities.	Budget not disclosed for new strategy but the four-year cost for the previous 2014-2017 strategy covering was approx. €16 m.[24]
France	Cyber Defence Pact (2014-2019)[25]	The pact aims to (1) raise the level of information system security and the Ministry of Defence's resources for cyber defence; (2) to scale up research in support of industry base; (3) reinforce human resources for cyber defence; (4) development of cyber defence centre; (5) promote emergence of national cyber defence community; and (6) cultivate a network of foreign partners.	€1 bn dedicated to cyber defence investments.
Germany	Cyber defence training pact[26]	A training collaboration initiative by the German Armed Forces and Deutsche Telekom to jointly train 15 000 soldiers and civilians by 2022. The initiative will be implemented through a network of commercial and federal information security hubs, regular information exchange and hosting of cyber experts for skill exchanges.	Budget not identified.
Spain	National Cyber Security Strategy (2013)	A comprehensive strategy outlining objectives and lines of actions. It covers (1) security of information and telecommunication systems; (2) security and resilience of networks and information systems and critical infrastructures; (3) prevention and coordination capabilities; (4) cyberspace awareness; (5) capacity building in terms of know-how and technology; and (6) international collaboration.	Budget not identified.
Netherlands	Dutch Cybersecurity Agenda[27]	The agenda overall seeks to support Dutch stakeholders in capitalising on the economic and social opportunities of digitalisation in a secure manner. It comprises 7 ambitions for: (1) digital capabilities to detect and respond to cyber threats; (2) contribution to international security in digital field; (3) being at forefront of digital secure hardware/software; (4) resilient digital processes and infrastructure; (5)	Structural investments of €95m

[22] https://www.fmn.dk/eng/news/Pages/New-sectoral-strategie-stop-repare-society-for-cyberattacks.aspx

[23] https://vm.ee/en/cyber-security

[24] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[25] https://www.defense.gouv.fr/english/actualites/articles/presentation-du-pacte-defense-cyber

[26] https://www.telekom.com/en/media/media-information/archive/dt-and-bundeswehr-cooperate-in-cyber-defense-542510

[27] https://www.ncsc.nl/organisatie/nederlandse-cybersecurity-agenda.html

Country	Title	Description	Budget
		barriers against cybercrime; (6) lead in cybersecurity knowledge development; and (7) integrated public-private approach to cybersecurity.	

Source: Technopolis Group based on ENISA country review

There are various gaps in national and European level cybersecurity strategies that hinder the development of a stronger cybersecurity industry.

- Some Member States lack the necessary capabilities to defend against emerging trends which makes the European cybersecurity architecture more vulnerable to potential attacks.[28] This heterogeneity of security and privacy regulations across the EU presents a hurdle to effective cross-border collaboration.
- Skills shortages in cybersecurity are to some extent a result of an inadequate education and training system that should offer more targeted support to the development of cybersecurity skills.
- To develop a strong European cybersecurity industry, firms would also need more entrepreneurial skills in order to capitalise on cutting-edge technology.
- There are important funding gaps especially in the growth phase that prevent SMEs from expanding into new markets.
- Cybersecurity companies would also need first customers who are willing to act as early adopters[29] and stimulate the uptake of cybersecurity solutions. Public procurement and pre-commercial public procurement schemes could address this challenge.

Table 2 lists some examples of national initiatives that foster the development of a stronger innovation ecosystem for cybersecurity ventures

Table 2: Examples of national initiatives in support of cybersecurity research and industry

Country	Title	Description
Austria	Digital Atlas of Austria 2.0/ KIRAS[30]	The Austrian security research programme 'KIRAS' implements three mutually complementary instruments ranging from testbed actions to cooperative research and innovation projects and R&D support actions. The aim of the Digital Atlas has been to identify and analyse internet-based digital services vital to the Austrian government and society, to provide an assessment of their criticality and to illustrate the interdependencies of these services. The study has been supported in the framework of the National Research Development Programme KIRAS.
Belgium	Cyber Security Coalition[31]	The Cyber Security Coalition in Belgium supports the creation of an innovative ecosystem for a cybersecurity industry. The coalition is a partnership between players from the academic world, public authorities and the private sector to join forces in the fight against cybercrime. Currently more than 80 key players from across these 3 sectors are active members. Among various training and awareness raising campaigns, the SME Security Scan is a tool that is intended for self-employed individuals and professionals, as well as SMEs. This website aims to raise awareness among small businesses by inviting them to test their IT security and giving them tailored advice and practical tools to implement a cybersecurity policy.

[28] https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf
[29] HM Government, National cybersecurity strategy 2016-2021
[30] https://www.kiras.at/en/home/#category-filter:path=default
[31] https://www.cybersecuritycoalition.be/

Country	Title	Description
Czech Republic	NSM Cluster[32]	The Czech Network Security Monitoring Cluster focuses on network security and security in IT at national and regional level. It currently counts 21 members together with Mararyk University in Brno. Its activities include networking and know-how sharing; education and training about network security monitoring; and information sharing on network security trends.
Denmark	Centre for Cyber Security[33]	The Centre for Cyber Security is the Danish national IT security authority and National Centre for Excellence within cyber security. The Centre's mission is to advise Danish public authorities and private companies that support functions vital to society on how to prevent, counter and protect against cyberattacks.
Germany	Cybersecurity Training centres[34]	Fraunhofer and a selected group of universities have developed a modular concept for cybersecurity training. This collaborative approach enables the latest theoretical or practical research findings to be immediately incorporated into the teaching program. Students work in modern laboratories equipped with simulation tools allowing real threat scenarios to be tested.
Netherlands	The Hague Security Delta[35]	The most important security cluster in the Netherlands is 'The Hague Security Delta', active in the field of cyber security, national and urban security, critical infrastructures and forensics. It currently associates more than 260 partners, including businesses (corporates, SMEs & start-ups), governments and knowledge institutions. The National Cyber Testbed is a programme focusing on solutions designed for the Internet of Things and critical infrastructure. It supports the development of innovative products and services based on trial implementations enabled by the platform.
Poland	CYBERSEC HUB[36]	The CYBERSEC HUB coalition aims at creating a local ecosystem that can harvest cybersecurity technology knowledge. It provides a wide range of cybersecurity opportunities for companies, from education and training, R&I possibilities, to the development of innovative products.

Source: Technopolis Group

[32] http://www.nsmcluster.com/en/
[33] https://fe-ddis.dk/cfcs/CFCSDocuments/Generel%20CFCS_A5_Engelsk_12092016.pdf
[34] https://www.fraunhofer.de/en/research/fields-of-research/communication-knowledge/it-security/cybersecurity-training-labs.html
[35] https://www.thehaguesecuritydelta.com/media/com_hsd/report/115/document/NNH-NCT-DEF-Site.pdf
[36] https://cybersechub.eu/

Bibliography

ECS (2016). European Cybersecurity Strategic Research and Innovation Agenda, for a contractual public-private partnership, https://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

ENISA (2019). Cybersecurity skills development in the EU, The certification of cybersecurity degrees and ENISA's Higher Education Database, December 2019

ENISA (2019). Good practices in innovation on cybersecurity under NCCS, November 2019

European Commission (2020). Europe's moment: Repair and Prepare for the Next Generation

{SWD(2020) 98 final}, Brussels, 27.5.2020

European Commission (2019). Twentieth Progress Report towards an effective and genuine Security Union, Brussels, 30.10.2019

European Commission (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels, 13.9.2017

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013

European Court of Auditors (2019). Challenges to effective EU cybersecurity policy, Briefing Paper

ITU (2018). Global Cybersecurity Index (GCI) 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Kosciuszko Institute (2018). EUROPEAN CYBERSECURITY MARKET RESEARCH, INNOVATION, INVESTMENT, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Strategic Forum for IPCEI (2019). Strengthening Strategic Value Chains for a future-ready EU Industry - report of the Strategic Forum for Important Projects of Common European Interest

https://ec.europa.eu/docsroom/documents/37824

About the 'Advanced Technologies for Industry' project

The EU's industrial policy strategy promotes the creation of a competitive European industry. In order to properly support the implementation of policies and initiatives, a systematic monitoring of technological trends and reliable, up-to-date data on advanced technologies is needed. To this end, the Advanced Technologies for Industry (ATI) project has been set up. The project provides policymakers, industry representatives and academia with:

- Statistical data on the production and use of advanced technologies including enabling conditions such as skills, investment or entrepreneurship;
- Analytical reports such as on technological trends, sectoral insights and products;
- Analyses of policy measures and policy tools related to the uptake of advanced technologies;
- Analysis of technological trends in competing economies such as in the US, China or Japan;
- Access to technology centres and innovation hubs across EU countries.

You may find more information about the 16 technologies here: https://ati.ec.europa.eu.

The project is undertaken on behalf of the European Commission, Directorate General for Internal Market, Industry, Entrepreneurship and SMEs and the Executive Agency for Small and Medium-sized Enterprises (EASME) by IDC, Technopolis Group, Capgemini, Fraunhofer, IDEA Consult and NESTA.

October 2020

EA-02-20-820-EN-N

Publications Office
of the European Union