EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 1/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

Table of contents

1 INTRODUCTION:…… 3
1.1 Political and legal context…… 3
2 PROBLEM DEFINITION 6
2.1 Problem Context…….....6
2.2 What are the problems to tackle? 6
2.3 What are the problem drivers?.... 16
2.4 How will the problem evolve? …… 20
3 WHY SHOULD THE EU ACT? 21
3.1 Legal basis 21
3.2 Subsidiarity: Necessity of EU action 21
3.3 Subsidiarity: Added value of EU action....22
4 OBJECTIVES: WHAT IS TO BE ACHIEVED? 22
4.1 General objectives 22
4.2 Specific objectives 23
4.3 Functionalities and governance of the Network and the Centre....23
5 WHAT ARE THE AVAILABLE POLICY OPTIONS? 29
5.1 What is the baseline from which options are assessed? 29
5.2 Description of the policy options analysed in detail 30
5.3 Options discarded at an early stage 35
6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS? 37
6.1 Option 1: Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation 37
6.2 Option 2: Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre lresearch and innovation activities 41
7 HOW DO THE OPTIONS COMPARE? 43
8 PREFERRED OPTION 45
9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? 46

Glossary

The below table explains the key terms or acronyms used in this document

Term or acronym	*Meaning or definition*
AI	Artificial Intelligence
cPPP	Contractual Public Private Partnership
CEF	Connecting Europe Facility
DSM	Digital Single Market
ECSO	European Cybersecurity Organisation
H2020	Horizon 2020 Framework Programme for Research & Innovation
HPC	High-Performance Computing
ICT	Information and Communication Technology
IoT	Internet of Things
JU	Joint Undertaking (as defined by article 187 TFEU)
LEIT	Leadership in Enabling and Industrial Technologies
MFF	Multi-Annual Financial Framework
R&D	Research and Development
R&I	Research and Innovation
SME	Small and Medium-sized Enterprise
SRiA	Strategic Research and Innovation Agenda
TFEU	Treaty on the Functioning of the European Union
NIS Directive	Directive on the Security of Network and Information Systems

1 INTRODUCTION:

1.1 Political and legal context

In September 2017 the Commission adopted the Joint Communication on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the EU's resilience, deterrence and response to cyber-attacks. The Communication, building also on previous initiatives[1], outlined a set of proposed actions, including, among others reinforcing the European Union Cybersecurity Agency (European Union Agency for Network and Information Security – ENISA), creating a voluntary EU-wide cybersecurity certification framework to increase the cybersecurity of products and services in the digital world as well as a Blueprint for quick, coordinated response to large scale cybersecurity incidents and crises.

The joint Communication highlighted also[2] that it is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services. Europe must be in a position to autonomously secure its digital assets. At the moment, Europe is a net importer of cybersecurity products and solutions and largely depends on non-European providers.[3]

Against this background, the European Commission announced in the Communication the proposal to set up a network of cybersecurity centres of expertise with a European Competence Centre at its heart to bring together resources, overcome fragmentation of efforts across the EU and stimulate the development and deployment of technology in cybersecurity. The Commission also identified the need to take advantage of the synergies between EU civilian and defence cybersecurity markets, which share many common challenges and which call for close collaboration between both communities.

In the context of this work, the Commission launched a call for proposals under the H2020 Work Programme to pilot the creation of efficient networks of competence centres across the EU, able to jointly respond to cybersecurity industrial challenges. A call for proposals for the projects was launched on 1 February 2018 and closed on 29 May, with projects starting at the end of 2018.[4] The learnings from the projects, will inform the process of creating the future Network and Competence Centre (please see Annex 5).

The proposal announced in the Communication should help meet the ambitious goal for Europe agreed by the Heads of State and Government at the Tallinn Digital Summit to be "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of

[1] The cross-border nature of cybersecurity threats and the need to tackle them at the EU level has been recognised already in 2013, when the first EU Cybersecurity Strategy[1] (JOIN (3013) was adopted. Cybersecurity, cybercrime and cyber defence have been systematically included in the Commission political priorities and key initiatives – Digital Single Market Strategy – COM/2015/0192, the European Agenda on Security – COM(2015) 185, the Joint Framework on countering hybrid threats, the Communication on Launching the European Defence Fund. , the Directive on concerning measures for a high common level of security of network and information systems across the Union, (the 'NIS Directive' - (EU) 2016/1148) and the contractual public-private partnership (cPPP) on cybersecurity C(2016) 4400 between the EU and the European Cybersecurity Organisation (ECSO); In 2017 a proposal for the European Defence Industrial Development Programme aiming at enhancing the competitiveness and innovation of the Union defence industry; underlining the importance of including cyber defence was adopted by COM in 2017. COM(2017) 294 final 2017/0125 (COD)

[2] JOIN(2017) 450 final: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU;

[3] Draft Final Report on the Cybersecurity Market Study, 2018

[4] https://ec.europa.eu/digital-single-market/en/news/commission-launches-call-proposals-eu50-million-pilot-support-creation-network-cybersecurity

our citizens, consumers and enterprises online and to enable a free and law-governed internet."[5]

At the moment the efforts of research and industrial communities are fragmented, lacking alignment, and a common mission, which may hinder and does not give impetus to the EU's competitiveness in this domain.[6]

The EU has been supporting research and innovation in the field of cybersecurity by providing funds under the Seventh Framework Programme and Horizon 2020 and has been striving to reinforce the links between research and industry through collaborative projects and by establishing the contractual public-private partnership (cPPP) on cybersecurity in 2016. The EU provides also, albeit at a very limited scale, support to pilot actions for the deployment of cybersecurity and trust solutions in areas of public interest within the CEF programme.

Cybersecurity products and services constitute an important and rapidly growing market.[7] However, Europe faces strong competition, with one study ranking Europe as a geographical entity in third place, following the United States and Asia, when considering a global perspective on cybersecurity markets. According to this study, in the top 20 of the leading cybersecurity countries from a market perspective, there are only 6 European countries.[8]

The EU's international counterparts have a clear strategy and make significant cybersecurity investment designed to increase technological and innovation capacities. They are developing competence centres bringing their assets (human, knowledge, financial) together to support their industries in the quest to become global cybersecurity champions.

The creation of the Public-Private Partnership[9] on cybersecurity in the EU was a solid first step bringing together the research, industry and public sector communities in Europe to facilitate innovation in cybersecurity and within the limits of the current financial framework eventually conclude with good, more focused outcomes in research and innovation. However, Europe can pursue a much larger scale investment and needs a more effective mechanism which would build lasting capacities, pool efforts, competences and stimulate the development of innovative solutions responding to industrial challenges for general cybersecurity technology (e.g. artificial intelligence, quantum computing, blockchain and secure digital identities) as well as cybersecurity in critical sectors (e.g. transport, energy, health, financial, government, telecom, manufacturing, defence, space).

The proposal to create European Cybersecurity Industrial, Technology and Research Competence Centre with the Network of National Coordination Centres is linked to the Commission's proposals for the next Multi-annual financial framework (MFF). It would be the main implementation mechanism for EU financial resources dedicated to cybersecurity under the proposed *Digital Europe Programme*. This programme, which is subject to a separate Impact Assessment[10], seeks to enlarge and maximise the benefits of digital transformation to European citizens and businesses, reinforcing the policies and supporting the ambitions of the Digital Single Market.

[5] 29 September 2017; conclusions by Prime Minister of Estonia Jüri Ratas
[6] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)
[7] Analyses, depending on the methodology used, range from €100 billion to €600 billion in terms of global market size and 12% to 15% annual growth rate.
[8] Draft Final Report on the Cybersecurity Market Study, 2018
[9] COM/2016/0410 final: Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry,.
[10] See Digital Europe Programme IA

The different elements within the Digital Europe Programme – besides cybersecurity high-performance computing (HPC), Artificial Intelligence (AI), deployment, digital capacity and interoperability, and Advanced Digital skills – will be mutually reinforcing: Attacks on ICT systems are facilitated by the advent of ever more powerful computing capabilities. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The adoption of AI means that systems need to be trained with large sets of data ("deep learning"), which need to be secure. Likewise, AI is likely to be part of future security solutions ("self-healing systems").All these areas will also require skilled workforce. .[11]

The network and Centre will also act as an implementation mechanism for cybersecurity under Horizon Europe, the next EU R&I Framework programme. Such a comprehensive approach would allow supporting cybersecurity across the entire value chain, from research to supporting the deployment and uptake of key technologies.

Likewise, in view of the dual-use character of many cybersecurity technologies, common priorities with the defence sector (e.g. in the areas of training, sharing industrial cybersecurity intelligence, building cybersecurity capabilities, testing and certification) and of the need to avoid double-spending, synergies need to be built between civilian cybersecurity and cyber defence research and industrial communities, in line with Member States' priorities (see section 2 of this document).

1.2 Initial Reactions from Member States

The Council Conclusions[12] adopted in November 2017, called on the Commission to provide rapidly an impact assessment on the possible options and propose by mid-2018 the relevant legal instrument for the implementation of the initiative establishing a Network of Cybersecurity Competence Centres and a European Cybersecurity Competence Centre. Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity. Specifically with regard to the possible Centre, Member States stressed the importance of its coordinating role in support of the network.

Therefore, any Commission initiative will have to find the right balance in the governance and implementation structures to ensure effective European coordination while taking into account developments at the national level. The scope of the initiative will also have to take into account the specificities of the area of cybersecurity, which has seen an important growth in activities by both private and public actors on all levels and in which considerations of national security and of European strategic autonomy play an important role. The initiative would therefore have to also find the right arrangements to work with and support industry, academia, and the public sector while giving a clear role to Member States' authorities.

[11] Idem

[12] Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.

2 PROBLEM DEFINITION

2.1 Problem Context

Europeans increasingly value and rely on digital technologies. Critical economic sectors such as transport, energy, health or finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things (IoT), interconnecting objects between one another and with people through communication networks, is already a reality and it is expected to boom in the near future: billions of IoT connections are forecasted in the EU in 2020[13]. Furthermore, cyberspace is considered by military forces as the fifth domain (besides land, sea, air and space) of military activity, equally critical to European Union Common Security and Defence Policy (CSDP).[14]

While the growing digital connectivity brings enormous opportunities, it also exposes the economy and society to cyber threats. Cyber-attacks are constantly on the rise. In some Member States, it has been estimated that half of all the crimes are cybercrimes[15]. Some of these attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecommunications companies and electoral commissions. The May 2017 "WannaCry" ransomware attack affected more than 230,000 computers in over 150 countries, impacting the operations of railways, health systems, telecoms operators and businesses across Europe. Attacks on cryptosystems are also facilitated by the advent on ever more powerful computing capabilities and will soon be even more at risk with the advent of quantum computers.

A 2016 study[16] revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years, while at least 80% of European companies have experienced at least one cybersecurity incident. In the third quarter of 2016 alone, 18 million new malware samples were captured, i.e. an average of 200,000 per day.

Cyber incidents cause major economic damage to European businesses, undermine the trust of citizens and enterprises in the digital society and affect citizens' fundamental rights. A 2014 study[17] estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around €55 bn) in 2013; with Germany being the most affected Member State (1.6 % of GDP). A recent report, in the aftermath of the "WannaCry" attack, estimated that a serious cyber-attack could cost the global economy more than $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy[18].

2.2 What are the problems to tackle?

The European Union has already put in place a number of policy and regulatory instruments to address fast evolving cyber threats (please see section 1.1.) and to secure its society, economy and democracy against them.

---

[13] Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014.

[14] https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf

[15] PWC, Global State of Information Security Survey, 2016, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

[16] Idem

[17] McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014

[18] Counting the cost – Cyber exposure decoded, Lloyd's and Cyence, 2017.

However, today the EU still lacks sufficient technological and industrial capacities to autonomously secure its economy and critical infrastructures and to become a global leader in cybersecurity field.

Within the broader course of action defined by the cybersecurity Package, the present initiative aims to contribute to tackling the following problems related to the EU's insufficient cybersecurity technological and industrial capacities:

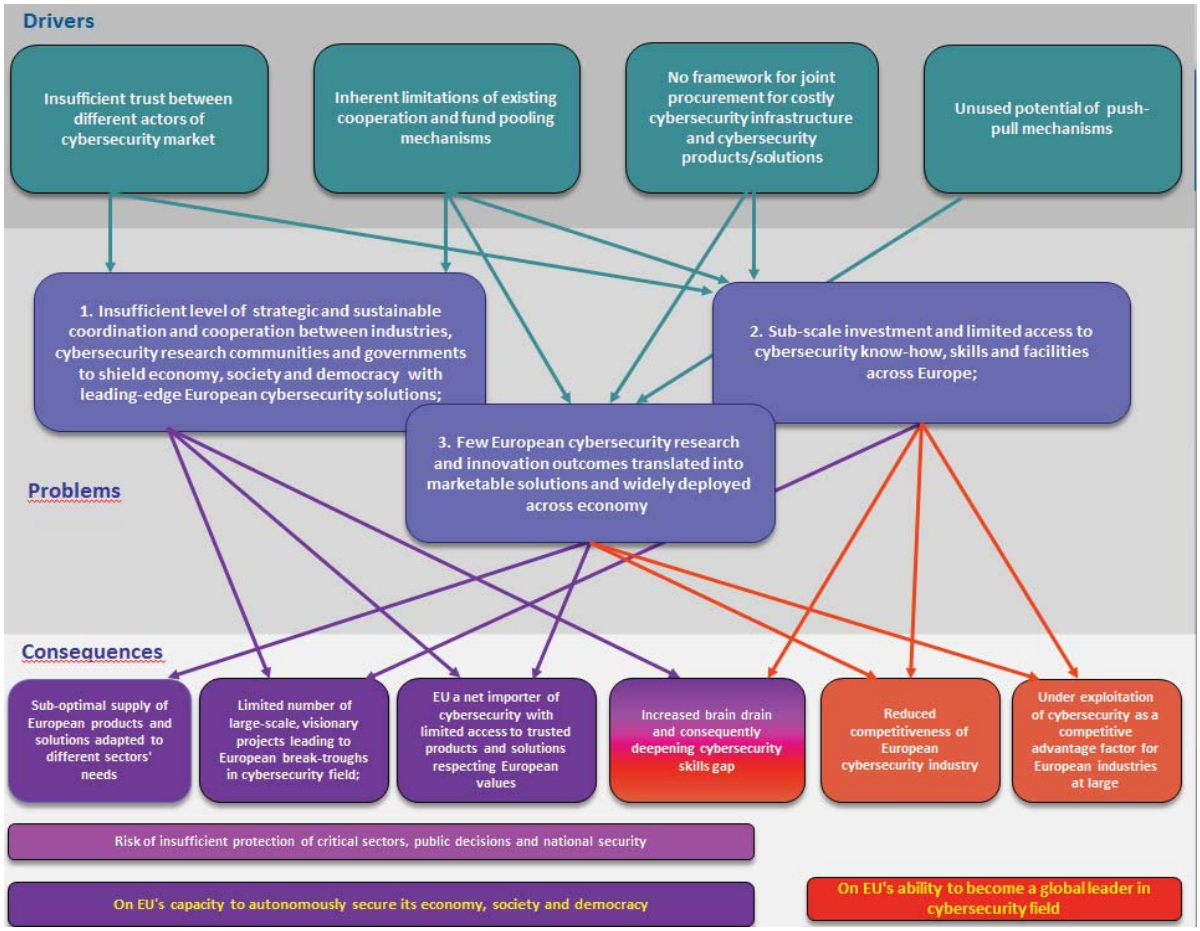
→ **Problem 1:** Insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;

→ **Problem 2:** Sub-scale investment and limited access to cybersecurity know-how, skills and facilities across Europe;

→ **Problem 3:** Few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across economy.

A problem tree portraying related problems, their drivers and consequences is presented in Figure 1 below and described in detail in the following sections.

Figure 1: Initiative Problem Tree



2.2.1 Problem 1: Insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities and governments to shield economy, society and democracy with leading-edge European cybersecurity solutions;

→ **Insufficient cooperation between cybersecurity demand and supply industries**

European industries but also public and essential services across all sectors are subject to digital transformation. This creates security challenges, which are driving demand for security services. The businesses face the challenge of both remaining secure and offering secure products and services to their clients. The automotive industry, for example, is considering specific processes to select and implement the adequate set of cyber security solutions for each subsystem of various vehicles.[19] [20]

Yet, often businesses are not able to appropriately secure their existing products, services and assets or to design secure innovative products and services (due to e.g. lack of resources, skills, access to testing facilities, different business priorities). Key cybersecurity assets (e.g. block-chain based solutions, infrastructures supporting quantum key distribution enabling highly-secure communications) are often too costly to be developed and set up by individual players.

At the same time, the links between the demand (both public and private from various sectors e.g. health, telecomm, energy, space, defence, finance, transport) and supply side of the cybersecurity market are not sufficiently well developed resulting in sub-optimal supply of European products and solutions adapted to different sectors' needs, as well as in insufficient levels of trust among market players. While some limited progress in this regard has been achieved with the establishment of the contractual Public Private Partnership on cybersecurity, this cooperation is still limited to exchange of views on the research agenda and does not seem to translate into cooperation on specific industrial challenges yet (please see also section 2.3.2).

→ **Lack of a cooperation mechanism among Member States for industrial capacity building**

At the moment there is also no efficient cooperation mechanism for Member States to work together towards building necessary capabilities supporting cybersecurity innovation across industrial sectors and deployment of cutting-edge European cybersecurity solutions. The existing cooperation mechanisms for Member States in the field of cybersecurity such as e.g. the Cooperation Group and CSIRT Network under the NIS Directive do not envisage this type of activities in their mandate. The European Cybersecurity Organisation – the Commission's counterpart in the cybersecurity cPPP has included in its governance structure an advisory committee of national public authorities. This mechanism, however, focuses primarily on

[19] Shifting Gears in Cybersecurity for Connected Cars, February 2017: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx

[20] See e.g.: ACEA Principles of Automobile Cybersecurity: http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

providing advice on the Association's activities and exchanging best practices. Beyond presenting the public administration's perspective on the research and innovation agenda of the cPPP and exchanging good practices, the Committee does not conduct specific activities directly supporting the enhancement of cybersecurity industrial capabilities (e.g. through agreeing on common investment plans).[21]

→ **Insufficient cooperation within and between research and industrial communities**

The research community can play a vital role in supporting both industry and public authorities in meeting cybersecurity challenges. While a wealth of cybersecurity expertise and experience is available across Member States at the moment, which can make Europe a leader in the cybersecurity field, the efforts and capacities of research and industrial communities are dispersed thus hindering the EU's competitiveness in this domain.

More than 660 organisations from across the EU registered to the recent mapping of cybersecurity centres of expertise conducted by the European Commission.[22] The analysis of data shows that there are many research teams working on cybersecurity issues across the EU and that their combined efforts could allow Europe to cover the whole cybersecurity value chain. However, the results also show that there is a clear need to better coordinate the research efforts if this is to be achieved. Insufficient synergies and coordination of efforts lead to a situation in which very few major cybersecurity research breakthroughs have been reported.[23]

The results of the mapping show that many organisations working on cybersecurity issues have quite small teams. In addition, many of these expertise centres also tend to take a horizontal approach and do research across many cybersecurity domains at the same time. This often does not allow for deploying a critical mass of resources (human, financial, infrastructure) to solve specific cybersecurity challenges. At the same as they cannot invest in human and infrastructural resources, they concentrate on domains and sectors that are less demanding in terms of resources.

In consequence, despite Europe's potential to cover the full cybersecurity value chain, there are relevant cybersecurity sectors (e.g. energy, space, defence, transport) and sub-domains that are today poorly supported by the research community, or supported only by a limited number of centres (e.g. post-quantum cryptography, cybercrime research, trust and cybersecurity in AI).

Another phenomenon observed by the mapping is that European scientific excellence very often turns into publications but rarely into patents (see figure 2 below). This points towards insufficient cooperation between research and industry[24]. The consultation process demonstrated that such collaboration exists, but it is very often a short-term, consultancy-type of arrangement, which does not allow engaging in long-term research plans to solve cybersecurity industrial challenges (see Annex 2 and 4).

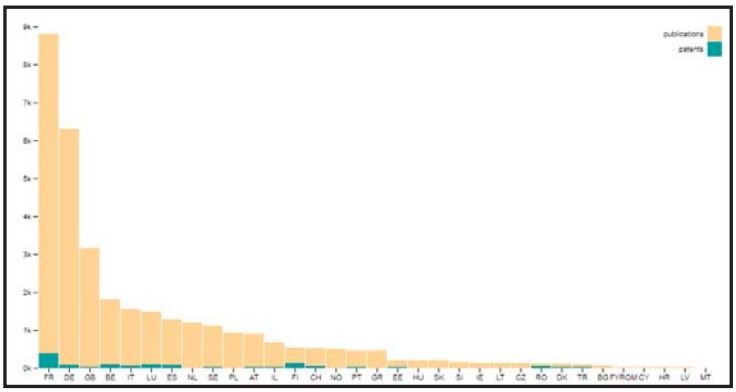
[21] http://ecs-org.eu/documents/ecso-asbl-statutes.pdf AND http://www.ecs-org.eu/documents/uploads/591d55b9be0a6.pdf

[22] JRC Technical Reports: European Cybersecurity Centres of Expertise, 201; 660 organisations registered until 31 March 2018, when the analysis for the purpose of this Impact Assessment was been undertaken. The mapping survey has remained open beyond that date to allow as many members of the cybersecurity competence community as possible to register.

[23] Idem

[24] While patent analysis in the cybersecurity field cannot provide the full picture of the innovation chain (e.g. it does not capture the phenomenon of software development and licensing), this piece of evidence, confirmed also by stakeholder consultation, reveals certain weakness in collaboration between the research community and the industry.

***Figure 2* Cybersecurity Publications/Patent ratio per country[25]**



→ **Insufficient cooperation between civilian and defence cybersecurity research and innovation communities**

The problem of insufficient levels of cooperation– both in terms of ideas and funding –also concerns the civilian and defence communities, as confirmed by evidence and consultation activities.[26]

Dual use technologies are an opportunity for the European cybersecurity market as in cybersecurity field transfers of solutions from one market to another are common practice. Unlike in other parts of the world in Europe, transfer from the civilian market to the defence market is more common. Defence clients use solutions initially developed for the civilian market.[27]

However, innovation cycles in the defence and civilian markets are relatively similar; although companies are less likely to engage in defence-oriented R&D activities without demand from Ministries of Defence. Lots of potential synergies can be identified in the experimental and development activities conducted by university research organisations and innovators (SMEs, start-ups, large players), as well as in the applied research focusing on pre-commercial development of a product. Both communities also face similar challenges related to successful transition of the technology into commercial market, which requires turning the R&D efforts into applicable and marketable product.[28]

Yet in Europe these synergies are not used to the full extent due to lack of efficient mechanisms allowing these communities to cooperate efficiently and build trust, which, even more than in other fields, is a prerequisite for successful cooperation. This is coupled with limited financial capabilities in the EU cybersecurity market, including insufficient funds to support innovation.

The fragmentation of efforts is visible, among others, at the European level as the major cybersecurity research and innovation programme – Horizon 2020 – puts clear boundaries to

[25] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)

[26] See: Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015);: https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets; See also consultation Annex 2.

[27] Study on synergies between the civilian and the defence cybersecurity markets…

[28] Idem

civilian-military cooperation. While the programme does not exclude developing and improving dual use technologies, it requires that the research activity is fully motivated by, and limited to, civil applications.[29]

Most of the 18 Member States that have responded to a recent request on cyber defence activities and needs have stressed the necessity to strengthen civil-military cooperation at EU level, notably in terms of training, education and exercises, as well as in the fields of information sharing, awareness raising and cyber defence capability development. Member States expect the EU to add value to national cyber defence efforts by supporting industry, particularly on research and development. [30]

With regard to the latter, Member States confirmed the need to reinforce synergies between civilian and military cyber research efforts, to strengthen the technological basis for cyber defence research and innovation, to promote and provide insights into technological developments, as well as to support academic and industry R&D projects specifically in artificial intelligence.[31]

The under-exploitation of the dual use opportunities should be also seen in the context of stiff competition from global players. The EU's global cybersecurity competitors – the US, Israel and China – actively stimulate cooperation and strong synergies between civilian and military communities.[32] An informative example is the Israeli CyberSpark Industry Initiative. Supported by the Israeli National Cyber Bureau, whose mission is to build Israel's lead in the cyber field, CyberSpark managed to create an effective ecosystem for joint cyber industry activities and academia-industry partnerships[33]. The Israeli government is also supporting dual cyber R&D (e.g. through the Masad Program) to promote national and defensive cyber technologies together.[34] This coherent approach allows not only to pool public and private investment but also to attract venture capital. In 2017 Israel's cybersecurity industry raised $814.5 million in venture capital and private equity investment - a 28% over 2016 that brings the country second only to the United States.[35]

2.2.2 Problem 2: Sub-scale investment and limited access to cybersecurity know-how, skills and facilities

Despite the importance of cybersecurity on the European agenda, the current investment levels remain sub-optimal.

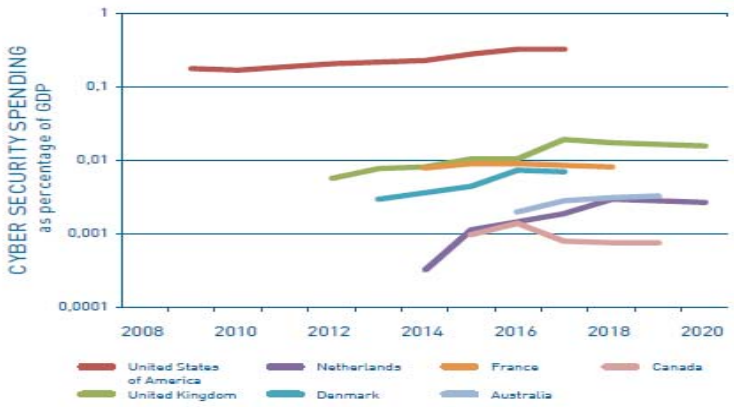
The EU public investment today – both at the EU and national level - including in the development and the deployment of cybersecurity technology and solutions - is below the critical mass needed to protect our economy and institutions, in particular if compared to other

[29] Article 19(2) stipulates: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications".
[30] EEAS, March 2018.
[31] Idem
[32] See for example: US Department of Defence Cyber Strategy 2015
https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
[33] http://cyberspark.org.il/
[34] World Development Report 2016: Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel:
http://pubdocs.worldbank.org/en/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf
[35] https://www.cyberscoop.com/israel-cybersecurity-venture-funding/

key international players. This has practical consequences on cybersecurity capacities of European research and industrial communities.

Public cybersecurity spending is not easily discernible from overall government spending but some available data analysis show that its levels (in terms of percentage of GDP) in Europe are low (please see Figure 3) and sub-optimal compared to other global players, who are massively investing in strategic cybersecurity programmes that are driven by public authorities with some leverage of private investments.

Figure 3: Government cybersecurity spending: a cross-country comparison over time (2008-2020)[36]



As an example, in the U.S.A., the government invested over USD 19 billion for cybersecurity as part of 2017 Budget (35% increase from 2016 in overall Federal resources for cybersecurity).[37] It devotes USD 760 Million in 2017 alone for cybersecurity research and innovation.[38]

At the EU level the investment in cybersecurity is channelled through different programmes of the EU budget: about EUR 600 million have been invested in cybersecurity and cybercrime projects under Horizon 2020 for the period 2014-2020 (including EUR 450 million devoted to cybersecurity cPPP for 2017-2020); the European Structural and Investment (ESI) Funds foresee a contribution of up to EUR 400 million for investments in trust and cybersecurity; about EUR 30 million were invested from CEF in the period 2014-2017.

While there is no clear picture of public investment in cybersecurity research and innovation across Member States, the reported figures from some Member States that are most active in the cybersecurity field indicate that the magnitude of the cumulative EU effort is significantly behind its global counterparts.[39] Member States are not in a position to develop individually a complete cybersecurity research and industrial ecosystem covering the full cybersecurity value chain in a competitive timeframe. While the necessary competences are available across

[36] Dutch investments in ICT and cybersecurity: putting it in perspective, *The Hague* Centre for Strategic Studies, December 2016

[37] White House, Factsheet Cybersecurity National Action Plan.

[38] The Networking and Information Technology Research and Development Program

[39] Among the Member States, who made public their investment plans: France earmarked an investment of around 165 million euros per year for cybersecurity between 2014 to 2019, with half of this budget allocated for research and innovation. The German "Self-Determination and Safety in the Digital World 2015-2020" envisages around €35 million/year for research in 4 main areas, namely High-tech for IT security, secure and trustworthy ICT systems, IT security in fields of application, privacy and data protection. In the Netherlands the vast majority of research programmes have been funded by several ministries. In 2013 which marked the second round for cybersecurity research funding, a sum of 6.4 million euros was made available by the government and public organisations.

Europe, individual Member States do not usually have the full range of know-how and most lack the necessary funding levels.

The research and industrial communities as well as the public sector in Europe struggle also with insufficient capacities and access to necessary facilities for cybersecurity experimentation, testing, and operations, which are often too large/costly for a single entity or even Member State to acquire.

During the consultation process both industrial and research communities strongly emphasised the need to reinforce the access of European industrial developers and researchers to critical-mass testing and experimentation infrastructure (e.g. quantum communication test beds; testing and penetration environment for different critical sectors, IoT environment, quantum computing facilities to validate post-quantum cryptography etc.).[40] This was supported by a comparison with the opportunities available in other markets (especially the US), where industry, researchers and public sector actors have access to real time data and testing facilities to advance their projects and get them to the market.

This challenge is also well-portrayed by the results of the mapping of Europeans cybersecurity centres of expertise. The analysis of the mapping respondents' declared activity shows that among key cybersecurity field of applications (HPC, AI, quantum etc.) that are poorly investigated at the European level are those that require deploying a critical mass of resources (see Figure 4). Looking at the distribution of the research from a sectorial perspective (see Figure 5), it is also clear that the sectors requiring costly facilities to perform experimentation and testing (e.g. energy, space, defence) are well covered only by those Member States, which traditionally have more resources available to invest.[41]

Figure 4 - Distribution of applications and technologies per country[42]

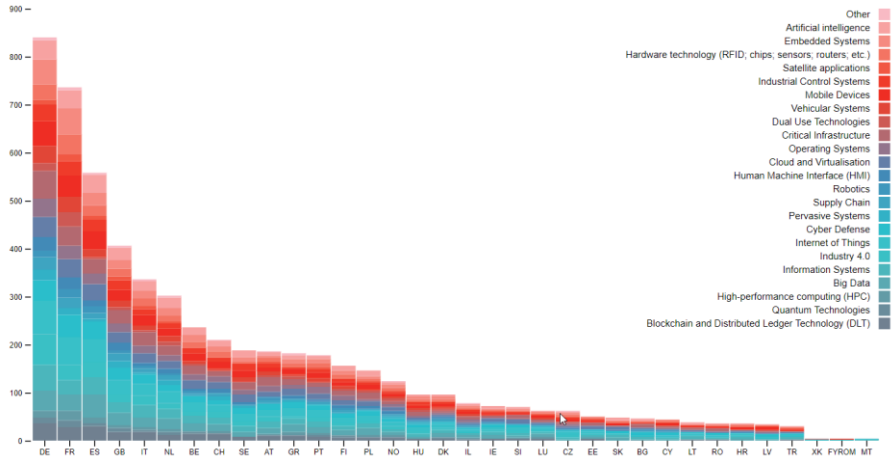
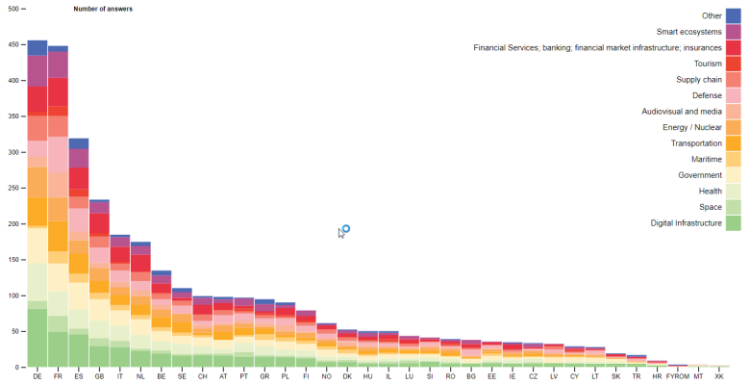


Figure 5 - Distribution of sectors per country[43]

[40] See Annex 2 on Consultation outcomes
[41] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)
[42] Idem
[43] Idem



The lack of access to such facilities is also a challenge for the industrial community. Within the cybersecurity supply industry, a very substantial part of innovation is driven by SMEs and start-ups. If they cannot test their ideas, they are likely to either turn towards less costly domains and technologies or to look for opportunities outside the EU. Either option is not opportune for the European cybersecurity competitiveness. An indirect consequence can be also the loss of know-how and brain-drain as innovators decide to move outside Europe to find an ecosystem allowing them to pursue their ideas.

This is also a challenge for other industries undergoing digital transformation, including but not limited to the sectors covered under the NIS Directive (i.e. transport, energy, banking, financial market infrastructures, health, water, as well as digital service providers). However, for businesses looking at cybersecurity as just one feature of their product, it is important to be able to use such capacities when needed, without the necessity to invest heavily in the area, which is not part of their core business.

Europe also lacks a culture of investing in cybersecurity. There are many innovative SMEs in the field but they are often unable to scale up their operations due to the lack of easily available funding to support them in the early phases of development. In a public consultation conducted by the European Commission, 75% of respondents stated they did not feel they had sufficient access to financial resources to finance cybersecurity projects and initiatives.[44]

Last but not least, industrial, research and public sector (including defence) communities also struggle to find skilled cybersecurity professionals for both research and business tasks. The skills gap for cybersecurity professionals working in industry in Europe is predicted to be 350 000 (globally 1.8 million) by 2022. This is coupled with huge global competition for talent. Two-thirds of the European security professionals surveyed for the 2017 Global Information Security Workforce Study said there was too few staff available in their field, a proportion in line with the worldwide figure, which rose from 62 percent worldwide in 2015.[45]

While there are opportunities for employment and European citizens who want to learn and/or specialize in cybersecurity can nowadays access almost 500 university courses and trainings across Europe[46], the non-alignment of curricula and lack of European certification mechanism for cybersecurity professionals further complicates the situation as it is difficult for potential employers to judge the skills level of professionals graduating from different types of education organisations.

[44] SWD (2016) 215

[45] 2017 Global Information Security Workforce Study commissioned by the Centre for Cyber Safety and Education and (ISC)2, was carried out from 22 June to 11 September, 2016, and surveyed 19,641 IT security professionals from 170 countries, including nearly 3,700 respondents in Europe: https://www.isc2.org/pressreleasedetails.aspx?id=14570

[46] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities

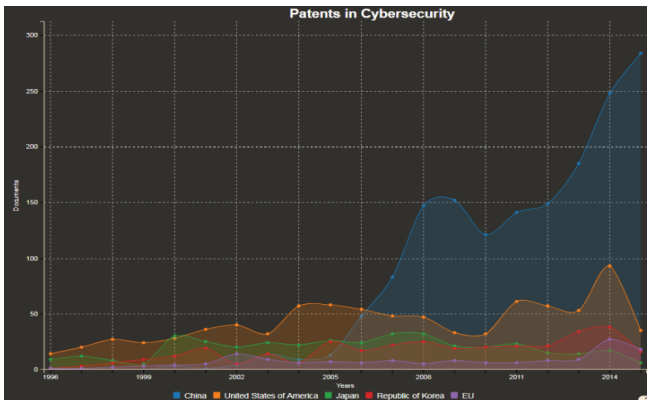
As the global competition for talent is fierce, the current lack of coordination of cybersecurity research and innovation efforts leads also to talent brain drain. Sub-optimal investment, which for talented researchers translates in practice into limited access to infrastructure as well as to large-scale visionary projects leading to European break-troughs, encourages them to look for opportunities at non-EU markets offering conditions and facilities allowing them to fulfil their ambitions.

2.2.3 Problem 3: Few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across economy

The two first problems are closely connected to the third major issue: while a lot of innovative cybersecurity research is taking place in Europe, its results often do not make it to the commercial world. And even when they do, they are not sufficiently deployed across the economy to allow the EU to become a leader neither on its own, European market nor globally.

The phenomenon of the "Valley of Death", which refers to the problematic shift from research to marketable product development[47], is of course not specific to the cybersecurity field or to Europe only. However, data suggests that European cybersecurity innovators have more difficulties to cross the Valley of Death than their competitors. The EU performs poorly, in comparison to its global counterparts, in the commercial exploitation of research outcomes. While patent analysis in the cybersecurity field cannot provide the full picture of the innovation chain[48], it shows certain trends. In fact in Europe private sector cybersecurity patenting is largely dominated by non-EU companies (see figure 6) - on average the EU owns less than 5% of cybersecurity related patents (with cryptography being the only exception with the result of 21%), while patent filing is dominated by China, followed by the USA.[49]

Figure 6: Cybersecurity Patents in Europe[50]



At the same time European cybersecurity products and solutions that manage to cross the Valley of Death are not widely deployed across European and global markets. The cybersecurity industry in Europe has developed largely on the basis of national governmental

[47] https://www.journals.elsevier.com/technovation/call-for-papers/special-issue-surviving-the-valley-of-death
[48] E.g. the patent analysis that does not capture the phenomenon of software development and licensing); or other elements such as the cost and complexity of the patenting process
[49] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)
[50] Idem

demand, including for the defence sector. In parallel a multitude of innovative SMEs has also emerged both in specialty/niche markets (e.g. crypto systems) and in well-established markets with new business models (e.g. antivirus software). Despite this evolving market structure companies still have difficulties growing outside their domestic, national market due to market fragmentation. As a consequence, while European companies tend to be strong and innovative, their size and capacity (mostly SMEs with few larger actors) are smaller in comparison to their US, Israeli, Chinese, South-Korean counterparts.

European companies, especially SMEs, have also little budget available for commercial development and marketing to improve their visibility across markets. They also lack sufficient resources to acquire competitive intelligence to understand where their product/service could fit in the market. This is coupled with the previously mentioned lack of EU cybersecurity investment culture with a high-risk aversion and scarcity of European venture capital willing to invest in the field.[51]

An additional issue is related to how government procurement and large tenders, which could be an opportunity for European providers to present their offer, are structured. In fact they often call for a complex package of services that single European companies (especially SMEs), unlike their global competitors, cannot provide. At the same time there is no mechanism that would facilitate swift creation of consortia of European companies that could effectively respond to such calls.

As a consequence, market leadership in the EU is in the hands of companies from third countries, which have greater resources than the EU suppliers. Despite its cybersecurity innovation potential, Europe imports 5.3% of all such products and services from outside the EU; what is more, up to 25% of the supply from within Europe is actually provided by companies with the headquarters outside Europe. At the same time major competitors (e.g. US, China) are net exporters in all cybersecurity sub-sectors.[52]

The difficulty to compete on the European and global levels often leads to mergers and acquisitions of European SMEs by non-European actors, weakening the European sector and leaving Europe also much more vulnerable and technologically dependent on others.[53]

Last but not least, it is also a missed economic opportunity. The global cybersecurity market is expected to be among the fastest growing segments of the ICT sector in the coming decade.[54]

2.3 What are the problem drivers?

The analysis of the evidence supporting the impact assessment identified the following main drivers contributing to the problem:

[51] Digital SME Cybersecurity Position: https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

[52] Draft Final Report on the Cybersecurity Market Study, 2018

[53] See: Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015); see also https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf

[54] Whereas there are differences between studies and their respective methodologies and results, one study values the cybersecurity market globally at €600 bn with an expected average growth of 17% in all the three aspects of sales, number of companies and employment in the next five years. Draft Final Report on the Cybersecurity Market Study, 2018

2.3.1 Driver 1: Insufficient level of trust between different actors of the cybersecurity ecosystem

For cybersecurity trust is a prerequisite of effective cooperation both between public authorities and between market actors across Europe. Thanks to the NIS Directive mechanisms and supporting non-legislative actions (e.g. cyber exercises) progress has been achieved in recent years in building trust among Member States helping to improve cooperation and information sharing at the EU level on cybersecurity issues.

However, the trust level between public authorities and the private sector from across Member States, within the private sector as well as between the private sector and the research community is still insufficient. Part of the problem is due to the fact that despite fast digitalisation of all fields of economy and society, cybersecurity is still perceived by some actors as mostly a national security issue, which should be predominantly dealt with at the national level and in smaller trusted circles. This also impacts the willingness of different actors to pool resources and invest together in developing industrial capacities (Problem 1 and 2 described above).

Some progress in building trust between actors of this European ecosystem has been achieved thanks to the Commission's initiative of creating a cPPP on cybersecurity in 2016[55], which allowed forming a sustainable platform of exchange of views between industry, research and public administration on cybersecurity research and innovation issues. However, the scale and impact of this effort is limited partially due to inherent limitations of this instrument (please see section 2.3.2).

In terms of market dynamics, the insufficient trust in the solutions offered 'cross-border' is the essential factor that clearly emerged from a number of consultations undertaken by the Commission at the time of and following the creation of the cPPP on cybersecurity.[56] As a consequence, much procurement still takes place within a given Member State and many companies struggle to achieve the economies of scale that would enable them to be more competitive both within the internal market and globally. This clearly impacts effective market deployment of European cybersecurity products and solutions (Problem 3).

2.3.2 Driver 2: Inherent limitations of existing cooperation mechanisms for highly complex cybersecurity ecosystem

The establishment of the cPPP on cybersecurity between the European Commission and the European Cybersecurity Organisation (ECSO) in 2016[57] was the first EU-wide attempt to bring together the cybersecurity industry, the demand side and the research community to build the platform of sustainable dialogue and create conditions for voluntary co-investment. Public authorities, who are an important buyer of cybersecurity products and solutions themselves, have also been invited to take part in the partnership.

The partnership indeed managed to create a platform of dialogue at the EU level and by developing the Strategic Research and Innovation Agenda actively contributed to the development of the Horizon 2020 Research & Innovation Work Programme's parts related to

[55] Study on synergies between the civilian and the defence cybersecurity markets; IPACSO (2015)
[56] See SWD (2016) 216.
[57] In its Digital Single Market Strategy for Europe(COM (2015) 192), the European Commission concluded that specific gaps still existed in the fast-moving area of cybersecurity technologies and a more joined-up approach was needed to step up the supply of more secure solutions at the European level. The establishment of a contractual public private partnership on cybersecurity to create the structural links between cybersecurity research and industrial communities aimed at stepping up work towards trusted collaboration COM (2016) 410

cybersecurity. It also allowed the member organisations of ECSO to discuss other issues relevant for the cybersecurity ecosystem e.g. certification or skills development.[58]

However, the impact of the partnership on actual research and innovation activities to respond to cybersecurity industrial challenges is limited due to the inherent limitation of this cooperation mechanism. The cPPP is a light collaboration structure well-suited to federate advice on cybersecurity communities' research priorities, which can then be supported through the regular instruments of the Union's Research Framework Programme. This mechanism, however, does not envisage the possibility of implementing R&I and demonstration programmes in an integrated way[59]; it does not allow for pooling and managing budget from different sources[60] (European Commission, Member States, industry) to ensure alignment of efforts; nor does it ensure budgetary certainty to stakeholders involved that would be a clear incentive to cooperate in a structured and sustainable way on specific strategic areas. It is also not suited for ensuring the availability of shared competence and infrastructures – one of the key needs identified by the stakeholders in the consultation process (see Annex 2).[61] Last but not least, it does not sufficiently stimulate synergies between the cybersecurity civilian and military research and innovation communities given that Horizon 2020, under which rule the cPPP is created, puts clear boundaries to civilian-military cooperation by requiring that the research activity is fully motivated by, and limited to, civil applications only.[62]

These inherent limitations of the existing cooperation mechanism are an important driver for both Problem 1 and 2 hampering effective cooperation and pooling of investment necessary to enable cybersecurity communities to take advantage of know-how, skills and resources that exist across the EU.

At the same time national initiatives across a few Member States aim to bring together the competencies and industrial players in this area[63], potentially helping European companies to join forces and expand across a number of European countries. These, however, do not have the capacity to effectively link know-how and resources spread across the EU.

2.3.3 Driver 3: Lack for framework for joint procurement for costly cybersecurity infrastructure

At the moment there is no common European strategy to develop, acquire and ensure access of industrial, research and public sector communities to cybersecurity testing and experimentation infrastructures. As highlighted in section 2.2.2, the mapping of cybersecurity capacities across the EU shows that the sectors (e.g. energy, space, defence) and applications (e.g. HPC, AI) requiring costly facilities to perform experimentation and testing are covered

[58] For an overview of the ECSO working groups please see www.ecs-org.eu

[59] Ad-hoc partnerships between the participants of the cPPP are of course possible, but the contractual arrangement does not allow for the indirect management of the EU budget.

[60] While cPPP industrial partners commit to a certain level of investment, the instrument does not allow for pooling budgets together to implement projects of common interest.

[61] See Annex 2

[62] Article 19(2) stipulates: "Research and innovation activities carried out under Horizon 2020 shall have an exclusive focus on civil applications".

[63] E.g. France: Aix-en-Provence, SAFE Cluster ; Denmark: Karup, CenSec; Finland: Tampere Region, Safety and Security Cluster; Germany: Karlsruhe, secUnity; Germany: Munich, Security Cluster; The Netherlands: The Hague Security Delta

to some extent only by those Member States which traditionally have more resources available to invest.[64]

Although most Member States share the same interests in advancing cybersecurity, they try to satisfy on their own, if feasible at all due to funding problems, the requirements of their national communities[65]. The specifications and procurement of the necessary equipment is done by each Member State on their own, without specific incentive to coordinate with other Member States. This solution allows some Member States to specialise in certain cybersecurity sectors or domains. This approach, however, due to the limited resources and fragmentation of the efforts, does not guarantee either the optimal coverage and access to such facilities by cybersecurity communities, nor does it constitute an economically viable solution both in terms of acquisition and optimal exploitation, as highlighted by both industrial and research communities during the consultation process.

Some Member States (e.g. Italy) are starting to consider the deployment of a public quantum communication infrastructure to secure their critical assets and communication needs, or investing in prototypes and testbeds (e.g. the Netherlands and the UK)[66]. Co-investing at EU level into the deployment of a well-interconnected quantum communication infrastructure would allow maximising the efficiency and covering many more use-cases across Europe, whilst building trust in the technology and acting as a market push for the adoption of such solutions in the private sector.

This driver directly contributes to Problem 2 and 3.

2.3.4 Driver 4: Unused potential of push-pull mechanism for effective market deployment of European cybersecurity products and solutions

The potential of a strong push-pull ecosystem between the (potentially big) demand and supply for cyber-security in Europe is far from being maximised to build up world industrial leadership in the field, ensuring autonomy and protecting our society and economy.

In the healthcare sector for example, hospitals have become incrementally digitalised while often experiencing complex and still largely un-solved security problems - partly relatedto the standards used and the lack of harmonisation of services and regulations. The potential of cybersecurity by design approach to medical devices is not sufficiently exploited either.. When new devices or systems are used, cyber security aspects should be planned and implemented and throughout the process – from the procurement, outsourcing and maintenance phases of new systems needs to be defined beforehand.[67]

In another example, cybersecurity remains a major challenge to enterprises involved in Industry 4.0 and using sophisticated digital Industrial Control Systems. For example, according to a survey carried out by Deloitte-MAPI, close to 70% of manufacturers transmit personal information via connected products, while just 55% encrypt the information they send. Challenges such as the difficulty to quantify losses from cyber intrusions, mismatching lifecycles between production machines and the IT layer, the presence of legacy industrial control systems which are more prone to cyber threats, and the risks associated to sharing data

[64] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 for details)
[65] See Annex 2 on Consultation outcomes
[66] See for example: https://www.thehaguesecuritydelta.com/projects/project/89-national-cyber-testbed
[67] ECSO Working Group on Sectoral Demand: Healthcare Sector Report. March 2018;

across digital supply networks call for better interaction between cybersecurity and industrial/manufacturing communities.[68]

2.4 How will the problem evolve?

The number, complexity and scale of cybersecurity incidents and their impact on economy and society are growing over time and they are expected to further increase in parallel to technological developments, for example with the proliferation of IoT devices. It is predicted that cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021.[69] A strong European cybersecurity sector is important for geo-strategic reasons. However, the three problems and related drivers described above affect EU's capacity to autonomously secure its economy, society and democracy as well as its ability to become a global leader in the cybersecurity field, allowing it to take full advantage of the opportunities presented by this fast growing ICT market.

EU's capacity to autonomously secure its economy, society and democracy

With no policy intervention strengthening cooperation mechanisms and aligning efforts, the cycle of European cybersecurity technology dependency is likely to further deepen. A closely linked consequence is the potential lack of access for European citizens and businesses to security products and solutions based on European values. An insufficient supply of European products and solutions adapted to different critical sectors' and public administrations' needs increases the risk of insufficient protection of these sectors, public decisions and might be weakening the national security of Member States. European industries and public administrations' access to cutting-edge specific and interdisciplinary know-how and testing infrastructure will continue to be limited. The lack of a clear strategy and concerted efforts to address the large cybersecurity skills gap will also leave Europe both less secure and less competitive.

In fact, as European industries have become increasingly digital, their demand for accessing innovative cybersecurity solutions will not be met in Europe and they will have to look for them outside of the EU. Adopting cybersecurity solutions from other geographies also comprises a certain level of risk, as the technologies could be used for other purposes than purely service-related ones.[70]

Missed economic opportunities of cybersecurity supply and demand sectors

Europe is a net importer of cybersecurity products and solutions. With no policy intervention addressing the fragmentation of European efforts and sub-scale, dispersed investment in cybersecurity industrial and innovation capacities, European cybersecurity industry is not likely to be able to face fierce global competition and take advantage of this opportunity.

The lack of policy intervention is likely to leave the European cybersecurity industry (especially SMEs and start-ups) more exposed to mergers and acquisitions[71] by non-European actors, weakening the European sector and leaving Europe also much more vulnerable and

[68] ECSO Working Group on Sectoral Demand: Industry 4.0. March 2018

[69] "Global State of Information Security Survey", PwC, 2016, http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.

[70] See for example: "China's ghost in Europe's telecom machine", https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine/.

[71] Some recent examples include the acquisition of Stonesoft (FI) by McAfee, Secusmart (DE) by Blackberry, Anubis Networks (PT) by BitSight; See also: *Cyber Security M&A Decoding deals in the global Cyber Security industry*,

technologically dependent on others. This is also closely linked with the risk of aggravated brain-drain - another side of already mentioned skills challenge.

Beyond the supply industry, cybersecurity is also a major opportunity for other European sectors and could become Europe's competitive advantage. However, without policy intervention allowing European businesses to access interdisciplinary cybersecurity knowledge and infrastructure to secure their products, Europe risks to under-exploit cybersecurity as a competitive advantage for European industries at large.

3 WHY SHOULD THE EU ACT?

3.1 Legal basis

EU action is justified based on two Treaty provisions in particular: The EU is empowered to encourage an environment favourable to cooperation between undertakings and fostering better exploitation of the industrial potential of policies of innovation, research and technological development (art. 173 of the TFEU). Furthermore, Art. 187 TFEU specifies that the EU may set up the structures needed for the efficient execution of EU research, technological development and demonstration programmes.

3.2 Subsidiarity: Necessity of EU action

Cybersecurity is an issue of common interest of the Union. As outlined in the joint Communication of September 2017[72] and endorsed by Council Conclusions[73] the EU needs to make sure that it has the technological capacities to secure its economy, democracy and society. The scale and cross-border character of incidents such as *WannaCry* or *NonPetya* are a point in case. For Europe to be prepared it needs to have a thriving cybersecurity ecosystem, including industrial and research communities.

As described in the sections above, the nature and scale of the cybersecurity technological challenges and insufficient coordination of efforts within and across the industry, public sector and research communities require the EU to further support coordination efforts both to pool a critical mass of resources and ensure better knowledge and assets management. This is needed in view of the resource requirements related to certain capabilities for cybersecurity research, development and deployment (see section 2.2.2 for examples); the need to provide access to interdisciplinary cybersecurity know-how across different disciplines (often only partially available at the national level); the global nature of industrial value chains, as well as the activity of global competitors working across the markets.

None of the options analysed in this Impact Assessment go beyond what is necessary to achieve the objectives set in the following section in a satisfactory manner. Furthermore, the scope of EU intervention would not impede any further national actions in the field of national security matters.

[72] JOIN(2017)450

[73] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

3.3 Subsidiarity: Added value of EU action

The consultation activities carried out for this Impact Assessment (see Annex 2) confirmed the relevance of the Commission's proposal as outlined in the *Communication on Resilience, Deterrence, and Defence adopted in September 2017*. Stakeholders from the industrial and research communities considered that the Centre and the Network could add value to the current efforts on the national level by helping create a Europe-wide cybersecurity ecosystem allowing better cooperation between the research and industry communities. They also considered it necessary that the EU and Member States take a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and innovation only. Stakeholders expressed the need to gain access to key capabilities such as testing and experimentation facilities and to be more ambitious in closing the cybersecurity skills gap e.g. through large-scale European projects attracting the best talents. All of the above was also seen as necessary for Europe to be recognised globally as a leader in cybersecurity.

In the consultation activities undertaken since September 2017[74] as well as in dedicated Council Conclusions[75] Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity. Specifically with regard to the possible Centre, Member States stressed the importance of its coordinating role in support of the network. In particular with regard to national activities and needs in cyber defence, most of the Member States who had responded to a dedicated request by the European External Action Service request stated that EU added value is seen inter alia in training and education and in supporting industry through research and development.[76] The potential network and capacity building activities would indeed be implemented together with Member States or entities supported by them. Collaborations between the industry, research and/or public sector communities would bring together and strengthen existing entities and efforts at not create new ones (for further information see Section 5). Member States would also be involved in defining specific actions targeting the public sector as a direct user of cybersecurity technology and know-how.

At the same time, this initiative will not target cybersecurity "operational cooperation" as governed by the NIS Directive and addressed at EU level by ENISA and the CSIRT Network set up by the Directive.

EU action is therefore justified on grounds of subsidiarity and proportionality.

4 OBJECTIVES: WHAT IS TO BE ACHIEVED?

Based on the problems identified in section 1, the following policy objectives for the current initiative have been set:

4.1 General objectives

The main policy objectives of the policy initiative are:

[74] See Annex 1 and 2

[75] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

[76] EEAS, March 2018

1. Ensure that the EU retains and develops the essential (technological and industrial) capacities to autonomously secure its digital economy, society and democracy, and that Member States benefit from the most advanced cybersecurity solutions
2. Increase global competitiveness of EU cybersecurity companies.
3. Ensure European industries have access to capacities and resources to turn cybersecurity into their competitive advantage.

4.2 Specific objectives

With the general objectives in mind, the initiative intends to achieve the following specific objectives:

1. Develop effective mechanisms for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement a mission-driven, strategic cybersecurity agenda responding to industrial and public authorities' needs;
2. Pool knowledge and resources to provide leading-edge capabilities and infrastructures to support industry and research community in developing and validating new technologically advanced products and solutions.
3. Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.
4. Support cybersecurity start-ups and SMEs to attract investment including venture capital.
5. Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

4.3 Functionalities and governance of the Network and the Centre

In its September 2017 Communication, the European Commission announced the intention to set up a network of cybersecurity centres of expertise with a European Research and Competence Centre at its heart to pool resources, overcome fragmentation of efforts across the EU and stimulate the development and deployment of technology in cybersecurity. It also envisioned it to contribute to the cooperation between Member States in the area of cyber defence.

This section outlines a number of functionalities and governance elements, which will need to be taken into consideration when assessing the options for creating the Centre.

Functionality 1: Flexibility to allow different cooperation models with the network of competence centres, in line with Member States' priorities, to optimise the use of existing knowledge and resources

---

To facilitate cooperation between all relevant actors across Europe different network structures could be considered:

- A geographically organised network (see figure 8), which would link the European Competence Centre with one Coordination Centre per Member State creating a structure dealing horizontally with cybersecurity industrial and research challenges;
- A thematically organised community (see figure 9), which envisages supporting projects related to challenges in a specific sector or cybersecurity domain (e.g. network security, cryptography, cybersecurity of the energy sector, etc.)
- A hybrid model combining the elements of both aforementioned models

Figure 8 Geographically organised network

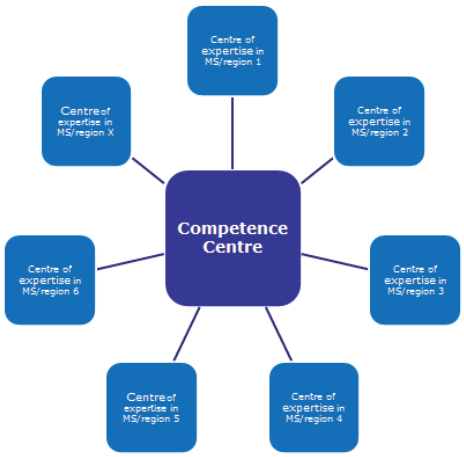
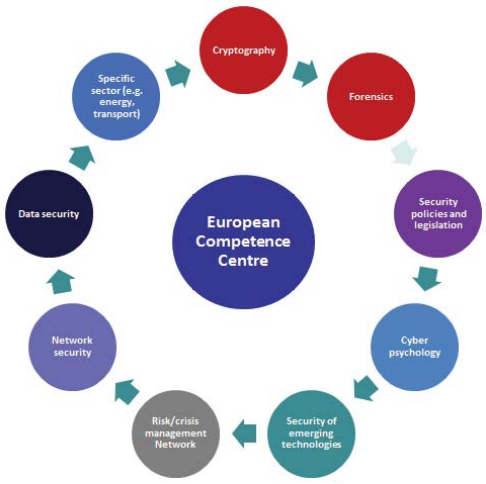


Figure 9: Thematically organised community



As highlighted by stakeholders (both the industry and research communities as well as Member States)[77] during the consultation process, the cooperation model chosen will have to take into consideration the need of:

- Linking the competences spread across the EU while allowing collaboration in smaller circles (e.g. on a regional level);
- Taking advantage of existing excellence while improving capacities of Member States that might still be lagging behind;
- Interdisciplinary approach allowing combining expertise coming from different disciplines;
- Ensuring flexibility to act along the value chain to respond to fast pace and fast evolving environment;
- Encouraging long-term cooperation while leaving space for competition.

This set of diverse requirements cannot be met by Model 1 or Model 2 only. A hybrid option building on the strengths of both models should be therefore used. A "network of networks" created according to a hybrid model and supported by the Centre to facilitate cooperation and synergies, could be structured as follows:

[77] See Annex 2 and e.g. High level Roundtable with Member States, VP Ansip, Commissioner Gabriel, 5 December 2017.

1. **The Network of National Coordination Centres** – each Member State will nominate a national competence centre (e.g. a public body or non-profit association/cluster), which would undertake a number of tasks:

   A. **Play the hub role of a "liaison or contact point"** at the national level for the Network and the European Cybersecurity Research and Competence Centre. Some funding should be made available for these National Coordination Centres to carry out specific tasks and in particular to allow them to engage in a sustainable manner in coordination activities with both the competence centres existing within their Member States as well as with the European Competence Centre and the Network. This funding could cover costs such as e.g. human resources costs for a liaison officer(s), meeting costs, necessary coordination tools, etc.

   B. **Capacity building for the network at the national level** –identifying capacity building needs at the Member States level (e.g. in terms of investment needed in testing and experimentation infrastructure at the national level, tools as well as training). In addition to their respective own national resources, the National Coordination Centres will be able to draw on EU funding in order to respond to these needs. Where economies of scale can be realised (e.g. on regional or European level), the National Cybersecurity Competence Centres would be taking active part in joint procurement activities at the European level.

   C. **Acting as a one-stop-shop for national players** (public bodies, industries across different sectors, competence centres themselves) seeking advice on how to solve different cybersecurity industrial and technological challenges. The National Centre could refer a specific request to relevant players within the national network. In case of lack of specific expertise at the national level, the request could be referred to the European Cybersecurity Competence Centre to look for necessary support across the EU.

   D. **Stimulating participation of national players in European and regional projects** – the National Cybersecurity Competence Centre would encourage the participation of relevant national players in European and regional cooperation projects (e.g. related to securing smart grids in a region) financed by the European Cybersecurity Research and Competence Centre.

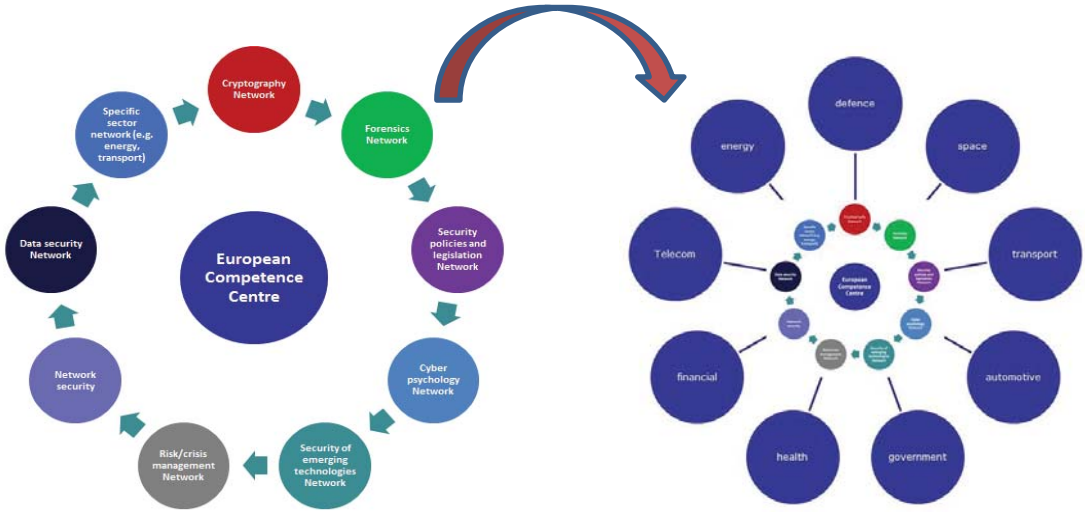
   E. **Implementing and promoting the relevant outcomes of the Network and the Centre's work** at the national level e.g. development of education/training activities following a common cybersecurity skills framework model developed by the Centre and the Network.

   The set-up of the Network of the National Coordination Centres should allow for creating a lasting cooperation structure (going beyond the scope and duration of specific projects) and ensuring full geographic representation of the Union in key cybersecurity development activities. It should also allow identifying specific needs at the national level and upgrading the capacities across the Union. Last but not least, it allows Member States to organise their work on cybersecurity industrial and research challenges in the most efficient way taking into consideration the specificities of their system and existing structures (e.g. clusters, national networks, etc.).

2. The Community

The work, in particular with regard to capacity building and coordination, done through the **Network of National Coordination Centres** should be complemented by an inclusive Cybersecurity Competence Community**.** This Community would seek to gather all relevant European actors involved in cybersecurity technology – in particular research entities, supply-side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network of National Coordination Centres.

Members of the Community should participate in working groups established by the Competence Centre (e.g. on specific cybersecurity domains or on specific application areas such as energy, health, transport). Financial support to collaborative projects on such topics should be allocated following a competitive process based on scientific excellence and industrial and policy relevance. Consortia should typically include all relevant actors of the value chain (from competence centres to supply industry and user (private, public) side).



The European Cybersecurity Competence Centre would facilitate cooperation within the Community as well as between different working groups.

Beyond strategic considerations related to setting up the Network and Community outlined above, practical learnings concerning day-to-day cooperation and research agenda implementation methods used by different networks created under the H2020 Pilot projects (see Annex 6)[78] should inform the process of setting up the actual European Competence Centres Network in 2021.

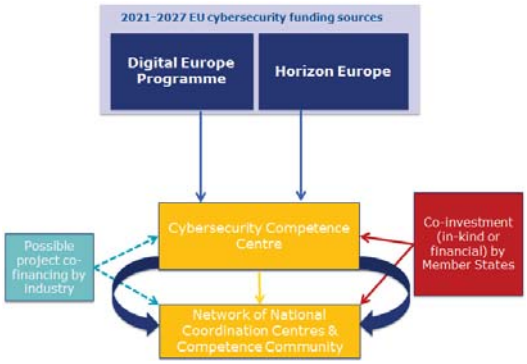
[78] The Commission announced a call for proposals to pilot the creation of efficient networks of competence centres across the EU, able to jointly respond to cybersecurity industrial challenges. The call for proposals was launched on 1 February 2018 and will close on 29 May, with projects starting at the end of (See Annex 6 for more details)

Functionality 2: The Centre as the main implementation mechanism for cybersecurity activities under a number of funding Programmes within the next Multi-annual Financial Framework (MFF)

The European Cybersecurity Competence Centre is also the Commission's proposal for the main implementation mechanism for cybersecurity industrial support activities (including deployment, investment and research) under both Horizon Europe and the Digital Europe programmes.

It is also expected that Member States will significantly contribute to the Centres' and Network's activities notably through financial and in-kind contributions.

Figure 11: Main EU cybersecurity funding sources under MFF 2021-2027



→ **Functionality 3: Safeguarding the Union's and Member States' interest notably by ensuring appropriate governance structure and flexible management**

Given the strategic nature of cybersecurity for European economy, democracy, society but also security the instrument should foresee the possibility for the EU represented by the Commission and to Member States to be part of its governance. This would ensure that the European Commission and Member States can play a significant role in the definition of the strategic orientation and priorities of the entity and take part in the decisions on how its budget is allocated and spent. At the same time an active role for both the private sector (representing supply and demand industries) and research communities should be possible. Last but not least the instrument should allow for flexible management to respond to the requests of different communities depending on their different needs.

The Option chosen should therefore allow the Centre to have the following governance structure consisting of the following bodies:

- The **Governing Board** should be composed of representatives of the public authorities, including the European Commission. The Governing Board should be responsible for strategic decision making, including the annual work plan and a multiannual strategic plan based on input from the Industrial and Scientific Board. The Governing Board should also have the possibility to discuss cybersecurity defence-related topics in an appropriate setting (e.g. ensuring appropriate information security and confidentiality). It is expected that Member States will significantly contribute to the Centres' activities notably through financial and in-kind contributions.

- The **Industrial and Scientific Board** will be responsible for providing input to the Governing Board in the elaboration of the annual work plan and the multiannual strategic plan. This group will be composed of members of the cybersecurity competence community and make use of the experience of the contractual PPP on cybersecurity (involving industry, scientific community, relevant public authorities and the European Commission supported by its scientific branch – Joint Research Centre).

In addition the governance and management provisions should allow for:

- Building close cooperation with the relevant existing bodies and structures such as ENISA, EUROPOL, CSIRTs Network, EDA to complement and support their action and profit from their specific knowledge. The collaboration with these entities should be defined on a case by case basis in order to profit from their evolving expertise, raise synergies and avoid duplication of resources and actions. ENISA and the future Competence Centre will engage in a structured cooperation in areas of mutual interest and in support of each other's respective mandates. In particular, the Competence Centre would be able to benefit from ENISA's experience so far with providing support to the definition of research priorities as well as its eventual market expertise from managing the cybersecurity certification scheme, while the Agency and its direct stakeholders would be among the "beneficiaries" of the outcome of the technology support to industry, research and the public sector provided by the Centre and network.
- In combination with the rules governing its "source" programmes, i.e. the Digital Europe Programme and Horizon Europe, the instrument should also make it possible to introduce provisions to protect the economic and strategic interests of the Union, i.e. protecting IPRs produced in the EU and first exploiting in Europe all EU-funded R&I results as well as to limit certain types of activities to EU-headquartered organisations only.
- Flexible approach to procuring and owning assets such as cybersecurity testing and experimentation facilities:
    - Member States should procure and own the facilities funded mainly by themselves;
    - The infrastructure co-financed from European funds across the Network should be interconnected and made available to the public and private users across Member States according to conditions defined by the Governing Body of the Centre.
    - In case of joint investment in European infrastructures and assets such as test beds, as a first step a hosting entity would be chosen – depending on the needs and capacities either in the Centre itself or in a Member State. The Governing Board should then establish the criteria for the selection of the hosting entity. The Centre and the hosting entity should sign a hosting agreement setting out the entity's responsibilities in installing and operating the infrastructure. Secondly, the Centre should launch the procedure to acquire the necessary infrastructure.

As an entity tasked with the implementation of cybersecurity-related financial support, the duration of the Competence Centre and the Network should be linked to the duration of the MFF (2021-2027). In view of the need to manage "legacy activities" launched towards the end of this timeframe, a duration of the mandate should run at least until 2029. The mandate

and activities of the Competence Centre and Network should be subject to regular evaluation. A proposal to extend its mandate would need to be made for the subsequent financial framework should evaluations (see section 8) prove their effectiveness, efficiency and added-value.

5 WHAT ARE THE AVAILABLE POLICY OPTIONS?

For the right assessment of the different options it is crucial to take into consideration both the objectives and the functional requirements outlined above in order to be able to assess the effectiveness criterion.

The following options have been looked at:

1. **Baseline scenario** - Collaborative Option
2. **Option 1:** Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation
3. **Option 2:** Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities only.

In view of the general commitment already made by the Commission for the present initiative as well as in view of the important role to be played by Member States, the main distinction between the two policy options analysed lies in their scope as reflected in their legal base: an entity only based on article 187 TFEU would limit the initiative to the sphere of research and innovation, and would typically presume a financial contribution from private actors. On the other hand, an entity based on a double legal base (research and innovation as well as industry) would mean a broader mandate covering also, inter alia, industry support measures, fostering collaboration with cyber defence actors and giving a more prominent role to Member States – both in terms of their role in the governance as well as in their role as potential procurers of cybersecurity technology.

The following options have been discarded at an early stage (a brief description is presented in section 5.2):

4. No action at all
5. Network of existing competence centres only
6. Using an existing agency (ENISA, REA, INEA)

5.1 What is the baseline from which options are assessed?

5.1.1. Baseline scenario (status quo) - Collaborative Option

This scenario assumes the continuation of the current approach to building cybersecurity industrial and technological capacities in the EU through supporting research and innovation and related collaboration mechanisms under Horizon Europe.

At the moment cooperation between different types of cybersecurity stakeholders (research organizations, industry, public authorities in their capacity as buyers of cybersecurity solutions) takes place through the cPPP on cybersecurity or directly within the projects financed by the EU funds. The partnership provides a platform of dialogue and helps align efforts by developing the Strategic Research and Innovation Agenda for the Horizon 2020

Work Programme.[79] The mandate of cybersecurity cPPP is limited in time and is foreseen to be revised after 2020.

The contractual Public Private Partnership is well-suited to federate advice on cybersecurity communities' research priorities, which can then be supported through the regular instruments of the Union's Research Framework Programmes.

Under this option the cooperation among expertise centres networks created through the pilot projects [80] could be further facilitated by the European Commission, possibly with the support of the cPPP on cybersecurity. However, this option assumes that the EU does not create a more robust mechanism (with relevant human and financial resources) to maintain and stimulate the network and facilitate structured cooperation between industries, public authorities, and the research community to build EU's cybersecurity technological and industrial capacities. It does not equip itself with a mechanism to effectively pool know-how and skills currently spread across the Union as proved by the mapping of cybersecurity expertise centres[81], nor creates the capacity to provide multinational project management support, testing or simulation services.

Due to inherent limitations of the cPPP legal construct (as described in detail in section 2.3.2), this option does not envisage the possibility of federating and managing budget from different sources (European Commission, Member States). This option allows industrial partners to express commitment about their individual spending (leverage factor) on areas defined in the Strategic Research & Innovation Agenda that could be further monitored by the cPPP. However, it does not envisage resource pooling for direct co-investment in e.g. necessary infrastructures or demonstration projects. The Baseline scenario entails that European industries and authorities will take up risky experimentation by themselves with their own resources and based on limited available infrastructure.

This option assumes the continuation of the support for implementing R&D projects funded through Horizon Europe but does not assume conducting activities to support the translation of the outcomes into marketable solutions nor their deployment across the market.

Last but not least this option also assumes that cybersecurity is not recognised as an area of strategic importance, which requires flexible rules to stimulate openness and exchange with other players on one hand, and to protect the Union's interest in case of work on strategic assets on the other. The cPPP's membership is open to non-EU actors. As a result the dominant, non-EU suppliers are today part of it, influencing the definition of the H2020 Work Programmes. This makes it more difficult for European market actors to develop competitive advantage.

5.2 Description of the policy options analysed in detail

Option 1 – Cybersecurity Competence Network with a European Cybersecurity Industrial, Technology and Research Competence Centre as an entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation

This option assumes creating the Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre as an EU entity with its own legal personality under art. 173 and 187 TFEU.

[79] JOIN (2017)450: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU
[80] See Annex 6
[81] See JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018

This delivery mechanism would allow the Centre together with the Network, in line with the governance model discussed in section 4.3 and taking into account advice from its Industrial and Scientific Advisory Board, to respond to the needs of the industrial and other communities both from the civilian and defence sectors and support them through the following tasks that would respond to the current gaps and needs highlighted by different communities during the consultation process (see Annex 2).

I. Enhancing capabilities, knowledge and infrastructures at the Member States' and EU-level at the service of industries, public sector and research communities.

- Co-invest with Member States in upgrading and interconnecting existing national or regional equipment/tools and related skills to upscale the capacities necessary for successful development of leading-edge cybersecurity products and solutions;
- Co-invest with Member States in infrastructure and tools for European use that are not available at the moment (e.g. Quantum key distribution and facilities for post quantum cryptography). These would be made available to industrial actors across Europe, as well as to the public authorities and the network of expertise centres;

  For example, assessment and validation of the robustness of post-quantum cryptography solutions and specification of implementation modalities (minimal key length, etc.) by the industry or by members of the network will require testing these solutions against attacks run on a supercomputer or a quantum computer that could be made available through the Network and Competence Centre.
- Provide access to these infrastructures and services to a wide range of users (industry, SMEs) to address cybersecurity related industrial challenges helping them to develop innovative products and services to reach global competitiveness.

  For example, the centre and network together with stakeholders could systematically enhance the security of EU medical technologies through vulnerability assessments of medical devices, code auditing of software installed in medical systems and devices, developing innovative security controls (software and hardware) appropriate for the EU medical technologies, and developing EU profiles of all EU medical products for certification.
- Provide proactive cybersecurity technical assistance for developers, integrators and manufacturers : The research community of the Network/Centre could deliver timely and context-relevant alerts, advisories and guidance to developers, integrators and manufacturers in all industries about the cybersecurity requirements and risks of new emerging technologies (e.g. neural networks for AI deep earning, robotics, Quantum tools, satellite, virtual reality technologies) and modules (e.g. new software libraries, modules, components) that wish to use in designing future products and services. This will be an effective single point of reference for civilian and military industrial developers, integrators and manufacturers.

II. Stimulating wide deployment of European cybersecurity products and solutions

- Ensure visibility and availability of European cybersecurity products and solutions to public authorities and demand side industries (e.g. for public procurement purposes; e.g. through developing and promoting a user-friendly database of European cybersecurity products and solutions, with information about their possible application across different domains);

- Respond to the demand created by the growing needs of fast digitising public and critical sectors (e.g. health, public administration) by working on joint procurement of leading-edge cybersecurity products and solutions;

III. Supporting cybersecurity start-ups and SMEs to attract investment including venture capital

- Develop tools and coordination mechanisms to facilitate access of cybersecurity start-ups and SMEs to venture capital (e.g. enhance visibility of cybersecurity projects/products European companies are working on; create database of venture capital funds interested in cybersecurity);
- Create a platform of cooperation for cybersecurity SMEs to connect them and foster cooperation on projects but also help them create consortia to respond to tenders and procurement offers;

IV. Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses:

- Provide appropriate input to education policy makers in order to enhance cybersecurity education in particular for the purpose of fostering high-end professional skills (e.g. by developing cybersecurity curricula in civilian and military educational systems); support the alignment, enhance and continuously assess cybersecurity professional certification programmes. Alignment of education and skills will help developing a qualified EU cybersecurity workforce – a key asset for cybersecurity companies as well as other industries with a stake in cybersecurity;
- Facilitate access by other cybersecurity and anti-cybercrime entities (Member State agencies as well as e.g. ENISA, EC3, EUROPOL, CERT-EU, Centre of Excellence for countering hybrid threats) and training centres to state-of -the art methodologies and tools (e.g. AI-analysis, simulation and Deep learning exercise platforms) to perform their operations (e.g. dynamic risk assessment and incident handling, cybersecurity/cyber defence exercises) as effectively as possible. Facilitate the necessary research focused specifically on advancing their cyber-ranges (e.g. Internet-scale simulation environments, modelling/visualization tools and virtual machines) so that interested entities can continuously help the civilian and military stakeholders to handle upcoming complex attacks and incidents and improve preparedness and resilience
- Facilitate access to specialised trainings available throughout the Network

V. Shaping and coordinating Research & Development supporting objectives of the initiative

- Shape, implement and coordinate industrial cybersecurity research and efforts towards a common, continuously evaluated and improved EU cybersecurity research agenda. Act as a single delivery mechanism for different funding programmes (Horizon Europe, Digital Europe Programme) and enhance synergies in relation to the European Defence Fund;
- In collaboration with the industry and the network, support a number of specific large research and demonstration projects in key next generation digital technological capabilities (including e.g. Artificial Intelligence, High Performance Computing, Virtual technologies, Quantum Communications, Post-quantum Encryption).

- Solve sector-specific cyber security industrial challenges: collaborate with industrial stakeholders to identify sector-specific (e.g. automotive, energy, transport, finance, governmental, telecom, defence, transport, space) cyber security needs requirements and challenges; develop and support cyber security research roadmaps for all sectors.

  For example, the centre with the members of the network could address the cybersecurity of connected, autonomous vehicles by developing penetration test beds for assessing the security risks and vulnerabilities of prototypes, developing innovative reference architectures, and providing a consistent set of cybersecurity guidelines across the manufacturing and connectivity value chain.

  For example, a cyber defence dimension could include supporting Member States' development of common capabilities, facilitating joint cyber defence training, exercises and testing, and supporting work on cyber defence taxonomies and standards, in line with priorities commonly agreed by Member States within the EU.[82]

- Support research to facilitate and accelerate certification processes[83] (e.g. build new certification methodologies and easy-to-use auditing tools).
- Develop knowledge management tool to ensure that the industrial community is able to access and take advantage of the expertise represented in the network.

Governance and management

The body would have its own governance structure, staff and a dedicated budget. The suggested legal base allows for the creation of the public-public governance structure with an important advisory role of the private sector and the research communities. It also allows pooling contributions and resources from both the Union and Member States and could also envisage contributions from the industry, where approporiate.

Experience from other bodies based on the same Treaties provisions shows that this model allows as well for flexible set-up of cooperation with the network[84], including the different possible structures discussed in section 4.3 – namely, a network organised along geographical lines, a Community organised along thematic lines, or a combination thereof.

5.2.1 Option 2 – Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities

This option assumes creating the Network of Competence Centres with the Cybersecurity Research and Competence Centre as a Union Body established under Art 187 TFEU[85] that can be used for the indirect management of the EU budget.[86]

[82] Further potential tasks with regard to defence are discussed in JOIN(2017)450.

[83] These activities would be without prejudice to the General Data Protection Regulation and in particular to its relevant provisions regarding certification.

[84] See example of the Knowledge and Innovation Communities and their relationship with the European Institute of Innovation and Technology.

[85] A JU is established by a Council Regulation, taking into account the opinion of the European Parliament and the European Economic and Social Committee

[86] In accordance with Art 58.1 (c)(iv) of the Financial Regulation (FR). Indirect management means that funding programme is implemented by a third-party organisation (e.g. public-private partnership in the form of a Joint Undertaking) and not by the EU institutions, executive agencies or Member States themselves. See: http://ec.europa.eu/budget/explained/management/managt_who/who_en.cfm

Under this option the Centre together with the Network could implement the following types of tasks that would respond to the current gaps and needs highlighted by different communities during the consultation process.

I. Shaping and coordinating Research & Development:

Under this option shaping the research efforts would focus on civilian communities. The Centre together with the Network could do the following tasks:

- Shape, coordinate and support cybersecurity research towards a common, continuously evaluated and improved EU cybersecurity research agenda.
- In collaboration with the network and the industry, support a number of specific large research and demonstration projects in key next generation digital technological capabilities (including e.g. Artificial Intelligence, High Performance Computing, Virtual technologies, Quantum Communications, Post-quantum Encryption).
- Solve sector-specific cyber security industrial challenges: collaborate with industrial stakeholders to identify sector-specific (e.g., energy, transport, finance, governmental, telecom, defence, transport, space) cyber security needs requirements and challenges; develop and support cyber security research roadmaps for all sectors.
- support research to facilitate and accelerate certification processes (e.g. build new certification methodologies and easy-to-use auditing tools).
- Develop knowledge management tool to ensure that the community is able to access and take advantage of the expertise represented in the network.

II. Enhancing EU-level and Member States' research capabilities, knowledge and infrastructures to support research and industrial communities as well as public authorities:

- Co-invest with Member States in upgrading and interconnecting existing national or regional research equipment/tools and related skills to upscale the capacities necessary for conducting leading-edge cybersecurity research activities.
- Co-invest with Member States in research infrastructure and tools for European use that are not available at the moment. They would then be made available the network of expertise centres and industrial actors across Europe (e.g. facilities for post quantum cryptography).
- Provide access to these infrastructures and services to a wide range of users (research organisations, industry, SMEs) to conduct research related to cybersecurity challenges.
- Provide proactive cybersecurity technical assistance for developers, integrators and manufacturers. The research community of the Network/Centre could deliver timely and context-relevant alerts, advisories and guidance to developers, integrators and manufacturers in all industries about the cybersecurity requirements and risks of new emerging technologies (e.g. neural networks for AI deep earning, robotics, Quantum tools, satellite, virtual reality technologies) and modules (e.g. new software libraries, modules, components).

III. Support closing the cybersecurity skills gap

- Helping to align cybersecurity skills programmes and adapting them to specific sectorial needs, which could serve as an input to education policy makers;

- Coordinating and facilitating necessary research to improve and advance training courses offered by different educational organisations to help them adapt programmes to constantly evolving and complex cybersecurity challenges; Facilitating access to specialised trainings available throughout the Network

Governance and features

An entity set up under art.187 TFEU is an autonomous EU legal entity, with its own budget, staff, structure, rules and governance that can be tasked to implement actions under Framework Programmes (e.g. H2020 or CEF under current budgetary perspective). It can combine budget with other sources of funding (national, private) allowing the implementation of Research & Innovation and demonstration programmes in an integrated way. It gives a key role to industry as the main partners of the Commission.

Experience from other bodies based on the same founding regulations – typically Joint Undertakings – shows that this model allows as well for a flexible set-up of cooperation with the network[87], depending on the final decisions that will be taken by co-legislators related to how the network should be structured and interact with the Centre (please see section 4.3). However, given the civilian character of the EU R&I Framework Programmes, such an entity would not be best placed to create synergies with the defence sector.

An entity limited to supporting research and innovation can carry out procurement procedures for infrastructures, necessary to support research and development activities (typically such a structure has its own procurement and financial rules adopted by the Governing Board). Established as a Union body, it can benefit from VAT and excise duties on its purchases in all EU Member States and may adopt procurement procedures not subject to the Directive on public procurement as implemented in national law.

This option would limit the intervention to the area of research and innovation. The capacity of such an entity to support the large-scale deployment and take up of new secure technologies through the Digital Europe Programme or any other programme would be limited.

5.3 Options discarded at an early stage

5.3.1 No action at all

This option would mean stopping all public support at the European level for research, innovation and industrial development in cybersecurity field. The option is discarded because it is contrary to key strategic documents, including the 2013 EU Cybersecurity Strategy, the Joint Communication of September 2017[88] as well as supporting Council Conclusions[89], which point to a clear vision set by the Heads of State and Government at the Tallinn Digital Summit for Europe to be "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."[90]

[87] See example of SESAR Joint Undertaking: http://www.sesarju.eu/
[88] JOIN(2017)450.
[89] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)
[90] Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit, 29 September 2017

5.3.2 Network of existing competence centres only

This option assumed that the delivery mechanism does not include any common governance structure to coordinate network activities. Partner organisations would simply cooperate to achieve a common goal based on programming documents and mutual agreement. Without a centre, there would be a lack of a focal point that would ensure accountability of all responsibilities taken by the network.

This type of networks has already been implemented in a number of projects financed under past Framework Programmes. Such collaboration can be quite effective in achieving the desired goals within their scope, but their sustainability beyond project timeline is very limited and knowledge management mechanisms allowing to take advantage of their outputs are insufficient. For example, the instrument of "Networks of Excellence", introduced with FP6, was discontinued under FP7. An independent expert group identified "achieving 'durable integration' and creating joint organisational arrangements and structures (…) the major problems for achieving the core objectives of NoEs."[91]

This option would focus the intervention on the capacity-building and ecosystem-building aspects at the regional and national level with limited positive impact in terms of reducing fragmentation and sustainable knowledge and capacity sharing at the European level. Without a central implementation mechanism and project manager, the procurement of particularly costly infrastructure and pan-European solutions would be practically impossible, and cooperation in this regard would likely be limited to bilateral or multilateral cooperation between larger and more advanced Member States, if at all.

5.3.3 Using an existing agency

This option would assume conferring the tasks of the Competence Centre to one of existing agencies – either ENISA or one of the executive agencies - Research Executive Agency (REA) or Innovations and Networks Executive Agency (INEA).

The option of using ENISA was discarded on the basis of a mismatch between the objectives, the desired functionalities of the Competence Centre and the mandate and related structure of ENISA (current, as established by Regulation of 2013[92], and future, as proposed by the Commission in September 2017[93]). In particular:

- ENISA is a decentralised EU Agency founded on the basis of article 114 of the TFEU. Its focus on policy advice and facilitation of operational cooperation is not suitable for the mission of the Centre. Furthermore, its mandate is limited to internal market issues, which leaves e.g. any defence issues out of the scope of its action.
- The tasks entrusted to ENISA, mostly focused on strategic advice on regulatory issues (support to EU policy development and implementation), capacity building and operational cooperation to prevent and respond to cybersecurity incidents are meant to satisfy different needs than the Competence Centre, with a strong focus on support to industry, research and development and public procurement.
- In order to support its objectives of enhancing cooperation and coordination at EU level, the structure of ENISA, as confirmed by the impact assessment supporting the current proposal for the new mandate, needs to stay "agile" and leverage on the EU

[91] An example of the Network of Excellence on cybersecurity was SYSSEC. Counting over 80 members, it was considered very successful. However with the end of the grant, also operations ended.

[92] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

[93] Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU)526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"); COM(2017) 477)

and Member States' competences. The Commission proposal opted for a structured cooperation between ENISA and the other EU bodies with competences/stakes in cybersecurity.

(Section 4.3 discussed the possible future relationship between ENISA and the cybersecurity competence centre and the network.)

The option of entrusting the tasks to the Research Executive Agency (REA) or Innovations and Networks Executive Agency (INEA) was discarded at an early stage due to a number of factors. Firstly, the governance of these Agencies does not allow for active participation of Member States. This is a disqualifying factor given that cybersecurity is perceived by many Member States as a field closely linked to national security. This would hamper achieving the objectives of the initiative (e.g. pooling resources). Secondly the tasks of the Network and Competence Centre as requested by stakeholders in the consultation process should go largely beyond managing EU funds for cybersecurity only, which is the core mandate of executive agencies. General purpose agencies such as REA and INEA could not nurture a specific in-depth cybersecurity expertise required by the Centre in a sustainable manner.

6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section analyses the economic, environmental and social impact of the options as compared to the baseline scenario, in line with the Better Regulation Guidelines together with the coherence with other policy and the views of stakeholders.

6.1 Option 1: Cybersecurity Competence Network with a European Cybersecurity Industrial, Technology and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation

Effectiveness

Objective 1: Develop an effective mechanism for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement mission-driven cybersecurity agenda responding to industrial and public authorities' needs;

A significant positive impact on improving coordination and alignment of the efforts is expected under this option as the suggested mechanism - with its own budget and human resources – should allow sustainably facilitate the efforts of all relevant communities (demand and supply side industry, public administration, research communities from both civilian and defence fields).

The suggested mechanism is suited for supporting a wide range of the Network's, community and own activities supporting industrial development (e.g. pooling resources and procuring and co-investing in infrastructure, in particular for testing, experimentation and certification, supporting deployment activities, skills development, etc.) as well as for implementing a strategic research agenda responding to industrial needs.

It can also act as a single implementation mechanism for cyber security -related financial support from the Digital Europe Programme and Horizon Europe programmes, and enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund.

In conclusion, the entity as described under Option 1 is effective to achieve Objective 1.

Objective 2: Pool knowledge and resources to provide leading-edge capabilities and infrastructures to support industry and research community in developing new technologically advanced products and solutions.

The mechanism suggested under Option 1 allows for pooling public and private resources to co-invest with Member States in upgrading available capacities and invest in developing assets that are still missing (e.g. facilities for post quantum cryptography) and which could then be made available to the industrial actors across Europe as well as to public authorities and the research community. In conclusion, Option 1 is effective to achieve Objective 2.

Objective 3: Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.

As described in section 5.2.1, the Option 1 allows to conduct activities supporting wide deployment of European cybersecurity products and solutions across the market helping Member States shield their economies and societies against cyber threats on one hand and increasing competitiveness of the European cybersecurity industry on the other (e.g. by working on joint procurement of leading-edge cybersecurity products and solutions in response to growing demand from fast digitising public and critical sectors such as e.g. health, public administration; conducting activities ensuring visibility of European cybersecurity products to the demand side industries, supporting access of SMEs to public procurement and venture capital). In conclusion, Option 1 is effective to achieve Objective 3.

Objective 4: Support cybersecurity start-ups and SMEs to attract investment including venture capital.

As described in section 5.2.1, Option 1 allows conducting activities start-ups and SMEs to attract investment to turn their research ideas into a marketable product or solution. Given that access to funding is one of key challenges for the European cybersecurity SME and start-up community, the mechanism is likely to improve the situation by helping the community gain visibility towards potential investors. This should help retain the know-how and business competences in Europe and avoid brain-drain of specialists, who currently need to look for opportunities to develop their ideas outside the EU. In conclusion, Option 1 is effective to achieve Objective 4.

Objective 5: Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

As described in detail in section 5.2.1, Option 1 allows to complement the efforts of the Member States by providing appropriate input to education policy makers in order to enhance cybersecurity education (e.g. by developing cybersecurity curricula in civilian and military educational systems but also input for basic cybersecurity education); The Option would also allow supporting the alignment and continuous assessment of professional cybersecurity certification programmes - all necessary activities to help close cybersecurity skills gap and facilitate industries' and other communities' access to cybersecurity specialists. The Option also allows supporting targeted research to enable other cybersecurity entities and training centres to have state-of -the art methodologies and tools to advance their cyber-ranges and therefore improve preparedness and resilience to cyber-attacks. In conclusion, Option 1 is effective to achieve Objective 5.

Efficiency/ Impact on economy, competitiveness, competition and SMEs

The Option 1 scenario would have a positive impact on the EU's competitiveness and SMEs as it assumes creating a mechanism capable of building Member States' and Union's cybersecurity industrial capacities and effectively translating European scientific excellence into marketable solutions that could be deployed across the economy.

This option allows pooling resources to invest in necessary capacities at the Member States' level or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). These assets could be used by industries and SMEs across different sectors to ensure that their products are cybersecure. This is likely to result in:

- Increased access of SMEs and industries from different sectors to such facilities, which will stimulate innovation, allow translating research results into real products and solutions and shorten the development processes. This will also cut costs for some demand-side businesses, who would not have to either invest in their own testing facilities or look for them outside Europe;
- Through support for capacity and ecosystem-building at national level and within thematic networks: better market insights and more contact with potential business partners for SMEs.
- Through support to demand-supply articulation: better market opportunities for SMEs
- Further turning cybersecurity into a competitive advantage factor for European industries at large;
- Allowing Member States to make investment economies thanks to coordinated efforts with other interested Member States;

The scenario also envisages mechanisms to support market deployment of cybersecurity products and solutions. While respecting the rules of fair competition, these activities would help the European cybersecurity industry to overcome current market barriers and increase their market share. In the mid-term this should help Europe reaching import-export balance as far as cybersecurity products and solutions are concerned and in the longer-term become a net exporter in the field.

This scenario also allows taking advantage of the dual-use market opportunities by allowing the defence and civilian communities to work together on shared challenges.

This option is also likely to add-value to the national efforts of addressing cybersecurity skills gap – a challenge not only in terms of securing economy but also a key resource for European industries to ensure their competitiveness.

At the EU level, this option also allows to improve coherence and synergies between different funding mechanisms (Digital Europe Program, Horizon Europe) and reduce administrative burden of managing different cybersecurity funding programmes. Pooling resources will also help to achieve the economies of scale and help avoid double-spending.

This option does not foresee any new regulatory obligations for businesses. At the same time the businesses and especially SMEs are likely to reduce their costs related to their efforts in designing innovative cyber secure products.

In conclusion, the Option 1 scenario has clear positive impact on economy, competitiveness, competition and SMEs, much higher than that of the baseline scenario. It is also likely to substantially increase Member States' capacities to autonomously secure their economies, including protecting the critical sectors, increasing competitiveness of European cybersecurity businesses as well as industries across different sectors, which will be able to appropriately

secure their existing assets and design secure innovative products while reducing security related R&D costs. This should ultimately allow the EU to become a leader in the next-generation digital and cybersecurity technologies.

Social and Environmental Impact

This Option is likely to have a positive impact on the social sphere. It will allow public authorities and industries across Member States to more effectively prevent and respond to cyber threats by offering and equipping themselves with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services).

Increased capacity of the European Union to autonomously secure its products and services is also likely to help citizens enjoy their democratic rights and values (e.g. better protect their information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life) and consequently increase their trust in the digital society and economy.

No specific or major impact on the environment is expected under this scenario. However, an indirect positive impact could be achieved through developing specific cybersecurity solutions for sectors having potentially huge environmental impact (e.g. nuclear power plants). This could help avoid potentially devastating consequences of cybersecurity attacks on this type of infrastructure.

Stakeholder support

The majority of industrial and research community stakeholders consulted argued in favour of setting up a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy (please see Annex 2 on Consultation outcomes). Stakeholders used the following key arguments:

- The cybersecurity support under next MFF should go beyond research and development activities only combining also market deployment activities;
- The Centre and the Network could add value to the current efforts at the national level by:
    - Helping create Europe-wide cybersecurity ecosystem allowing to cooperate public authorities, industries and research communities from both civilian and military sectors;
    - Helping the community work with a longer-time, strategic perspective;
    - Ensuring access to industrial and research communities across Europe to key capabilities such as testing and experimentation facilities;
    - Helping achieve interdisciplinary approach to cybersecurity in Europe and becoming a knowledge management platform, which could be used by the whole cybersecurity community;
    - Helping close the cybersecurity skills gap and preventing brain drain by offering interesting challenges for European researchers (e.g. large-scale, ambitious European projects attracting highly-skilled people).
    - Ensuring visibility of European cybersecurity know-how and competence both within the EU and globally;

At the same time, stakeholders emphasised that the key to success will be a well-defined role of the Centre and an inclusive, collaborative approach to the Network to avoid creating new silos. The structure should also be flexible so that it can be easily adapted given that

cybersecurity is a fast-pace environment.

6.2 Option 2: Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre limited to research and innovation activities

Effectiveness

Objective 1: Develop effective mechanism for long-term strategic cooperation of all relevant actors (public authorities, industries, research community from both civil and defence areas) to set and implement mission-driven cybersecurity agenda responding to industrial and public authorities' needs;

The mechanism suggested under Option 2 (based on art. 187 of TFEU) due to its nature (legal entity with its own staff, budget, structure, rules and governance) is likely to have a positive impact on achieving better coordination of the efforts of a wide range of stakeholders (public administration, demand and supply side of the industry, research communities). However, given the nature of the research programmes for which this instrument is dedicated, it would be possible to involve the defence community in this cooperation only to a very limited extent and only for work on civilian cybersecurity applications. This instrument does not allow for coordinating activities going beyond research and development only e.g. supporting market deployment of cybersecurity products and solutions, nor would it allow the involvement of actors from cyber defence. In conclusion, such an entity is partially effective to achieve Objective 1.

Objective 2: Pool knowledge and resources to provide leading-edge capabilities and infrastructures to support industry and research community in developing new technologically advanced products and solutions.

As described in section 5.2.2, an entity limited to supporting research and innovationallows for pooling public and private resources to co-invest with Member States in upgrading available capacities and invest in developing assets that are still missing at the European level and which could then be made available to the public authorities, the network of expertise centres and industrial actors across Europe; The use of these resources should be, however, limited to research and development activities. In conclusion, such an entity is partially effective to achieve Objective 2 given the limitation related to the purpose for which improved capacities could be used.

Objective 3: Stimulate wide deployment of European cybersecurity products and solutions across the economy and the public sector through, among others, joint procurement.

An entity limited to supporting research and innovation could not implement the tasks related to stimulating deployment of cybersecurity products and solutions in view of the limitations imposed by the Treaty legal base. This means that the Centre could not support e.g. joint procurement of leading-edge cybersecurity products and solutions nor other activities encouraging market deployment. In conclusion, Option 2 is not effective to achieve Objective 3.

Objective 4: Support cybersecurity start-ups and SMEs to attract investment including venture capital.

An entity limited to supporting research and innovationcould support these tasks as long as they concern financing for research and development and not for marketing and deployment of products and solutions across the market. Given that access to funding, including venture capital, is one of the weaknesses of the European cybersecurity ecosystem, the Centre is not likely to substantially improve this situation as investors are looking for business opportunities rather than for the research outcomes only. Such an entity is therefore effective to achieve Objective 4 to a very limited extent.

Objective 5: Support closing the cybersecurity skills gap by aligning cybersecurity skills programmes, adapting them to specific sectorial needs and facilitating access to targeted specialised training courses.

An entity limited to supporting research and innovationcould have a positive impact on closing the cybersecurity skills gap as it would be in a position to carry out targeted research to enable other cybersecurity entities to improve their training and cyber ranges. However a whole range of tasks related to aligning cybersecurity skills curricula and assessing the cybersecurity professional certification programs would fall outside the scope of the Centre due to the mandate limitations imposed by the EU Treaties. In conclusion such an entity is partially effective to achieve Objective 5.

Efficiency/ Impact on economy, competitiveness, competition and SMEs

The Option 2 scenario would have a positive impact on EU's competitiveness and SMEs as it allows for creating a mechanism fostering Member States' and Union's cybersecurity research and innovation capacities.

- This option allows creating synergies and pooling resources to invest in necessary capacities at the Member States' level or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). These assets could be used by researchers, industries and SMEs across different sectors for research and development purposes. This effort is likely to result in increased access of SMEs and industries from different sectors to such facilities, which will stimulate innovation. This will also cut costs for some demand businesses, who would not have to either invest in their own testing facilities or look for them outside Europe. However the efficiency gains under this option are limited as the capacities should serve only research and development processes and not e.g. turning prototypes into real products that could be directly deployed across the market.
- As in Option 1, allowing Member States to make investment economies thanks to coordinated efforts with other interested Member States;

As an entity limited to supporting research and innovation does not allow for activities directly supporting the market deployment of cybersecurity products and solutions, its impacts on helping the industry overcome the current market barriers and increasing their market share would be substantially limited.

Europe would also not be able to take economic advantage of the dual-use market opportunities as such an entity is not the right instrument to encourage defence and civilian cooperation on shared challenges.

This option is also likely to add-value to the national efforts of addressing cybersecurity skills gap to a limited extent as it does not envisage the possibility of going beyond research

activities for skills development.

At the EU level, this option is also likely to have limited impact on improving coherence and synergies between different funding mechanisms (Digital Europe Program and Horizon Europe and reducing administrative burden of managing different cybersecurity funding programmes.

This option does not foresee new regulatory obligations for businesses. At the same time the businesses and especially SMEs are likely to reduce their costs related to their research efforts.

In conclusion, the Option 2 scenario has a mixed neutral-positive impact on economy, competitiveness, competition and SMEs. This option is likely to contribute to increased competitiveness of European cybersecurity industry although it would not have a direct positive impact on improving its global market position in terms of market share. It is also likely to help Member States get access to the outcomes of cybersecurity research and innovation projects but would not be sufficient to help their wide deployment across key sectors relevant for public domain.

Social and Environmental Impact

This Option is likely to have some positive impact on the social sphere as it would help accelerate the research on the cybersecurity topics of social and environmental relevance. However, this impact is likely to be weaker than in case of Option 1 as this mechanism does not envisage supporting the transition from prototypes to products that could be deployed widely across sectors.

Stakeholder support

As mentioned in the analysis of the impacts of the Option 1 a majority of industrial and research community stakeholders consulted argued in favour of setting up a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy (see also Annex 2). According to stakeholders, while supporting research and innovation activities is important, it will not be sufficient to achieve the policy objectives outlined.

7 HOW DO THE OPTIONS COMPARE?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the three core criteria of effectiveness, efficiency and coherence, as well as taking into account the support expressed by the different stakeholders.

Effectiveness of the instrument

Both an entity based on art. 173 and 187 TFEU and an entity limited to supporting research and innovation would be more effective in achieving the objectives than the baseline scenario. However, an entity only based on Art.187 would not be able to achieve one of key objectives related to supporting market deployment. It is also less effective in reaching 4 out of 5 remaining objectives than the entity described under Option 1.

Impact on economy, competitiveness, competition and SMEs

Both instruments, an entity based on art. 173 and 187 TFEU and an entity only based on Art.187, would have a positive impact as compared to the baseline scenario. However, the impact of an entity only based on Art.187is expected to be much lower than that of the entity

based on art. 173 and187 . This is mainly due to the limitation and scope to supporting research and development, which do not allow for market deployment activities and which are crucial to both help Member States shield their economies and societies and for the industry to become global leaders and increase their market share.

An entity limited to supporting research and innovationis also not in a position to best stimulate collaboration between defence and civilian parts of the cybersecurity market as it is an instrument dedicated to the implementation of the Framework Research Programmes, which does include dual use technologies but only with a have civilian application.

Social and environmental impact

Both options are likely to have positive impact on the social sphere. However, also in this case the impact of an entity based only on art.187 would be weaker if compared to entity based on art. 173 and 187 due to the limitation of the scope of its activity to research and development only. The ability to support deployment is likely to generate much higher positive impact as it will allow public authorities and industries across Member States to more effectively prevent and respond to cyber threats by not only having access to research results but actually equipping themselves with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services).

Stakeholder opinion

According to the outcome of the consultation and evidence gathering processes (please see Annexes 1, 2, and 4) there is a clear demand for a mechanism allowing the EU to have a coherent cybersecurity industrial policy to stimulate the development of capacities allowing Europe to autonomously secure its economy, society and democracy. Stakeholders are of the opinion that support to increasing industrial and technological capacities should go beyond research and development activities only if Europe is to fulfil the vision outlined by the Heads of States and Governments at the Tallin Digital Summit for Europe to be "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."[94]. Stakeholders emphasised that the key to success will be a well-defined role of the Centre in supporting and facilitating the efforts of the Network and relevant communities and an inclusive, collaborative approach to the network to avoid creating new silos. The structure should also be flexible so that it can be easily adapted given that cybersecurity is a fast-pace environment.

Based upon the impact analysis preformed in Section 6, the following table compares the merits of Options 1 and 2 against the baseline scenario:

Impacts	Option 0 Baseline scenario	Option 1 Entity based on art. 173 and 187 TFEU	Option 2: Entity based on art.187 TFEU only
Effectiveness			
Objective 1 *Effective cooperation mechanism*	**0**	√√√	√√
Objective 2 *Pooling knowledge and resources*	0	√√√	√√
Objective 3 *Supporting market deployment*	0	√√√	x
Objective 4 *Support to attracting investment*	0	√√√	√

[94] Conclusions of the Prime Minister of Estonia Jüri Ratas after the Tallinn Digital Summit, 29 September 2017

Objective 5 *Closing cybersecurity skills gap*	**0**	√√	√
Efficiency/Impact on economy, competitiveness, competition and SMEs	**0**	√√√	√
Social and Enviornmental Impact	**0**	√√√	√
Flexibility to allow different cooperation models with the network of competence centres	**0**	√√√	√√√
Safeguarding Union's interests	**0**	√√√	√√√
Acting as an implementation mechanism for different EU cybersecurity funding sources	0	√√√	x

Table 1: Comparing the impact of the different options. The symbols "√" and "x" indicate respectively positive and negative impacts, the number of the symbols is the net result of the summing-up of the respective individual ratings of the policy option and indicates the magnitude of the change compared to Baseline scenario. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

The above comparison demonstrates that an EU-wide collaborative effort stimulated by an entity described under Option 1 offers indeed significant added value for the European economy, society and environment when compared to the baseline scenario and Option 2.

8 PREFERRED OPTION

The above analysis has shown that an entity based on art. 173 and 187 TFEU (Option 1) represents the best instrument capable to implement the goals of the initiative while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests.

In summary, the main arguments in favour of setting the European Cybersecurity Industrial and Research Competence Centre supporting the Network as an EU entity based on art. 173 and 187 TFEU are:

- It ensures flexibility to allow different cooperation models with the network of competence centres to optimise the use of existing knowledge and resources including financial tools and other incentives supporting members of the network
- It provides a visible legal, contractual and organisational common framework to structure the joint commitments of the public and private stakeholders coming from all relevant sectors, including defence;
- It allows creating a real cybersecurity industrial policy by supporting activities related not only to research and development but also to market deployment activities (the latter one with the exception of defence area).
- It fulfils all functional requirements of the legal entity to implement the objectives;
- It can act as an implementation mechanism for different EU cybersecurity funding streams under the next Multi-annual financial framework (Digital Europe Program, Horizon Europe) and enhance synergies between the civilian and defence dimensions of cybersecurity in relation to the European Defence Fund

- It has a positive impact and highest estimated effectiveness of achieving all specific objectives.

Apart from being supported by stakeholders (see previous sections and Annex 2 on Consultation outcomes) this option is also in line with the report of the Estonian presidency on partnerships, which emphasised that in order to reach a higher level of impact "the partnership instruments should cover a much wider set of activities and modalities than research and innovation only." Among other activities mentioned as likely to make a higher impact were, co-creation with end-users, development and experimentation in large scale real life virtual and physical platforms, mission oriented research, deployment activities.[95]

The administrative burden of establishing the network and the Centre is explored in the Annex 3.

9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

Monitoring will start with the establishment of the new legal instrument. An explicit clause to monitor the key performance indicators (KPIs) will be included in the legal instrument. Also, an explicit evaluation and review clause, by which the European Commission will conduct an interim evaluation, will be included in the legal instrument, in order to measure the impact of the instrument and its added value. The European Commission will subsequently report to the European Parliament and the Council on its evaluation. Following this evaluation, the Commission may propose a review and extension of the Competence Centre and Network's mandate . The Commission Better Regulation methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholder consultations.

The Executive Director of the legal entity should present to the Governing Board an ex-post evaluation of European Industry and Research Competence Centre's and Network activities every two years. The legal entity should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Governing Board should be responsible to monitor the adequate follow-up of such conclusions.

Alleged instances of maladministration in the activities of the legal body may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

The list of KPIs that could be used to monitor progress towards meeting the objectives, impact and success of the entity is as follows:

- Number of cybersecurity infrastructure/tools jointly procured.
- Access to testing and experimentation time made possible for European researchers and industry across the Network and within the Centre. Whenever the facilities already exist, increased number of hours available for those communities in comparison to the hours currently available.
- The number of user communities served and number of researchers getting access to the European cybersecurity facilities increases when compared to the number of those having to look for such resources outside Europe.

[95] https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf

- Competitiveness of European suppliers starts increasing, measured in terms of global market share (target 25% market share by 2027), and in terms of share of European R&D results taken up by industry.
- Contribution to next cybersecurity technologies, measured in terms of copyright, patents, scientific publications and commercial products.
- Number of cybersecurity skills curricula assessed and aligned, number of cybersecurity professional certification programmes assessed;
- Number of scientists, students, users (industrial and public administrations) trained.

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 2/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

Annex 1: Procedural information

1. LEAD DG, DECIDE PLANNING/CWP REFERENCES

This Impact Assessment report was prepared by Directorate H "Digital Society, Trust and Cybersecurity" of the Directorate General "Communications Networks, Content and Technology" (DG CONNECT).

The Decide Planning reference of the initiative "Proposal to create a Cybersecurity Competence Network with European Cybersecurity Research and Competence Centre" is PLAN/2017/1743.

The present initiative has been included in the Commission Work Programme 2018 by way of amendment to the text. The Programme Committee unanimously voted for the amendment of the Work Programme on 18 January 2018.

2. ORGANISATION AND TIMING

Several services of the Commission with an interest in this initiative have been associated in the development of this analysis. DG CONNECT worked closely with the Joint Research Centre (JRC) to gather evidence for the Impact Assessment. The initiative has been also regularly presented at the meetings of the cybersecurity sub-group of the Security Union Task Force, which gathers all relevant DGs. DG CONNECT has also engaged in bilateral exchanges with other DGs relevant for the initiative, notably DG GROW, DG HOME as well as the European External Action Service (EEAS).

On 26 March 2018, a meeting of the ISG was held on the draft of the Impact Assessment and on the results of the targeted consultation of relevant stakeholders, before the submission to the Regulatory Scrutiny Board (RSB). The representatives of all relevant DGs, including DG CONNECT, JRC, DG DIGIT, DG RTD, DG HOME and SG were present.

Should the RSB issue a positive opinion, a final Fast Track ISG meeting is expected to be held in early to mid-May 2018 on the legal proposal and on the final version of the Impact Assessment. DG CONNECT will have updated the Impact Assessment Report by taking into account the comments received at-and following-the ISG meeting. The meeting was chaired by SG, and DG CONNECT was flanked by DG GROW, DG HOME, JRC, DG BUDG, DG MOVE, DG REGIO, DG HR DS, DG FISMA, DG COMP, DG ENER, DG JUST, DG EAC, DG EMPL) as well as European External Action Service

3. EXCEPTIONS TO THE BETTER REGULATION GUIDELINES

DG CONNECT has identified one exception to the Better Regulation guidelines. Specifically, a *dedicated* open public consultation has not been conducted. However, stakeholders were given the opportunity to express their views on this initiative and the overall thematic in the following open and targeted public consultations:

- A general open public consultation on the topic of security in relation to the next MFF. For results see Annex 2, section 3.1.1.
- A general open public consultation on the topic of investment, research & innovation, SMEs and the single market. For results see Annex 2, section 3.1.2.
- A self-registration survey open to all cybersecurity centres of expertise across Europe, giving them the opportunity to register their competence and domains of expertise within the remit of the cybersecurity taxonomy developed by the Commission prior to opening the Survey (see Annexes 4 and 5)
- A series of targeted workshops and meetings:

- **Consultation workshop with competence centres** - on 23 February 2018 the Commission organised a full-day consultation workshop with cybersecurity expertise centres from across Europe to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness. Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants.

- **Consultation with the Management Board of the European Cybersecurity Organisation** – the European Commission's counterpart in the contractual Public Private Partnership during a meeting held on 21 March 2018. The representatives of the Board include high-level representatives of cybersecurity companies and SMEs, cybersecurity associations across the EU, representatives of users/operators community, representatives of public administration, research and technology organisations, universities as well as of regional structures e.g. cybersecurity clusters.

- **Consultation workshop with industry, research community and Member States** - on 22 March 2018 the Commission organised a full-day consultation workshop with the representatives of industry (supply and demand side), competence centres as well as Member States to discuss current challenges, gaps and best ways to mitigate them to ensure that the EU has the capacity to autonomously secure its economy, society and democracy against cyber threats. The workshop also identified the areas where the Network and the Centre would provide added-value to the work already done at the national level.

- **Consultation with the Management Board of ENISA** (15 March 2018) as well as a request for targeted contribution, which ENISA provided in April 2018.

- **Consultation with European Defence Agency** through a request for contribution, which EDA provided in April 2018.

- Consultation activities with Member States:

  - A high-level workshop with Member States on 5 December 2017
  - Discussions at the Horizontal Working Party on Cyber (08 March 2018)
  - Member States were also invited to the consultation workshop on 22 March 2018

4. CONSULTATION OF THE REGULATORY SCRUTINY BOARD (RSB)

The Regulatory Scrutiny Board has been consulted as per the procedural rules for the submission of new proposals. The Impact Assessment Report was submitted to the Board on 11 April 2018. The RSB examined the Impact Assessment and issued its Opinion on 07 May. The Board gave a positive opinion with reservations. The Impact Assessment was subsequently reviewed in light of the Board's comments.

The table below presents and overview how these comments were addressed. As point C of the Opinion includes specific considerations detailing the main considerations included under point B of the Opinion, the table below focuses on specific consideration to provide thorough explanation while avoiding duplication.

Board's Recommendations in the Opinion	Implementation of the recommendations into the revised IA Report
(1) The report should better describe what has already been decided and which aspects of coordinating cybersecurity research at EU level are still open. In particular, it should clarify whether the principle of the establishment of the network and the European centre has already been agreed in the Council. Additionally, on the basis of the results of the consultations, it should identify the remaining sensitive points for stakeholders, in particular for the Member States.	Section 1 ***Political and legal context*** has been updated to further illustrate the political and legal context. It now spells out more clearly the feedback from the Member States, the decisions taken as well as remaining sensitive points – all creating basic strategic assumptions guiding the Impact Assessment analysis. In particular, the report makes now a clearer reference to: • The consultation with Member States at the time of reviewing the 2013 EU Cybersecurity Strategy as well as following the announcement of the initiative in the September 2017 Cybersecurity Package, which indicated that any efforts in cybersecurity field need to take advantage of and be complementary with the existing capacities at the national level; • The Council Conclusions, in which Member States welcomed the intention to set up a network of cybersecurity competence centres to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and to pay special attention to complementarity of European and national level efforts – these two elements being the key sensitive issues from the Member States' perspective mentioned throughout the consultation process. • Explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded at an early stage of the process and is now mentioned in the section "Options discarded at an early stage".
(2) The report should more clearly spell out what makes the sector special. What specific characteristics of the cybersecurity sector justify a particular solution that differs from other sectors facing similar challenges? Additionally, it should clarify the prominent role of the public sector as this significantly shapes the character of the initiative. In this context, the report should also expand on the envisioned limited role of industry and the reasons for that. Finally, the report should describe the state of existing competence centres.	Section 1 ***Political and legal context*** has been updated and spells out more clearly now what makes the cybersecurity sector special. In particular, the report now mentions that: • Over the last decade, cybersecurity has become a cross-cutting, horizontal issue, which concerns not only IT sector but virtually any part of our economy and society, including also the critical sectors our societies depend on – from energy, through transport, financial services, public services and healthcare, to mention just a few. • Europe must be therefore in a position to autonomously secure its digital assets and to do so it needs to ensure its competitiveness in the field of cybersecurity. At the same time for most sectors cybersecurity is not part of their core business so they need to have easy access to knowledge and support to make their own products secure. • Despite the fact that a wealth of expertise and experience in cybersecurity exists - more than 660 organisations from across the EU registered to the recent mapping of cybersecurity centres of expertise conducted by the European Commission.[1] Yet, the efforts of research and industrial communities are fragmented, lacking alignment, and a common mission, which hinders EU's competitiveness in this domain as well as its ability to secure its digital assets. Despite Europe's potential to cover the full cybersecurity value chain, the relevant

[1] JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018

	cybersecurity sectors (e.g. energy, space, defence transport) and sub-domains are today insufficiently supported.[2] • Synergies between the civilian and defence cybersecurity sectors are not fully exploited in Europe either. • The specificities of the area of cybersecurity, in which considerations of national security and of European strategic autonomy play an important role justify different approach compared to other, less sensitive sectors. The initiative has to find the right arrangements to work with and support industry (both the supply and demand side), academia, and the public sector - from both civilian and defence sectors - while giving a clear role to Member States' authorities in key areas. In addition ***section 2.2.1***. now points to the fact that public authorities have multiple roles in supporting cybersecurity industrial development. They are users of cybersecurity solutions themselves as they are responsible for securing a wide range of public services. The role of public sector is also crucial in e.g. ensuring that researchers and industries from different economic sectors have access to necessary testing and experimentation infrastructure. In case of cybersecurity such facilities (e.g. quantum test beds) are often too large/costly for a single entity - be it private or public - to acquire alone so the public authorities' intervention is needed.
(3) The report should present the differences between the two options in a more accessible way (e.g. in a table). It should discuss how each option would set up the interaction with non-civilian stakeholders and industry. The report should also include a discussion of the pros and cons of the alternative options with regard to the envisaged division of responsibilities between the European competence centre and national competence centres. The report should detail the reasons for selecting the preferred option, for example in terms of avoiding conflicts of interest of industry and anticipating demand from non-civilian stakeholders.	Following the recommendation of the Board, Section 7 of the report ***How do the options compare,*** in addition to the standard comparison of the assessment against the core criteria of effectiveness, efficiency and coherence, has now been supplemented with an overview table summarising the differences between the two options in terms of possible scope of activity. The relation and possible interactions with civilian and non-civilian stakeholders and industry are outlined in Section 5.2.1 and 5.5.2 as well as in the section 6 analysing the impacts of the option. The table summarising the differences between the options described above now makes clearer the difference between the Options in terms of possible interactions with non-civilian stakeholders. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now makes it clear that the governing rules should allow the possibility to discuss cybersecurity defence-related topics in an appropriate setting (e.g. ensuring appropriate information security and confidentiality) and how the Centre should do this. In addition to explaining why the "network only" option has been discarded at an early stage, the Report provides now the explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded as well. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now provides a more detailed description of how the network would work, what would be the role of the National Coordination Centres vs the European Competence Centre. Following the recommendation of the Board, section 8 on preferred option has now been adapted, summarising all key arguments used throughout the report in the sections describing the options and assessing their impacts. In addition to the important aspect of finding synergies between civilian and defence communities, the section more clearly outlines the advantage of the Option in supporting cybersecurity industrial policy by conducting activities related not only to research and development but also to market deployment activities. This includes both providing infrastructure for research and innovation as well as undertaking efforts to bring innovations to the market (e.g. through joint procurement of cybersecurity products and solutions to

[2] JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)

	shield critical sectors under the responsibility of the public authorities (the latter one with the exception of defence area). The Report also points to the fact that the public-public governance structure, while allowing for pro-active advisory engagement of the industry and other stakeholders, is better suited to reflect the sensitive nature of cybersecurity initiatives as well as to avoid potential conflicts of interest in case of e.g. joint procurement;
(4) The report should meticulously describe the envisioned implementation (alternatives) of both the European competence centre and the network of national competence centres. This should cover in particular, but not exclusively, their governance; the practicalities of the co-investment scheme; the degree of centralisation; and the link to other (research) bodies (existing competence centres, HPC JU, FP9, EIT, cPPP, the Innovation House, ENISA, etc.). Additionally, the report should explain the interaction with the education sector in order to build missing skills.	As mentioned above, in addition to explaining why the "network only" option has been discarded at an early stage, the Report provides now the explanation why the option of creating a fully centralised structure (as opposed to the network with the European centre) has been discarded as well. In addition, the section 4.3 ***Functionalities and governance of the Network and the Centre*** now provides a more detailed description of how the network would work, what would be the role of the National Coordination Centres vs the European Competence Centre. The report addresses and reinforces the message about the links with different structures (HPC, EIT, cPPP, innovation Hubs, ENISA) in a number of sections throughout the text (Section 1: Policy and legal Context as well as Section 4.3 on functionalities and governance of the Network and the Centre). In addition, an explanation on the relation with the education sector has been added in the sections describing possible tasks of the Centres both under Option 1 and 2.
(5) The report should upfront be clearer that this initiative is about cybersecurity research and innovation and not cybersecurity in general (a field with many more existing networks and pooling of resources at the EU level). Related to this, the report should set out that deployment, carried out in the process of implementing the Digital Europe Programme, in this context means providing hard- and software for research purposes. Finally, the report should clarify whether the initiative includes efforts to bring innovations to the market, and if so, how that would be done.	Section 1 on ***Political and Legal Context*** now makes it clearer that the aim of the initiative is to support cybersecurity industrial and technological development in the EU. The text also points out to most relevant existing cooperation mechanisms in the field of cybersecurity - the Cooperation Group and CSIRT Network under the NIS Directive and explains how this initiative is different. The preferred option would allow supporting cybersecurity industrial policy by conducting activities related not only to research and development but also to market deployment activities both in terms of providing infrastructure for research and innovation as well as undertaking efforts to bring innovations to the market (e.g. through joint procurement of cybersecurity products and solutions to shield critical sectors under the responsibility of the public authorities (the latter one with the exception of defence area). While this was mentioned already in the initial report, a summary point was added in the section "Preferred Option" to provide more clarity in this respect.

5. EVIDENCE, SOURCES AND QUALITY

The Commission gathered qualitative and quantitative evidence from various sources. Sources have been categorized according to the nature of the documents: EU official documents, Reports issued by EU institutions and bodies, Reports issued by other entities and online sources.

5.1. EU official documents

- JOIN(2013) 1 final: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace .
- COM(2015) 192: A Digital Single Market Strategy for Europe.
- COM(2015) 185: The European Agenda on Security (The European Agenda on Security)).
- COM(2016) 410 final: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry.
- JOIN(2017) 450 final: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
- COM(2017) 477 final: Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act").
- Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
- 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.
- Council Conclusions 14435/17 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.
- COMMISSION STAFF WORKING DOCUMENT, SWD(2016) 210 An assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007 - 2013).
- COMMISSION STAFF WORKING DOCUMENT, SWD(2018) 69 Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and the Council establishing a European Labour Authority.
- H2020 Work Programme 2018-2020 http://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html#h 2020-work-programmes-2018-20.
- Tallinn Digital Summit Conclusions, 29 September 2017; https://www.eu2017.ee/news/press-releases/tallinn-digital-summit-conclusions-published-creating-digital-continent.

5.2. Reports, position papers and other sources

- Synergies between the civilian and the defence cybersecurity markets, Final Report, June 2016: https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets.
- Investing in the European Future we want, Report of the independent High Level Group on maximising the impact of EU Research & Innovation Programmes, European Commission, July 2017.
- Cybersecurity Industry Market Analysis Draft Final Report, Leaders in Security (KU Leuven) in collaboration with PriceWaterhouseCoopers, 2017.
- JRC Technical Report: European Cybersecurity Centres of Expertise Map, Cybersecurity Competence Survey, JRC, 2018 (see Annex 4).
- JRC Technical Report: European Cybersecurity Centres of Expertise Map, Definitions and Taxonomy, JRC, 2018 (see Annex 5).
- JRC, Technical Report: European Cybersecurity Centres of Expertise Map, Preliminary Mapping Exercise, JRC, 2018.
- "Position paper on European Cybersecurity Strategy: fostering the SME ecosystem", https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf.
- Internet Organised Crime Threat Assessment (IOCTA), Europol, 2017, https://www.europol.europa.eu/iocta/2017/index.html.
- Supply Chain Attacks, ENISA, August 2017, https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks.
- Cyber Insurance: Recent Advances, Good Practices and Challenges, November 2016, ENISA: https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges/at_download/fullReport.
- The European Cybersecurity Market, Investment or necessity?, Cybersec Hub, http://cybersechub.eu/files/European-Cybersecurity-Market-Vol.1-Issue-1.pdf.
- ECSO suggestions on the future European Cybersecurity, ECSO, 2018.

- Healthcare Sector Report, ECSO Working Group on Sectoral Demand, March 2018.
- Industry 4.0, ECSO Working Group on Sectoral Demand: Industry 4.0., March 2018.
- Stratégie national sécurité numérique, France, https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.
- Le livre blanc de la defense 2013, http://www.livreblancdefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf.
- Les budgets nationaux de cyberdéfense en croissance constante, https://www.frstrategie.org/publications/defense-et-industries/les-budgets-nationaux-de-cyberdefense-en-croissance-constante-1-7.
- Selbstbestimmt und sicher in der digitalen Welt 2015-2020 Forschungsrahmenprogramm der Bundesregierung, Self-determined and secure in the digital world 2015-2020 The German Government's research framework programme on IT security https://www.bmbf.de/pub/IT_Security.pdf.
- De Nationale Cyber Security Strategie (NCSS), Slagkracht door samenwerking, The Netherlands, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/28/nationale-cyber-security-strategie.html.
- National Cyber Security Strategy 2, From awareness to capability, The Netherlands, https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html.
- "Dutch investments in ICT and cybersecurity: putting it in perspective", The Hague Centre for Strategic Studies, December 2016 https://hcss.nl/report/dutch-investments-ict-and-cybersecurity.
- "Recommendations on Cybersecurity in Europe", European Cybersecurity Industry Leaders, Page 11, https://ec.europa.eu/digital-single-market/en/news/commissioner-oettinger-receives-final-report-european-cybersecurity-industrial-leaders.
- "Net Losses: Estimating the Global Cost of Cybercrime", McAfee & Center for Strategic and International Studies, 2014.
- "Counting the cost – Cyber exposure decoded", Lloyd's and Cyence, 2017.
- "2015 Cost of Cyber Crime Study", Global, Ponemon Institute October 2015.
- "Global State of Information Security Survey", PwC, 2016, http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.
- "National Cyber Testbed (NCT) Programme", https://www.thehaguesecuritydelta.com/projects/project/89-national-cyber-testbed.
- "Increased coherence and openness of European Union research and innovation partnerships", https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf.
- "Shifting Gears in Cybersecurity for Connected Cars", February 2017: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/shifting-gears-in-cyber-security-for-connected-cars.ashx.
- "Study on synergies between the civilian and the defence cybersecurity markets" IPACSO (2015), https://ec.europa.eu/digital-single-market/en/news/study-synergies-between-civilian-and-defence-cybersecurity-markets.
- "DARPA Military Researchers ask Industry for new Cyber Security Tools for Large Computer Network", John Keller, 2017, http://www.militaryaerospace.com/articles/2017/06/cyber-security-computer-networks-military-researchers.html.
- "Automated Program Analysis for Cybersecurity (APAC)", DARPA, https://www.darpa.mil/program/automated-program-analysis-for-cybersecurity.
- "The Networking and Information Technology Research and Development Program", https://www.nitrd.gov/pubs/2018supplement/FY2018NITRDSupplement.pdfACEA.
- "Principles of Automobile Cybersecurity", http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf.
- "Cyber Security M&A Decoding deals in the global Cyber Security industry", IMAA, https://imaa-institute.org/cyber-security-ma-decoding-deals-in-the-global-cyber-security-industry/.
- "Cybercrime Report", Cybersecurity Ventures, 2016.
- "Increased coherence and openness of European Union research and innovation partnerships", Ministry of Education and Research of Estonia, 2017, https://www.hm.ee/sites/default/files/eu_ri_partnerships_final_report.pdf.
- 2017 Global Information Security Workforce Study Benchmarking Workforce Capacity and Response to Cyber Risk, A Frost & Sullivan Executive Briefing and The Center for Cyber Safety and Education partnered with (ISC)2: https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

- Europeans' attitudes towards cyber security, Special Eurobarometer 464a, 2017, https://www.cncs.gov.pt/content/files/ebs_464a_en.pdf.
- Europeans' attitudes towards cyber security, Special Eurobarometer 464b, 2017, http://data.europa.eu/euodp/en/data/dataset/S1569_87_4_464B_ENG.
- "The European Cybersecurity Market", Kosciuszko Institute, http://cybersechub.eu/files/European-Cybersecurity-Market-Vol.1-Issue-1.pdf .
- "A platform to experience the intelligent Cybersecurity for the real world", Report on Cisco Cyber Range Service, https://www.servicesdiscovery.com /en/article.php?idx=218 and https://www.servicesdiscovery.com/ download/Cyber_Range_At_a_Glance_2015.pdf.

5.3. International sources and international competence centres

- "The DoD Cyber Strategy", US Department of Defence, 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
- "IoT Cybersecurity Coalition Letter", USA Chamber, https://www.uschamber.com/iot%26cybersecurity.
- "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", President of the USA, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
- Collegiate Cyber Defense Competition USA – attracting both public and private sectors, http://www.nationalccdc.org/index.php/competition/about-ccdc
- "Factsheet Cybersecurity National Action Plan", White House.
- "Cybersecurity", USA Homeland Security, https://www.dhs.gov/topic/cybersecurity.
- NIST Establishes National Cybersecurity Center of Excellence https://www.nist.gov/news-events/news/2012/02/nist-establishes-national-cybersecurity-center-excellence.
- Scalable Quantum Cryptography Network for Protected Automation Communication, US Department of Energy, https://www.energy.gov/sites/prod/files/2017/05/f34/Qubitekk_QKD_FactSheet.pdf.
- High Performance Computing Centre, Stanford University, https://hpcc.stanford.edu/.
- "Global Cybersecurity Index 2017", ITU, the United Nations specialized agency for information and communication technology, https://www.itu.int/pub/D-STR-GCI.01-2017.
- "National Cyber Security Organisation: ISRAEL", https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf.
- "Structuring Israel's Cyber Defense", INSS, 2016, http://www.inss.org.il/publication/structuring-israels-cyber-defense/.
- "World Development Report 2016: Best Practices and Lessons Learned in ICT Sector Innovation: A Case Study of Israel", http://pubdocs.worldbank.org/en/868791452529898941/WDR16-BP-ICT-Sector-Innovation-Israel-Getz.pdf.
- The Cybersecurity Sector in Israel, Preliminary Market Analysis, Embassy of India, Tel Aviv, 2015, http://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc.
- "6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry", https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#6e555ab3420a.
- "Israel accounts for 16 percent of global cybersecurity investment, second only to U.S.", https://www.cyberscoop.com/israel-cybersecurity-venture-funding.
- Canada adds new cybersecurity center, hikes funding for electronic spy agency, https://www.defensenews.com/international/2018/02/28/canada-adds-new-cybersecurity-center-hikes-funding-for-electronic-spy-agency/.
- 2018 Federal Budget: Focus on Data and Data-Driven Technologies, https://www.canadiancybersecuritylaw.com/2018/03/2018-federal-budget-focus-on-data-and-data-driven-technologies/.
- The Australian Cyber Security Strategy 2016: Where is the money going? https://www.itsecuritytraining.com.au/articles/australian-cyber-security-strategy-2016-where-money-going.
- The Australian Cyber Security Centre (ACSC), website https://www.acsc.gov.au.
- Cybersecurity Strategy, Government of Japan, 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.
- Defence programme and budget of Japan, Ministry of Defence, http://www.mod.go.jp/e/d_budget/.

- Japan Cyber Readiness at a Glance, Potomac Institute for Policy Studies, 2016, http://www.potomacinstitute.org/board-of-regents/150-cyber-readiness-index/cyber-readiness-translations/2437-japan-cyber-readiness-at-a-glance.
- Keio Establishes World's First InterNational Cyber Security Center of Excellence (INCS-CoE), https://www.keio.ac.jp/en/news/2016/Nov/15/48-18788/.
- "NUS launches shared national cybersecurity infrastructure to spur research and test innovations", National university of Singapore, 2017, http://news.nus.edu.sg/press-releases/nus-launches-shared-national-cybersecurity-infrastructure-spur-research-and-test.
- Budget 2018-19: Government May Allocate Funds For Cyber Security, http://www.india.com/news/india/budget-2018-19-government-may-allocate-funds-for-cyber-security-2833070/,

5.4. Online Sources

- "A conversation with Jarno Limnéll on Cybersecurity and the Digital Summit", Interview of Professor Jarno Limnéll by the Estonian Presidency, October 2017, https://e-estonia.com/a-conversation-with-jarno-limnell-on-cybersecurity-and-the-digital-summit.
- "The EU as a Coherent (Cyber) Security Actor?", http://onlinelibrary.wiley.com/doi/10.1111/jcms.12575/pdf.
- How the Fraunhofer Institutes' funding model contributes to success, https://www.eef.org.uk/campaigning/news-blogs-and-publications/blogs/2013/jul/fraunhofer-friday-part-2--how-the-fraunhofer-institutes-funding-model-contributes-to-success,
- CERN, Website, https://home.cern/about/structure-cern,
- Who funds CERN's research, https://voisins.cern/en/en-bref/who-funds-cerns-research,
- ECSEL Joint Undertaking, Electronic Components and Systems for European Leadership, http://www.ecsel-ju.eu,
- JRC, Smart Grid Laboratories Inventory, JRC, 2016, http://ses.jrc.ec.europa.eu/smart-grid-laboratories-inventory,
- "FireEye Releases First Mandiant M-Trends EMEA Report", https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html.
- "What Are The Biggest Challenges Facing The Cybersecurity Industry?", https://www.forbes.com/sites/quora/2017/09/15/what-are-the-biggest-challenges-facing-the-cybersecurity-industry/#41f0e4372d62.
- "Key Reinstallation Attacks. Breaking WPA2 by forcing nonce reuse", https://www.krackattacks.com/.
- "Spectre and Meltdown processor security flaws – explained", https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-computer-processor-intel-security-flaws-explainer.
- "Ransomware's history and evolution in facts and figures", https://www.kaspersky.com/blog/ransomware-blocker-to-cryptor/12435/.
- "The MeDoc Connection", http://blog.talosintelligence.com/2017/07/the-medoc-connection.html.
- The ACDC project launched by EU: https://www.acdc-project.eu/,
- The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS, FP7) http://www.nessos-project.eu,
- Main Science and Technology Indicators, OECD, http://www.oecd.org/sti/msti.htm,
- "China's ghost in Europe's telecom machine", https://www.politico.eu/article/huawei-china-ghost-in-europe-telecom-machine/.
- "Special Issue 'Surviving the Valley of Death", https://www.journals.elsevier.com/technovation/call-for-papers/special-issue-surviving-the-valley-of-death.
- "High Performing Aviation for Europe", http://www.sesarju.eu/.
- "List of 200 cybersecurity startups that received venture capital in 2017", Steve Morgan, CEO at Cybersecurity Ventures and editor in chief of the Cybersecurity Market Report.
- "Dragonfly: Western energy sector targeted by sophisticated attack group", Dragonfly, 2017, https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks.
- The Cyber Security Body Of Knowledge, Project website, https://www.cybok.org

With regard to the quality of the evidence, the following points must be noted:

For the purpose of mapping the centres of expertise, the Commission developed a comprehensive taxonomy of cybersecurity. However, it is to be noted that such taxonomy is not universally agreed upon and may include or exclude areas that would otherwise be included or excluded in other taxonomies. However, the Commission went to great lengths to take into consideration all relevant standards and consult with stakeholders, including the research and industrial communities, which have either developed or are working on similar projects. This is one of the issues that this initiative itself would tackle.

The quality of this report is impacted by the overall scarcity of evidence in the field of cybersecurity as a whole.

Annex 2: Stakeholder consultation

1. STAKEHOLDER CONSULTATION STRATEGY

Cybersecurity is a broad, cross-sectoral topic. The Commission used different consultation methods in order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in this initiative. This method ensures transparency and accountability in the Commission's work.

In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups (please see section 2.1 of this Annex).

The second step has been to identify the best way to consult them in order to gather relevant input. The Commission pays attention to differentiate data gathering tools and adapts them to different types of contributions the stakeholders might have.

While no open public consultation was conducted specifically for this initiative given its target audience (industrial and research community and Member States), the thematic was already covered by several other open public consultations:

- A general open public consultation carried out in 2018 on the topic of security in relation to the next MFF. For results, see section 4.1.1.
- A general open public consultation carried out in 2018 on the topic of investment, research & innovation, SMEs and the single market. For results, see section 4.1.2.
- A 12-week online public consultation launched in 2017 to seek views of the wider public (approx. 90 respondents) on ENISA evaluation and review.
- A 12-week online public consultation that was carried out in 2016 at the occasion of the launch of the contractual public-private partnership on cybersecurity (approx. 240 respondents).

The Commission also organised targeted consultations on this initiative including workshops, meetings and targeted requests for input (from ENISA and EDA).

The Commission also analysed the feedback to the Inception Impact Assessment published at "Have Your Say" website, which allows citizens and stakeholders to contribute to EU policy and law-making process.

The consultation period spanned over 6 months, starting in November 2017 until March 2018.

2. IDENTIFICATION OF GROUPS OF STAKEHOLDERS CONSULTED, MEANS OF CONSULTATION, AND CONSULTATION TOPICS

2.1 Whom has the Commission consulted?

A list of stakeholders that have been consulted either directly, or through consultation efforts related to open public consultations on the thematic, includes the following bodies:

- The EU Member States national authorities;
- Member State's local and regional administrations taking part in public-private partnership on cybersecurity
- European Commission's services;
- Industrial community representing both supply and demand side of cybersecurity products and solutions, including SMEs – through European Cybersecurity Organisation, which includes a wide variety of stakeholders such as large companies, SMEs and Start-ups, end-users, operators, clusters and association

- Cybersecurity competence centres across Europe - apart from reaching to the members of the public-private partnership on cybersecurity, the Commission also conducted a mapping exercise of relevant centres of expertise across the EU. In addition to desktop research conducted by the Commission services, a self-registration survey allowing cybersecurity expertise centres across Europe to declare their know-how, activity and achievements was launched, to which 665 cybersecurity expertise centres registered by 08 March 2018
- Relevant EU agencies bodies, including targeted consultation activities with European Network and Information Security Agency (ENISA) and European Defence Agency (EDA);
- Citizens

2.2 How has the Commission consulted stakeholders?

Different tools and methods were used in order to conduct the consultation.

- **Mapping of centres of expertise** conducted jointly by DG CONNECT and JRC, which allowed to gather input from 665 cybersecurity expertise centres across Europe and Associated countries on their know-how, activity, working fields, international cooperation. The survey was launched in January and closed on 08 March 2018. (see Annex 4).
- **Targeted Consultations:**
    - A series of targeted workshops and meetings:
        - **Consultation workshop with competence centres** - on 23 February 2018 the Commission organised a full-day consultation workshop with cybersecurity expertise centres from across Europe to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness. Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants.

        - **Consultation with the Management Board of the European Cybersecurity Organisation** – the European Commission's counterpart in the contractual Public Private Partnership during a meeting held on 21 March 2018. The representatives of the Board include high-level representatives of cybersecurity companies and SMEs, cybersecurity associations across the EU, representatives of users/operators community, representatives of public administration, research and technology organisations, universities as well as of regional structures e.g. cybersecurity clusters.

        - **Consultation workshop with industry, research community and Member States** - on 22 March 2018 the Commission organised a full-day consultation workshop with the representatives of industry (supply and demand side), competence centres as well as Member States to discuss current challenges, gaps and best ways to mitigate them to ensure that the EU has the capacity to autonomously secure its economy, society and democracy against cyber threats. The workshop also identified the areas where the Network and the Centre would provide added-value to the work already done at the national level.

- **Consultation with the Management Board of ENISA** (15 March 2018) as well as **a request for targeted contribution**, which ENISA provided in April 2018.

- **Consultation** with **European Defence Agency through a targeted request for contribution**, which EDA provided in April 2018.

- **Consultation activities with Member States:**

  - High Level Roundtable chaired by Vice President Ansip on the creation of Cybersecurity Network and Competence Centre (5 December 2017),
  - Bilateral meetings with Member States' national cybersecurity authorities
  - Discussions with Member States in the Programme Committee at the occasion of launching a Pilot Project
  - Discussions at the Council Horizontal Working Party on Cyber (08 March 2018)
  - Discussions at the 22 March 2018 workshop, where Member States were invited

3. HAVE THE COMMISSION STANDARDS BEEN MET?

The Commission standards as set in the Better Regulation Guidelines have been met. At the same time please see the exception to the Better Regulation Guidelines identified in Annex 1, Section 3.

4. LEARNINGS FROM THE CONSULTATION PROCESS

4.1 Learnings from Open Public Consultations on the next generation Multiannual Financial Framework

Both open public consultations presented below were launched in the context of the proposals for the next generation of financial programmes for the post-2020 Multiannual Financial Framework (MFF), which is the EU's long–term budget. These consultations are part of a careful assessment both of what has worked well in the past and what could be improved in the future and their objective is to collect the views of all interested parties on how to make the most of every euro of the EU budget. These consultations are highly relevant for the initiative covered by this Impact Assessment, given that it is meant to be the main implementation mechanism for cybersecurity funds under different MFF Programmes.

4.1.1 The general open public consultation on the topic of security in relation to the next MFF

This consultation ran from 10 January until 8 March 2018 and was open to all citizens, organisations and stakeholders with an interest and/or involvement in issues related to security.

This consultation collected the views of 153 respondents. 114 replies were sent on behalf of organisations while 39 were coming from individuals. Respondents were given a list of pre-identified policy challenges for the future of Europe, in which respondents had to identify which challenges were the most important in their opinion. "Promoting strong cybersecurity" comes as the second challenge[3] perceived to be "very important" by respondents, with 64.05% of respondents choosing this option. These results confirm the earlier results of the 2017 Eurobarometer, which identified cybercrime as one of the first forms of crime citizens are worried about. At the same time, 43.52%[4] of respondents consider that the current programmes/funds address only to some extent, or do not address at all the promotion of strong cybersecurity in the EU.

[3] The first policy challenge identified as "very important" was the fight against cross-border crime, including terrorism, with more cooperation between law enforcement authorities (73.20%).

[4] 41,83% of respondents believe that strong cybersecurity is addressed to some extent only, while 1,96 % believe they are not addressed at all.

4.1.2 The general open public consultation on the topic of investment, research & innovation, SMEs and the single market in relation to the next MFF

This consultation ran from 10 January until 8 March 2018 and was open to all citizens, organisations, SMEs and stakeholders with an interest and/or involvement in issues related to investment, entrepreneurship, research and innovation.

This consultation collected the views of 4052 respondents, including 2244 organisations and 1808 individuals. 81.10% of respondents identified the need to foster research and innovation across the EU as "very important". Thus making this the first policy challenge deemed very important by respondents in this consultation. This is particularly relevant to the present initiative as fostering research and development through the pooling of efforts and resources is one of the key objectives of the proposal for a network and Competence Centre.

This initiative also aims to support education, skills and training which is the second policy challenge deemed "very important", with 62.86% of respondents choosing this option. The Commission noted the recurrent mentioning of the cyber skills gap by stakeholders including the cybersecurity industry, which is lacking experts in the field[5], and aims to address this issue with the present initiative.

4.1.3 The online public consultation on ENISA evaluation

The open public consultation on the evaluation and review of ENISA took place between 18 January and 12 April 2017. The public consultation aimed to gather the views of stakeholders on evolving needs and challenges in the cybersecurity landscape and to evaluate ENISA's overall performance. The results of this consultation were insightful for the purpose of this impact assessment as they highlighted gaps and challenges in the current cybersecurity ecosystem identified by the stakeholders, and their perception on the progress achieved since the 2013 Cybersecurity Strategy.

Main results related to the questions on the broad cybersecurity ecosystem:

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU; in particular the top 5 (in a list of 16) were: the cooperation across Member States in matters related to cyber security; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks; skills development, education and training of professionals.
- Respondents were also asked if the current instruments and mechanisms at the European level are adequate to promote and ensure cybersecurity in relation to the needs previously identified. Only 6% of the respondents judged the current instruments and mechanisms at the European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be "fully adequate" to promote and ensure cybersecurity. 83% of respondents regarded them as either "partially" or only "marginally adequate" and 5% found them "not at all adequate". National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives of private enterprises or business associations and "other" respondents.

4.1.4 The online public consultation that was carried out at the occasion of the launch of the contractual Public Private Partnership on cybersecurity.

The public consultation on the contractual Public Private Partnership on cybersecurity took place from 18 December 2015 to 11 March 2016. Respondents represented a wide variety of organisations, with a good balance between big businesses (41), SMEs (33), microbusinesses (6) as well as other stakeholders e.g. research bodies (20), national public administrations (7) and regulators (1), NGOs

[5] These remarks were noted during bilateral meetings with stakeholders and during the first workshop organised for this initiative (summary of which can be found in Annex 2, section 4.2.1).

(13). While the first steps to tackle some of the challenges identified by the consultation were taken with the creation of the contractual public private partnership for which it was conducted, due to inherent limitations of this instrument as described in section 2.3.2 of the Impact Assessment the following challenges are still relevant:

- **Competitiveness and EU's technological dependency:** The majority of respondents to the survey saw Europe's cybersecurity market as insufficiently competitive in several areas. Among the reasons mentioned is technological dependency on security solutions (software and hardware) produced or supplied by vendors headquartered in other regions of the world. It was also observed that there is not a single EU company that offers integrated security solutions for the whole (IT) value chain. Instead, the EU market is described by respondents as being dominated by large global vendors from outside the EU, whereas European suppliers are operating in specific niches and the majority of them is small in size. More than 44.3% of respondents (78 out of 176) also stated that they experience barriers related to market access and export within the EU and/or beyond EU countries, particularly due to the fragmentation of the EU cybersecurity market along with EU internal borders. A large majority of respondents (60,8%) state that a shortage of supply in Europe jeopardize the security of the whole digital value chain.
- **Insufficient access to finance, especially for SMEs** - the majority of respondents (75%) felt access to finance for their cybersecurity initiatives or projects is a challenge.
- **Insufficient human capital at industry's disposal** - the large majority of respondents (73.3%) felt that ICT security and supply industry in Europe did not have enough skilled workforce at its disposal. There was a consensus among respondents on the lack of cybersecurity experts. One of the challenges mentioned in this context is that cybersecurity experts are not produced by Universities and other training institutes, but rather develop an extensive practical competence over time, both to become an expert and to keep their knowledge and skills up to date.

4.2 Learnings from workshop with Cybersecurity Centres of expertise

4.2.1. Workshop with national cybersecurity competence centres

On 23 February 2018 DG CONNECT organised **a full-day consultation workshop with cybersecurity expertise centres from across Europe** to exchange views on, among others, possible ways of reinforcing the EU cybersecurity research capabilities; better coordinating research and innovation efforts with the industry partners; and promoting industrial innovation and competitiveness.

Given the big number of cybersecurity expertise centres across the EU, a list of executive-level invitees to the first workshop was prepared taking into consideration the activities of the cybersecurity centres (scientific criteria such as e.g. publications and patents), geographical balance and results of the mapping of the cybersecurity expertise centres across the EU conducted by the Joint Research Centre (JRC). Last but not least, Member States were asked to provide additional suggestions of possible participants in case they felt that the list prepared by the Commission services should be complemented with other centres.

The workshop gathered therefore experts in cybersecurity with a broad overview of the cybersecurity research landscape, needs and challenges. The represented institutions included a number of leading cybersecurity centres across Europe.[6]

[6] **Belgium:** KULeuven; **Croatia:** University of Zagreb; **Estonia:** Tallinn University of Technology, Centre of Digital Forensics and Cyber Security **AND** Estonian Information System Authority; **Finland:** VTT Technical Research Centre of Finland **AND** Helsinki-Aalto Center for Information Security; **France:** INRIA Institut National de Recherche en Informatique et en Automatique **AND** TELECOM ParisTech, INFRES Network and Computer Science Department **AND** CEA - Commissariat for Atomic Energy and Alternative Energies; **Germany:** Fraunhofer Institute **AND** Ruhr University Bochum - Horst Görtz Institute; **Greece:** Department of Computer Science, University of Crete **AND** University of Pireaus Security Lab; **Ireland:** Centre for Cybersecurity and Cybercrime investigation, University College of Dublin; **Italy:** Institute for Informatics and Telematics, Consiglio nazionale della Ricerca **AND** National Laboratory for Cybersecurity; **Luxembourg:** SECURITYMADEIN.LU; **Netherlands:** The cybersecurity group, Delft University; **Poland:** Division of Cybersecurity, Warsaw University of Technology, Faculty of Electronics and Information Technology; **Portugal:** University

Summary of the workshop outcomes:

Though a full-day discussion a number of key challenges and related needs of the research community were identified by the participants, where the EU-action would be of added-value:

- ***Need to align resources & create lasting structures of cooperation/exchange and knowledge management***: Participants agreed with most of the initial conclusions of the cybersecurity expertise centres' mapping presented by the Joint Research Centre, which showed that:
    - The capacities in Europe are dispersed. While there are many teams working on cybersecurity issues, they are often quite small and scattered across Europe, which often does not allow deploying a critical mass of resources to solve cybersecurity challenges.
    - Many expertise centres do research across many cybersecurity domains but with small teams. Europe could have the potential to cover the whole cybersecurity value chain if Member States/centres would specialise in different domains and exchange knowledge and expertise.
    - There are important areas of cybersecurity which are not sufficiently covered by the current efforts. Participants agreed that this might be due to limited resources and inaccessibility to necessary infrastructure (e.g. experimentation/testing facilities).
- ***A strong need to gather industry, academia, government and users together:*** Participants have largely brought to light the need of creating a common place that would ideally fill a perceived gap between the academia and the industry. Europe needs to have a place that would become a real engine for research and investment, with the capacity of being an attractive working place with good conditions for its experts. Also, participants gave as a model an entity that would be the middle point between industry and academia and which would attract the best experts (e.g. the MITRE institute in the US). Participants also noted that there is a semantic gap between government, industry and academia with regard to expectations from each other. Creating a common platform to bring these communities together and exchange views on strategic challenges could help accelerate European progress in the cybersecurity field. In this context participants emphasised that collaboration does not necessarily happen spontaneously. It is important to have, apart from funds, human resources to animate and sustain it.
- ***Need for interdisciplinary approach*** - participants emphasised that the cybersecurity is a very broad and complex area, which requires a multidisciplinary approach. Europe should put in place mechanisms allowing researchers from different areas (e.g. ICT, engineering, psychology, legal) to work together as challenges cannot be resolved by experts of one discipline only. Participants emphasised that this very often boils down to having a place for all those people to come/meet to discuss challenges and work together on common projects. In this context, participants highlighted the need to provide access to widest possible set of skills and knowledge as one entry point/one shop stop across Europe. They mentioned that Europe needs a dedicated cybersecurity knowledge management space/expertise hub, where there is data and means, and where experts can meet and address common challenges. Participants underlined the current problem of small organisations to conduct broader research (e.g. sometimes it is even not possible to buy basic small standards for software).
- ***Need of "infrastructures"/"capacities" for researchers in Europe***: Participants highlighted the need to reinforce the access of European researchers to testing and experimentation infrastructure. The examples given included access to hardware (e.g. access to HPC), software (e.g. access to AI, creation of software testing platforms) or real time data sets. This was supported by a comparison with the opportunities available in the US, where researchers and industry have access to very large scale real time data and laboratories where these can be tested helping them to advance their

of Porto – Centro de Competencias em Ciberseguranca e privacidade; **Spain:** Centro nacional de Protección de Infraestructuras y Ciberseguridad **AND** INCIBE (Instituto Nacional de Ciberseguridad);

projects and get them to the market. Participants warned about the current state-of-play where innovation is led by large private companies from outside Europe. Participants encouraged collaborative co-investing in large scale experimentation, which could be then used by researchers from across Europe.

- ***Need to address deployment challenges*** – the participants emphasized the challenges related to getting the outcomes of the research projects to the market.
  - The misalignment in the supply-demand timeline was highlighted working as an obstacle to the translation of research, including EU-funded research, into marketable products. This in turn makes it difficult to compete with off-the-shelf products supplied by global players already present on the market (e.g. an operator will buy the product made elsewhere because the EU funded one takes too long to enter the market).
  - Participants accentuated the current challenge of the dissemination and communication on the entry onto the market of new EU products.
  - Finally, participants largely asserted that H2020 is a well-functioning instrument but evoked a paramount need to continue supporting projects after their completion to help them overcome the "*valley of death*". Europe should find an effective mechanism to support the full innovation cycle.
  - In addition, the H2020 framework was acknowledged as a good incentive for encouraging start-ups. However, participants mentioned the need of new mechanisms and category of project reviewers with a "venture capital type of approach", which would be mandated to take the risk to invest in promising start-ups/SMEs as they can yield great results. Further support mechanisms such as e.g. European incubator for cybersecurity start-up to leverage their solutions would be desirable.
- ***Cybersecurity skills gap and brain drain:*** Participants emphasized the current gap in cyber skills. Participants have largely called for more action in countering the actual "skills gap" and related "brain drain".
  - There is a strong need to increase the number of engineers and other profiles specialised in cybersecurity.
  - There is a need for more structural support to cyber skills that would go beyond providing funding to researchers (e.g. in FP9-projects) only.
  - The "skills gap" is currently linked not only to not having enough people specialising in cybersecurity but also to not losing the best of the educated and specialized ones, who in a highly competitive global market decide to leave Europe. There is an urgent need for creating an attractive work environment in order for the EU's best assets to remain. In this context the basic resource challenges in smaller institutes were mentioned. This is challenge, according to participants, is also very much linked to the access to testing/experimentation facilities.
  - In this context participants emphasised that there is a strong lack of instrument for continuous academic collaboration (not only on an ad-hoc, project basis). Additionally, some participants brought forward the need of considering the opportunity of offering more PhDs and MAs programmes for students in the EU.
- ***Dual use and possible link with defence***: Although a multi-dimensional approach is needed in the conceptualization of the competence centre, the defence sector deserves particular attention. On the one hand, some participants raised the challenge of the involvement of civilian entities in defence projects due to applicable law. On the other hand, other participants reported good and effective cooperation with the national Ministries in charge of Defence. The benefits of having additionally civil research on defence were highlighted. Besides emphasizing the currently limited synergies between civilian and military sectors, participants acknowledged that addressing dual-use synergies is necessary. At the same time, some participants emphasised that the issue of "mutual trust" is crucial in case of dual-use projects conducted by civilian and military sectors

(e.g. because of the need to access classified data). Therefore, trust building efforts will be essential for a good achievement of the cooperation.

- ***Added-value of creating the network and the Centre*** **-** participants welcomed the idea and emphasised that the Centre and the network could add value to the current efforts on the national level by:

  - Helping create Europe-wide cybersecurity ecosystem
  - Helping research and industries communities to work together
  - Helping the community work with a longer-time, strategic perspective
  - Ensuring access to key capabilities such as testing and experimentation facilities, which could be used by the network of expertise centres across Europe.
  - Helping achieve interdisciplinary approach to cybersecurity in Europe
  - Becoming a knowledge management platform, which could be used by the whole cybersecurity community
  - Helping close the cybersecurity skills gap and preventing brain drain by offering interesting research challenges for young researchers (e.g. large-scale, ambitious European projects attracting highly-skilled people)
  - Ensuring visibility of European cybersecurity know-how and competence both within the EU and globally;

At the same time, the participants emphasised that the key to success will be a well-defined role of the Centre and an inclusive, collaborative approach to the network to avoid creating new silos.
Participants also emphasised the fact that the structure will have to be flexible to be easily adaptive as cybersecurity is a fast-moving and fast-pace environment.

Last but not least participants shared a number of challenges where aggregating efforts across the network and pulling European resources could bring added-value:

- Hardening software/hardware - building trustworthy systems on top of untrustworthy ones.
- Working towards "every device as a non-compromisable device". While this might be not totally feasible in practice, working towards a far-fetched goal brings often surprising side-results (e.g. an US research project, which managed to create a system which sustained attacks for 6 weeks compared to usual much shorter limits (measured in days if not hours))
- Vulnerabilities and certification of products
- Blockchain; Artificial Intelligence; Post-quantum encryption
- European projects (across different sectors) that are secure by design
- Tools to protect against massive malicious attacks (e.g. state-sponsored cyber-attacks)
- Resilience and recovery mechanisms (stress testing)
- Tools allowing to learn fast when the system was compromised
- Societal challenges with essential security aspects: e.g. digital identity, online voting, connected cars;

4.2.2. Workshop with Industry, Research community and Member States

On the 22th of March 2018, a full day high-level consultation workshop was organised. The workshop gathered about 100 stakeholders from industry (both supply and demand side, research community and national and public authorities. It allowed gathering stakeholders' views on whether there is a need for increased cooperation at the EU level as well as on possible priorities and strategic orientations for the network of the competence centres with the European Research and Competence Centre at its heart. The discussion generally confirmed the challenges identified during the workshop on 23 February and provided some practical suggestions for possible actions. During the workshop, the Commission also presented the preliminary results of the cybersecurity competence centres' mapping undertaken in the recent months (see point 4.3 of this Annex).

Workshop Conclusions:

Main challenges of the network and the Centre **-** The participants identified several needs and challenges existing in the area of cybersecurity that in majority were consistent with the ones

identified during the workshop in February. Therefore, this part will highlight the main needs/challenges and summarise new challenges and findings:

- ***Need for alignment and connection of economic/industrial strategies and research goals***: The participants highlighted the need to create a clear connection between industry and research that should be supported by a strategic approach at the EU level. Such approach should involve a framework that would ensure possibility of planning not only in the medium but also in the long-term. The participants highlighted that there is a strong need for such strategic cooperation to focus on both priorities and ideas as well as on funding. It was also highlighted that while such cooperation is needed it should leave the space for the competition in a market and allow flexibility to address challenges from evolving cybersecurity environment. Some participants pointed out that there is a need to take into account and use existing competences and capacities of the Member States.

  The participants stressed as well the need of continuing the basic research for the years to come, as this will allow Europe to develop and innovate beyond the market needs at a given moment.

- ***Need for interdisciplinary approach:*** As during the previous workshop, the participants indicated the need for working together across different sectors, as well as along value-chain. Some participants pointed out to the necessity of interoperable solutions, as well as the need for raising awareness on cybersecurity among companies on the demand side and for addressing sectoral needs.

- ***Need of "infrastructures"/"capacities" in Europe***: participants from both industrial and research communities emphasised that there is a strong need for creating shared competences, infrastructure and testing facilities (a possibility could be considered to open current facilities to other users and fill in the gaps by creating the lacking ones);

- ***Need to address deployment challenges***: the participants stressed the need for developing a clear industrial strategy for the EU. At the same time, many participants highlighted the need to involve and give the opportunity to participate for the SMEs that could benefit from the economy of scale. In this context, the participants stressed the need for a more strategic approach to public procurement.

- ***Need to gather industry, academia, government and users together:*** similarly to the first workshop, the majority of participants raised this issue. The need to create a reliable system of trust in a digitalized world that would be based on two-way collaboration was highly visible. Some participants pointed out that while linking competences spread in the EU, there is also a need to allow the cooperation in smaller groups and ensure flexibility.

- ***Dual use and possible link with Defence***: the participants on one hand stressed the need for multidisciplinary approach which could include the civil and military initiatives but on the other hand special position and characteristics of the defence sector were also mentioned to be taken into account.

- ***Need to close the cybersecurity skills gap and preventing brain drain:*** the participants raised this issue similarly to the discussions during the first workshop and stressed that the EU should offer interesting research challenges for young people.

Recommendations - In response to these challenges, participants also formulated recommendations regarding the network and the Centre:

- Strategic leadership in the EU. A strategic plan developed at the EU level is recommended, together with coordination and leadership needed;
- Connection between research and industry, both on the demand as on the supply side (‘applied’ and ‘sectorial’ research);
- Research that serves the industry in the short term, but also funding and supporting the long-term research;

- The possibility to invest and fund bigger projects, also allowing to benefit from the economy of scale; need to develop testing facilities and build common infrastructure;
- Need to create a framework for a two-way collaboration;
- Help to include various stakeholders;
- Creation of common rules/principles of procurement;
- Improving education at early stages and ensuring reduction of skills gap. Creating a platform that offers interesting work and keeps young people in Europe;
- More efficient dialogue between industry and academia;
- Help to create trust for cross-border solutions, strengthening capacities in the EU;
- Creation of both the Centre and the network of competence centres to overcome fragmentation in the EU but allowing flexibility. The centres of the network must have their independence. The mission and mandate of the Centre must be clearly stated;
- Make use of smart tools, such as trade agreements;
- Create a place to share ideas and newest technology/tools.

4.3 Learnings from the EU Survey for the self-registration of Centres

The main learnings from this survey are presented below. For a full analysis of the mapping exercise and survey please refer to Annex 4. The survey was open for participation from middle January until middle March of 2018 and over 665 centres participated.

The preliminary analysis of the survey results and the desktop research mapping exercise[7] provides a detailed and complex picture of the situation of cyber-security research in Europe.

In general, the full picture provided by this analysis shows a European cybersecurity research community vibrant, productive and recognised at global level, which however has often difficulties in reaching the critical mass to truly make the difference, and which is not always able to tightly connect with the industry.

Answers of the survey related to the domains covered by the research centres in Europe show that there are competencies in all the domains identified in the EU Cybersecurity Taxonomy, however the analysis of research subdomains in fact shows that the real coverage of the subdomains is heavily jeopardised with the majority of the centres active in the reality only in a minor number of sub-fields. This means that a full coverage of the cybersecurity domains by European players is far from being complete. The same trend was observed at the country level.

The analysis of the sectors of application of cybersecurity research, as well as of the technological applications covered, shows again a heterogeneous landscape at Member State level, with some sectors developed in few countries, and poorly developed in all the others.

Looking at the distribution of the scientific production among European institutions, the scientific literature analysis per domain shows that each domain is dominated by a restricted number of institutions in term of number of publications, and that the numerical difference between the top 10 for each domain and the rest of the institutions publishing in that domains is not negligible. In other words, the picture that the analysis of scientific publications combined with the results provided by the survey gives, is that of a Europe where few institutions polarise the scientific production and are able make a difference in the domain.

Looking at the ratio between scientific publications and patents, the report concludes that it seems evident that to the relatively high scientific production does not automatically correspond an equal "innovation" push.

[7] JRC Technical Report "European Cyber Security Centres of Expertise, Preliminary Mapping Exercise"

For what concerns the collaborations between industry and academy, the H2020 programme had surely contributed to strengthen the relations between industry and academy but it also showed that few institutions were successful to access the H2020 funds continuously. This created polarisation with only institutions from some Member States benefiting while others benefiting more from national funding and limited international collaboration.

These last considerations call for the definition of new measures to:

- Strengthening and enlarging the collaboration of cyber-security research organisations across Member States;
- Streamline and stabilise the R&D cooperation between industry and academy;
- Better coordinate research funding across the Union;
- Co-design of research plans between funding bodies and recipients;
- Support the sharing of highly expensive infrastructures (in an Open Laboratory initiative fashion).

4.4 Learnings from the contributions from EU agencies and other bodies.

The EU agencies EDA and ENISA were requested to provide their contribution in the consultation process. The main points are presented below.

4.4.1 European Defence Agency contribution

The European Defence Agency drew attention to their work promoting capability development in the field of cyber defence through intergovernmental cooperation among Member States.

In their contribution, EDA pointed out that cross-sectoral research agendas, identification of areas where civil/military efforts and investments could be combined, development of common training and exercises curricula or conduct of coordinated or joint cyber activities could be some of the topics where a future Cybersecurity Competence Centre and Networkcould add value. The Network and Centre should build upon and seek for complementary efforts to the existing structures/mandates and competences (e.g. beyond EDA also of other entities which are active in similar fields such as the European Security and Defence College-ESDC) as well as to map and define the role of all actors. EDA stressed the need for synergetic approach with these actors.

The main issues from the defence perspective are: to reflect Member States armed forces' needs, to take into account the specificity of the defence sector (question of national sovereignty, differences in the cyber technologies application, the industry competencies should be addressed to fill the capability gaps of the Member States and prioritisation should follow this approach.) With regard to cyber defence funding priorities that have been identified with Member States and that cut across also the civilian sector, a coordinated action and co-funding could be elaborated. Such approach could be envisaged not only in the field of research but also in the field of capabilities.

EDA also sees a task for the Centre in development and maintaining an overview on cybersecurity related activities, raising awareness of all relevant national and EU entities' activities, support synergies and cross-fertilisation. A synergetic approach to testing on requirements and solutions between the cybersecurity network and Centre and EDA could promote effective solutions.

4.4.2 ENISA contribution

A discussion on the creation of the network of competence centres with a European Research and Competence Centre at its heart took place at the ENISA's Management Board on 15 March 2018. Additionally, ENISA provided a reply to the targeted consultation in April 2018 welcoming the Commission's proposal and strongly supporting its goal of increasing coordination and enhancing cybersecurity competencies within the European Union. According to ENISA, the proposal of the European Cybersecurity Competence Network Centres offers a great opportunity to supplement existing policy measures by specifically targeting the cybersecurity competencies that underlie these existing instruments.

ENISA identified the following priorities that the Centre and the network should focus on: developing of the strategy and governance system, identifying its short/long term objectives; developing and maintaining Digital Skills throughout the EU and prioritising technical work. The network and the Centre should cooperate with other important cybersecurity actors and networks (such as Europol EC3, EDA, CERT EU within the EU institutional framework and with established industry networks in the private sector), provide input to the relevant policy development. ENISA believes it could substantially contribute to the project being well position in the cybersecurity environment, among other through supporting networking activities and helping the Network and the Centre develop their strategies.

4.4.3 European Cybersecurity Organisation's contribution

The Management Board (MB) of the European Cybersecurity Organisation's – the Commission's counterpart to the contractual Public Private Partnership (cPPP) on cybersecurity provided a contribution to the targeted consultation in April 2018.

Within the network of cybersecurity competence centres, the cPPP MB envisions clusters of competence centres contributing to the development of a full trustworthy European value chain: standards, certification, trustworthy elements of the supply chain for different applications / vertical sectors (also transversal technologies used in different verticals).

Local / regional / national critical infrastructure / essential services would be used as platforms for introducing and validate trustworthy innovations. They would improve R&I approaches to better bring research to market based upon regional needs yet with an EU added value. They could also contribute to the creation of cybersecurity diploma in universities and skill development.

The European Cybersecurity Research and Competence Centre should provide, according to the cPPP MB overall "coordination" of the network providing support for exchange of information and coordinating funding for cybersecurity. It would support the definition and implementation of EU policies and legislations related to cybersecurity and could be the EU training centre on cybersecurity. If developed in a NIST-like approach (with seconded experts), such centre could also drive highly advanced research on special topics as well as provide specific operational support (upon request).

The above would be complemented by the evolution of the present cPPP, currently focused on research, towards a wider capability and competitiveness PPP, supporting also strategic capabilities development and initial procurement.

The cPPP MB concludes with a set of recommendations for future actions in the cybersecurity area including the definition of a European cybersecurity industrial policy, tackling not only R&D but also capability development, which could be done through an enhanced cPPP, allocating more resources to R&D and capability building, raising awareness of companies and citizens, harmonising security standards for IoT, and developing private EU Sectoral CERTs with rapid reaction capabilities to threats.

4.4.4. Feedback received to the Inception Impact Assessment

The Commission has also received feedback to the Inception Impact Assessment (IIA) published at "Have Your Say" website, which allows citizens and stakeholders to contribute to EU policy and law-making process (12 responses including private sector, research organisations, citizens as well as one association from a third country) .

Stakeholders providing feedback to IIA pointed to the fact that fragmentation and low level of coordination in between the EU cybersecurity experts groups in public and private sectors are undermining the impact of the efforts deployed in a field whereas other economical regions are strong and well-organized (examples of USA, Israel and China were provided). Stakeholders also pointed to the need of sharing investment as research requires equipment levels that are out of reach of many organisations - be it public or private. Most stakeholders providing feedback on the IIA supported the option, which would include both industrial support measures and research and development activities.

At the same time all stakeholders providing their views on core aspects of the IIA supported policy action going beyond baseline scenario only.

Other issues brought up by stakeholders concerned the need of interdisciplinary approach encompassing not only computer-science aspects of IT-security, but also humanities/social-science-based aspects of the challenge as well as the need to stimulate a dual approach where civil and military stakeholders interact in the development of a new security technology.

Annex 3: Who is affected and how?

6. PRACTICAL IMPLICATIONS OF THE INITIATIVE

This annex describes the practical implications of the preferred option identified in the Impact Assessment – the establishment of a Cybersecurity Competence Network with a European Cybersecurity Industrial and Research Competence Centre entity empowered to pursue measures in support of industrial technologies as well as in the domain of research and innovation (Option 1) – for stakeholder groups likely to be directly or indirectly affected by the initiative.

Member States

The EU Member States will have at disposal an effective mechanism to help them build their cybersecurity technological capabilities, support the scaling up of the cybersecurity industry and increase the protection of essential services (e.g. transport, health, banking and financial services) in their territories while strengthening the collective resilience of the EU.

The initiative will enable Member States to coordinate together with the Commission their investments in necessary cybersecurity infrastructure at the national and European levels. The mechanism will allow Member States to pool expertise as well as resources for tools and infrastructures which would otherwise be more costly or not affordable for individual Member States. Such approach would allow economies of scale and rationalisation.

The return from such investments would be also proportionally higher as the Member States would benefit from the access to upgraded capacities and facilities that could not be achieved through national efforts only.

The increased coherence and synergies between different funding mechanisms (Digital Europe Program, FP9, and possibly cyber defence under European Defence Fund) would also reduce the administrative burden of managing different cybersecurity funding programmes, with a positive impact on the EU budget to which Member State contribute.

The preferred option will also impact positively Member States' capability to deal with the wide range of issues related to education and skills. The functionalities of the Centre linked to the education paths, for example the development of cybersecurity curricula and the support to the cybersecurity certification programs, will complement the efforts of the Member States by providing appropriate input to education policy makers. At the same time, the access for researchers to cutting-edge projects will help contain the "brain drain" phenomenon and increase the chances of retaining the best talents in the EU and attracting foreign highly skilled professionals.

Businesses

European companies, both on the cybersecurity demand and the supply side will be among the most impacted stakeholder groups. The Network and the Centre under this option would ensure access for businesses to necessary testing and experimentation infrastructure helping them to ensure that their products are cyber-secure and turning cybersecurity into their competitive advantage. This should also help them cut research and development costs and speed up the development process, which would further reinforce their competitiveness.

In addition, the chosen mechanism will ensure coordination between research and industry and therefore direct the research efforts towards concrete industrial needs. The provision of cutting-edge

expertise and tools in cybersecurity will indirectly support economic operators in complying with the NIS Directive.

In addition one of the key functionalities of the Competence Centre and the Network is to support the deployment of European cybersecurity leading-edge products and solutions across the market

SMEs

The European SMEs and micro-enterprises operating in the cybersecurity filed will experience direct and indirect economic benefits from the initiative as highlighted above. While the set-up of the Competence Centre and the Network does not impose regulatory obligations upon them, it will open up opportunities in terms of costs reduction for the design of new products and it will help them gaining easier access to the investors' community and attract the necessary funding to deploy marketable solutions. In the case of SMEs and micro-enterprises the access to publically funded testing and experimentation facilities is even more important as they are lacking resources to either purchase or to travel outside their market (and often outside the EU) to find necessary infrastructure. It is also hoped that this initiative would open up new markets for European SMEs and micro-enterprises active in the field of cybersecurity.

Research Community

Research and development organisations throughout the EU, both on the civilian and the defence side, will enjoy the benefits deriving from better coordination, resource pooling and increased availability of advanced methodologies and tools (such as testing and experimentation facilities). They will be able to achieve the critical mass to carry out projects of common interest with a longer-time, strategic perspective. In addition, the chosen mechanism will ensure coordination between research and industry and therefore direct the research efforts towards concrete industrial needs helping the process of turning the outcomes of the research into applicable and marketable solutions that could be then used by different industries and public authorities.

The hosting of several programmes under a common "umbrella" would also allow the research community to experience cross-fertilisation among the different stakeholder groups related to cybersecurity and increase the visibility of the EU excellence in research on the global scene.

Citizens

Stronger European know-how in cybersecurity should result in an overall higher level of protection for citizens in the Digital Single Market, e.g. in Internet of Things domains such as smart energy, medical devices, or connected automated vehicles. The initiative should result in an improved provision of products and services which reflect European values and are directly in line with European policies and regulations.

EU institutions, agencies and bodies

The EU institutions, agencies and bodies will benefit both from the outcome of the research and development and the procurement activities of the Competence Centre and the Network, and from the access to state-of -the art methodologies and tools to perform their operations as effectively as possible.

This is in particular true for the bodies in cybersecurity field, such as ENISA, the EU cybersecurity Agency, the European Cybercrime Centre at Europol, the European Defence Agency (interested in e.g. dynamic risk assessment and incident handling) and the several sectoral agencies with an interest in the area (for example the European Aviation Security Agency).

7. SUMMARY OF COSTS AND BENEFITS

II. Overview of costs – Preferred option							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
Network of Competence Centres with European Industrial and Research Competence Centre	Direct costs	0	0	0	0	0	EUR 15-20 million EU budget
	Indirect costs	0	0	0	0	0	0

Comments:

Recurrent costs related to the functioning of the Centre itself as well as the financial support by the Centre to the Network (support for the national centres chosen by Member States to act as a national Competence Centre hub as well as for thematic networks) have been presented in the below budget overview[8]. The overall amount dedicated to the Centre is very modest in comparison with the overall level of funding expected under the new Multiannual Financial Framework.

The costs would be covered under the EU budget and are considered as additional as no such costs are incurred under the Baseline scenario.

Please note that this overview does not include the operational costs related to the implementation of different funding programmes, which are decided within separate processes.

[8] *The costs related to facilitation of the network cooperation by a central entity were base, to the extent possible, on comparable experiences e.g. The European Reference Network for Critical Infrastructure Protection.*

	2021	2022	2023	2024	2025	2026	2027	€ Total in millions
Title 1	**1.561**	**4.62**	**6.896**	**7.526**	**7.786**	**7.776**	**7.636**	**43.801**
Staff Expenditure of the Centre								
Salaries & allowances	1.331	4.34	6.576	7.206	7.486	7.486	7.346	41.771
- of which establishment plan posts	0.48	1.104	1.38	1.38	1.38	1.38	1.38	8.487
- of which external personnel	0.85	3.236	5.196	5.826	6.106	6.106	5.966	33.284
Expenditure relating to Staff recruitment	0.06	0.06	0.04	0.04	0.02	0.02	0.02	0.26
Mission expenses	0.15	0.2	0.25	0.25	0.25	0.25	0.25	1.6
Socio-medical infrastructure & training	0.02	0.02	0.03	0.03	0.03	0.02	0.02	0.17
Title 2	**3.305**	**3.52**	**3.935**	**3.99**	**3.99**	**3.99**	**3.99**	**26.72**
Infrastructure and operating expenditure of the Centre								
Rental of buildings and associated costs	0.9	0.9	0.9	0.9	0.9	0.9	0.9	6.3
Information and communication technology	0.15	0.25	0.3	0.35	0.35	0.35	0.35	2.1
Movable property and associated costs	0.02	0.03	0.06	0.06	0.06	0.06	0.06	0.35
Current administrative expenditure	0.015	0.02	0.035	0.04	0.04	0.04	0.04	0.23
Postage / Telecommunications	0.08	0.08	0.1	0.1	0.1	0.1	0.1	0.66
R&D support (evaluations and reviews)	1	1	1	1	1	1	1	7
Innovation	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.28
Communication	0.6	0.7	1	1	1	1	1	6.3
Audits	0.5	0.5	0.5	0.5	0.5	0.5	0.5	3.5
Title 3	**5.19**	**7.552**	**8.192**	**8.832**	**9.472**	**9.472**	**9.472**	**58.182**
Operational expenditure								
Projects under relevant MFF Programmes	TBC	TBC	TBC	TBC	TBC	TBC	TBC	TBC
Support for national Centres (hubs)								
Support for HR expenditure - national coordinators	2.106	4.212	4.212	4.212	4.212	4.212	4.212	27.378
Missions/meetings/ budget for networking at national level	2.7	2.7	2.7	2.7	2.7	2.7	2.7	18.9
Support for thematic networks								
Support for HR expenditure *(assume 1 coordinator per network; growth from 3 to 20 networks)*	0.234	0.39	0.78	1.17	1.56	1.56	1.56	7.254
Support for networking activities	0.15	0.25	0.5	0.75	1	1	1	4.65
TOTAL EXPENDITURE	**10.056**	**15.692**	**19.023**	**20.348**	**21.248**	**21.238**	**21.098**	**128.703**

Benefits analysis:

1. With regard to creation of the Network and the Centre economic benefits can be assumed for MSs, industries and research communities as the services of the Centre will be free of charge and therefore the reduced investment from these stakeholders from their own resources is needed (e.g. on testing and experimentation infrastructure).
2. Other indirect economic impacts can be assumed as a result of the initiative as it could help MSs and industry to reduce the costs of cybersecurity/cybercrime incidents for which the estimated economic impact stands 0.41% of GDP (around 55 billion).
3. Additional indirect economic benefits are expected due to: 1) increased access for businesses to necessary testing and experimentation infrastructure helping them to ensure that their products are cyber-secure and turning cybersecurity into their competitive advantage thus increasing volumes of sales. This should also help them cut research and development costs and speed up the development process, which would further reinforce their competitiveness. 2) the increased market opportunities for businesses, including SMEs thanks to deployment support activities of the Centre and the Network.

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 3/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

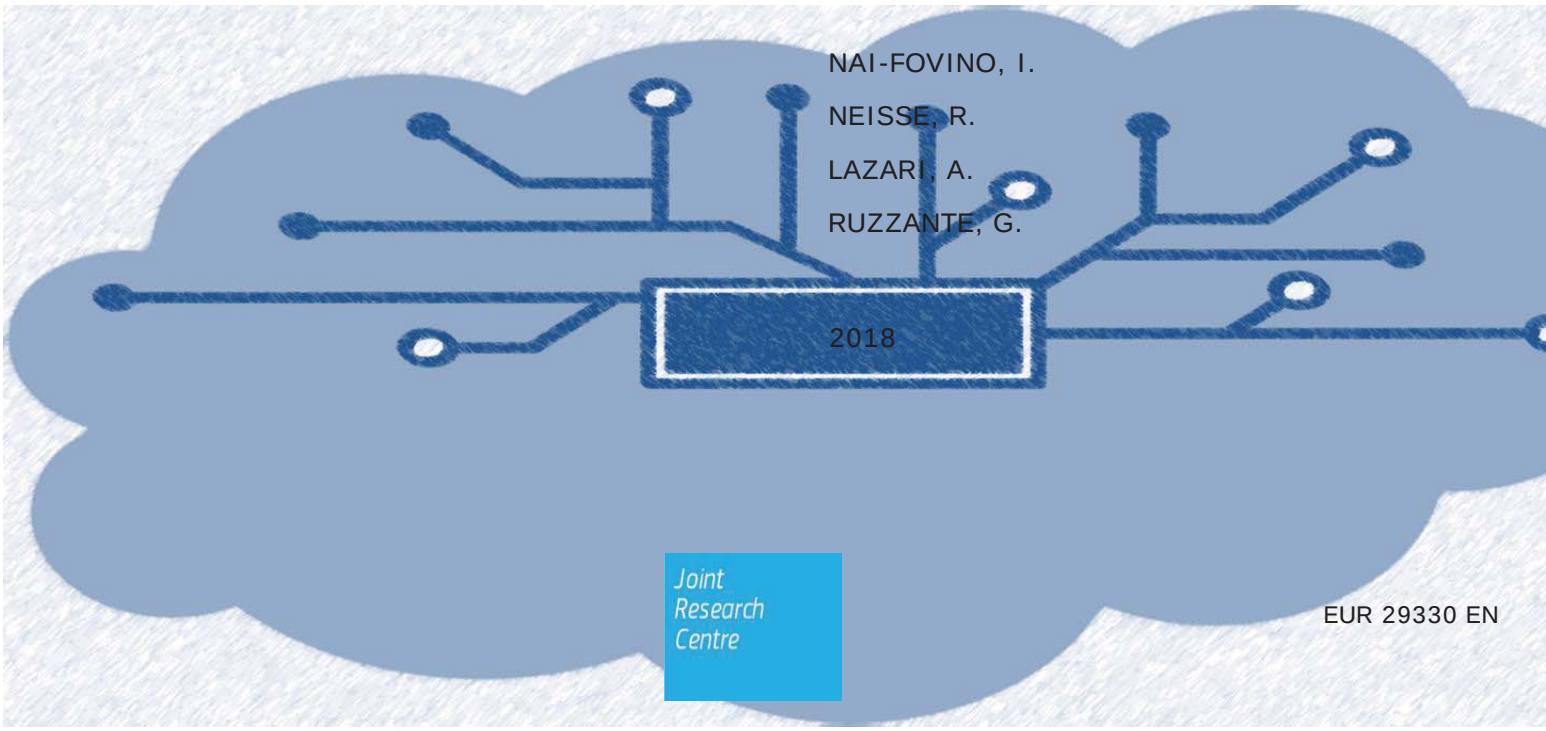
{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

European Commission

JRC TECHNICAL REPORTS

European Cybersecurity Centre of Expertise

Cybersecurity Competence Survey



NAI-FOVINO, I.

NEISSE, R.

LAZARI, A.

RUZZANTE, G.

2018

Joint Research Centre

EUR 29330 EN

JRC Science Hub

https://ec.europa.eu/jrc

JRC 111211

EUR 29330 EN

PDF ISBN 978-92-79-92954-0 ISSN 1831-9424 doi: 10.2760/42369

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: NAI-FOVINO, I.; NEISSE, R.;'LAZARI, A.; RUZZANTE, G. European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey. EUR 29330 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92954-0, doi: 10.2760/42369, JRC111211.

Contents

1 Introduction 5

2 Survey Description and Design 6

3 Survey Dissemination Strategy and Analysis of Results 9

3.1 Survey Dissemination Strategy 9

3.2 Number and Geographical Distribution of Participants 10

3.3 Entity Type and Legal Status of Participants 11

3.4 Cybersecurity Domains and Subdomains 13

3.5 Types of Funding Sources 18

3.6 Type and Number of Employees (FTE) 18

3.7 Publications 20

3.8 Sectors, Applications and Technologies 23

3.9 International Collaborations and Joint Programs 25

3.10 Missing/Overstated Elements and Mitigation Strategy 26

4 Scientific and Technological Development Analysis 28

4.1 Analysis of publications 28

4.2 H2020 projects 30

4.3 Patent Analysis 31

5 Conclusions 33

Annex I – Cybersecurity Survey 36

List of figures 54

Abstract

In its September 2017 Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[1] the European Commission announced the intention to support the creation of a network of cybersecurity competence centres to stimulate the development and deployment of technology in cybersecurity. In the scope of this initiative, the main goal of this document is to present the design and results of the survey conducted in order to identify the cybersecurity competence centres (e.g. research organisations /laboratories/associations/academic groups /institutions, operational centres) in Europe. The survey was open for participation from middle January until middle March of 2018 and 665 centres participated. This report also presents a scientific and technological development analysis comparing the survey results presented here with a desktop research mapping exercise performed by JRC and described in a separated JRC Technical Report ("European Cyber Security Centres of Expertise, Preliminary Mapping Exercise")

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

1. Introduction

In its September 2017 Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[2] the European Commission announced the intention to support the creation of a network of cybersecurity competence centres to stimulate the development and deployment of technology in cybersecurity.

The first step of this ambitious initiative is the clear definition of the cybersecurity context, its domains of application, research and knowledge. The DG-JRC, in collaboration with DG-CNECT, proposed a cybersecurity taxonomy and classification scheme for this purpose aligning the cybersecurity terminologies, definitions and domains. This taxonomy considers the different dimensions of the cybersecurity domain using as sources some of the most widely accepted cybersecurity standards, international working group classification systems, regulations, best practices, and recommendations. The goal of this taxonomy was to provide a high level set of definitions and categorisation domains are proposed so that they:

- can be used by the EC cybersecurity initiatives;
- become a point of reference for the cybersecurity activities (research, industrial, marketing, operational, training, education) in the DSM by all sectors/industries (health, telecom, finance, transport, space, defence, banking etc.);
- can be used to index the cybersecurity research entities (e.g. research organisations/laboratories/ associations/academic institutions/groups, operational centres*/academies*) in Europe;
- *meet compliance* with international cybersecurity standards*;*
- *can be* sustainable, easily modifiable and extensible.

The second step of this initiative is the identification and mapping of existing EU cybersecurity centres (e.g. research organisations/laboratories/associations/academic groups /institutions, operational centres) according to their cybersecurity expertise in specific domains using the proposed taxonomy. This mapping exercise was performed through two parallel activities:

- A desktop research taking as input online data from scientific publication databases, patent registries, H2020 projects;
- An online survey addressed to the European cyber-security research entities.

In the scope of this mapping exercise, the goal of this document is to present the design and results of the survey conducted in order to identify the cybersecurity competence centres in Europe. The survey was open for participation from middle January until middle March of 2018 and over 660 centres participated.

This report is organised as follows: Section 2 presents a description of the designed survey including the questions and information expected to be obtained. Section 3 summarizes the survey results including a quantitative analysis and a list of missing and misplaced survey elements with a mitigation strategy to be followed where the centres that participated will be invited to update and complement their data. Section 4 presents a scientific and technological development analysis comparing the survey results with a manual desktop research. Section 5 finishes this report with conclusions and final considerations.

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

2. Survey Description and Design

The scope of the survey was to call on all cybersecurity competence centres across the EU, whether public or private, to register their organisations and share information about their contact details, work and expertise. The expected time to complete the 27 either open-ended or closed-ended questions was from 20 minutes to 1 hour depending on the level of details shared. The survey also included a glossary of terms defined together with the cybersecurity taxonomy. The full survey as published is presented in Annex I, in this section only a few screenshots are presented as an example in order to give an overview of the information requested.

The following sections were defined:

1. General information;
2. Cybersecurity expertise;
3. Sectors, applications and technologies;
4. International collaborations and joint programs;
5. Confirmation and agreement with the privacy policy.

The **general information** section requested the name of the centre both in English and national language, department, address, country, website, management and general contact information. For the purpose of classification of the entity this section also requested the entity type, legal status, types of funding received, and number/type of Full Time Equivalent (FTE) employees). The following figure shows the entity type, legal status, and funding types made available for the survey participants to choose from:

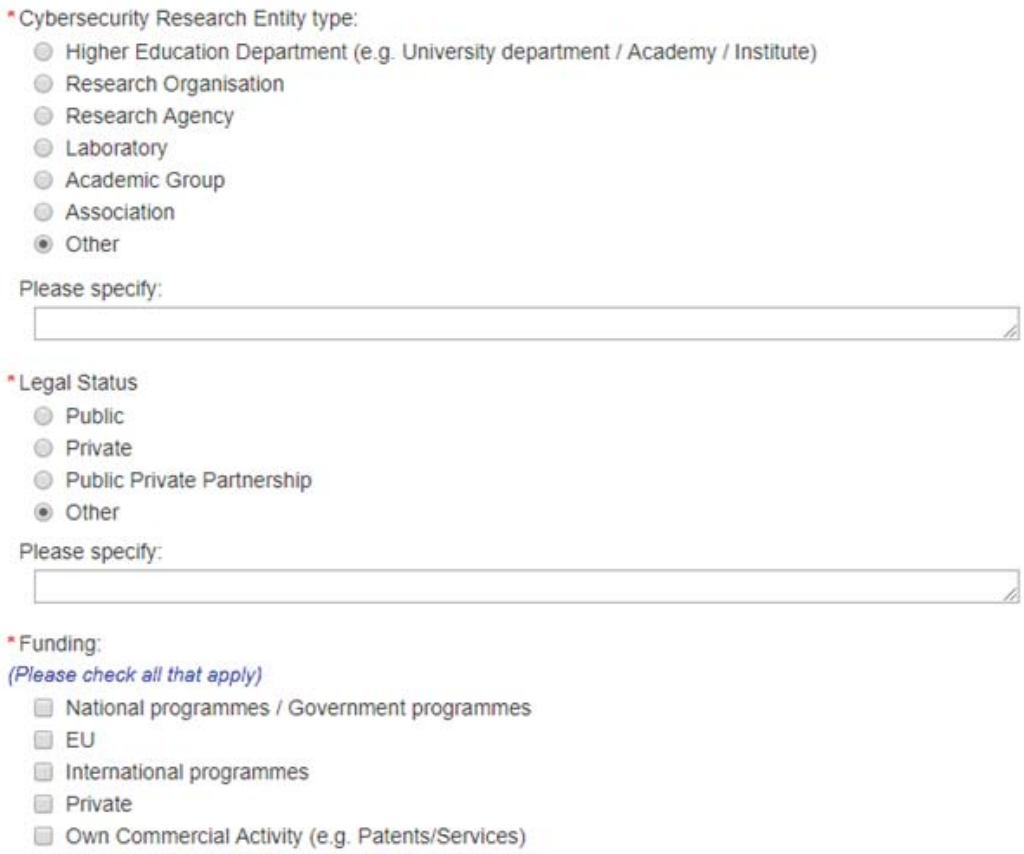


Figure 1. Entity type, legal status, and funding types.

The **cybersecurity expertise** section requested information about the cybersecurity **domains and subdomains of expertise**, which were defined using the cybersecurity taxonomy as input. The following figure shows the list of cybersecurity domains displayed to the survey participants:

	I have expertise in this domain.	I don't.
* Assurance, Audit, and Certification	○	○
* Cryptology	○	○
* Data Security and Privacy	○	○
* Education and Training	○	○
* Operational Incident Handling and Digital Forensics	○	○
* Human Aspects	○	○
* Identity and Access Management (IAM)	○	○
* Security Management and Governance	○	○
* Network and Distributed Systems	○	○
* Software and Hardware Security Engineering	○	○
* Security Measurements	○	○
* Technology and Legal Aspects	○	○
* Theoretical Foundations of Security Analysis and Design	○	○
* Trust Management, Assurance, and Accountability	○	○

Figure 2. Cybersecurity domains.

For each cybersecurity domain the participant could specify if they have or not expertise in this domain, and in case they declared to have expertise in each particular domain a list of **subdomains** was displayed asking the participant to specify the particular subdomains of expertise, a textual description of the core competencies, a list of key researchers in the domain, the total number of publications and patents in this domain. Considering that the proposed taxonomy may not be complete participants were also given the choice to provide using an text field other subdomains of expertise not listed. The following figure shows as an example the subdomains defined for the Cryptology domain.

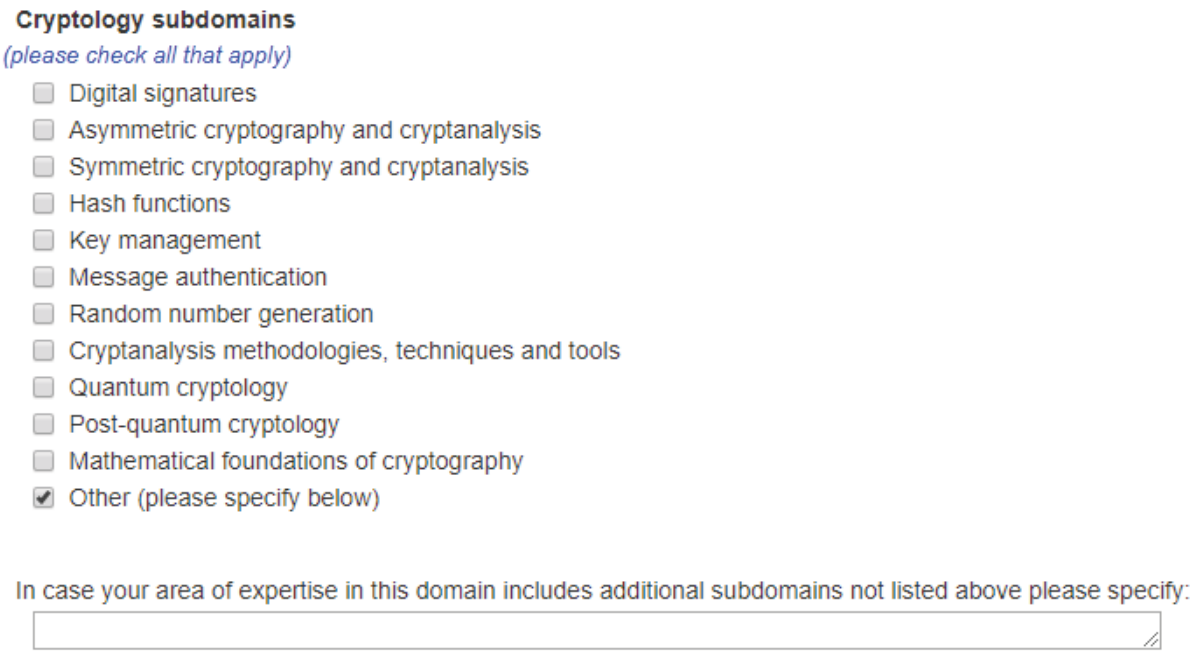


Figure 3. Cryptology subdomains.

After specifying the domains and subdomains of expertise the survey participants was requested to specify the **sectors, applications and technologies**. This information is useful to further refine and identify the area of work of the centre, for example, cryptology work in embedded systems versus cloud computing are of significant different nature considering the restrictions of each technology. The following figure shows the survey items displayed in this section.

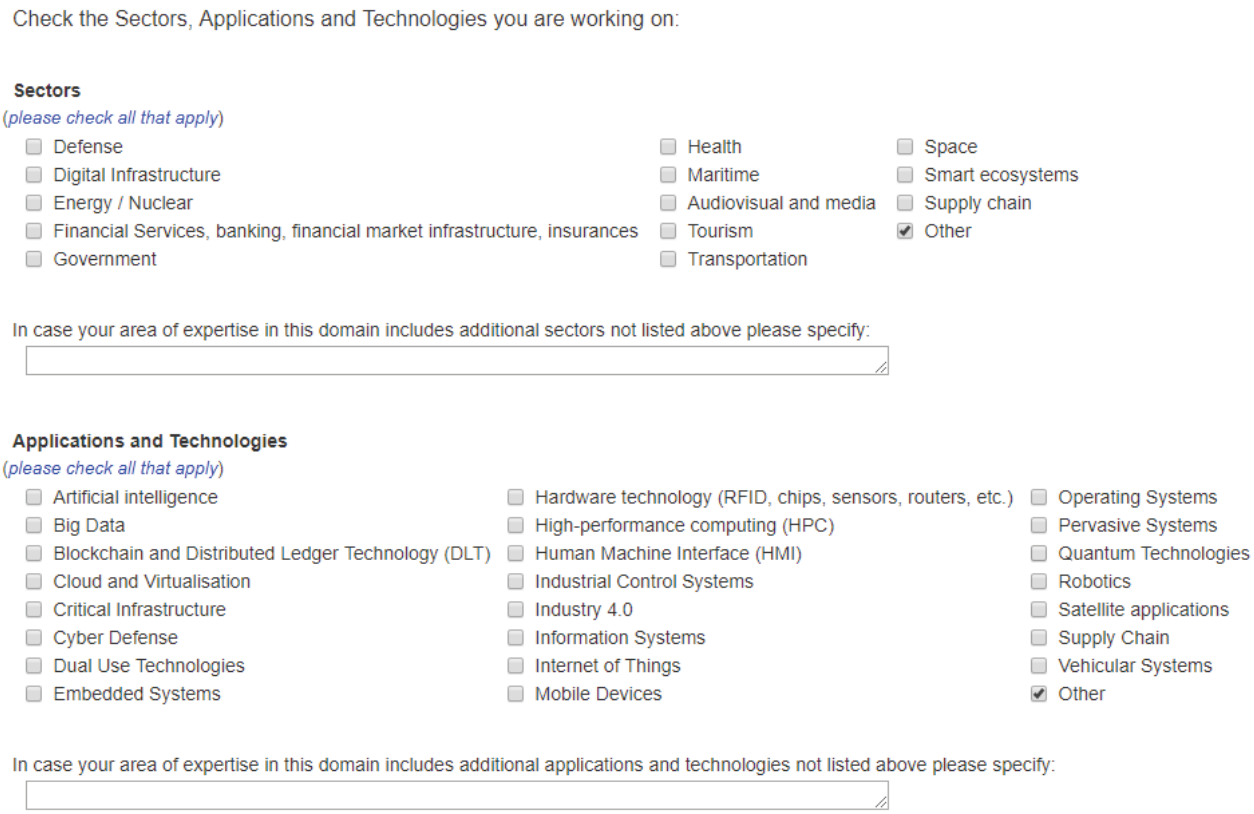


Figure 4. Sectors, applications, and technologies.

In the **international collaborations and joint programs** section the survey participants were asked to informed the number of cybersecurity research projects (EU and national), cybersecurity patents, agreements/contracts with industries and governments, and memorandums of understanding with other organizations.

Finally, in the **confirmation and agreement with the privacy policy** section the participants had the option of providing supporting documents and to check the box informing if they agree to make the declared information public and confirm that the declared information is correct.

Survey Dissemination Strategy and Analysis of Results

In this chapter the survey dissemination strategy and the analysis of the results are presented. As a disclaimer, the numbers presented here are the straightforward analysis of the numbers provided by the survey participants, which in a few cases may not be accurate, and no thorough manual analysis of the entries was done.

2.1. Survey Dissemination Strategy

The survey was initially disseminated through the following channels:

- DG-CNECT and DG-JRC social media;
- DG-CNECT newsletter contacts;
- ERNCIP mailing list;
- ECSO mailing lists;
- The three (3) CSAs (cyberwatching.eu, AEGIS, EUNITY) mailing lists;
- The National Contact Points network.

After the initial dissemination many entities used their national distribution channels to further disseminate the survey, for example, national cybersecurity mailing lists, twitter accounts, etc. As a result, the dissemination strategy was successful considering the high number of participants.

2.2. Number and Geographical Distribution of Participants

The total number of surveys completed by March 5th, 2018 was **665**, of which **61** centres provided supporting documents. As it is possible to see in Figure 5, the survey results cover all the EU MS plus additional countries having access to the H2020 research program. Figure 6 presents the same data showing the number of participants per country using a bar chart, with the countries in crescent order considering the number of participating centres.

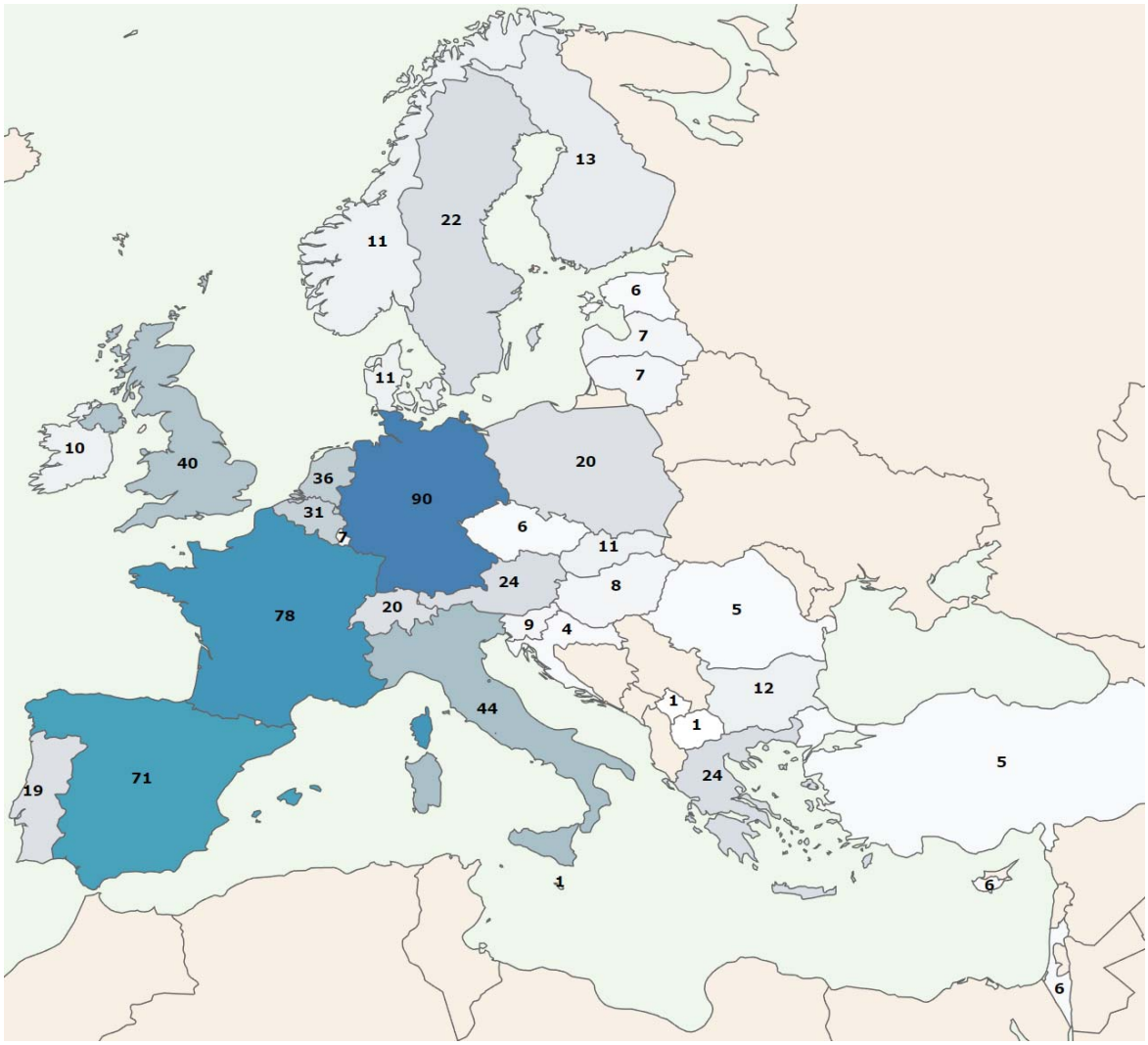


Figure 5. Geographical distribution of number of survey participants per country with a color legend indicating with darker blue color countries with a higher number.

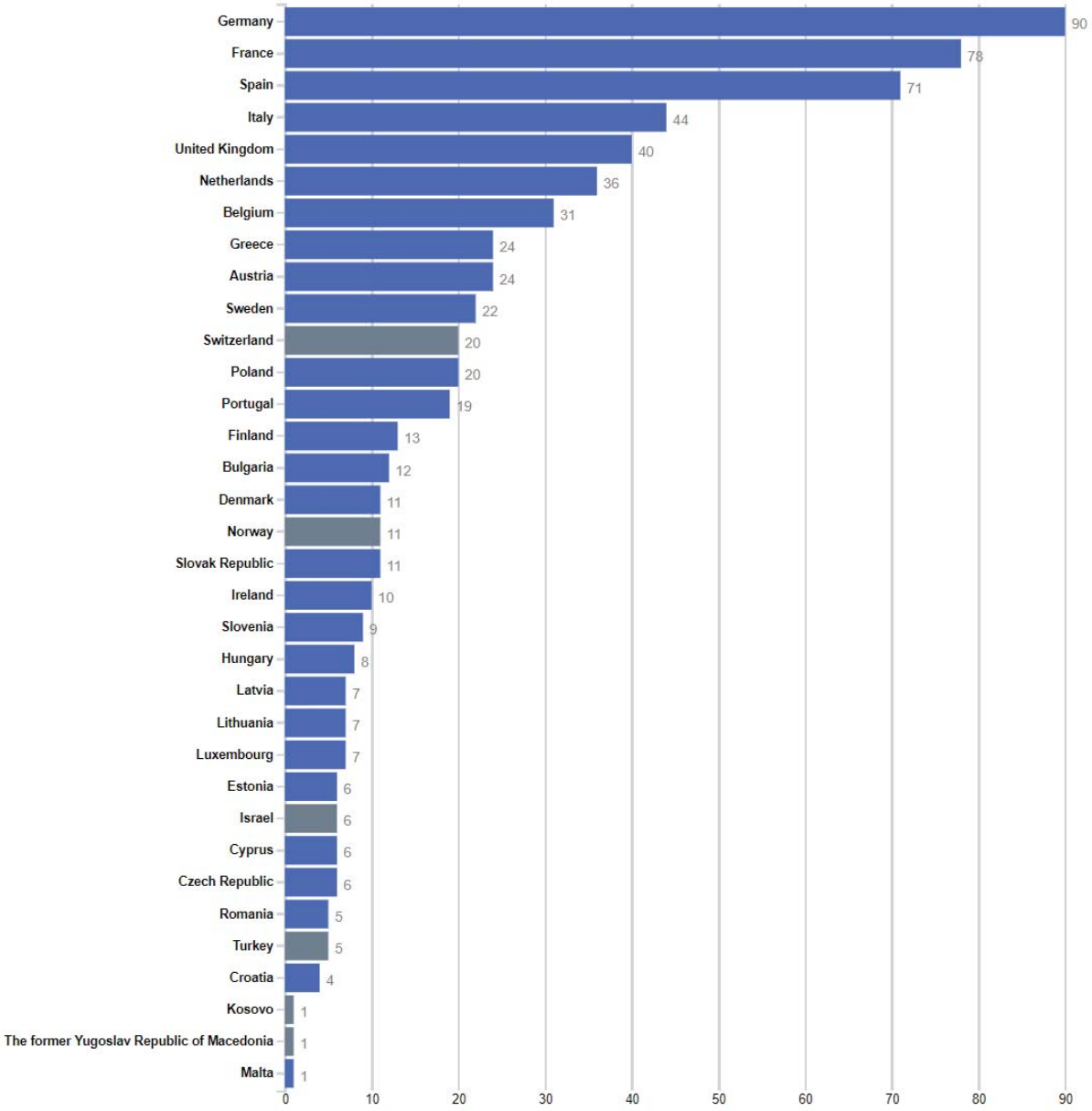


Figure 6. Number of survey participants per country. Non-EU participants are highlighted in in grey.

2.3. Entity Type and Legal Status of Participants

The responders were clustered per type of institution (see **Figure 7**), where higher education departments were the majority. The "Other" entity type, which ranked 2nd place in the participation, clustered together Small and medium-sized enterprises (SMEs), private Non-governmental organizations (NGO) and other more generic entities.

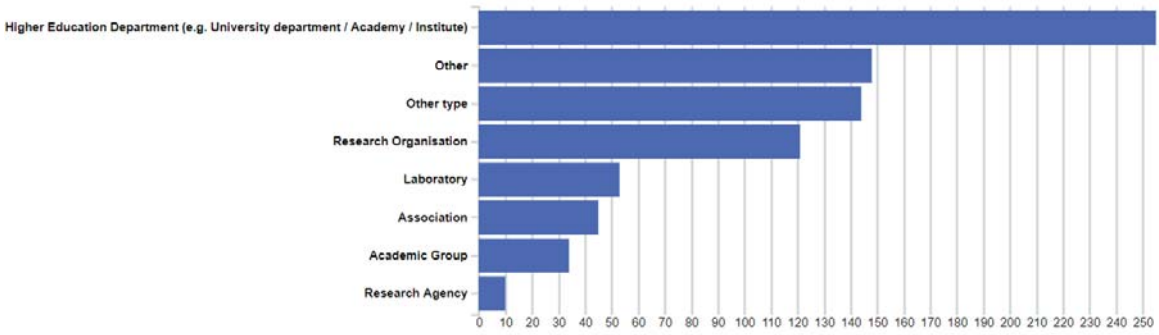


Figure 7. Distribution of participants according to their entity type.

Figure 8 summarizes the clustering of entity types per country, showing that among the survey participants the bulk on the research activities reported seems to be performed mainly by higher education departments (universities).

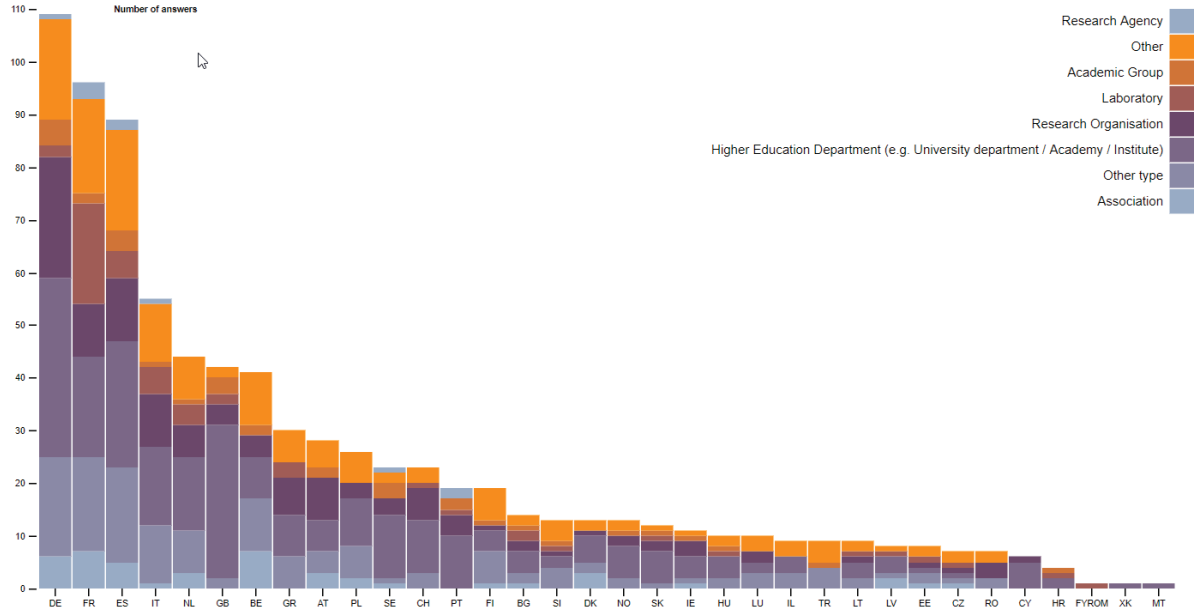


Figure 8. Distribution of entity types per country.

Figure 9 shows the overall distribution of all participants according to their legal status where the "Other" status usually represents entities without an independent legal status (e.g. research centre dedicated institutes or university departments).

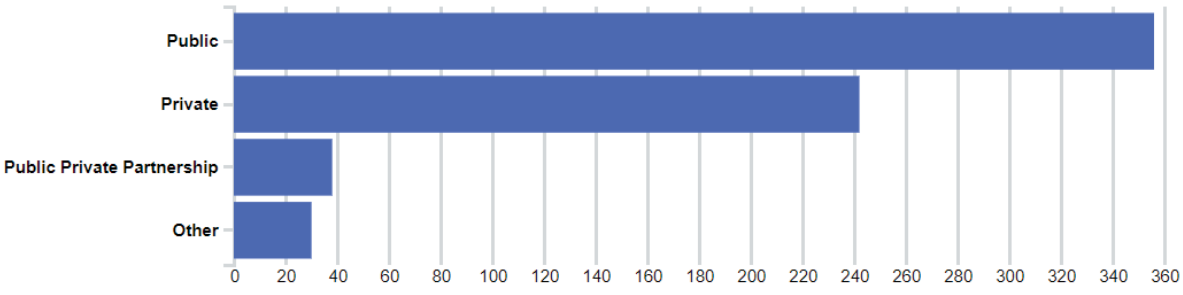


Figure 9. Distribution of participants according to their legal status.

Figure 10 shows instead the distribution per country and per type of "legal status" of the responders (public, private or Public Private Partnership - PPP). It is interesting to note how, with a few exceptions, that there is a certain numerical balance between public and private organisations, as well as the fact that, despite being a new instrument, PPPs on cybersecurity research exist in the majority of the countries of the responders.

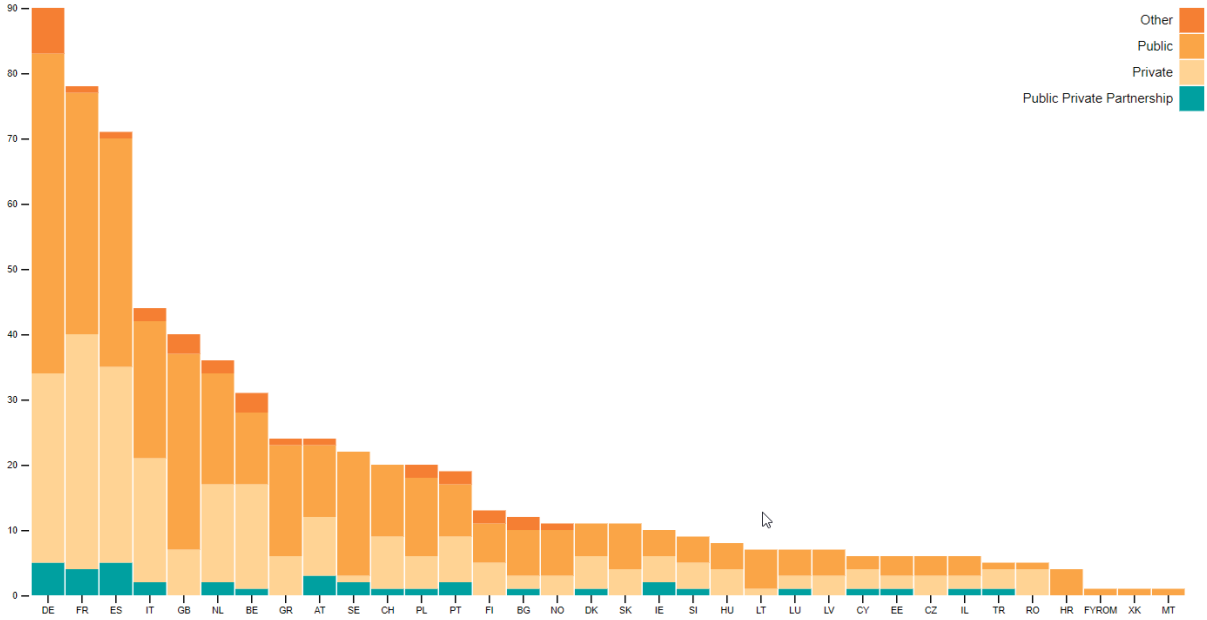


Figure 10. Distribution of entities per country according to their legal status.

2.4. Cybersecurity Domains and Subdomains

The analysis of the answers related to the domains of research of the responders, shows that all of them are covered (**Figure 11**) at European level as well as per at country level (**Figure 12**). It interesting to note that 39 institutions declared to cover all the 14 cybersecurity domains. Taking into consideration all the institutions that declared to cover at least 10 out of the 14 cybersecurity domains specified in the survey the number become an impressive 191.

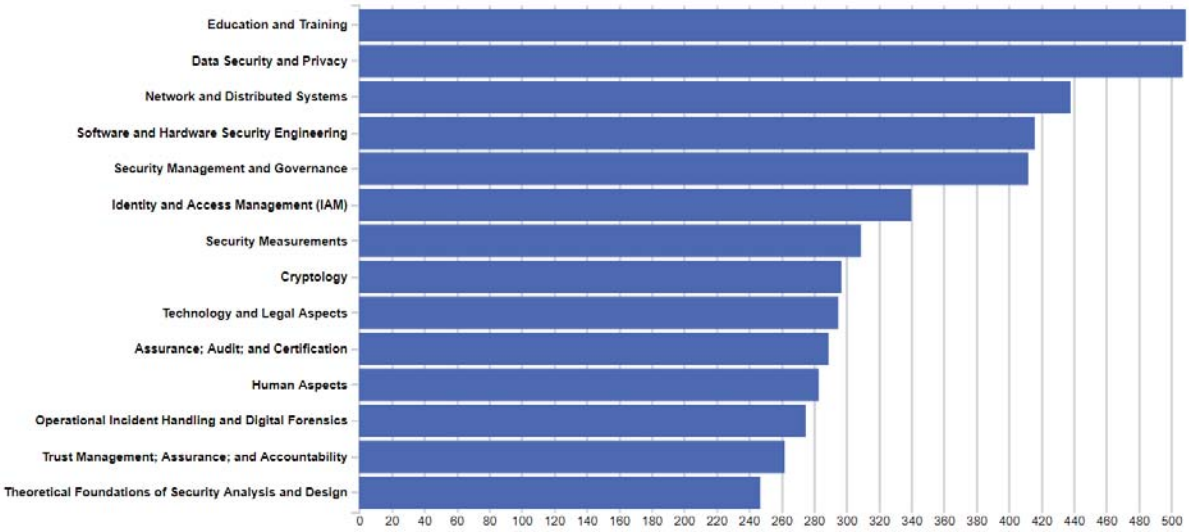


Figure 11. Distribution of participants according to their expertise in the cybersecurity domains.

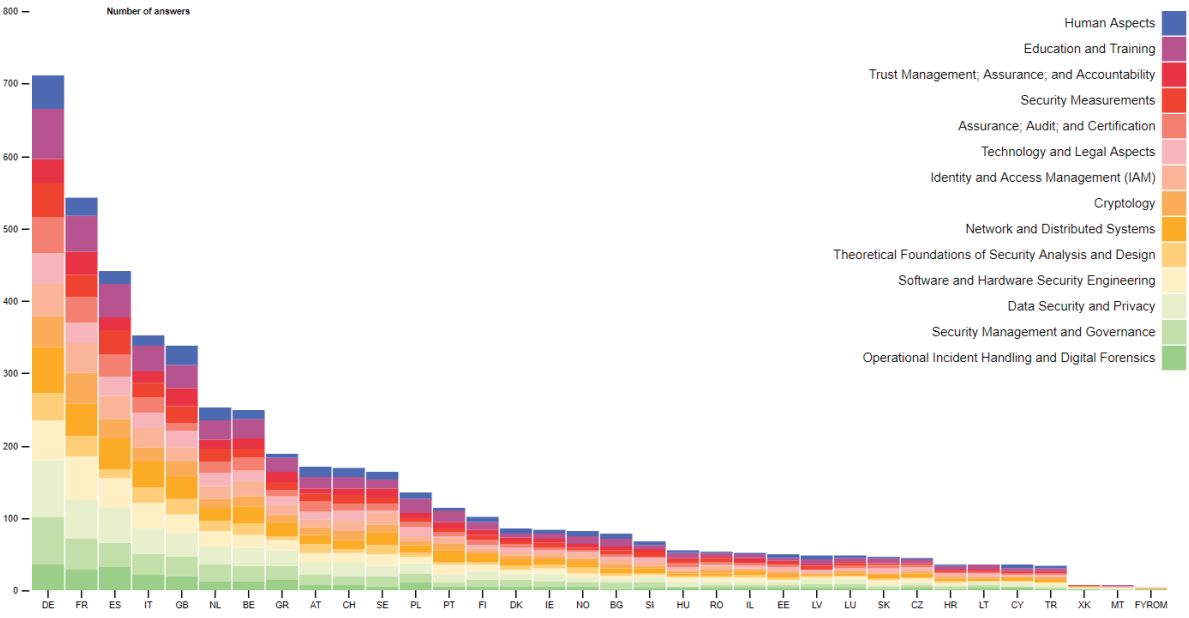


Figure 12. Distribution of domains per country using stacked columns showing total of replies per country and partition per domain.

These graphs however, do not tell all the truth. In fact, by analysing each domain and checking the coverage of the related subdomains, it results remarkably less homogeneous. In other words, there are relevant sub-domains that are today poorly investigated (post-quantum cryptography is a clear example).

Figure 13 and **Figure 14** shows the bar chart listing all selected subdomains and the number of participants that selected each of them. Again, since the majority of survey participants are of higher education institutions it is no surprise that “Cybersecurity education” was selected by almost 400 entities. Another interesting trend the the presence of “privacy and data protection” related subdomains in the first positions Figure 13, meaning that several research institutions in Europe have research interest in this

domain. This result could be read probably as a direct effect of the entry into force of the General Data Protection Regulation at European level and the general attention is paid today at MS level to privacy and data protection issues.

Identity management, secure architectures and network security score also quite high in term of number of institutions working on these domains; again this is not surprising as they are historically the “containers” where the majority of general purpose cybersecurity research activities fall.

On the other side of the ranking (Figure 14) it is interesting to note as relevant domains such as quantum and post-quantum cryptography, trusted computing, cybercrime are addressed in the best case by less than 1/6 of the research institutions which responded to the survey.

The meaning of these results needs to be better analysed. On a side it seems to indicate that there is a huge number of horizontal research organisation in Europe, which is, per se positive to ensure a geographically homogeneous coverage of all the different research domains. On the other, this picture is only superficial, as, when looking into the subdomains, it emerges that the majority of the research institutions focus only on a minor portion of the research spectrum aggregated under each high-level cybersecurity domain. Moreover, the analysis of the scientific literature and the study of the participants to cyber-security related H2020 projects (see in the following the related section), provides a completely different picture, where few research institutions polarise the research and knowledge production. The reasons of this dichotomy might be several, but the most plausible is the dispersion of resources (too many actors trying to do all with little resources), and the lack of overall coordination and collaboration.

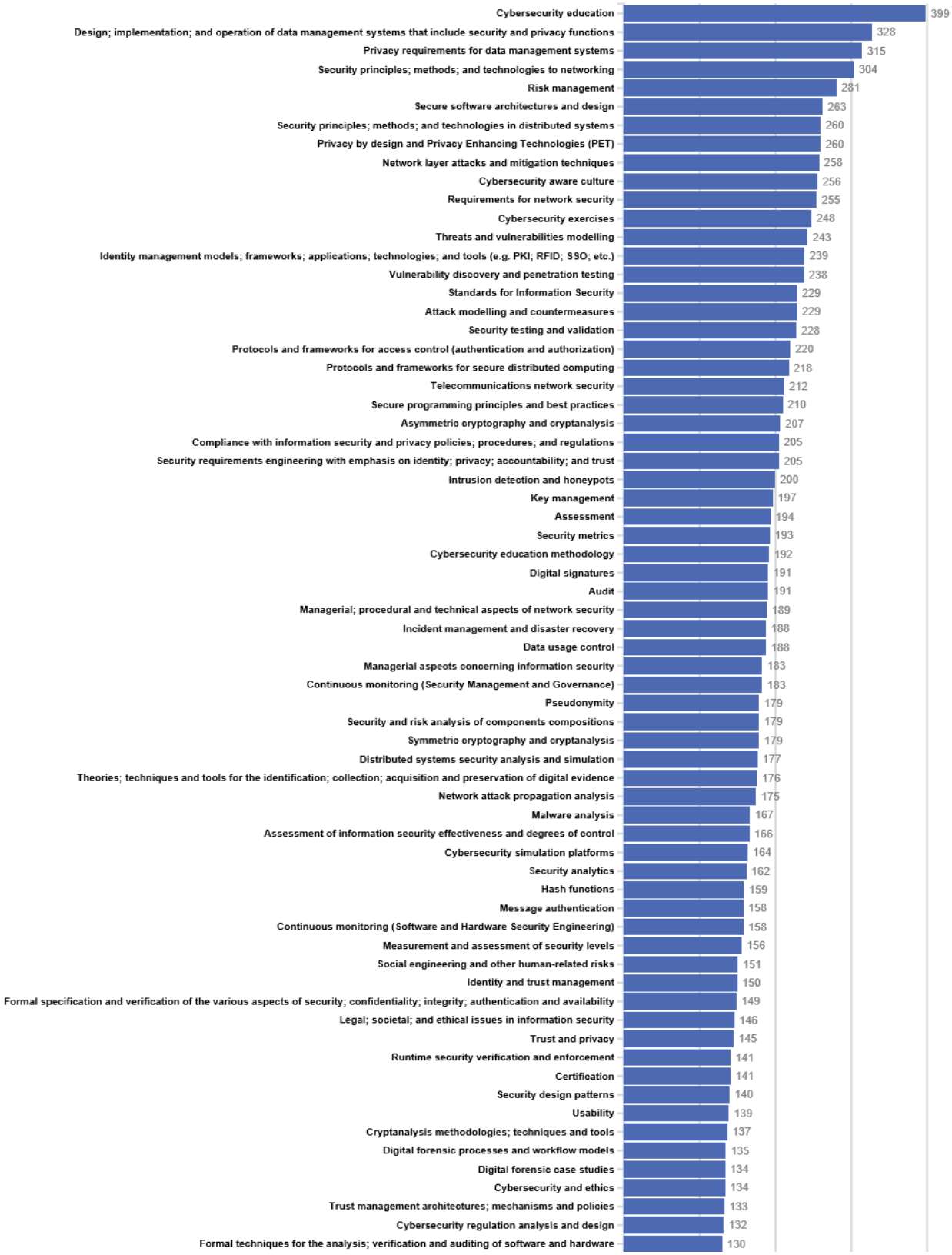


Figure 13. Distribution of participants according to their expertise in the cybersecurity subdomains, first half.

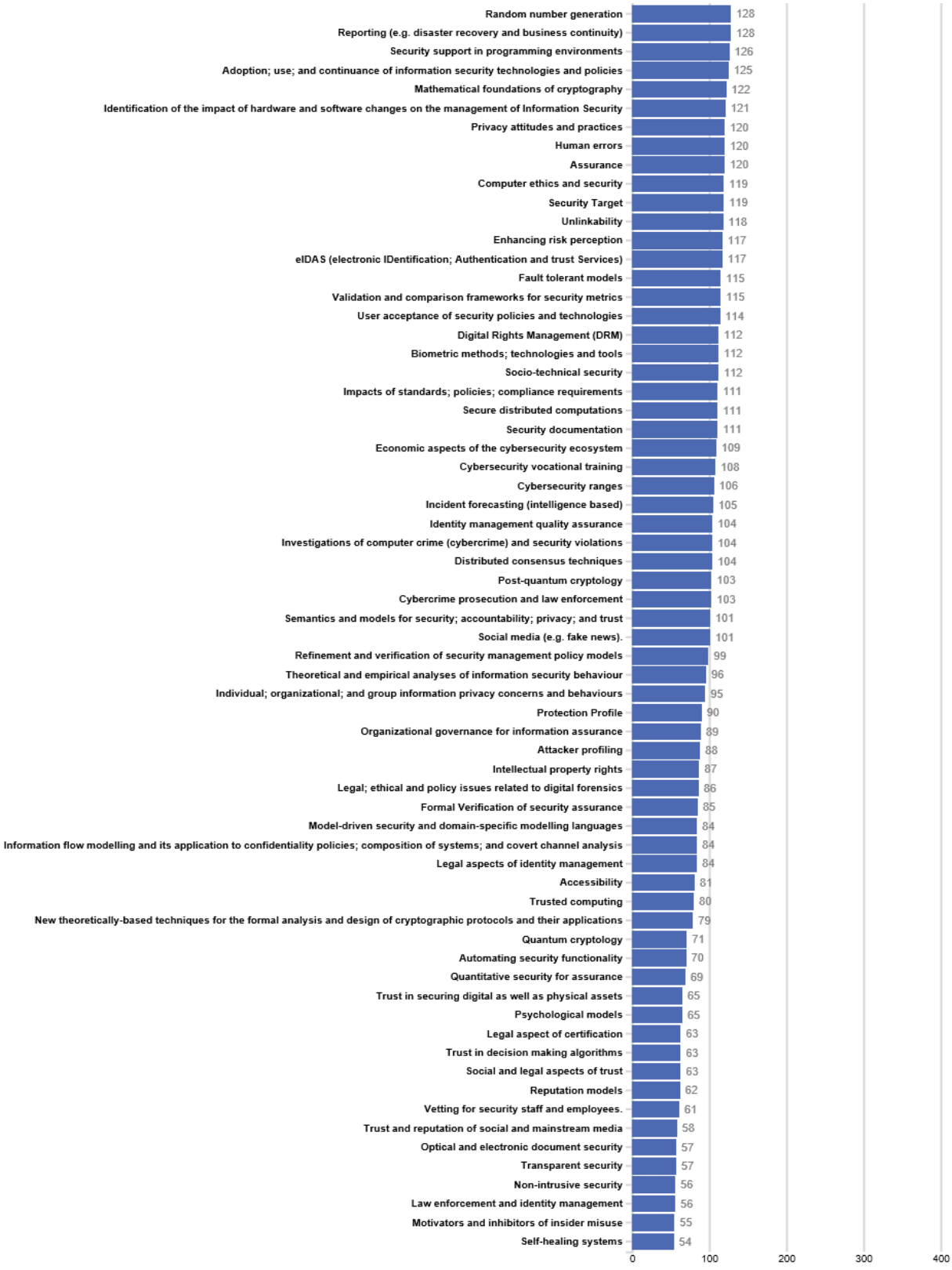


Figure 14. Distribution of participants according to their expertise in the cybersecurity subdomains, second half.

2.5. Types of Funding Sources

Figure 15 shows the overall distribution of funding sources while **Figure 16** shows the type of funding sources reported for each country. The ratio per country follows the same overall proportion with a lower number of international programmes for countries with fewer number of survey participants, which may imply that these countries do not collaborate internationally as much as the others. Again, this may lead to the conclusion that resources are dispersed and there are not enough cooperation/coordination schemes in place across borders.

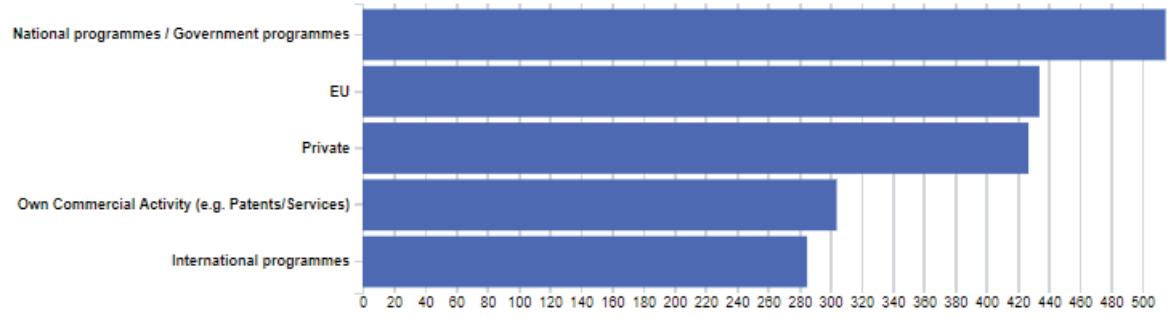


Figure 15. Distribution of funding sources.

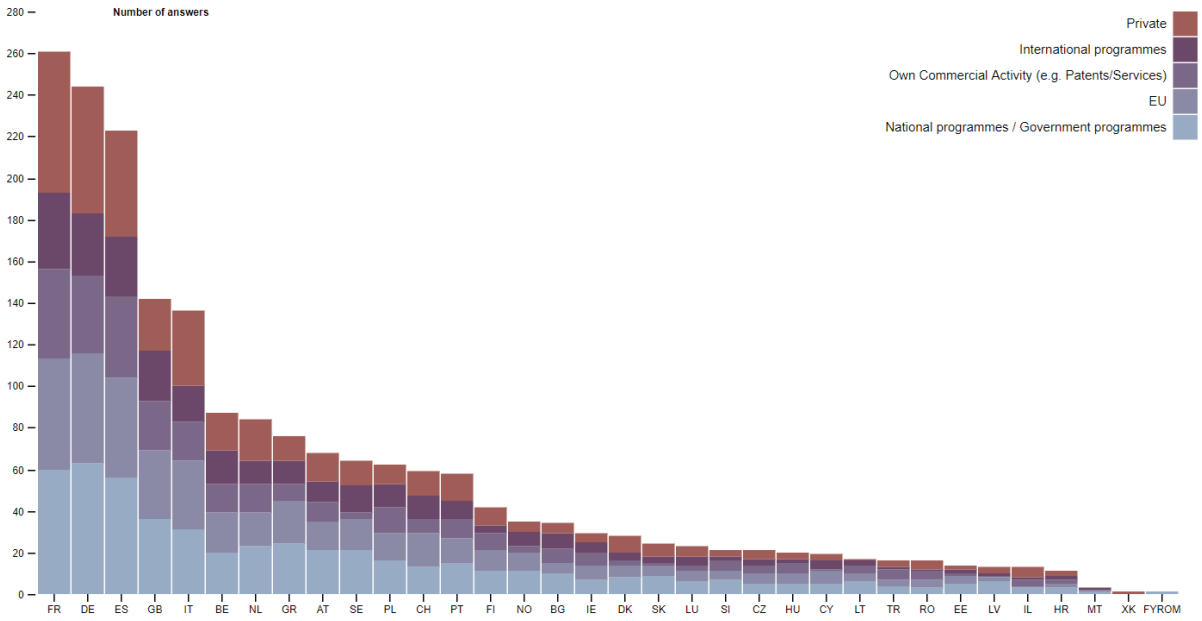


Figure 16. Distribution of funding sources per country.

2.6. Type and Number of Employees (FTE)

Figure 17 shows the number of senior and junior researchers reported overall while **Figure 18** shows the same numbers considering each country. Overall the proportion is the same while some countries have a significantly higher number of senior researchers in contrast to junior (e.g. Spain, the Netherlands, and Italy).

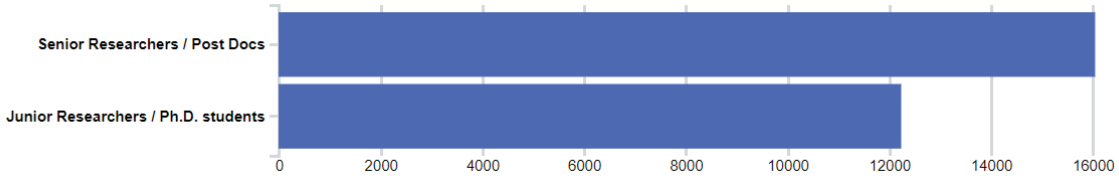


Figure 17. Overall distribution of FTE declared to be working on cybersecurity be all survey participants.

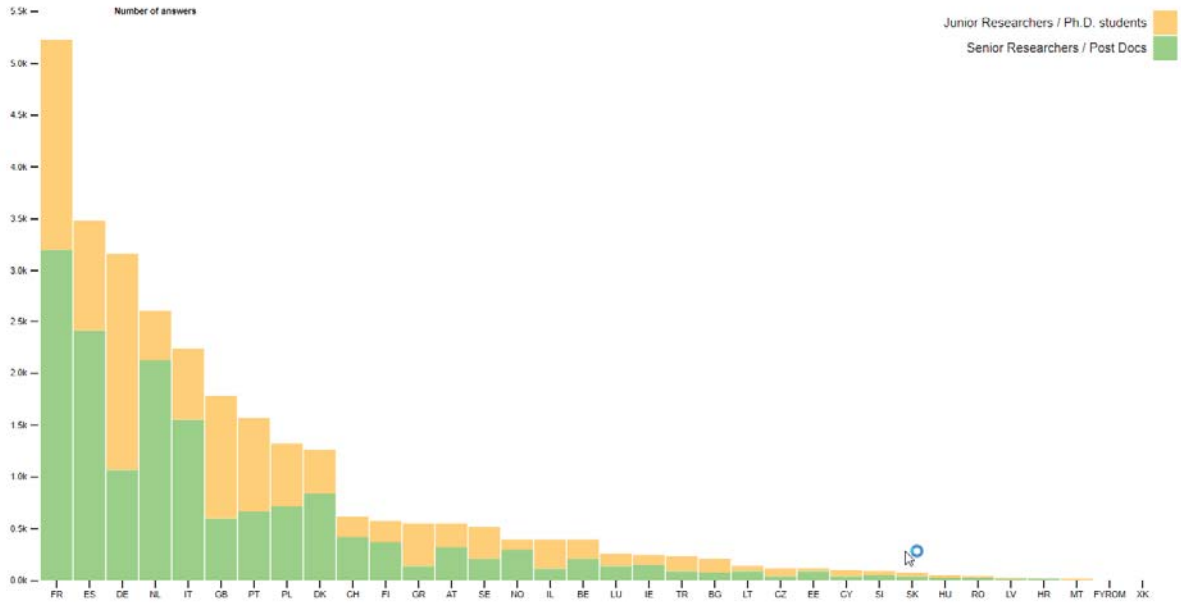


Figure 18. Distribution of FTE working on cybersecurity per country.

Figure 19 shows the total number of FTEs reported for each country in a map. Since a few numbers seemed a bit too large a few survey replies were checked manually revealing that many centres did not report cybersecurity specific FTEs but their total FTE. Therefore, an update should be requested to the survey participants in order to have a better overview of the real cybersecurity workforce of each institution (see Section 3.10 – Missing Elements and Mitigation Strategy).

The large number reported revealed that the Centers included in their cybersecurity teams all ICT experts in their departments. However, someone may argue that since cybersecurity experts work hand-in-hand with ICT experts to design/integrate a secure ICT system they are all considered to be in the same team. Furthermore, another problem is that since there is not any formal certification of cybersecurity skills, the Centres cannot distinguish the cybersecurity experts for the general ICT experts.

In a future survey the question needs to be more explicit.

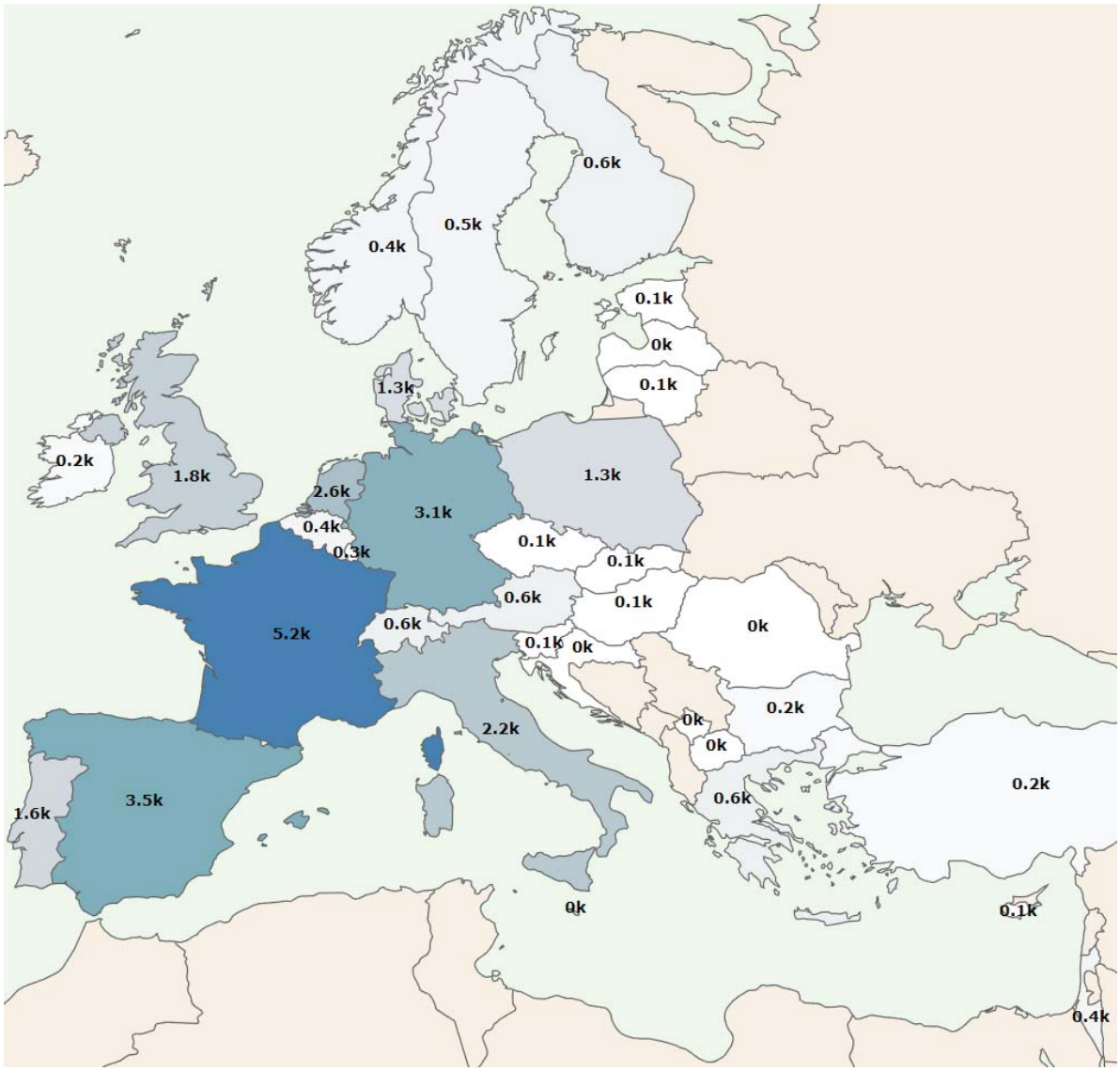


Figure 19. Geographical distribution of FTE working per country showing number of thousands (k) FTE with a color legend indicating with darker blue color countries with a higher number.

2.7. Publications

From all survey participants only 362 reported their publications in at least one of the cybersecurity domains. **Figure 20** shows the total number of publications reported by all survey participants showing a relative low number of patents overall. **Figure 21** shows the total number of publications reported for each cybersecurity domain, showing that cryptology is the domain with the highest number of publications.

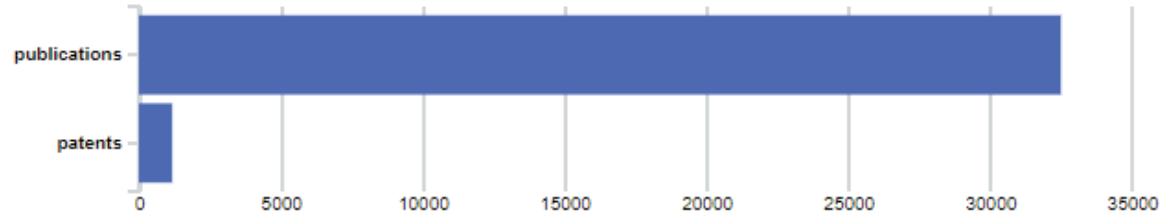


Figure 20. Total number of declared publications.

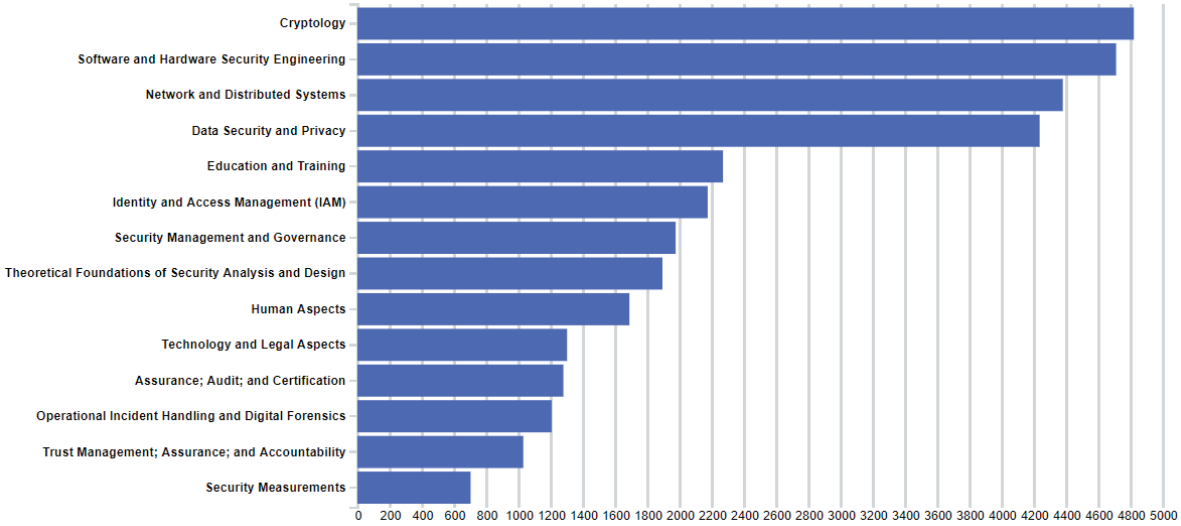


Figure 21. Number of publications reported for each cybersecurity domain.

Figure 22 and **Figure 23** shows the distribution of publications per country in a map and bar chart, showing that participants from Germany and France together represent around 50% of the total number of publications. Again, as already seen previously, the number of patents is not particularly significant for any country.

Cryptography results to be the top ranking domain for what concerns the number of publications, however this evidence should be treated with due care as under this category of publication are grouped both foundational cryptography (i.e. research where indeed new cryptographic schemes and algorithms are designed, evaluated etc.) and applied cryptography (i.e. where cryptography developed by others is applied used to solve a particular applicative problem). The big majority of publication present in the scientific literature under cryptography fall in the second list (simply because the process of designing a new cryptographic algorithm based on some mathematical foundation, is typically much harder and time consuming than applying existing algorithms on new problems). Considering that the majority ICT-related application today has to deal with encryption/authentication/signatures, it is then not surprising to see cryptography score so high in term of number of publications despite the fact that it is not the top ranked domain in term of number of research centres working on it as showed in Figure 13.

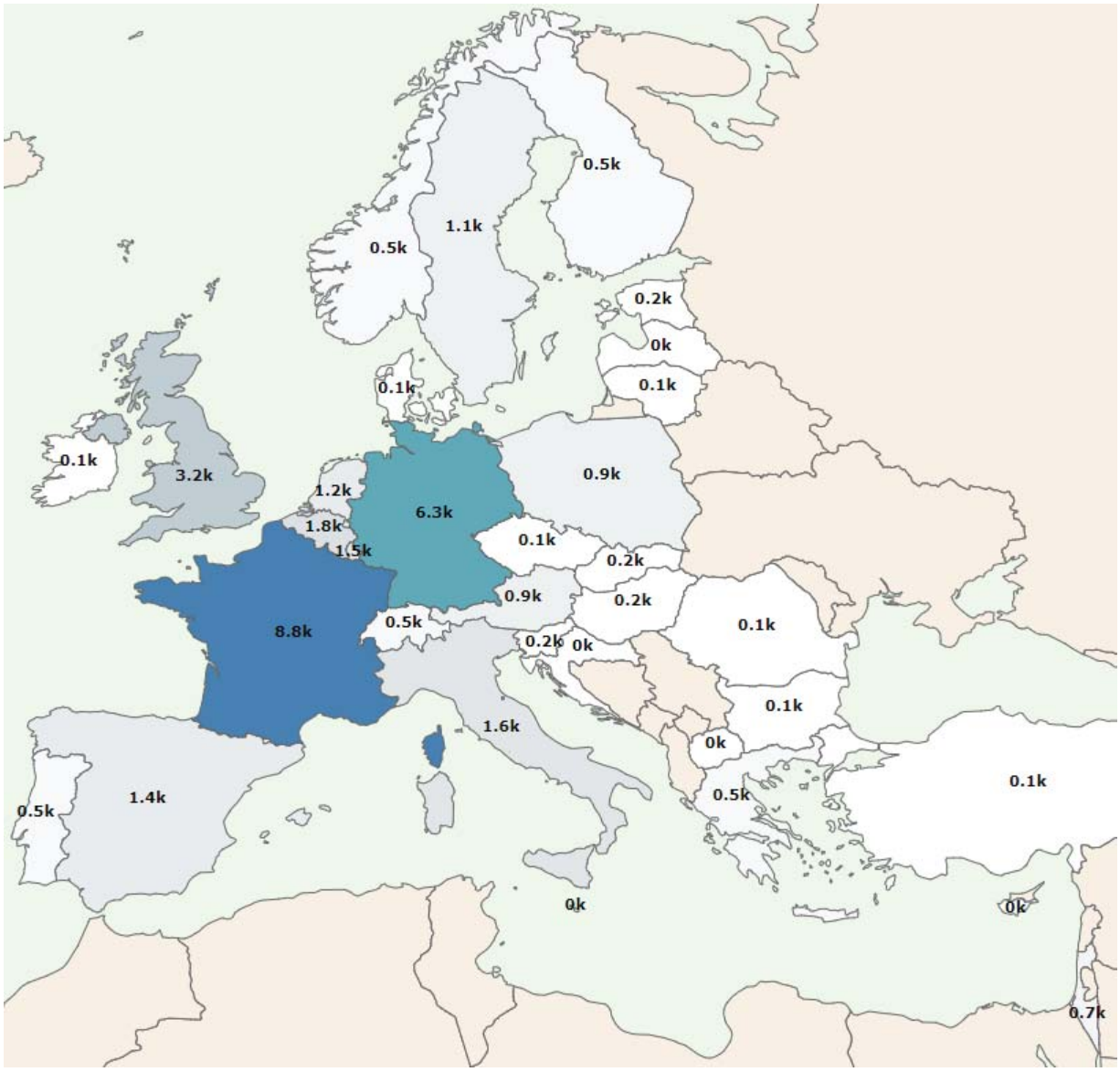


Figure 22. Geographical distribution of total number of publications per country showing number of thousands (k) publications with a color legend indicating with darker blue color countries with a higher number.

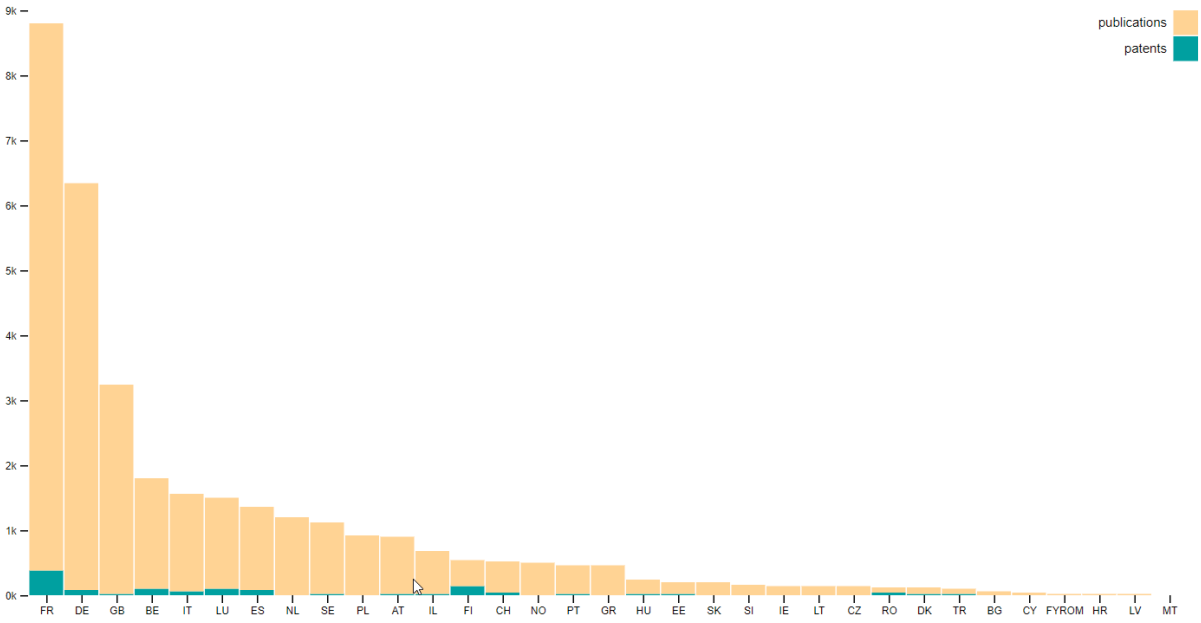


Figure 23. Number of publications per country.

Figure 24 shows the division of publications for each cybersecurity domain per country, showing again fragmentation of the domains across and inside the countries where very few publications in many different topics were reported by the countries.

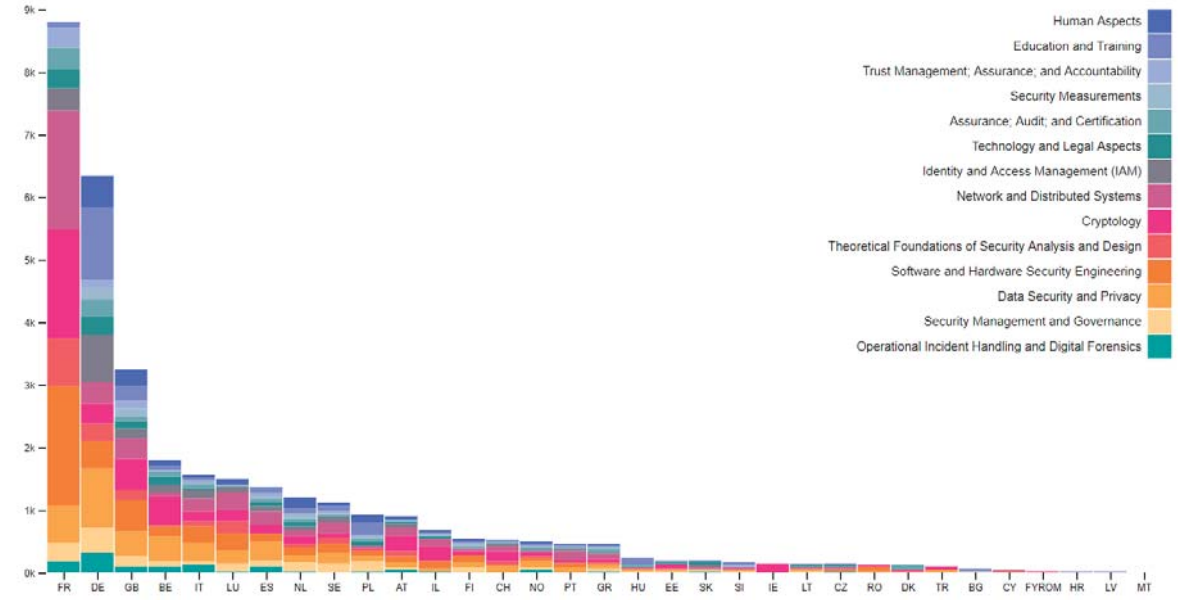


Figure 24. Number of publications for each cybersecurity domain per country.

2.8. Sectors, Applications and Technologies

As shown in **Figure 25** all the sectors mentioned in the survey are subject of work of a number of institutions; however, looking at the distribution among countries (**Figure 26**) it is evident for example that the sectors where costly facilities are needed to perform cyber-security research (e.g. energy, space, defense etc.) are well covered only by those countries which traditionally have more resources available to invest in big facilities.

This is again confirmed analysing the field of applications (**Figure 27** and **Figure 28**): as it is possible to see the fields requiring more investments (HPC, artificial intelligence, quantum etc.) are well covered only in countries with traditionally highest availabilities in term of investments.

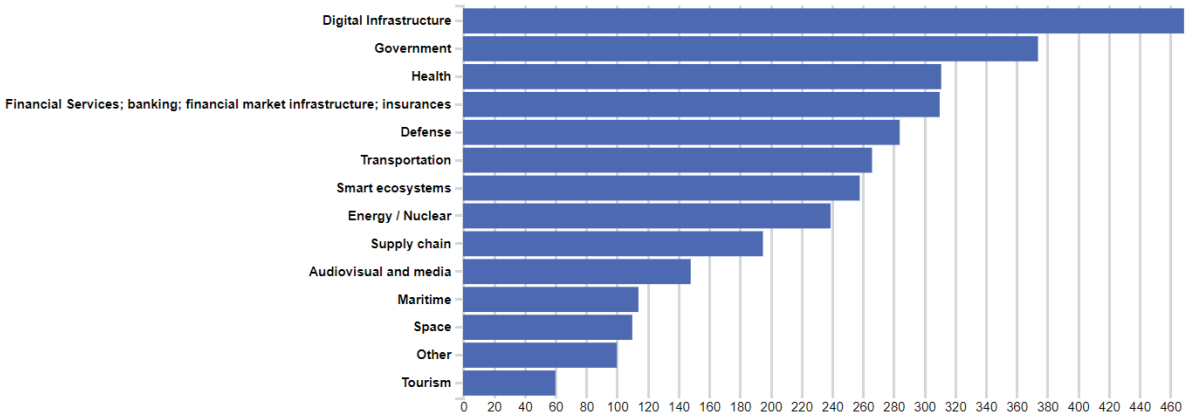


Figure 25. Overall distribution of sectors.

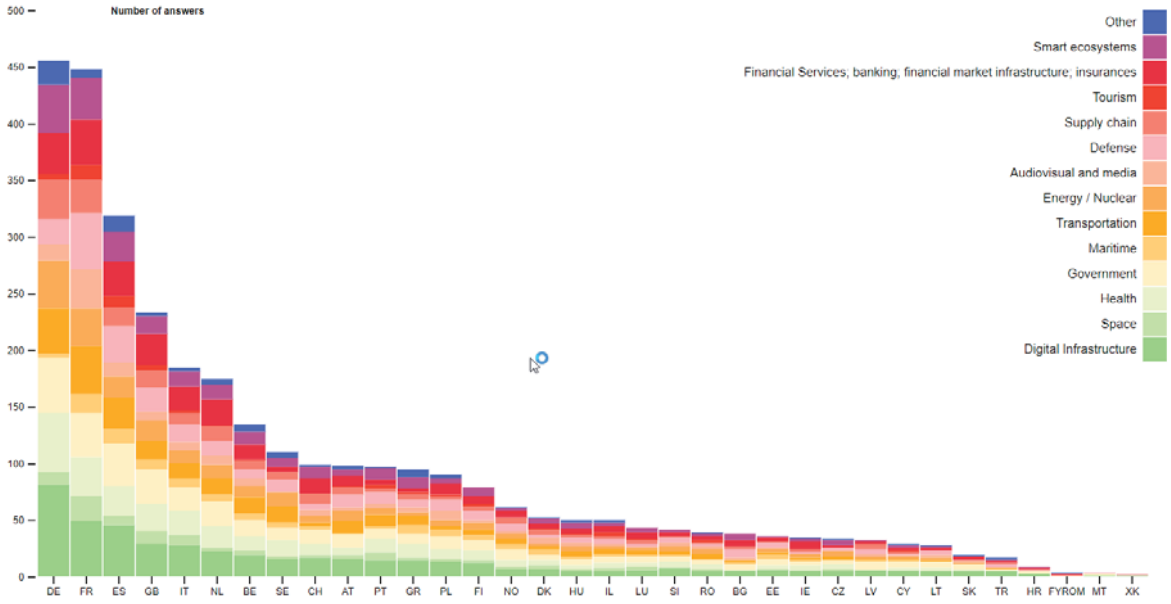


Figure 26. Distribution of sectors per country.

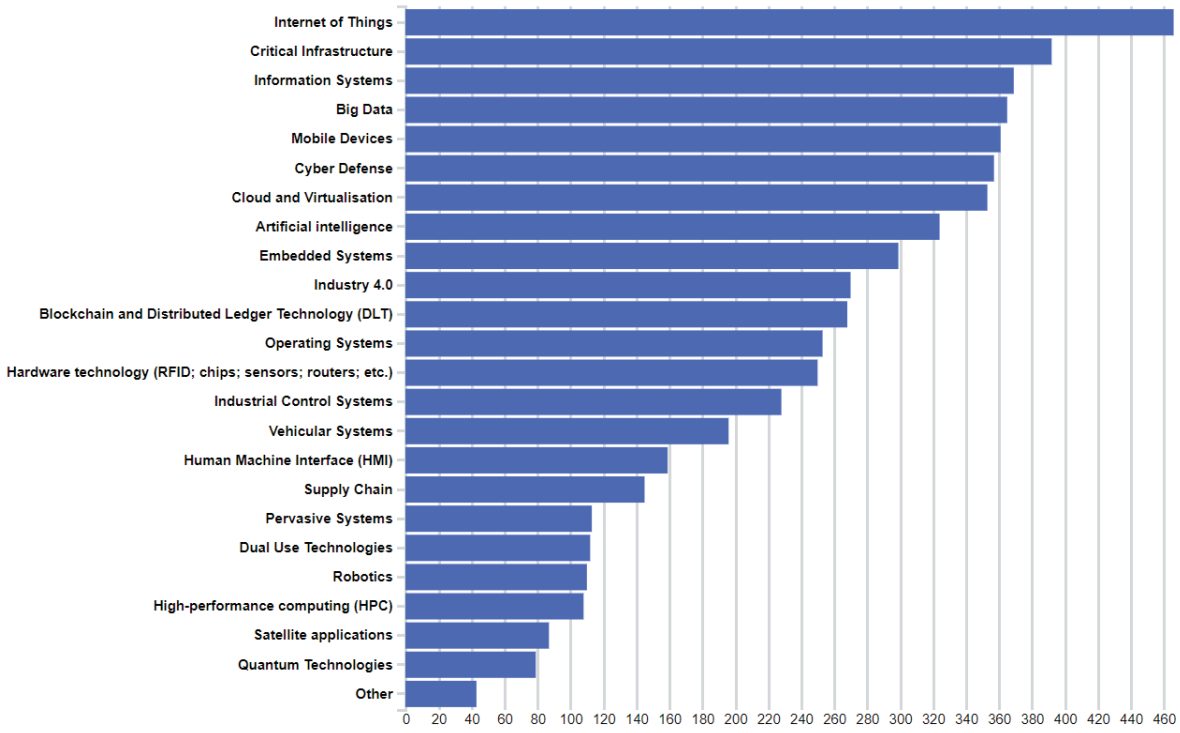


Figure 27. Overall distribution of applications and technologies.

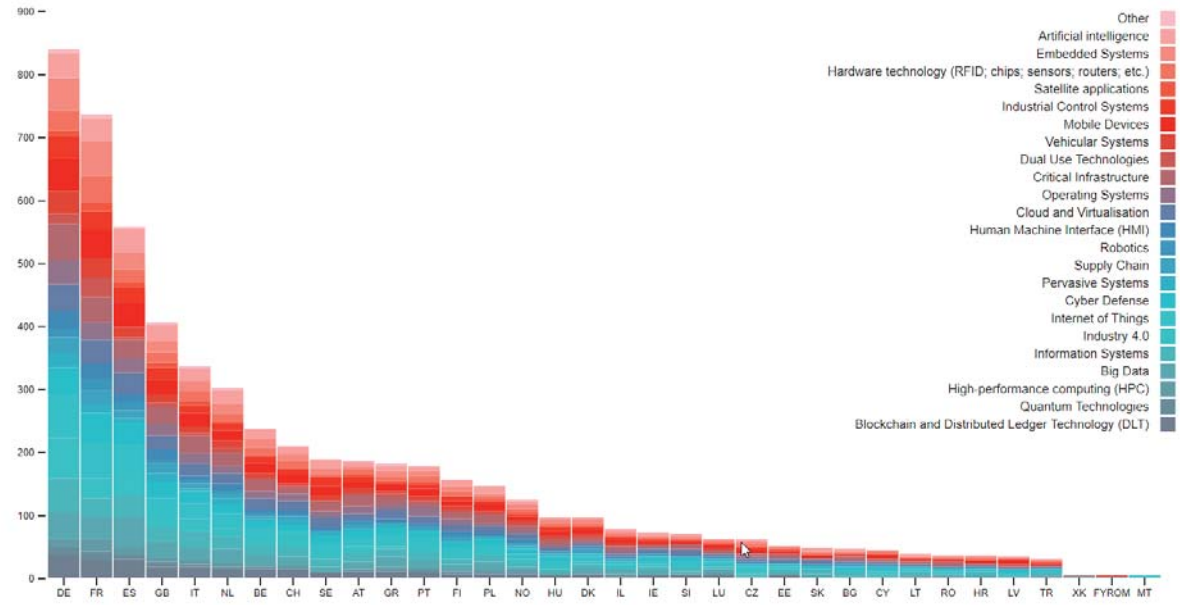


Figure 28. Distribution of applications and technologies per country.

2.9. International Collaborations and Joint Programs

Figure 29 and **Figure 30** shows respectively the collaborations and joint programs reported overall for all participants and for each country. These numbers do not report the total amount in Euros only the total number, for example, of EU cybersecurity projects.

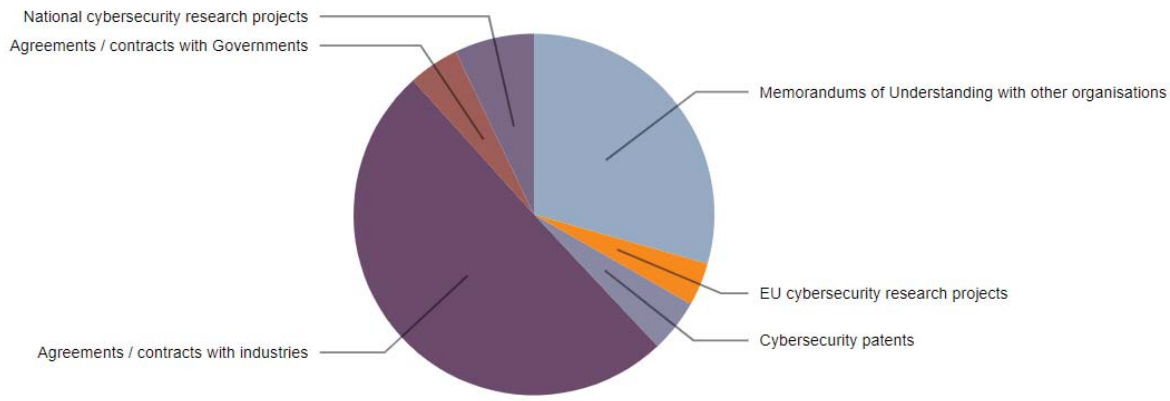


Figure 29. Overall distribution of number of international collaborations or joint programs declared by survey participants.

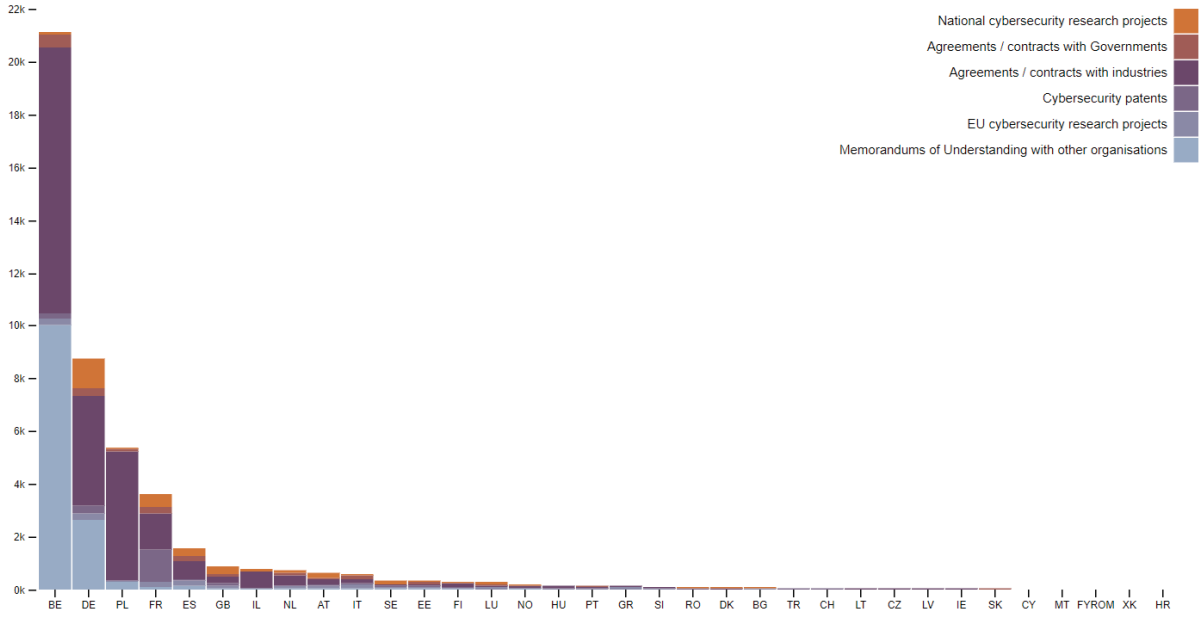


Figure 30. Distribution of number of international collaborations or joint programs declared by survey participants for each country

It seems that many of the Centers have already agreements with the Industries, however, froom the answers to the survey, it was not clear that these Agreements were Consortium Agreements thru EC projects. The sustainability of these Agreements could not be evaluated. In a future version of the survey these points need to be clarified.

2.10. Missing/Overstated Elements and Mitigation Strategy

After analysing the survey results a few missing elements from the survey were identified where further investigation could be required for a better overview of the cybersecurity expertise. A possible mitigation strategy is to update or complement the survey questions with the missing elements and to ask the participants to update their information. The following list summarizes these elements:

- **Open-ended questions**: the survey allowed the participants to specify a few items in case the list of answers was not complete considering their entity type, legal status, cybersecurity domains, sectors, applications and technologies. These

inputs should be taken into considering in order to refine the cybersecurity taxonomy and the set of possible answers in order to make the survey more precise, for example, regarding the report legal status **Figure 31** shows the distribution corrected manually considering additional categories not available in the survey;

- **Cybersecurity specific FTE**: in a many cases the survey participants reported their total FTE, including not only the FTE working on cybersecurity topics, which is a relevant information especially considering that some entities reported over one thousand FTE. The question that remain open is how cybersecurity specific is the expertise of each centre/department;
- **Funding numbers**: it would be interesting to request from the participants and update regarding the funding received in order to evaluate how much investment in cybersecurity is currently available per country;
- **Network and connections**: they survey participants could be asked to update their answers including the names of the EU projects and list the principal collaborating entities in order to define a graph of connections between institutions. The same option could be used to define a social graph of collaborating researchers from the different institutions, which could be extracted automatically from publication databases. To include this information, the survey could ask the participants to fill in supporting spreadsheets listing project names, researchers, and collaborating institutions that could be processed automatically in order to create these collaboration graphs;
- **Software licenses and open source projects**: in addition to publications and patents the survey participants could be requested to update their response in order to include the number of software licenses and list open source projects in order to evaluate more objectively technology transfer and collaboration with industry;

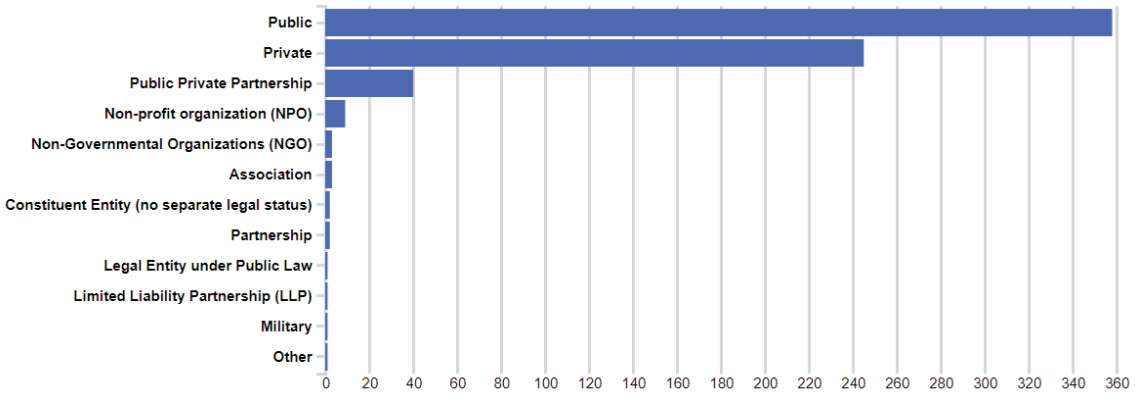


Figure 31. Distribution of participants according to their legal status after manual correction.

3. Scientific and Technological Development Analysis

Scientific and technological developments are not easy to measure. The number of publications, the participation to H2020 projects, and the analysis of the number of patents could however be used together in order to build a better picture of the scientific and technological development in a certain domain. Therefore, in this section the survey results are compared with a desktop research in order to provide a better overview of cybersecurity expertise and to draw a few conclusions on the data reported by the survey participants.

The details of the of the desktop research analysis are presented in the JRC Technical Report *"European Cyber Security Centres of Expertise Preliminary Mapping Exercise"*, while in this section only the relevant evidences instrumental to the survey analysis are reported.

3.1. Analysis of publications

The analysis of the cyber-security scientific literature (i.e. scientific papers published in Conferences and international journals in the last 8 years, see **Figure 32**) indicates that USA is today leading the scientific research in cybersecurity with approximately 2/4 of the number of publications. EU follows, with ¼ of the total number of publications aggregated publications), while the remaining ¼ aggregates the scientific production of all the remaining non-EU countries (dominated by China, Canada and Japan).

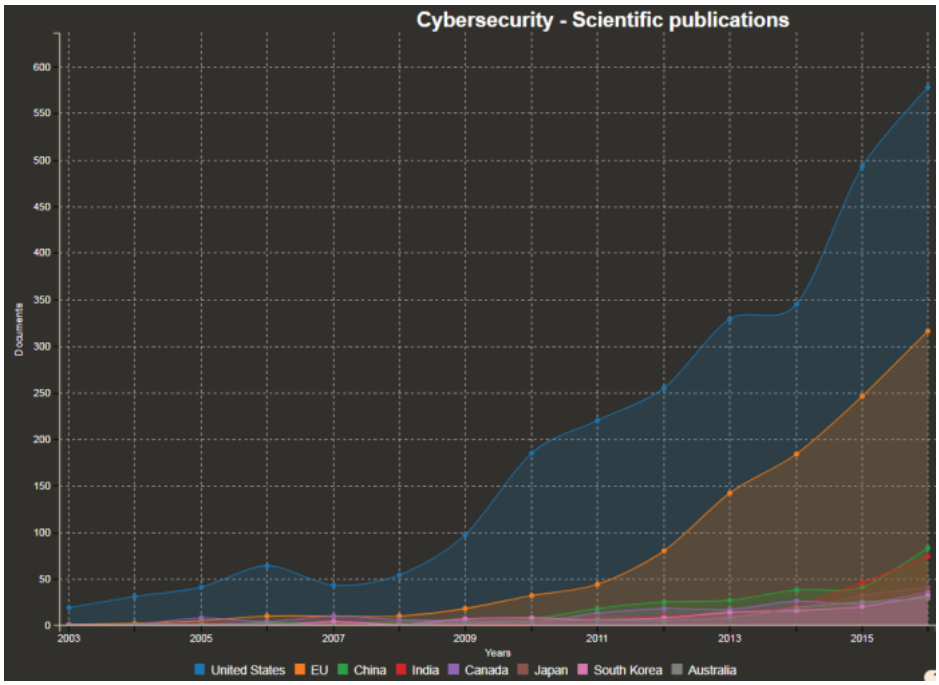


Figure 32. Scientific publications in Cybersecurity per country (Europe = orange).

The scientific production seems to cover all the traditional domains of cybersecurity (confirming the picture provided by the results of the Survey), however, the majority of the efforts are concentrated in the following domains:

- Security Management

- Network Security
- Data Security and Privacy
- Cryptology

It is interesting to note that these domains match with the domains ranking which emerged by the analysis of the surveys.

Concerning this analysis, it is important to underline how the preliminary analysis has been quantitative, i.e. the relevance of the publication has not been weighted (a publication to a conference here is counted as a publication on an international journal). Moreover, even if the four domains just mentioned dominate on all the others in term of scientific production, several of their subdomains results underdeveloped (an example is Cryptology ranking forth in term of total number of publications, but where the post-quantum subdomain results poorly developed (again this confirm the picture provided by the survey).

An analysis of the collaboration networks shows how US is the strongest partner of EU with regard scientific production in cybersecurity, followed by Switzerland and Israel (see **Figure 33**).

Figure 33. Size of node = Country share of scientific publications in Cybersecurity (size of nodes = number project, edge between nodes = project(s) in common, colours identify communities of countries collaborating more often together).

Looking at the distribution of the scientific production among European institutions, emerges (as already anticipated in the previous section) a relevant anomaly with respect to what declared in the surveys. In fact, more than 190 institutions declared to cover at least 10 on the cyber-security research domains. However, the scientific literature analysis per domain, shows that each domain is dominated by a restricted number of institutions in term of number of publications, and that the numerical difference between the top 10 for each domain and the rest of the institutions publishing in that domains is not negligible. In other words, the picture that the analysis of scientific publications combined with the results provided by the survey gives, is that of a Europe where few

institutions polarise the scientific production and are able make a difference in the domain.

3.2. H2020 projects

This picture of a polarised Europe find some confirmation analysing the participation to cybersecurity H2020 projects, where is even more evident this polarisation around a number of restricted academic institutions (see **Figure 34**)

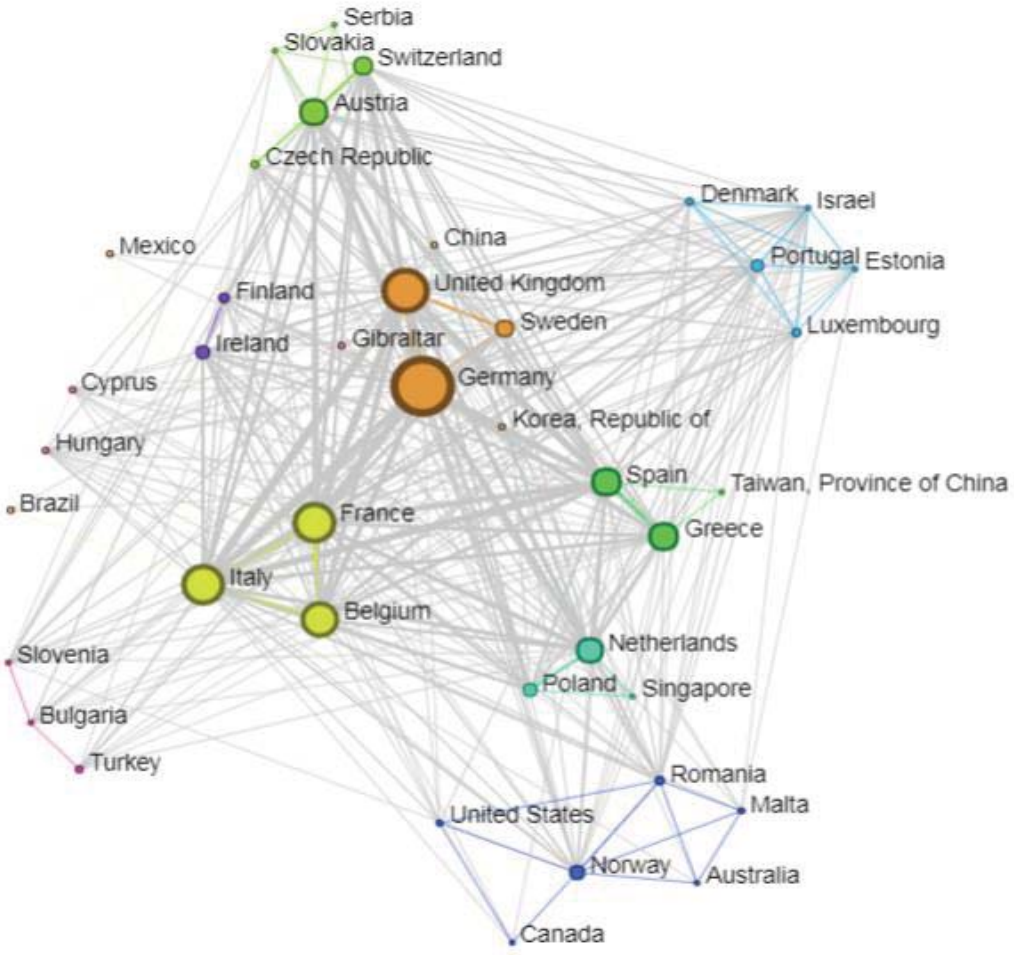


Figure 34. Participants in H2020 Cyber-Security related projects (academic partners).

It is worth noting that considering the private companies participating to H2020 cybersecurity projects, the weight of the different countries is quite similar.

3.3. Patent Analysis

Figure 35 provides the picture of the patents in the cybersecurity sector. As it possible to see, the patent filling is dominated by China, followed by US, while the EU is not in a prominent position.

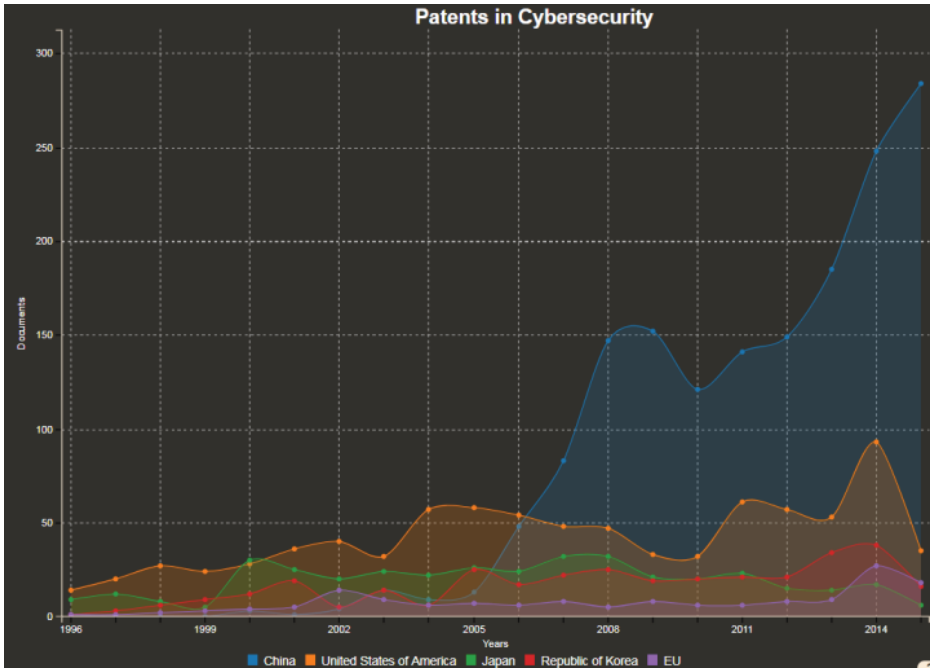


Figure 35. Patents in Cybersecurity per country (Europe = pink)

A more detailed analysis (still under validation), shows that the number of patents in average filled by a European entity on cybersecurity is around the 5%, with the exception of cryptology (21%).

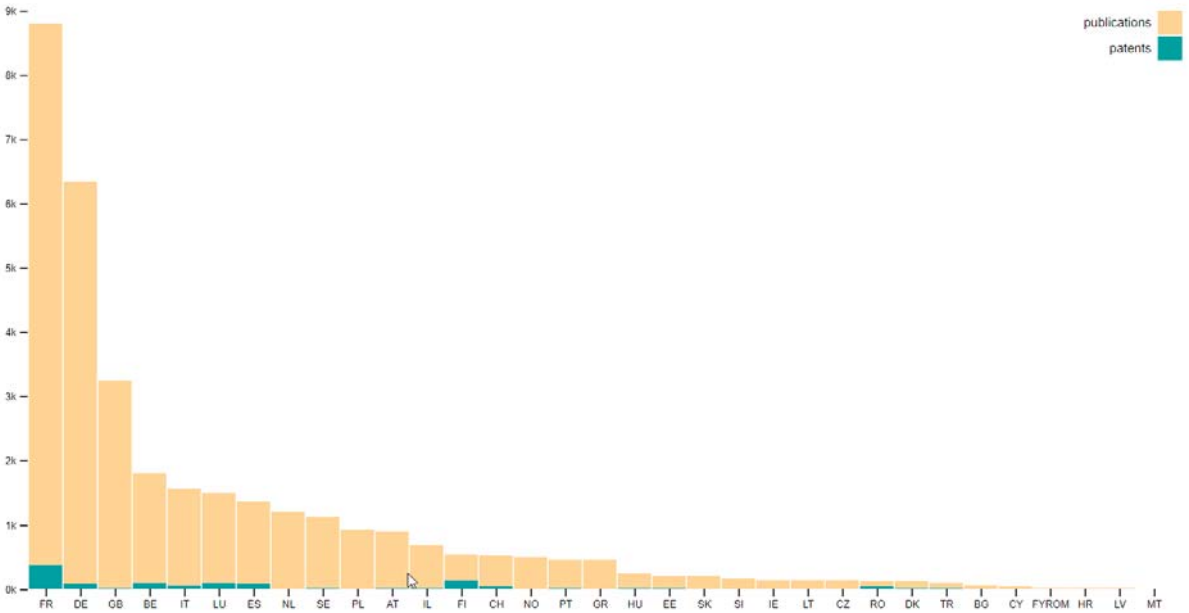


Figure 36. Cybersecurity Publications/Patent ratio per country

Considering the ratio between scientific publications and patents, it seems evident how to the relatively high scientific production does not automatically correspond an equal “innovation” push. There are several reasons that might explain this phenomenon:

1. The patent filling is a costly and complex process
2. The collaboration between industry and academies is little, or “consultancy oriented” (i.e. one-shot collaborations without a multi-annual collaboration and development plan)
3. The patent analysis is not able to capture completely the innovation chain

The last point is certainly true for what concerns ICT and cybersecurity as patents analysis does not allow to capture for example the phenomenon of software development and licensing, for which unfortunately, is not easy to provide a projection. However, even considering the fact that a relevant element is missing in the picture, still is true that other countries patent much more in cybersecurity than Europe.

4. Conclusions

Between the end of 2017 and the first months of 2018, the European Commission Joint Research Centre conducted a study taking account of the input of more than 660 cybersecurity centres from across the EU, to map the European cyber-security research competencies, strengthens and weaknesses.

The findings emerging from this multi-dimensional analysis are summarised briefly in the following paragraphs.

The analysis put in evidence that, in term of scientific production, Europe all together is the second most relevant cyber-security actor in the global research arena (after the USA). The same relevance however, is not reflected in the patenting domain. As normally patenting is associated to industrial activities, this evidence could be read as a **weakness** in the capacity of **establishing (long-term) collaboration between industry and academy,** which could be translated in the production of patents. However, it is worth noting that patents cover only one aspect of the cybersecurity value chain with software licensing occupying the other half of the moon. Unfortunately, no data is now available to estimate the size and "value" of licensing or other software business models based on open source software solutions.

In this context, the H2020 program has surely contributed to strengthening the relations between industry and academia; however, the analysis of the participants to H2020 calls related to cybersecurity shows that only few institutions proved to be equally capable to successfully and continuously access to the H2020 funds. This phenomenon contributed to create a sort of polarisation of the cybersecurity research around few institutions in a small number of member states, while other member states benefit more from national funding programmes with limited international collaborations. This trend finds confirmation also from data collected through the survey (involving as said before, more than 600 EU cyber-security research institutes).

Looking at the answers of the mentioned survey related to the domains covered by the research centres in Europe, it emerges that in the Union there are competencies **in all the domains** identified in the EU Cybersecurity Taxonomy, however this consideration needs to be carefully weighted.

The analysis of the research subdomains in fact shows that even in domains where the majority of the responders declared to have a stake (e.g. cryptography), the **real coverage of the subdomains is heavily jeopardised** with the majority of the centres active in the reality only in a **minor number of sub-fields**. This results in having several relevant sub-domains poorly supported by the research community, or supported only by a limited number of centres (post-quantum and quantum cryptography, cybercrime research, trust and cybersecurity in AI etc.) (see Table 1). This confirms a trend emerged in the scientific literature analysis and means that EU full coverage of the cybersecurity domains is far from being complete.

Most explored Subdomains	Less explored Subdomains
• Protocols and frameworks for access control (authentication and authorization)	• Self-healing systems
• Security testing and validationAttack modelling and countermeasures	• Transparent security
• Standards for Information Security	• Optical and electronic document security
• Vulnerability discovery and penetration testing	• Trust and reputation of social and mainstream media
• Identity management models; (e.g. PKI; RFID; SSO; etc.)	• Trust in decision making algorithms
• Threats and vulnerabilities modelling	• Legal aspect of certification
• Network layer attacks and mitigation techniques	• Quantum cryptology
• Privacy by design and Privacy Enhancing Technologies (PET)Security principles;	• Post-Quantum
	• Trusted computing
	• Information flow modelling and its application to confidentiality policies
	• Formal Verification of security assurance
	• Digital forensics, Cybercrime prosecution and law enforcement
	• Attacker profiling

Table 1. Most and least explored subdomains.

At country level, the survey put in evidence that all the MS have cybersecurity capabilities. However their capacity to impact on the scientific and technological production is heterogeneous with the **most influential institutions concentrated in few MS** (trend confirmed by the H2020 analysis). The coverage of subdomains at MS level is as well heterogeneous, probably due to a lack of coordination among national funding schemes and priorities.

The analysis of the sectors of application of cybersecurity research shows again a heterogeneous landscape at MS level, with some sectors (e.g. Energy, Space, Defense, Transport) **strongly developed in a few countries, and poorly developed in all the others.**

A possible interpretation of this trend is related to t**he cost of the infrastructures needed to conduct "on-field" research in these sectors,** which can be sustained only by a few big countries. This finding seems to find confirmation when looking at the technological applications covered by research in cyber-security, with those requiring the availability of costly facilities deeply explored only by a limited number of institutions in few countries.

In term of work-force (i.e. number of researchers), the survey does not provide a clear view: only 1/3 of the responders provided information on full time equivalent (FTE) working on cybersecurity research, and in several cases the numbers provided does not seem to be realistic (a probable misinterpretation of the related question). Further investigation will be required on this particular point.

In general, the full picture provided by this analysis shows a European cybersecurity research community vibrant, productive and recognised at global level, which however has often **difficulties in reaching the critical mass to truly make the difference, lacks of coordination in synergic domains and which is not always able to tightly connect with the industry.**

These last considerations call for the definition of new measures to:

- Strengthening and enlarging the collaboration of cyber-security research organisations across Member States;
- Streamline and stabilise the R&D cooperation between industry and academy;
- Better coordinate research funding across the Union;
- Co-design of research plans between funding bodies and recipients;
- Support the sharing of highly expensive infrastructures (in an Open Laboratory initiative fashion).

Annex I – Cybersecurity Survey

In order to keep this report self-contained in this annex the complete list of the survey questions is presented as shown to the participants.

Survey indexing the European cybersecurity centres of expertise

Fields marked with * are mandatory.

Are you a center of excellence in the field of cybersecurity?

Register before 15 February 2018 !

European Commission

Thanks to the centres that have self-registered by the deadline of 15 February. We will start work on a preliminary mapping based on those inputs.
However, due to the huge response received we have decided to leave the tool open a few more weeks and allow centers to self-register until 8 March.

****

Context: It is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy. To achieve that the EU needs to make a better use of its research and innovation capacities spread across the EU.

In its September 2017 Joint Communication *"Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"* the European Commission announced the intention to support the creation of a network of cybersecurity competence centres to stimulate the development and deployment of technology in cybersecurity.

As a first step in this direction, the European Commission is conducting a mapping of the existing centres of expertise in the field of cybersecurity (e.g. university department, research centre, etc). The results of this mapping will be translated into a **"Cybersecurity Atlas"** (an index of existing EU cybersecurity Centres) that will be made publicly available. This Atlas aims at becoming a valuable tool and a reference for the cybersecurity community to look for potential partners and pool resources.

Scope of the Survey: The Commission is calling on all cybersecurity competence centres across the EU, whether public or private, to register their organisations and share information about their work and expertise.

How to register your organisation: The registration tool allows your organisation to share information about your cybersecurity work, expertise as well as your contact details.

Filling in the survey should take between 20 minutes and one hour depending on the level of details you wish to share. The registration tool will be **open until 15 February 2018.** We thank you for your cooperation! Please do not hesitate to share information about the registration tool with your partners and any other relevant stakeholders!

For the purpose of filling this survey, you can refer to the following **Glossary of terms:**
Glossary.docx

Privacy Statement
privacy_statement.pdf

I General Information

*Institution name in national language:

Provide all the names in case of multiple official national languages.

*Institution name in English:

*Department or organizational unit:

*Address:

*Country

*Website:

*Cybersecurity Research Entity type:

- Higher Education Department (e.g. University department / Academy / Institute)
- Research Organisation
- Research Agency
- Laboratory
- Academic Group
- Association
- Other

Please specify:

*Legal Status

- Public
- Private
- Public Private Partnership
- Other

Please specify:

*Funding:

(Please check all that apply)

- National programmes / Government programmes
- EU
- International programmes
- Private
- Own Commercial Activity (e.g. Patents/Services)

Please detail the **Full Time Equivalent** of your employees (only numbers):

Full-time equivalent (FTE) is a unit that indicates the workload of an employed person (or student). An FTE of 1.0 is equivalent to a full-time worker, while an FTE of 0.5 signals half of a full work load (part time).

Full Time Equivalent Senior Researchers / Post Docs:

Full Time Equivalent Junior Researchers / Ph.D. students:

Full Time Equivalent Administrative Officials / Support Staff:

Management Contact details

*First Name:

*Family Name:

*Position (e.g. Director, Chair person):

*e-mail:
@

*General contact e-mail:
(e.g. e-mail address for your department)
@

II Cybersecurity Expertise

Please select the areas of expertise for each cybersecurity domain listed below. If the expertise is focused on a particular set of sectors, applications and technologies please select them accordingly in the relevant section. Please use the glossary for terminology.

	I have expertise in this domain.	I don't.
*Assurance, Audit, and Certification	◉	○
*Cryptology	◉	○
*Data Security and Privacy	◉	○
*Education and Training	◉	○
*Operational Incident Handling and Digital Forensics	◉	○
*Human Aspects	◉	○
*Identity and Access Management (IAM)	◉	○
*Security Management and Governance	◉	○
*Network and Distributed Systems	◉	○
*Software and Hardware Security Engineering	◉	○
*Security Measurements	◉	○
*Technology and Legal Aspects	◉	○
*Theoretical Foundations of Security Analysis and Design	◉	○
*Trust Management, Assurance, and Accountability	◉	○

Assurance, Audit, and Certification

Assurance, Audit, and Certification Subdomains
(please check all that apply)

- [ ] Assurance
- [ ] Audit
- [ ] Assessment
- [ ] Certification
- [ ] Protection Profile
- [ ] Security Target
- [ ] Other (please specify below)

Briefly describe your core competencies in this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Cryptology

Cryptology subdomains
(please check all that apply)

- [ ] Digital signatures
- [ ] Asymmetric cryptography and cryptanalysis
- [ ] Symmetric cryptography and cryptanalysis
- [ ] Hash functions
- [ ] Key management
- [ ] Message authentication
- [ ] Random number generation
- [ ] Cryptanalysis methodologies, techniques and tools
- [ ] Quantum cryptology
- [ ] Post-quantum cryptology
- [ ] Mathematical foundations of cryptography
- [x] Other (please specify below)

In case your area of expertise in this domain includes additional subdomains not listed above please specify:

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Data Security and Privacy

Data Security and Privacy Subdomains
(please check all that apply)

- ☐ Privacy requirements for data management systems
- ☐ Design, implementation, and operation of data management systems that include security and privacy functions
- ☐ Pseudonymity
- ☐ Unlinkability
- ☐ Privacy by design and Privacy Enhancing Technologies (PET)
- ☐ Digital Rights Management (DRM)
- ☐ Data usage control
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Education and Training

Education and Training Subdomains
(please check all that apply)

- ☐ Cybersecurity education
- ☐ Cybersecurity aware culture
- ☐ Cybersecurity simulation platforms
- ☐ Cybersecurity exercises
- ☐ Cybersecurity ranges
- ☐ Cybersecurity education methodology
- ☐ Cybersecurity vocational training
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Operational Incident Handling and Digital Forensics

Operational Incident Handling and Digital Forensics Subdomains
(please check all that apply)

- ☐ Theories, techniques and tools for the identification, collection, acquisition and preservation of digital evidence
- ☐ Digital forensic processes and workflow models
- ☐ Digital forensic case studies
- ☐ Legal, ethical and policy issues related to digital forensics
- ☐ Incident forecasting (intelligence based)
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Human Aspects

Human Aspects Subdomains
(please check all that apply)

- [ ] Accessibility
- [ ] Usability
- [ ] Social engineering and other human-related risks
- [ ] Socio-technical security
- [ ] Human errors
- [ ] Enhancing risk perception
- [ ] Psychological models
- [ ] User acceptance of security policies and technologies
- [ ] Automating security functionality
- [ ] Non-intrusive security
- [ ] Individual, organizational, and group information privacy concerns and behaviours
- [ ] Motivators and inhibitors of insider misuse
- [ ] Impacts of standards, policies, compliance requirements
- [ ] Organizational governance for information assurance
- [ ] Privacy attitudes and practices
- [ ] Computer ethics and security
- [ ] Transparent security
- [ ] Attacker profiling
- [ ] Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Identity and Access Management (IAM)

Identity and Access Management (IAM) Subdomains
(please check all that apply)

- ☐ Identity management models, frameworks, applications, technologies, and tools (e.g. PKI, RFID, SSO, etc.)
- ☐ Protocols and frameworks for access control (authentication and authorization)
- ☐ Identity management quality assurance
- ☐ eIDAS (electronic IDentification, Authentication and trust Services)
- ☐ Optical and electronic document security
- ☐ Legal aspects of identity management
- ☐ Law enforcement and identity management
- ☐ Biometric methods, technologies and tools
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Security Management and Governance

Security Management and Governance Subdomains
(please check all that apply)

- ☐ Risk management
- ☐ Continuous monitoring
- ☐ Threats and vulnerabilities modelling
- ☐ Attack modelling and countermeasures
- ☐ Managerial aspects concerning information security
- ☐ Assessment of information security effectiveness and degrees of control
- ☐ Identification of the impact of hardware and software changes on the management of Information Security
- ☐ Standards for Information Security
- ☐ Incident management and disaster recovery
- ☐ Reporting (e.g. disaster recovery and business continuity)
- ☐ Theoretical and empirical analyses of information security behaviour
- ☐ Adoption, use, and continuance of information security technologies and policies
- ☐ Compliance with information security and privacy policies, procedures, and regulations
- ☐ Vetting for security staff and employees.
- ☐ Economic aspects of the cybersecurity ecosystem
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Network and Distributed Systems

Network and Distributed Systems Subdomains
(please check all that apply)

- [ ] Security principles, methods, and technologies to networking
- [ ] Security principles, methods, and technologies in distributed systems
- [ ] Managerial, procedural and technical aspects of network security
- [ ] Requirements for network security
- [ ] Telecommunications network security
- [ ] Protocols and frameworks for secure distributed computing
- [ ] Network layer attacks and mitigation techniques
- [ ] Network attack propagation analysis
- [ ] Distributed systems security analysis and simulation
- [ ] Distributed consensus techniques
- [ ] Fault tolerant models
- [ ] Secure distributed computations
- [ ] Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Software and Hardware Security Engineering

Software and Hardware Security Engineering Subdomains
(please check all that apply)

- ☐ Security requirements engineering with emphasis on identity, privacy, accountability, and trust
- ☐ Security and risk analysis of components compositions
- ☐ Secure software architectures and design
- ☐ Security design patterns
- ☐ Secure programming principles and best practices
- ☐ Security support in programming environments
- ☐ Security documentation
- ☐ Refinement and verification of security management policy models
- ☐ Runtime security verification and enforcement
- ☐ Continuous monitoring
- ☐ Security testing and validation
- ☐ Vulnerability discovery and penetration testing
- ☐ Quantitative security for assurance
- ☐ Intrusion detection and honeypots
- ☐ Malware analysis
- ☐ Model-driven security and domain-specific modelling languages
- ☐ Self-healing systems
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Security Measurements

Security Measurements Subdomains
(please check all that apply)

- [ ] Security analytics
- [ ] Security metrics
- [ ] Validation and comparison frameworks for security metrics
- [ ] Measurement and assessment of security levels
- [ ] Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Technology and Legal Aspects

Technology and Legal Aspects Subdomains
(please check all that apply)

- ☐ Cybercrime prosecution and law enforcement
- ☐ Cybersecurity and ethics
- ☐ Intellectual property rights
- ☐ Cybersecurity regulation analysis and design
- ☐ Investigations of computer crime (cybercrime) and security violations
- ☐ Legal, societal, and ethical issues in information security
- ☐ Legal aspect of certification
- ☐ Social media (e.g. fake news).
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Theoretical Foundations of Security Analysis and Design

Theoretical Foundations of Security Analysis and Design Subdomains
(please check all that apply)

- ☐ Formal specification and verification of the various aspects of security, confidentiality, integrity, authentication and availability
- ☐ Formal techniques for the analysis, verification and auditing of software and hardware
- ☐ Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis
- ☐ New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications
- ☐ Formal Verification of security assurance
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

Trust Management, Assurance, and Accountability

Trust Management, Assurance, and Accountability Subdomains
(please check all that apply)

- ☐ Semantics and models for security, accountability, privacy, and trust
- ☐ Trust management architectures, mechanisms and policies
- ☐ Trust and privacy
- ☐ Identity and trust management
- ☐ Trust in securing digital as well as physical assets
- ☐ Trust in decision making algorithms
- ☐ Trust and reputation of social and mainstream media
- ☐ Social and legal aspects of trust
- ☐ Reputation models
- ☐ Trusted computing
- ☐ Other (please specify below)

Briefly describe your core competencies on this domain:

List the key researchers or area leaders for this domain:

What is your total number of publications in this domain during the last 5 years:
(please enter a number, no text)

What is your total number of patents in this domain during the last 5 years:
(please enter a number, no text)

III Sectors and Applications

Check the Sectors, Applications and Technologies you are working on:

Sectors
(please check all that apply)

- ☐ Defense
- ☐ Digital Infrastructure
- ☐ Energy / Nuclear
- ☐ Financial Services, banking, financial market infrastructure, insurances
- ☐ Government
- ☐ Health
- ☐ Maritime
- ☐ Audiovisual and media
- ☐ Tourism
- ☐ Transportation
- ☐ Space
- ☐ Smart ecosystems
- ☐ Supply chain
- ☑ Other

In case your area of expertise in this domain includes additional sectors not listed above please specify:

Applications and Technologies
(please check all that apply)

- ☐ Artificial intelligence
- ☐ Big Data
- ☐ Blockchain and Distributed Ledger Technology (DLT)
- ☐ Cloud and Virtualisation
- ☐ Critical Infrastructure
- ☐ Cyber Defense
- ☐ Dual Use Technologies
- ☐ Embedded Systems
- ☐ Hardware technology (RFID, chips, sensors, routers, etc.)
- ☐ High-performance computing (HPC)
- ☐ Human Machine Interface (HMI)
- ☐ Industrial Control Systems
- ☐ Industry 4.0
- ☐ Information Systems
- ☐ Internet of Things
- ☐ Mobile Devices
- ☐ Operating Systems
- ☐ Pervasive Systems
- ☐ Quantum Technologies
- ☐ Robotics
- ☐ Satellite applications
- ☐ Supply Chain
- ☐ Vehicular Systems
- ☑ Other

In case your area of expertise in this domain includes additional applications and technologies not listed above please specify:

IV International Collaborations or Joint Programs

*Please enter the **Numbers** of completed / ongoing international collaborations / joint programs in the **last 5 years**:*

EU cybersecurity research projects:

National cybersecurity research projects:

Cybersecurity patents:

Agreements / contracts with industries:

Agreements / contracts with Governments:

Memorandums of Understanding with other organisations:

Confirmation and Agreement

Please add any comment(s) you feel would be useful in reading your input (optional):

Please upload any relevant supporting document(s) (optional)

The maximum file size is 1 MB

Select file to upload

*I agree that the information provided can be made public by the European Commission

*I declare that all the above is correct

Thank you for your contribution!

Submit

List of figures

Figure 1. Entity type, legal status, and funding types. 6

Figure 2. Cybersecurity domains. 7

Figure 3. Cryptology subdomains. 8

Figure 4. Sectors, applications, and technologies. 9

Figure 5. Geographical distribution of number of survey participants per country with a color legend indicating with darker blue color countries with a higher number. 10

Figure 6. Number of survey participants per country. Non-EU participants are highlighted in in grey. 11

Figure 7. Distribution of participants according to their entity type. 12

Figure 8. Distribution of entity types per country. 12

Figure 9. Distribution of participants according to their legal status. 12

Figure 10. Distribution of entities per country according to their legal status. 13

Figure 11. Distribution of participants according to their expertise in the cybersecurity domains. 14

Figure 12. Distribution of domains per country using stacked columns showing total of replies per country and partition per domain. 14

Figure 13. Distribution of participants according to their expertise in the cybersecurity subdomains, first half. 16

Figure 14. Distribution of participants according to their expertise in the cybersecurity subdomains, second half. 17

Figure 15. Distribution of funding sources. 18

Figure 16. Distribution of funding sources per country. 18

Figure 17. Overall distribution of FTE declared to be working on cybersecurity be all survey participants. 19

Figure 18. Distribution of FTE working on cybersecurity per country. 19

Figure 19. Geographical distribution of FTE working per country showing number of thousands (k) FTE with a color legend indicating with darker blue color countries with a higher number. 20

Figure 20. Total number of declared publications. 21

Figure 21. Number of publications reported for each cybersecurity domain. 21

Figure 22. Geographical distribution of total number of publications per country showing number of thousands (k) publications with a color legend indicating with darker blue color countries with a higher number. 22

Figure 23. Number of publications per country. 23

Figure 24. Number of publications for each cybersecurity domain per country. 23

Figure 25. Overall distribution of sectors. 24

Figure 26. Distribution of sectors per country. 24

Figure 27. Overall distribution of applications and technologies. 25

Figure 28. Distribution of applications and technologies per country. 25

Figure 29. Overall distribution of number of international collaborations or joint programs declared by survey participants. 26

Figure 30. Distribution of number of international collaborations or joint programs declared by survey participants for each country 26

Figure 31. Distribution of participants according to their legal status after manual correction. 27

Figure 32. Scientific publications in Cybersecurity per country (Europe = orange). 28

Figure 33. Size of node = Country share of scientific publications in Cybersecurity (size of nodes = number project, edge between nodes = project(s) in common, colours identify communities of countries collaborating more often together) 29

Figure 34. Participants in H2020 Cyber-Security related projects (academic partners). 30

Figure 35. Patents in Cybersecurity per country (Europe = pink) 31

Figure 36. Cybersecurity Publications/Patent ratio per country 31

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc


@EU_ScienceHub


EU Science Hub - Joint Research Centre


Joint Research Centre


EU Science Hub

doi: 10.2760/42369

ISBN 978-92-79-92954-0

EUROPEAN
COMMISSION

Brussels, 12.9.2018
SWD(2018) 403 final

PART 4/4

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

European Commission

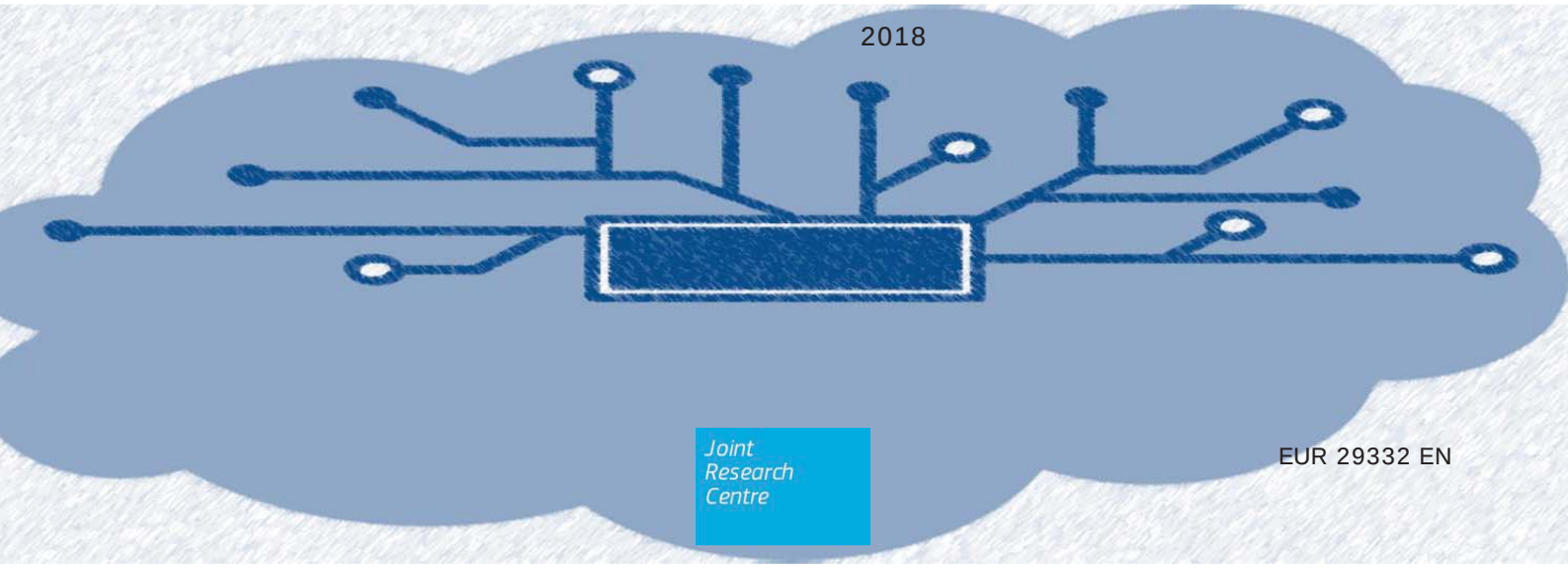
JRC TECHNICAL REPORTS

European Cybersecurity Centres of Expertise Map

Definitions and Taxonomy

NAI-FOVINO, I.
NEISSE, R.
LAZARI, A.
RUZZANTE, G.
POLEMI, N.
FIGWER, M.

2018



Joint Research Centre

EUR 29332 EN

JRC Science Hub
https://ec.europa.eu/jrc

EUR 29332 EN

JRC 111441

PDF ISBN 978-92-79-92956-4 ISSN 1831-9424 doi: 10.2760/622400

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: NAI-FOVINO, I.; NEISSE, R.;'LAZARI, A.; RUZZANTE, G.; POLEMI, N.; FIGWER, M. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. EUR 29332 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-92956-4, doi: 10.2760/622400, JRC111441.

Contents

Abstract ..... **Error! Bookmark not defined.**

1 Introduction ..... **Error! Bookmark not defined.**

2 Methodology and Reference Sources analysis ..... **Error! Bookmark not defined.**

2.1 Methodology ..... **Error! Bookmark not defined.**

2.2 Reference Sources and State of the Art..... **Error! Bookmark not defined.**

2.2.1 Existing cybersecurity clustering approaches**Error! Bookmark not defined.**

2.2.1.1 Cyberwatching..... **Error! Bookmark not defined.**

2.2.1.2 ACM Classification System..... **Error! Bookmark not defined.**

2.2.1.3 NIST CSRC Taxonomy ..... **Error! Bookmark not defined.**

2.2.1.4 IEEE Taxonomy ..... **Error! Bookmark not defined.**

2.2.1.5 ETSI TC-Cyber working group domains **Error! Bookmark not defined.**

2.2.1.6 IFIP TC11 Working Groups taxonomy... **Error! Bookmark not defined.**

2.2.1.7 IT-baseline protection catalog (IT-Grundschutz) ..**Error! Bookmark not defined.**

2.2.2 International Standards and Reference documents ....**Error! Bookmark not defined.**

2.2.2.1 ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27005 ..**Error! Bookmark not defined.**

2.2.2.2 ISA 62443 ..... **Error! Bookmark not defined.**

2.2.2.3 ISO/IEC 15408 (Common Criteria) ..... **Error! Bookmark not defined.**

2.2.2.4 NIST SP 800..... **Error! Bookmark not defined.**

2.2.3 International Working Groups and Organisations .....**Error! Bookmark not defined.**

2.2.4 Regulations and Policy Documents..... **Error! Bookmark not defined.**

2.2.5 Cybersecurity Market Studies and Observatory Initiatives .**Error! Bookmark not defined.**

2.2.6 General Considerations on the analysed sources.....**Error! Bookmark not defined.**

3 A Holistic Taxonomy for Cybersecurity Research Domains .....**Error! Bookmark not defined.**

3.1 Cybersecurity Domains..... **Error! Bookmark not defined.**

3.1.1 Assurance, Audit, and Certification ..... **Error! Bookmark not defined.**

3.1.2 Cryptology (Cryptography and Cryptanalysis) .....**Error! Bookmark not defined.**

3.1.3 Data Security and Privacy ..... **Error! Bookmark not defined.**

3.1.4 Education and Training ..... **Error! Bookmark not defined.**

3.1.5 Operational Incident Handling and Digital Forensics ...**Error! Bookmark not defined.**

3.1.6 Human Aspects ..... **Error! Bookmark not defined.**
3.1.7 Identity and Access Management (IAM) ..... **Error! Bookmark not defined.**
3.1.8 Security Management and Governance ..... **Error! Bookmark not defined.**
3.1.9 Network and Distributed Systems..... **Error! Bookmark not defined.**
3.1.10 Software and Hardware Security Engineering.....**Error! Bookmark not defined.**
3.1.11 Security Measurements ..... **Error! Bookmark not defined.**
3.1.12 Legal Aspects ..... **Error! Bookmark not defined.**
3.1.13 Theoretical Foundations ..... **Error! Bookmark not defined.**
3.1.14 Trust Management, Assurance, and Accountability.....**Error! Bookmark not defined.**
3.2 Sectorial Dimensions..... **Error! Bookmark not defined.**
3.2.1 Audiovisual and media..... **Error! Bookmark not defined.**
3.2.2 Defence..... **Error! Bookmark not defined.**
3.2.3 Digital Infrastructure ..... **Error! Bookmark not defined.**
3.2.4 Energy ..... **Error! Bookmark not defined.**
3.2.5 Financial..... **Error! Bookmark not defined.**
3.2.6 Government and public authorities ..... **Error! Bookmark not defined.**
3.2.7 Health ..... **Error! Bookmark not defined.**
3.2.8 Maritime..... **Error! Bookmark not defined.**
3.2.9 Nuclear ..... **Error! Bookmark not defined.**
3.2.10 Public Safety ..... **Error! Bookmark not defined.**
3.2.11 Tourism..... **Error! Bookmark not defined.**
3.2.12 Transportation..... **Error! Bookmark not defined.**
3.2.13 Smart Ecosystems ..... **Error! Bookmark not defined.**
3.2.14 Space ..... **Error! Bookmark not defined.**
3.2.15 Supply Chain..... **Error! Bookmark not defined.**
3.3 Applications and Technologies Dimension..... **Error! Bookmark not defined.**
4 Final Remarks..... **Error! Bookmark not defined.**
Annex 1 –Glossary of terms..... **Error! Bookmark not defined.**
List of figures ..... **Error! Bookmark not defined.**

Abstract

The Commission made a commitment in the Communication adopted in September to launch a pilot phase under Horizon 2020 to help bring national cybersecurity centres together into a network. In this context, the goal of this document is that of aligning the cybersecurity terminologies, definitions and domains into a coherent and comprehensive taxonomy to facilitate the categorisation of EU cybersecurity competencies.

1 Introduction

The Commission made a commitment in the Communication adopted in September to launch a pilot phase under Horizon 2020 to help bring national cybersecurity centres together into a network. The first step of this ambitious initiative is the clear definition of the cybersecurity context, its domains of application, research and knowledge. In this context, the goal of this document is that of aligning the cybersecurity terminologies, definitions and domains to allow the categorisation and mapping of existing EU cybersecurity centres (e.g. research organisations, laboratories, associations, academic institutions, groups, operational centres, etc.) according to their cybersecurity expertise in specific domains.

For the purpose of this document **cybersecurity** is considered an interdisciplinary domain. This starting point finds support in the Cybersecurity Report issued by the High Level Advisory Group of the EC Scientific Advice Mechanism in March 2017, where it is stated clearly that:

> "*cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments and the pace of technical change and innovation. In short, cybersecurity is much more than a science*".

This definition implies that there is not available today a globally accepted and standardised definition of cybersecurity and a clear identification of its domain of development and of application. In this report, after an initial reflection on the different dimensions of the cybersecurity domain, and using as sources some of the most widely accepted standards, international working group classification systems, regulations, best-practices, and recommendations in the cybersecurity domain, a high level set of definitions and categorisation domains are proposed so that they:

- can be used by the EC cybersecurity initiatives;
- become a point of reference for the cybersecurity activities (research, industrial, marketing, operational, training, education) in the DSM by all sectors/industries (health, telecom, finance, transport, space, defence, banking etc.);
- can be used to index the cybersecurity research entities (e.g. research organisations/laboratories/ associations/academic institutions/groups, operational centres*/academies*) in Europe;
- *meet compliance* with international cybersecurity standards*;*
- *can be* sustainable, easily modifiable and extensible.

This report is organised as follows: Section 2.1 presents the methodology adopted to build the Cybersecurity taxonomy, illustrating each step. Section 2.2 presents instead the information sources used to build the taxonomy together with their analysis including a summary of the main concepts that emerged from the analysis. Section 3 presents in detail the proposed taxonomy. Annex 1 provides, based on international standards, definitions and terms of references for the concepts used in the taxonomy.

2 Methodology and Reference Sources analysis

This section presents the methodology that has been adopted to build the taxonomy presented in Section 3, the reference sources which have been taken into consideration (i.e. the state of the art in the domain), and the aggregation of the comparison analysis among these sources.
The details of each single reference source analysed are instead provided in Annex 1.

2.1 Methodology

Taxonomy is defined as "*the practice of classification of things or concepts, including the principles that underlie such classification*"[1].

One of things to bear in mind about taxonomies is that there is never one uniquely valid taxonomy for a given domain, but that taxonomy might be more representative and expressive than another in a given context.

The traditional approach to the definition of a taxonomy follows a number of well-defined steps (as showed in Figure 1):

(1) **Define subject scope**: this phase consists in the identification of the scope of the taxonomy (i.e. the purpose for which the taxonomy is created). In this case the scope as described in the introduction, is that of providing a clear definition of the cybersecurity context, its domains of application, research and knowledge to be used to be used to facilitate the establishment of a cybersecurity competence network;

(2) **Identify sources**: selection of sources that are widely recognised and adopted by the scientific and technological community. In this case they have been identified through desktop research taking into consideration standards, activities performed by existing international working groups and organisations, scientific literature (see Section 2.2);

(3) **Collect terms and concepts:** Each of the identified sources has been analysed to extrapolate:

   a. Relevant concepts and sub-domains;

   b. Terminology (i.e. the building blocks of every taxonomy);

(4) **Group similar concepts together:** concepts have then been clustered (see Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis

(5) **Add other term relationships and details**: to identify communalities and to simplify the structure of the taxonomy. The identified terms have instead been used to build a glossary using as definitions' source international standards (where available), or scientific references.

[1] http://km4ard.cta.int/2016/11/27/developing-a-taxonomy-for-agriculture-and-rural-development/

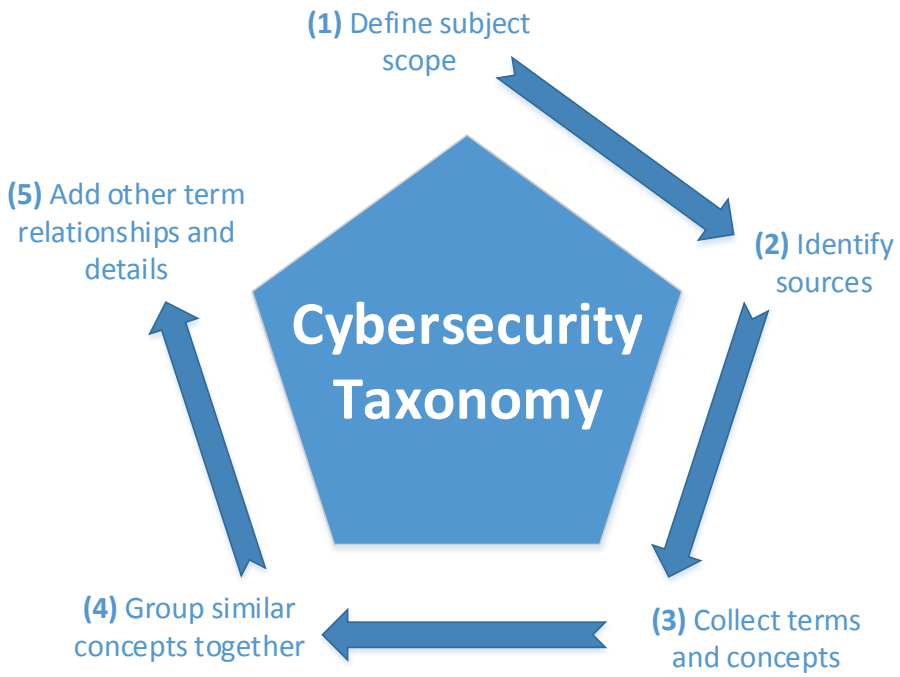


Figure 1. Cybersecurity taxonomy definition steps.

The resulting corpus of knowledge has been then structured in a three dimensional Taxonomy as described in Section 3 and validated against the few existing taxonomy covering at least a portion of the cybersecurity domain already identified among the sources.

2.2 Reference Sources and State of the Art

This section summarises steps (2) and (3) presented in section 2.1. It takes stock of existing concepts and terminologies to define a unifying, holistic and forward-looking cybersecurity taxonomy that takes into consideration at the same time:

- Existing cybersecurity clustering activities;
- International Standards and Reference documents;
- International Working Groups results/activities;
- Regulations and policy initiatives;
- Cybersecurity Market studies and Observatory initiatives.

In what follows, for each of the listed sources the state of the art is presented.

2.2.1 Existing cybersecurity clustering approaches

As already mentioned in the introduction, due to the heterogeneous nature of the cybersecurity domain, a uniquely accepted and consolidated taxonomy does not exist in the literature. Many organisations however defined their own taxonomy tailored for their own specific needs. The following subsections describe the most structured and comprehensive approaches identified in the literature.

2.2.1.1 Cyberwatching

The *European observatory of research and innovation in the field of cybersecurity and privacy* (Cyberwatching)[2] is an initiative falling under the *Coordination and Support Action* scheme aiming at "*defining and promoting a pragmatic approach to implement*

[2] https://www.cyberwatching.eu

and maintain an EU Observatory to monitor R&I initiatives on cybersecurity & privacy, throughout EU & Associated Countries".

To support its activities, Cyberwatching defined a taxonomy of cybersecurity composed by four vertical technical development areas, which are complemented by two horizontal service-based cross cutting cybersecurity clusters (see the following figure). Their goal is to use this taxonomy with a score system to cluster European Research and Innovation initiatives dealing with cybersecurity and privacy where entities can position themselves by assigning a value from 1 to 5 as to how important each area is to developments ongoing within each of their ongoing projects.

Figure 2. Vertical and horizontal cybersecurity development areas

Moreover, it created a catalogue of European Projects on cybersecurity organised according to two dimensions:

Characteristics	Vertical Markets
• Cloud security • Collaborative platform • Cyber security • Privacy • Big Data	• Digital Health • Energy • Engineering & manufacturing • Finance & insurance • ICT • Local & public administrations • National government agencies • Smart cities

Table 1. European Projects Catalogue dimensions

The areas identified by Cyberwatching are aligned with those identified by NIST (Section 2.2.1.3) and, partially, with those of ETSI (Section 2.2.1.5). The taxonomy proposed in this report is also in alignment with the areas defined by the EU Cyberwatching, however, additional horizontal dimensions are considered addressing the sector of actuation, and the target applications and technologies.

2.2.1.2 ACM Classification System

The Association for Computing Machinery (ACM) proposed a Computing Classification System (CCS)[3] that includes **Security and privacy** as a top generic area. The first version was created in 1998 and the latest version was updated on 2012. The purpose of the CCS is to classify publications submitted to ACM events and published in the ACM digital library, which is considered one of the main global sources of high quality peer-reviewed scientific publications. The following table summarizes the main categories and sub-categories for the Security and privacy top generic area:

[3] https://dl.acm.org/ccs/ccs.cfm

Cryptography • Key management • Public key (asymmetric) techniques: • Digital signatures • Public key encryption • Symmetric cryptography and hash functions • Block and stream ciphers • Hash functions and message authentication codes • Cryptanalysis and other attacks • Information-theoretic techniques • Mathematical foundations of cryptography	**Formal methods and theory of security** • Trust frameworks • Security requirements • Formal security models • Logic and verification	**Security services** • Authentication • Biometrics • Graphical / visual passwords • Multi-factor authentication • Access control • Pseudonymity, anonymity and untraceability • Privacy-preserving protocols • Digital rights management • Authorization
Intrusion/anomaly detection and malware mitigation • Malware and its mitigation • Intrusion detection systems • Artificial immune systems • Social engineering attacks • Spoofing attacks • Phishing	**Security in hardware** • Tamper-proof and tamper-resistant designs • Embedded systems security • Hardware security implementation • Hardware-based security protocols • Hardware attacks and countermeasures • Malicious design modifications • Side-channel analysis and countermeasures • Hardware reverse engineering	**Systems security** • Operating systems security • Mobile platform security • Trusted computing • Virtualization and security • Browser security • Distributed systems security • Information flow control • Denial-of-service attacks • Firewalls • Vulnerability management • Penetration testing • Vulnerability scanners • File system security
Network security • Security protocols • Web protocol security • Mobile and wireless security • Denial-of-service attacks • Firewalls	**Database and storage security** • Data anonymization and sanitization • Management and querying of encrypted data • Information accountability and usage control • Database activity monitoring	**Human and societal aspects of security and privacy** • Economics of security and privacy • Social aspects of security and privacy • Privacy protections • Usability in security and privacy
Software and application security • Software security engineering • Web application security • Social network security and privacy • Domain-specific security and privacy architectures • Software reverse engineering		

Table 2. ACM Classification System Categories

This taxonomy covers in an extensive way the traditional academic research sub-domains of cybersecurity, while it does not cover the more operational subdomains, such as cybercrime forensics, assurance, certification, auditing, standardisation and the legislative angle. Moreover, it does not capture sectorial specific competences.

2.2.1.3 NIST CSRC Taxonomy

NIST Computer Security Resource Centre (CSRC)[4], which is an important reference resource of NIST for what concerns cybersecurity, defined a comprehensive model for clustering cybersecurity knowledge. NIST adopts a multidimensional clustering approach based on six cross-cutting areas of classification:

- Security and privacy specific research domains;
- Technologies (where the research is performed);
- Applications (field of application of the knowledge);
- Laws and regulations;

[4] https://csrc.nist.gov/topics

- Type of activities;
- Business sectors.

Table 3 provides a view of the second-level classification taxonomy. As it is possible to see it covers explicitly some aspects not fully addressed by the others taxonomies, in particular for what concerns the application fields, the sectorial specific competencies, laws and regulations.

Security and Privacy	**Technologies**	**Applications**
cryptography	big data	cyber-physical systems
general security & privacy	biometrics	cybersecurity education
identity & access management	Basic Input/Output System	cybersecurity framework
privacy	cloud & virtualization	cybersecurity workforce
risk management	communications & wireless	forensics
security & behavior	databases	industrial control systems
security measurement	firewalls	Internet of Things
security programs & operations	firmware	small & medium business
Laws and Regulations	hardware	supply chain
executive documents	mobile	telework
laws	networks	voting
regulations	operating systems	**Sectors**
Activities and Products	personal computers	energy
annual reports	sensors	financial services
conferences & workshops	servers	healthcare
reference materials	smart cards	hospitality
standards development	software	manufacturing
	storage	public safety
		retail
		transportation

Table 3. Cybersecurity Topic Clustering (NIST Computer Security Resource Center)

While on a side this approach is very well structured, it is important to note how (a) it doesn't capture some peculiarities of the European landscape (e.g. in the Law and Regulation context, in the sectors identified etc.), and (b) the number of dimensions to take into considerations which is so large to risk to introduce a high fragmentation in clustering of competencies.

Nevertheless, this classification is, to the best of our knowledge, the most articulated and precise and was taken as one of the main starting points to elaborate in Section 3 the taxonomy fit for the purpose of this report.

2.2.1.4 IEEE Taxonomy

Following a similar approach as ACM, the Institute of Electrical and Electronics Engineers (IEEE) also proposes a taxonomy[5] with the same purpose, to categorize the publications of events that are made available through the IEEE Xplore Digital Library. The following list summarizes the main concepts and sub-categories of this taxonomy:

- **Access control**: Authorization, Capability-based security
- **Computer security:** Authentication, Computer crime, Computer hacking, Firewalls (computing), Identity management systems, Permission

[5] 2017 IEEE Taxonomy: https://www.ieee.org/documents/taxonomy_v101.pdf last access 06/12/2017

- **Cryptography:** Ciphers, Encryption, Public key, Quantum cryptography, Random number generation, Side-channel attacks;
- **Data security:** Cryptography, Message authentication; Digital signatures;
- **Information security**: Intrusion detection; Network security; Power system security; Reconnaissance; Security management;
- **Terrorism:** Bioterrorism, National security; Watermarking

Similarly to the ACM taxonomy, the IEEE taxonomy covers in general all the traditional technical academic (sub-)domains of cybersecurity, however, is significantly more concise and less comprehensive since little emphasis is put on relevant aspects such as privacy and data protection (covered here only by "data security", but limited to cryptographic methods), on sectorial applications and obviously on social and legal aspects. Standards, certification, economic aspects, law implication and cyber-crime are not clustered as well as sectorial specific competences. Nevertheless, this taxonomy, allows anyway to validate the taxonomy of NIST and complements it regarding some second level concepts.

2.2.1.5 ETSI TC-Cyber working group domains

The European Telecommunications Standards Institute (ETSI) established a technical committee[6] dedicated to the development of standards to increase privacy and security for organizations and citizens across Europe and worldwide. The TC covers a set of domains that can be taken as input in the definition of a taxonomy of cybersecurity taking into consideration industry interests (see Table 4).

Horizontal cybersecurity	Securing technologies and systems	Security tools and techniques
• Privacy by design • Security controls • Network and Information Security • Critical infrastructures • Information Security Indicators	• Mobile/Wireless systems (3G/4G, TETRA, DECT, RRS, RFID…) • IoT and Machine-to-Machine (M2M) • Network Functions Virtualisation • Intelligent Transport Systems, Maritime • Broadcasting	• Lawful Interception and Retained Data • Digital Signatures and trust service providers • Secure elements • Exchangeable CA/DRM solutions • Cryptography

Table 4. ETSI TC-Cyber working group domains

Moreover, ETSI presents an overview of the Global Cyber Security Ecosystem defining a short glossary of cybersecurity definitions, an analysis of the basic cybersecurity components, and an extensive survey of the main worldwide entities working on the field. There is no inventory of the respective actuation areas, only a list defined by entity type (e.g., standardization body, research institute, centres of excellence, forums, etc.).
For the purposes of a cybersecurity classification scheme the components are an important cross-cutting dimension that should be taken into consideration from a cybersecurity management perspective, for example, companies may specialize on protection, detection, or recovery after an incident (see **Error! Reference source not found.**).

[6] http://www.etsi.org/technologies-clusters/technologies/cyber-security

Figure 3. ETSI cross-cutting cybersecurity clusters

2.2.1.6 IFIP TC11 Working Groups taxonomy

The International Federation for Information Processing[7] (IFIP) is a non-governmental, non-profit umbrella organization for national societies working in the field of information processing. It was established in 1960 under the auspices of UNESCO as a result of the first World Computer Congress held in Paris in 1959. Among its Technical Committees (TC), of particular interest is TC11 on Security and Privacy Protection in Information Processing Systems[8].

The TC11 committee is organised in thematic working groups (see Figure 4). The structure and content of the thematic groups can be indeed considered as a sort of embryonic cybersecurity and privacy taxonomy (definitions and vocabulary are obviously missing as the structure of the TC was not meant to be considered as a real taxonomy).

[7] http://ifip.org/
[8] https://www.ifiptc11.org/

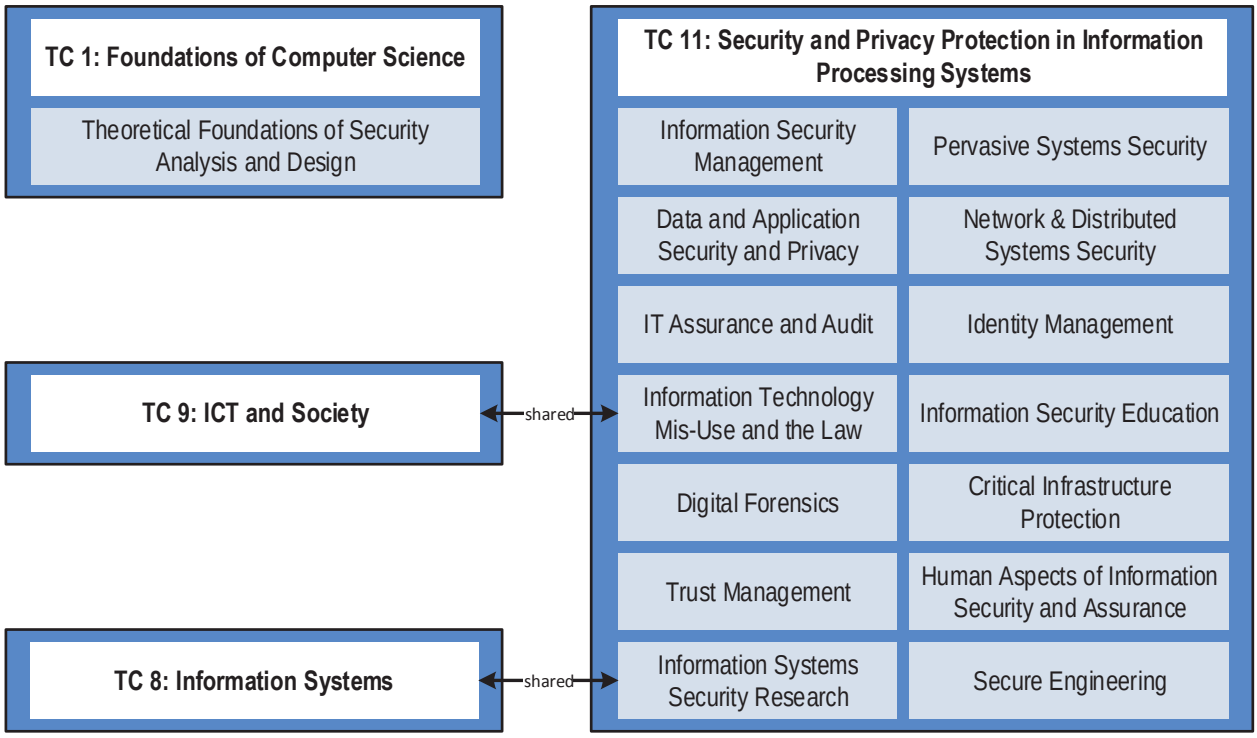


Figure 4. IFIP TC 11 Structure

In the following table a summary of the different field of application of the working groups is presented.

WG 1.7 - Theoretical Foundations of Security Analysis and Design • Formal definition and verification of the various aspects of security, confidentiality, integrity, authentication and availability; • New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their manifold applications (e.g., electronic commerce); • Information flow modelling and its application to the theory of confidentiality policies, composition of systems, and covert channel analysis; • Formal techniques for the analysis and verification of mobile code; • Formal analysis and design for prevention of Denial of Service (DoS).	**WG 11.1 Information Security Management** • Upper management awareness on information security • Managerial aspects concerning information security • Assessment of information security effectiveness and degree of control by managers; • Risk analysis • Identification of threats and vulnerabilities • Measurement and assessment of security levels in a company • Identification of the impact of hardware and software changes on the management of Information Security; • Technical aspects; • Standards for Information Security; • Disaster recovery.	**WG 11.2 Pervasive Systems Security** • Information security particularly related to pervasive systems

WG 11.3 Data and Application Security and Privacy • Statement of security and privacy requirements for data management systems; • Design, implementation, and operation of data management systems that include security and privacy functions; • Assurance that implemented data management systems meet their security and privacy requirements.	**WG 11.4 Network & Distributed Systems Security** • Management and technicians awareness in respect of the reliable and secure operation of the information networks; • Education and training in the application of security principles, methods, and technologies to networking; • Network aspect of information systems security; • Managerial, procedural and technical aspects of network security; • Requirements for network security; • Network oriented cybersecurity risk analysis; • Network security controls	**WG 11.5 IT Assurance and Audit** No detailed information was available about this working group.
WG 11.6 Identity Management • Identity management • Biometric technologies • National identity management	**WG 11.7 / 9.6 Information Technology Misuse and Law** No detailed information was available about this working group.	**WG 11.8 IT Security Education** • Education and training in information security. • Courses in information security at the university level; • Business educational training on information security modules • Collection, exchange and dissemination of information relating to information security courses conducted by private organizations for industry; • Collection and periodical dissemination of annotated bibliography of information security books, feature articles, reports, and other educational media.
WG 11.9 Digital Forensics • Theories, techniques and tools for extracting, analyzing and preserving digital evidence; • Network and cloud forensics; • Embedded device forensics; • Digital forensic processes and workflow models; • Digital forensic case studies; WG 11.9 Digital Forensics • Theories, techniques and tools for extracting, analyzing and preserving digital evidence; • Network and cloud forensics; • Embedded device forensics; • Digital forensic processes and workflow models; • Digital forensic case studies; • Legal, ethical and policy issues related to digital forensics.	**WG 11.10 Critical Infrastructure Protection** • Infrastructure vulnerabilities, threats and risks; • Security challenges, solutions and implementation issues; • Infrastructure sector interdependencies and security implications; • Risk analysis, risk assessment and impact assessment methodologies; • Modeling and simulation of critical infrastructures; • Legal, economic, policy and human factors issues related to critical infrastructure protection; • Secure information sharing; • Infrastructure protection case studies; • Distributed control systems/SCADA security; • Telecommunications network security;	**WG 11.11 Trust Management** • Semantics and models for security and trust; • Trust management architectures, mechanisms and policies; • Trust in e-commerce, e-service, e-government; • Trust and privacy; • Identity and trust management; • Trust in securing digital as well as physical assets; • Social and legal aspects of trust.

WG 11.12 Human Aspects of Information Security and Assurance	WG 11.13 / 8.11 Information Systems Security Research	WG 11.14 Secure Engineering
• Information security culture; • Awareness and education methods; • Enhancing risk perception; • Public understanding of security; • Usable security; • Psychological models of security software usage; • User acceptance of security policies and technologies; • User-friendly authentication methods; • Automating security functionality; • Non-intrusive security; • Assisting security administration; • Impacts of standards, policies, compliance requirements; • Organizational governance for information assurance; • Simplifying risk and threat assessment; • Understanding motivations for misuse; • Social engineering and other human-related risks; • Privacy attitudes and practices; • Computer ethics and security.	• Theoretical and empirical analyzes of information security behaviour; • Adoption, use, and continuance of information security technologies and policies; • Compliance with information security and privacy policies, procedures, and regulations; • Investigations of computer crime and security violations; • Motivators and inhibitors of employee computer crime; • Forensic analysis of security breaches and computer crimes; • Individual, organizational, and group information privacy concerns and behaviors; • Legal, societal, and ethical issues in information security; • investigations of information security behaviour (Neurosecurity).	• Security requirements engineering with emphasis on identity, privacy and trust: • Secure Service Architectures and Design: • Security support in programming environments • Service composition and adaptation: • Risk and Cost-aware Secure Service Development: • Security assurance for services: • Quantitative security for assurance

Table 5. IFIP WG 11 Research sub-groups

The organisation of the TC11 clearly cannot be considered a formal and complete taxonomy. It reflects existing groups of interest and research communities. This explains why it contains several redundancies and it results unbalanced in term of deepness. Nevertheless, it provides the most extensive collection of concepts and topics analysed in this report and it constitutes without doubts a good starting point for the definition of a general taxonomy of the cybersecurity domain.

2.2.1.7 IT-baseline protection catalog (IT-Grundschutz)

The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) proposed the IT Baseline Protection (IT-Grundschutz) methodology to support the identification and implementation of cybersecurity measurements in organizations. In addition to the methodology BSI also provides an extensive catalogue (IT-Grundschutz Catalogue) of threats and countermeasures including a glossary of terms.

This catalogue is organized considering the components, threats, and measures. The component catalogue is organized in the following layers: general aspects, infrastructure, IT systems, networks, and IT applications. Each component layer targets a specific group in the organization, for example, management, technicians, system administrators, users, network administrators, etc.

This classification and separation in target groups makes it easy to find the relevant information and guidance when using the catalogue. For the purposes of a cybersecurity classification scheme this layered structure is useful and is also reflected in the topics proposed by the NIST Computer Security Resource Center.

2.2.2 International Standards and Reference documents

Under this group goes all the standards and documents helping in building the basic building block of a taxonomy, i.e. the glossary of definitions. To make an example under this category fall all the ISO/IEC standards. (see the following subsections for a detailed list)

The following standards have been taken into consideration to build the taxonomy proposed in Section 3.

ISO/IEC 5127	ISO/IEC 25010	ISO/IEC 27033	ISO/IEC 15408 (Common Criteria)
ISO/IEC 9735	ISO/IEC 25237	ISO/IEC 27037	ISA 62443
ISO/IEC 10118	ISO/IEC 27000	ISO/IEC 28000	NIST SP 800
ISO/IEC 10181	ISO/IEC 27001	ISO/IEC 29100	NIST SP 800 55
ISO/IEC 11770	ISO/IEC 27002	ISO/IEC 29109-1	NISTIR 8105
ISO/IEC 11889	ISO/IEC 27004	ISO/TR 18307	ETSI:tr (cyber)
ISO/IEC 18033	ISO/IEC 27005	ISO/TR 11633-2	
ISO/IEC 23006-4	ISO/IEC 27019	ISO/TS 80004	

Table 6. List of Standards taken into consideration

Some of the listed international standards are strictly related with the cybersecurity realm. It is important however to underline that in general these standards have been conceived for some very specific certification or procedural task and not to describe or define the cybersecurity ecosystem. However, they can in any case be considered as an important reference source for cybersecurity vocabularies, glossaries and, in some case, very specific domains (e.g. information security management for what concerns ISO/IEC 27000, 27001, 27005).

The description of the content of all the mentioned standards is out of the scope of this report. The majority of them has been used to cover some specific vocabulary definition (see the glossary at the end of the report). A little subsection however has been used much more extensively, not only as source for the glossary, but also to identify specific concepts and domains of the taxonomy and for that reason in the following a more detailed description is provided.

2.2.2.1 ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27005

These standards provide the ground for the definition and implementation of an Information Security Management System (ISMS) with an architecture similar to several others ISO/IEC standards such as ISO/IEC 9000 and ISO/IEC 14000.

ISO/IEC 27000 provides definitions and vocabulary for the cybersecurity context, which can be used as one of the sources for the glossary of the categorisation presented in this report. ISO/IEC 27001 and ISO/IEC 27005 as they provide the description of a specific domain of the cybersecurity realm, the ISMS and the Cybersecurity Risk Assessment process which merit to be included in the set of knowledge clusters proposed in Section 3.

2.2.2.2 ISA 62443

The 62443 series of standards have been developed jointly by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS).

The goal in applying the 62443 series is to improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, including the procurement aspects. The 62443 series builds on established standards for the security of general purpose information technology systems (e.g., the ISO/IEC 27000 series), differentiating from the 27000 mainly for what concerns (a) some additional aspects as safety, health and environment (not present in ISO/IEC 27001 and ISO/IEC 27005), and (b) for some additional terms and definitions. Of interest for this report is in particular the ISA 62443-1-2 technical report containing a master glossary of terms and abbreviations used throughout the series.

2.2.2.3 ISO/IEC 15408 (Common Criteria)

Standard containing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation.
The standard is composed by three parts:

- **Part 1, Introduction and general model**: is the introduction to ISO/IEC 15408. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation;
- **Part 2, Security functional requirements**: establishes a set of functional components as a standard way of expressing the functional requirements for TOEs (Targets Of Evaluation);
- **Part 3, Security assurance requirements**: establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs.

Each part of the standard contains a catalogue of components (mostly functional) tackling different aspects of the cybersecurity functional and assurance requirements. However, as for the others standards analysed so far, this catalogue is instrumental to the specific scope of the Common Criteria, hence it is too specific to be taken as reference for a taxonomy of the cybersecurity knowledge.

2.2.2.4 NIST SP 800

NIST maintains a series of "Special Publications" (SP) on cybersecurity best practices related to cybersecurity. This collection of publications is extremely practical and each issue is devoted to a particular, technical domain (spanning from security guidelines to LTE, to cybersecurity education etc.).

Hence, for the purposes of this report, the NIST SP 800 is not very useful as it is too much specialised. However, the NIST Computer Security Resource Center, which is the reference resource of NIST for what concerns cybersecurity, defined a model for clustering cybersecurity knowledge extremely interesting and comprehensive, which can be taken as reference.

2.2.3 International Working Groups and Organisations

International working groups have been taken as additional sources for reference definitions, or, in some case to analyse the structure of the sub-working groups to extrapolate the related taxonomy. Here below a summarising list is provided[9].

- *Association for Computing Machinery (ACM)*: see Section 2.2.1.2
- *National Institute of Standards and Technology (NIST)*: see Section 2.2.1.3
- *Institute of Electrical and Electronics Engineers (IEEE)*: see Section 2.2.1.4
- *European Telecommunications Standards Institute (ETSI)*: see Section 2.2.1.5
- *International Federation for Information Processing (IFIP)*: see Section 2.2.1.6

The following sources have been taken into consideration as a source for the glossary on this report:

- Internet Engineering Task Force (IETF): Request for Comments (RFC) 4949[10] "Internet Security Glossary, Version 2" produced by the Network Working Group;
- Intel Threat Agent Library (TAL)[11] and Threat Agent Motivation[12];

[9] Contributions coming from ACM, NIST, IEEE, ETSI AND IFIP have been already described in the previous sub-sections, hence, to avoid information redundancy, in the following list the related entries will only point to the proper sub-section.
[10] https://tools.ietf.org/html/rfc4949
[11] https://communities.intel.com/docs/DOC-23853

- MACE Taxonomy, Adversary Types[13];
- CAPEC ATT&CK from Mitre[14];
- Cyber Kill Chain[15];

- *Open Web Application Security Project Foundation (OWASP)*: OWASP is a worldwide not-for-profit charitable organization focused on improving the security of software. The corpus of definitions available on the OWASP portal[16] has been taken into consideration to cover definition gaps in the glossary on this report.
- *Information Systems Audit and Control Association (ISACA)*: ISACA has been used as source of definitions and references for what concerns the information security governance aspects, in particular leveraging on the ISACA "*cybersecurity fundamentals glossary*"[17]
- *European Union Agency for Network and Information Security (ENISA)*: ENISA has a very active role in the European Cybersecurity ecosystem. Among its large portfolio of activities, is worth mentioning the release of cybersecurity related reports and studies. In particular, for the purposes of this report, have been taken into consideration as relevant sources
  - "Definition of Cybersecurity, Gaps and overlaps in standardisation", ENISA report, December 2015
  - "Review of Cyber Hygiene practices", ENISA report, December 2016
  - "An evaluation Framework for National Cyber Security Strategies", ENISA report, November 2014
  - "EP3R 2013 – Position Paper Task Forces on Terminology Definitions and Categorisation of Assets (TF-TDCA)", December 2013
  - "Recommended cryptographic measures - Securing personal data", ENISA report, November 2013

  Incident taxonomies collected by ENISA under the CSIRT initiative[18] have also been taken into consideration, as well as the ENISA and NIS WG3 cybersecurity education map.
- *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):* The NATO CCD COE is a multinational and interdisciplinary hub of cyber defence expertise. The Centre organises the world's largest and most complex international technical cyber defence exercise Locked Shields and the annual conference on cyber conflict, CyCon. Of particular interest for what concerns the definition of a cybersecurity taxonomy, is the International Cyber Developments Review (INCYDER) database. This interactive research tool focuses on the legal and policy documents adopted by international organisations active in cyber security. The collection of documents is periodically updated and supported by a comprehensive system of tags that enable filtering the content by specific sub-domains.

---

[12] https://lists.oasis-open.org/archives/cti/201607/msg00044/Intel_Corp_Threat_Agent_Motivations_Feb2015.pdf
[13] http://cradpdf.drdc-rddc.gc.ca/PDFS/unc218/p803340_A1b.pdf
[14] https://attack.mitre.org/mobile/index.php/Main_Page
[15] https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[16] https://www.owasp.org/index.php/Glossary accessed in November 2017
[17] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf accessed in November 2017
[18] https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies accessed in November 2017.

- *European Cyber Security Organisation (ECSO)*: it represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity.
    - In its Industry proposal[19] ECSO has elaborated an analysis of the following different class of market solutions/services:
        - Governance, vulnerability and cybersecurity management;
        - Identity and access management;
        - Data security;
        - Cloud Security;
        - Applications security;
        - Network systems security;
        - Hardware (device/endpoint) security;
        - Audit, planning and advisory services;
        - Management and operations services;
        - Managed Security Services (MSS);
        - Security training services.
    - The activities of ECSO are organised around 6 working groups:
        - WG1: Standardisation, certification, labelling and supply chain management
        - WG2: Market deployment, investments and international collaboration
        - WG3: Sectoral demand
        - WG4: Support to SMEs, coordination with countries (in particular East and Central EU) and regions
        - WG5: Education, awareness, training, exercises
        - WG6: Strategic Research and Innovation Agenda (SRIA)

      Of particular interest for the scope of this report are WG5 and WG6.

2.2.4 **Regulations and Policy Documents**

European Regulation and policy documents were considered as sources for legal definitions and to cover the gaps left by the vocabularies extracted from standards when dealing with non-technical definitions. Here below the list of the most relevant taken into consideration:

- 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 (NIS directive)
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)
- European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cybersecurity (2011/2284(INI)) (CIIP)
- COM(2017) 477 final 2017/0225 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity

[19] http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

- COM(2016) 705 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Space Strategy for Europe
- JOIN(2014) 9 final - JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL For an open and secure global maritime domain: elements for a European Union maritime security strategy
- JOIN(2016) 18 final JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response
- EU Cyber Defence Policy Framework [Consilium 15585/14] and Joint Communication on 'Cybersecurity
- Strategy of the European Union: An Open, Safe and Secure Cyberspace', February 2013 [JOIN(2013)1].

Several of these regulations and policy documents are related to specific sectors, and have been used to understand the position occupied by cybersecurity and privacy in a specific policy sector. However two of these policy documents (NIS and GDPR) can be considered overarching and cross-sectorial and have been used in the taxonomy presented in Section 3 as relevant sources to identify regulatory and sectorial sub-domains.

2.2.5 Cybersecurity Market Studies and Observatory Initiatives

Observatory initiatives and market studies have been used to capture taxonomy aspects related to the industry and business world.

- *PWC and LSEC Cybersecurity Industry Market Analysis study:* this study, analyses the European cybersecurity industry. Within the study data related to the EU industry is clustered according the following cybersecurity categories:
    - Anti-Malware;
    - Application Security;
    - Business Continuity;
    - Cyber Consultancy;
    - Cyber Insurance;
    - Encryption;
    - Identity and Access Control;
    - Infrastructure;
    - Mobile;
    - Outsourced/Managed Services;
    - Situational Awareness;
    - System Recovery.

  This list provides a good market oriented overview, which validates several of the key-domains already emerged in the analysis of the others sources. However it does not fully cover the research, regulatory and sectorial domains.
- *Security Research Map (SEREMA):* The purpose of the Security Research Map is to increase the visibility of security related research in Europe and to optimize the networking between research facilities, universities, public authorities, end users, suppliers of security solutions and operators of critical infrastructures. Serema contains the profiles of universities, research centres and companies that are

active in the field of security with the aim of creating a network among those that are interested in forming a consortium for H2020 or similar funding schemes. The database has been developed within the network of National Contact Points for Security in the 7th EU-Framework Programme (SEREN 2). The classification scheme adopted is in line with those identified so far.

- *Cyber Growth Partnership (CGP)*: CGP is a UK initiative aiming to provide oversight and give strategic guidance to the government on supporting the development of the UK cyber security ecosystem. Within the CGP, the Cyber Exchange is an online platform enabling participants across industry, academia and government to list news, events and resources.
- *Cyberwatching.eu: see Subsection 2.2.1.1.*

2.2.6 General Considerations on the analysed sources

The sources presented in the previous section have been used to identify:

- A common set of vocabularies and terms;
- A set of specific sub-domains;
- A set of applicative sectors.

Ad-hoc desktop research activities have been conducted to identify relationships among domains, synonyms and to discriminate between cybersecurity peculiarities and generic items. Table 7 summarises the contribution provided by all the identified sources to the definition of the taxonomy presented in section 3, while Figure 1 and Figure 5 provides a high-level overview of the concepts and vocabularies emerged from the analysis described in this section.

On the basis of the analysis conducted, it is possible to draw some general considerations:

- The analysed standards provided a good source reference for the definition of terms, and for the identification of some domain areas linked to the risk-assessment domain. The same risk-assessment elements can be found in the resilience function areas defined by NIST and well as in the NIST CSRC categorisation. When instead coming to the identification of research domains, the analysed standards can be considered negligible as conceived to drive a technical standardisation process in very specific domains and not to classify knowledge and scientific activities
- The NIS directive and the NIST CRSC share, with some variations, a common understanding of the sectors where cybersecurity must be considered paramount, hence by merging these two sectorial views it is possible to identify a relevant element of the taxonomy which will be presented in Section 3
- The taxonomies of IEEE, IFIP, ECSO, ETSI and Cyberwatch.eu often overlap with the NIST CRSC resulting the better detailed and logically structured. The merging of these three sources could provide a good starting point for what concerns the technological and scientific domains.
- NIST CRSC considers into its categorisation also law and regulation aspects; this is perfectly in line with the scope of the taxonomy subject of this study, however the sub-domains listed are obviously related to the US regulation landscape, and cannot be considered as useful to map the EU law and regulation cybersecurity expertise. However, the NIS directive and the GDPR can be used there to close the gap

As it is possible to see the identified sources well complement each other allowing to cover almost all the cybersecurity spectrum.

By using the identified concepts and leveraging on standards for what concerns definitions and vocabulary, a more general and EU oriented taxonomy of the cybersecurity and privacy domain is presented in Section 3.

Source	General concepts	Academic Research	Regulatory	Operational	Sectorial	Application	Economic and Business	Social	Standards	Vocabulary
Cyberwatching	x	x		x						
ACM Classification System	x	x				x	x	x		
NIST CSRC Taxonomy	x	x	x	x	x	x	x	x		
IEEE	x	x								
ETSI TC-Cyber	x	x		x					x	
IFIP WG 11	x	x				x	x	x		
IT-Grundschutz	x	x				x				
International Standards (Section 2.2)	x		x	x	x	x			x	x
OWASP	x									x
ENISA	x		x	x	x					x
ECSO	x					x	x			
EU Regulations (Section 2.2.4)	x		x	x	x	x		x	x	x
PWC Study						x	x			
SEREMA						x	x			
CGP						x	x			

Table 7. Sources contributions to the Cybersecurity Taxonomy

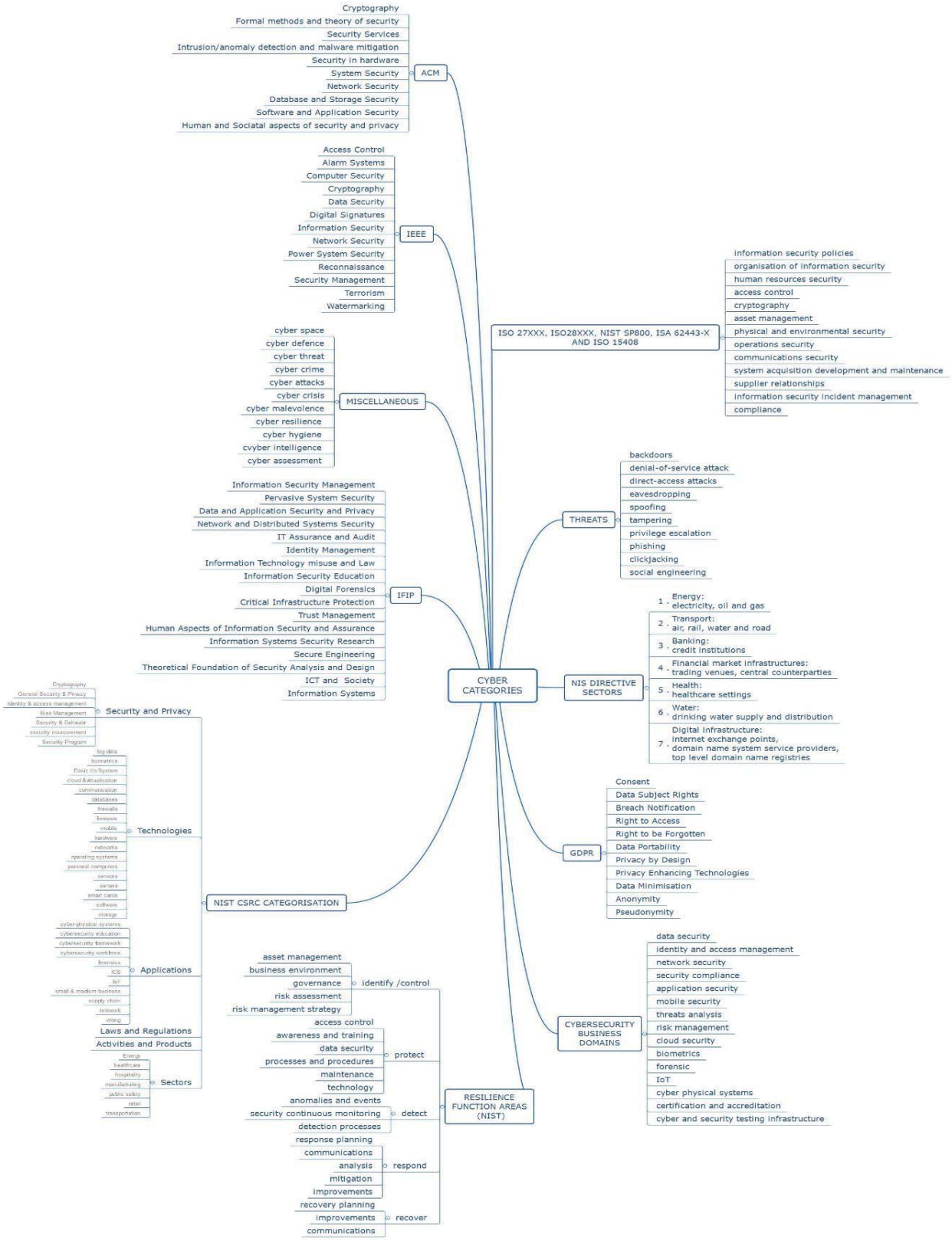


Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis

3 A Holistic Taxonomy for Cybersecurity Research Domains

The analysis of the reference sources described in the previous section highlights the complexity and heterogeneity of the cybersecurity discipline. In a similar situation, in order to ensure capturing every aspect of this domain, the taxonomy proposed in this document might risk to become super-specialised, with a multitude of nested domains. The goal of the taxonomy proposed in this report is that of supporting the mapping of the European cybersecurity competencies available.

The analysis conducted so far however suggests adopting a different, more agile approach. The analysis of the scientific/technological working groups activities (e.g. IFIP, ETSI etc.) and of the "knowledge management entities" (e.g. ACM, IEEE etc.) gives a clear and precise indication of the **areas of fundamental research** within the cybersecurity domain. On the other side, the analysis of policy documents and regulations allowed to magnify which **sectorial domains** are perceived as the most relevant for the wellbeing of the European Society (the assumption here is that regulations and policy packages answer to a precise European citizen and industry regulatory needs). Finally, the analysis of the market studies, of the observatory initiatives and of the R&D programs (H2020), provides an indication of the field of **technological applications** of the cybersecurity foundational research results.

This reasoning reached the conclusion that a taxonomy trying to cluster a complex and multifaceted discipline as cybersecurity needs to be structured on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and applications. Figure 6, depicts, in a graphical way, the proposed three-dimensional taxonomy, based on the following dimensions:

- Cybersecurity domains;
- Sectors (to protect which applications, technologies and cybersecurity research are developed and used);
- Applications and Technologies (on which the cybersecurity research results are applied).

Each dimension has been fine-tuned and detailed on the basis of the analysis presented in the previous section to:

a) ensure its alignment with the European Regulatory landscape;

b) ensure its comprehensiveness (merging together where needed sub-domains highlighted in different classifications and standards);

c) avoid redundancy of terms and definitions.

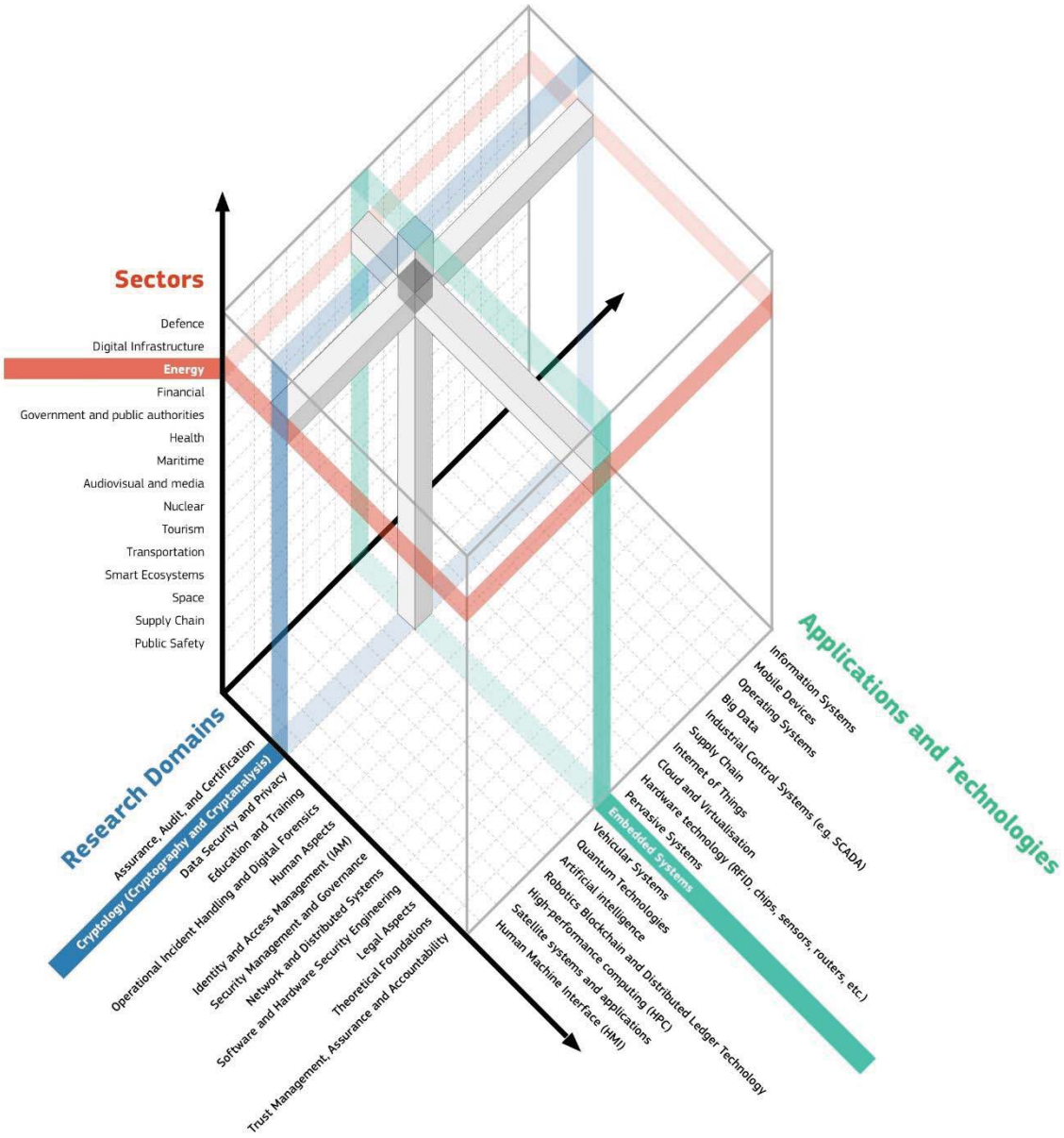


Figure 6. High Level view of the Cybersecurity Taxonomy

In what follows, definitions for each dimension of the proposed taxonomy are presented. More in details, Subsection 3.1 lists for each of cybersecurity domains the relevant sub-domains. Subsection 3.2 details the sectorial sub-domains, and Subsection 3.3 illustrates the list of applications and technologies. The taxonomy is completed with the glossary of concepts and vocabulary included in Annex 1. The cybersecurity subdomains defined for each domain, sectors, applications, and technologies are by no means an **exhaustive list**, these elements will be complemented in the future based on the input from cybersecurity centre of excellences surveyed.

3.1 Cybersecurity Domains

The following subsections provides a definition for each cybersecurity domain and lists the respective subdomains.

3.1.1 Assurance, Audit, and Certification

This domain refers to the methodologies, frameworks and tools that provide ground for having confidence that a system or network is working or has been designed to operate at the desired security target or according to a defined security policy.

- Assurance;
- Audit;
- Assessment;
- Certification;
- Protection Profile;
- Security Target.

3.1.2 Cryptology (Cryptography and Cryptanalysis)

Cryptology groups together by definition of Cryptography and Cryptanalysis. For the scope of this taxonomy, under this sub-domain fall the mathematical aspects of cryptology, the algorithmic aspects, their technical implementation and infrastructural architectures as well as the implementation of cryptanalytic methodologies, techniques and tools.

- Digital signatures;
- Asymmetric cryptography and cryptanalysis;
- Symmetric cryptography and cryptanalysis;
- Hash functions;
- Key management;
- Message authentication;
- Random number generation;
- Cryptanalysis methodologies, techniques and tools;
- Quantum cryptology;
- Post-quantum cryptology;
- Mathematical foundations of cryptography;
- Steganography.

3.1.3 Data Security and Privacy

This domain includes security and privacy issues related to data in order to (a) reduce by design privacy and confidentiality risks without impairing data processing purposes or (b) by preventing misuse of data after it is accessed by authorized entities.

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Pseudonymity;
- Unlinkability;
- Privacy by design and Privacy Enhancing Technologies (PET);
- Digital Rights Management (DRM);
- Data usage control.

3.1.4 Education and Training

The learning process of acquiring knowledge, know-how, skills and/or competences necessary to protect network and information systems, their users, and affected persons from cyber threats

- Cybersecurity education;
- Cybersecurity aware culture;

- Cybersecurity simulation platforms;
- Cybersecurity exercises;
- Cybersecurity ranges;
- Cybersecurity education methodology;
- Cybersecurity vocational training;
- Certification Programmes.

3.1.5 Operational Incident Handling and Digital Forensics

This domain refers to the theories, techniques, tools and processes for the identification, collection, acquisition and preservation of digital evidence that can be of evidential value.

- Incident analysis & Documentation;
- Containment Strategy design;
- Forensic evidence collection;
- Tracking/Tracing;
- Incident response;
- Vulnerability analysis & response;
- Artifact analysis & response;
- Digital evidence preservation;
- Incident forecasting (intelligence based);
- Digital forensic processes and workflow models;
- Digital forensic case studies;
- Legal, ethical and policy issues related to digital forensics.

3.1.6 Human Aspects

The interplay between ethics, relevant laws, regulations, policies, standards, psychology and the human being within the cybersecurity realm.

1. Accessibility;
2. Usability;
3. Social engineering and other human-related risks;
4. Socio-technical security;
5. Human errors;
6. Enhancing risk perception;
7. Psychological models;
8. User acceptance of security policies and technologies;
9. Automating security functionality;
10. Non-intrusive security;
11. Individual, organizational, and group information privacy concerns and behaviours;
12. Motivators and inhibitors of insider misuse;
13. Impacts of standards, policies, compliance requirements;
14. Organizational governance for information assurance;
15. Social engineering and other human-related risks;
16. Privacy attitudes and practices;
17. Computer ethics and security;
18. Transparent security;
19. Attacker profiling;
20. Security Psychology;
21. Legal and Regulatory Issues.

3.1.7 Identity and Access Management (IAM)

This domain covers authentication,authorization and access control of individuals and smart objects when accessing resources. These concerns may include

physical and digital elements of authentication systems and legal aspects related to compliance and law enforcement.

- Identity management models, frameworks, services (e.g. identity federations, single-sign-on, Public Key Infrastructure) ;
- Authentication/Access Control Technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF etc.)
- Protocols and frameworks for IAM;
- Identity management quality assurance;
- electronic IDentification, Authentication and trust Services (eIDAS);
- Optical and electronic document security;
- Legal aspects of identity management;
- Law enforcement and identity management.

3.1.8 Security Management and Governance

Governance and management activities, methodologies, processes and tools aimed at the preservation of confidentiality, integrity and availability of information as well as other properties such as authenticity, accountability and non-repudiation [SOURCE ISO/IEC 27000].

- Risk management;
- Continuous monitoring;
- Threats and vulnerabilities modelling;
- Attack modelling and countermeasures;
- Managerial aspects concerning information security
- Assessment of information security effectiveness and degrees of control;
- Identification of the impact of hardware and software changes on the management of Information Security;
- Standards for Information Security;
- Incident management and disaster recovery;
- Reporting (e.g. disaster recovery and business continuity)
- Theoretical and empirical analyses of information security behaviour;
- Adoption, use, and continuance of information security technologies and policies;
- Compliance with information security and privacy policies, procedures, and regulations;
- Vetting for security staff and employees;
- Economic aspects of the cybersecurity ecosystem;
- Vulnerability Assessment and Penetration Testing (VAPT);
- Attack prevention and detection;
- Capability Maturity Models.

3.1.9 Network and Distributed Systems

Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. [SOURCE ISO/IEC TR 29181-5]. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network. A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages [3]. In this context cybersecurity deals with all the aspects of computation, coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

- Network security (principles, methods, protocols, algorithms and technologies);
- Distributed Systems Security;
- Managerial, procedural and technical aspects of network security;

- Protocols and frameworks for secure distributed computing;
- Network layer attacks and mitigation techniques;
- Network attack propagation analysis;
- Distributed systems security analysis and simulation;
- Distributed consensus techniques;
- Fault tolerant models;
- Secure distributed computations;
- Auditability and Accountability;
- Honey nets and Honey Pots.

3.1.10 Software and Hardware Security Engineering

Security aspects in the software and hardware development lifecycle such as risk and requirements analysis, architecture design, code implementation, validation, verification, testing, deployment and runtime monitoring of operation.

- Security requirements engineering with emphasis on identity, privacy, accountability, and trust;
- Security and risk analysis of components compositions;
- Secure software architectures and design;
- Security design patterns;
- Secure programming principles and best practices;
- Security support in programming environments;
- Security documentation;
- Refinement and verification of security management policy models;
- Runtime security verification and enforcement;
- Continuous monitoring;
- Security testing and validation;
- Vulnerability discovery and penetration testing;
- Quantitative security for assurance;
- Intrusion detection and honeypots;
- Malware analysis;
- Model-driven security and domain-specific modelling languages;
- Self-healing systems;
- Side Channel Attacks (e.g. Power attacks, Electromagnetic Radiation attacks, etc.);
- Fault Injection Attacks.

3.1.11 Security Measurements

Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements [SOURCE NIST SP800-55].

- Security analytics and indicators;
- Security metrics;
- Validation and comparison frameworks for security metrics;
- Measurement and assessment of security levels.

3.1.12 Legal Aspects

This domain refers to the legal and ethical aspects related to the misuse of technology, illicit distribution and/or reproduction of material covered by IPR and the enforcement of law related to cybercrime and digital rights.

- Cybercrime prosecution and law enforcement;

- Cybersecurity and ethics;
- Intellectual property rights;
- Cybersecurity regulation analysis and design;
- Investigations of computer crime (cybercrime) and security violations;
- Legal, societal, and ethical issues in information security;
- Legal aspect of certification;
- Social media (e.g. fake news).

3.1.13 Theoretical Foundations

This domain refers to the use of formal analysis and verification techniques to provide theoretical proof of security properties either in software, hardware and algorithm design. Formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics.

- Formal specification and verification of the various aspects of security;
- Formal techniques for the analysis, verification and auditing of software and hardware;
- Information flow modelling and its application to confidentiality policies, composition of systems, and covert channel analysis;
- New theoretically-based techniques for the formal analysis and design of cryptographic protocols and their applications;
- Formal Verification of security assurance.

3.1.14 Trust Management, Assurance, and Accountability

This domain comprises trust issues related to digital and physical entities such as applications, services, components, or systems. Trust management approaches can be employed in order to provide assurance and accountability guarantees.

- Semantics and models for security, accountability, privacy, and trust;
- Trust management architectures, mechanisms and policies;
- Trust and privacy;
- Identity and trust management;
- Trust in securing digital as well as physical assets;
- Trust in decision making algorithms;
- Trust and reputation of social and mainstream media;
- Social and legal aspects of trust;
- Reputation models;
- Trusted computing.

3.2 Sectorial Dimensions

The following subsections list sectors and subsectors proposed for cybersecurity taxonomy.

3.2.1 Audiovisual and media

- Broadcasting;
- Publishing;
- Internet.

3.2.2 Defence

- Aeronautics;
- Space;
- Electronics;

- Land systems;
- Telecomm;
- Shipbuilding;
- Cyber defence;
- Dual-use cybersecurity technologies;
- Critical Information Infrastructures (CIIs).

3.2.3 Digital Infrastructure

- IXPs;
- DNS service providers;
- TLD name registries;
- Telecomm Infrastructures.

3.2.4 Energy

- Electricity;
- Distribution system operators;
- Transmission system operators;
- Energy Production Operators;
- Energy prosumers;
- Energy Third party services;
- Smart meters and equipment;
- Energy CIIs;
- Oil;
- Operators of oil transmission pipelines;
- Operators of oil production;
- Refining and treatment facilities, storage and transmission;
- Gas;
- Distribution system;
- Transmission system operators;
- Storage system operators;
- LNG system operators and services;
- Natural gas undertakings;
- Operators of natural gas refining and treatment facilities;
- Green Energy.

3.2.5 Financial

- Credit institutions;
- Operators of trading venues;
- Central counterparties (CCPs);
- Banking services;
- Insurance services;
- Financial CIIs;
- Brokerage services.

3.2.6 Government and public authorities

- Data collection;
- eGovernment systems and services;
- Law enforcement;
- Governmental CIIs.

3.2.7 Health

- Health care settings (including hospitals and private clinics);
- Healthcare supply chain;
- Medical devices industrial sector;

- Pharmaceutical industry;
- e/m Health;
- Helath CIIs.

3.2.8 Maritime

- Surveillance services;
- Border control services;
- Environmental protection;
- Fisheries;
- Port Authorities
- Port services;
- Maritime supply chains.

3.2.9 Nuclear

- Radiation protection;
- Transport of radioactive substances and waste;
- Waste management;
- Safeguarding nuclear materials;
- Safety of nuclear installations;
- Nuclear research and training activities.

3.2.10 Public Safety

- Fire services;
- Rescue services;
- Medical services;
- Police;
- Emergency communications;
- Civil protection;
- Inspections services;
- First Responders.

3.2.11 Tourism

- Accommodation;
- Food and Beverage Services;
- Recreation and Entertainment Infrastructures and Services;
- Travel Services.

3.2.12 Transportation

- Air transport;
- Air carriers;
- Airport managing bodies;
- Automotive industry;
- Traffic management control operators;
- Rail transport;
- Infrastructure managers;
- Railway undertakings;
- Water transport;
- Inland, sea and coastal passenger and freight water transport companies;
- Managing bodies of ports;
- Operators of vessel traffic services;
- Road transport;
- Road authorities;
- Operators of Intelligent Transport Systems;
- Sea transport;

- Container Ships;
- Passenger's Ships- Cruise Lines;
- Fisheries;
- Multi modal transport;
- Transport CIIs.

3.2.13 Smart Ecosystems

- Smart infrastructures (e.g. Industry 4.0);
- Smart (cities, vehicles, infrastructures, objects);
- Smart environments;
- Smart governance;
- Smart energy;
- Smart Networks (e.g. Home Networks).

3.2.14 Space

- Space industry;
- Satellite operators, including ground based stations;
- Positioning and timing information;
- Navigation services;
- Earth observation;
- Satellite data providers, including data storage.

3.2.15 Supply Chain

- Natural resources;
- Raw materials;
- Components;
- Retails.

3.3 Applications and Technologies Dimension

The following list details, as described at the begin of this section, the applications and technology dimensions:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.);
- High-performance computing (HPC);
- Human Machine Interface (HMI);
- Industrial Control Systems (e.g. SCADA);
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems;
- Pervasive Systems;
- Quantum Technologies;
- Robotics;
- Satellite systems and applications;
- Supply Chain;
- Vehicular Systems.

4 Final Remarks

The goal of this document is that of aligning the cybersecurity terminologies, definitions and domains to allow the categorisation of existing EU cybersecurity centres (e.g. research organisations/laboratories/ associations/academic institutions/groups, operational centres) according to their cybersecurity expertise in specific domains.

Due to the intrinsically multifaceted nature of cybersecurity the accomplishment of a similar task required an “horizontal, cross-silos effort” to collate, organise and integrate existing classifications with the goal of defining a comprehensive cybersecurity taxonomy not limited to the traditional academic research domain, but able to transversal capture competencies, concepts and definitions.

The resulting three-dimensional taxonomy presented in Section 3 is not static, but it is open to modifications and must be understood as a living semantic structure which will change during the years to keep the pace of the fast evolution of the digital world.

Annex 1 –Glossary of terms

Accessibility

(ISO/IEC TR 13066-2:2016) Degree to which a computer system is easy to use by all people, including those with disabilities.

Access control

(ISO/IEC 27000) means to ensure that access to assets is authorized and restricted based on business and security requirements.

Accountability

(ISO/IEC 2382:2015) property that ensures that the actions of an entity may be traced uniquely to that entity.

Acquisition

(ISO/IEC 27037:2012) process of creating a copy of data within a defined set (the product of an acquisition is an evidentially reliable copy of the original source data).

Assurance

(ISA 62443-1-2) Attribute of a system that provides grounds for having confidence that the system operates such that the system security policy is enforced.

Audit

(ISO/IEC 27000:2016) systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (An audit can be an internal audit or an external audit, and it can be a combined audit).

(ISA 62443-1-2) independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Asymmetric cryptographic algorithm

(ISO/IEC 10181-1:1996, definition 3.3.1) algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

Attack

(ISO/IEC 27000:2016) attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Authentication

(ISO/IEC 27000) provision of assurance that a claimed characteristic of an entity is correct.

Availability

(ISO/IEC 27000:2016) property of being accessible and usable upon demand by an authorized entity.

Biometrics

(ISO/TR 18307:2001) use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities.

Certification

(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency") Certification consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance. Certification serves the purpose to inform and reassure purchasers and users about the security properties of the products and services that they buy or use.

Collection

(ISO/IEC 27037:2012) process of gathering the physical items that contain potential digital evidence.

Confidentiality

(ISO/IEC 27000:2016) property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Conformity

(ISO/IEC 27000:2016) fulfilment of a requirement.

Cryptanalysis

(ISO/IEC 7498-2:1989, definition 3.3.18 and ISO/IEC 18033-1 2015) the analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.

Cryptology

(Computer Security – Dieter Gollmann – Johnson Wileys and Sons) Cryptology groups together by definition of Cryptography (i.e. “the science of secret writing”) and Cryptanalysis (i.e. the science of “breaking ciphers”) . For the scope of this taxonomy, under this domain go not only the mathematical foundations, but also the technical implementations of cryptographic algorithms and architectures, as well as the implementation of cryptanalytic methodologies, techniques and tools.

Cybercrime

(ISO/IEC 27032:2012) criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime.

Cybersecurity

(ISO/IEC 27032:2012) preservation of confidentiality, integrity and availability of information in the Cyberspace.

(the) Cyberspace

(ISO/IEC 27032:2012) complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

Data

(ISO/IEC 27000:2016) collection of values assigned to base measures, derived measures and/or indicators.

Digital evidence

(ISO/IEC 27037:2012) information or data, stored or transmitted in binary form

that may be relied on as evidence.

Digital signatures

(ISO/IEC 14888) process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature.

Digital Rights Management

(ISO/IEC 5127:2017) digital technology that is separate to the product form of a specific digital publication and which is used to control access to content.

Distributed System

(Coulouris, George; Jean Dollimore; Tim Kindberg; Gordon Blair (2011). Distributed Systems: Concepts and Design (5th Edition). Boston: Addison-Wesley. ISBN 0-132-14301-1) A distributed system is a model in which components located on networked computers communicate and coordinate their actions by passing messages. In this context cybersecurity deals with all the aspects of coordination, message integrity, availability and (if required) confidentiality. Message authentication is also in the scope.

Documented information

(ISO/IEC 27000:2016) information required to be controlled and maintained by an organization and the medium on which it is contained.

eIDAS

(Regulation (EU) No 910/2014) EU regulation proposed to ensure that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available;

Effectiveness

(ISO/IEC 27000:2016) extent to which planned activities are realized and planned results achieved.

Event

(ISO/IEC 27000:2016) occurrence or change of a particular set of circumstances.

Executive management

(ISO/IEC 27000:2016) person or group of people who have delegated responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organization.

Governance of information security

(ISO/IEC 27000:2016) system by which an organization's information security activities are directed and controlled.

Governing body

(ISO/IEC 27000:2016) person or group of people who are accountable for the performance and conformance of the organization.

Hash functions

(ISO/IEC 10118-1:2016) Hash-functions map strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, using a specified algorithm. They can be used for reducing a message to a short imprint for input

to a digital signature mechanism, and committing the user to a given string of bits without revealing this string.

Human errors

Mistakes that unwittingly create opportunities for cyber hackers to exploit.

Identity

(ISO/IEC 24760-1:2011) set of attributes related to an entity.

Identity management

(ISO/IEC 24760-1:2011) processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain.

Indicator

(ISO/IEC 27000:2016) measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs (2.31).

Identification

(ISO/IEC 27037:2012) process involving the search for, recognition and documentation of potential digital evidence.

Information security

(ISO/IEC 27000:2016) preservation of confidentiality, integrity and availability of information.

Information security continuity

(ISO/IEC 27000:2016) processes and procedures for ensuring continued information security operations

Information security event

(ISO/IEC 27000:2016) identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.

Information security incident

(ISO/IEC 27000:2016) single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information security incident management

(ISO/IEC 27000:2016) processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Information system

(ISO/IEC 27000:2016) applications, services, information technology assets, or other information handling components.

Integrity

(ISO/IEC 27000:2016) property of accuracy and completeness.

ISMS project

(ISO/IEC 27000:2016) structured activities undertaken by an organisation (2.57) to implement an ISMS.

Key management

(ISO/IEC 11770-1:2010 PART 1, definition 2.28) administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

Level of risk

(ISO/IEC 27000:2016) magnitude of a risk (2.68) expressed in terms of the combination of consequences (2.14) and their likelihood.

Likelihood

(ISO/IEC 27000:2016) chance of something happening.

Malware

(ISO/IEC 27033-1:2015) malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

Management system

(ISO/IEC 27000:2016) set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.

Message authentication

(ISO/IEC 9797-1) process to authenticate a message, often done through Message authentication codes (string of bits which is the output of a MAC algorithm.

Monitoring

(ISO/IEC 27000:2016) determining the status of a system, a process (2.61) or an activity.

Network security

(ISO/IEC TR 29181-5) Network security is concerned with hardware, software, basic communication protocols, network frame structure, and communication mechanisms factors of the network. Information Security in the network context deals with data integrity, confidentiality, availability and non-repudiation while is sent across the network.

Non-conformity

(ISO/IEC 27000:2016) non-fulfilment of a requirement.

Non-repudiation

(ISO/IEC 27000:2016) ability to prove the occurrence of a claimed event for action and its originating entities.

Organization

(ISO/IEC 27000:2016) person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.

Outsource

(ISO/IEC 27000:2016) make an arrangement where an external organization performs part of an organization's function or process.

Performance

(ISO/IEC 27000:2016) measurable result.

Personally Identifiable Information (PII)

(ISO/IEC 24745:2011) any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains; from which identification or contact information of an individual person can be derived, or that is or might be directly or indirectly linked to a natural person.

Policy

(ISO/IEC 27000:2016) intentions and direction of an organization as formally expressed by its top management.

Post-quantum cryptology

(NISTIR 8105) the goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

Preservation

(ISO/IEC 27037:2012) process to maintain and safeguard the integrity and/or original condition of the potential digital evidence.

Process

(ISO/IEC 27000:2016) set of interrelated or interacting activities which transforms inputs into outputs.

Protection Profile

(ISO/IEC 15408-1:2009) implementation-independent statement of security needs for a Target of Evaluation (TOE) type.

Privacy

(ISO/TS 25237:2008) freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.

Privacy Enhancing Technology (PET)

(ISO/IEC 29100:2011) privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system.

Pseudonymity

(ISO/IEC 25237:2017) particular type of de-identification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.

Quantum cryptology

(ISO/TS 80004-12:2016(en), 6.6) use of quantum phenomena for cryptographic purposes.

Reliability

(ISO/IEC 27000:2016) property of consistent intended behaviour and results.

Reputation

(ISO/IEC 23006-4:2013) measure of the credibility of or the possibility (e.g., legal) for a user to be a party in a transaction.

Requirement

(ISO/IEC 27000:2016) need or expectation that is stated, generally implied or obligatory.

Residual risk

(ISO/IEC 27000:2016) risk remaining after risk treatment.

Review

(ISO/IEC 27000:2016) activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk

(ISO/IEC 27000:2016) effect of uncertainty on objectives. In the context of information security (2.33) management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Risk acceptance

(ISO/IEC 27000:2016) informed decision to take a particular risk.

Risk analysis

(ISO/IEC 27000:2016) process to comprehend the nature of risk and to determine the level of risk.

Risk assessment

(ISO/IEC 27000:2016) overall process of risk identification, risk analysis and risk evaluation.

Risk evaluation

(ISO/IEC 27000:2016) process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk identification

(ISO/IEC 27000:2016) process of finding, recognizing and describing risks.

Risk management

(ISO/IEC 27000:2016) coordinated activities to direct and control an organization with regard to risk.

Risk management process

(ISO/IEC 27000:2016) systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk owner

(ISO/IEC 27000:2016) person or entity with the accountability and authority to manage a risk.

Risk treatment

(ISO/IEC 27000:2016) process to modify risk (eg. avoidance, removal, change, share, retain, mitigation).

Scale

(ISO/IEC 27000:2016) ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.

Security implementation standard

(ISO/IEC 27000:2016) document specifying authorized ways for realizing security.

Security management policy

(ISO/IEC 28000:2007) overall intentions and direction of an organization, related to the security and the framework for the control of security-related processes and activities that are derived from and consistent with the organization's policy and regulatory requirements.

Security Measurements

(NIST SP800-55) Information security measures are used to facilitate decision making and improve performance and accountability through the collection, analysis and reporting of relevant cybersecurity performance-related data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective actions based on observed measurements.

Security Target

(ISO/IEC 15408-1:2009) implementation-dependent statement of security needs for a specific identified Target of Evaluation (TOE).

Symmetric cryptographic algorithm

(ISO/IEC 9735-1, definition 4.111) algorithm employing the same value of key for both enciphering and deciphering or for both authentication and validation.

Threat

(ISO/IEC 27000:2016) potential cause of an unwanted incident, which may result in harm to a system or organization.

Testing

(ISO/IEC 29109-1:2009) determination of one or more characteristics of an object of conformity assessment, according to a procedure.

Top management

(ISO/IEC 27000:2016) person or group of people who directs and controls an organization at the highest level.

Trust

(ISO/IEC 25010:2011) degree to which a user or other stakeholder has confidence that a product or system will behave as intended.

Unlinkability

(ISO/TS 12812-2:2017) security property of a protocol that protect it against an unauthorized party being able to link two executions of the protocol to a specific mobile device.

Validation

(ISO/IEC 27000:2016) confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Verification

(ISO/IEC 27000:2016) confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vetting (referred to employees' recruitment)

(Collins online dictionary) Employees screening.

Vulnerability

(ISO/IEC 27000) weakness of an asset or control that can be exploited by one or more threats.

List of figures

Figure 1. Cybersecurity taxonomy definition steps. 8

Figure 2. Vertical and horizontal cybersecurity development areas 9

Figure 3. ETSI cross-cutting cybersecurity clusters 13

Figure 4. IFIP TC 11 Structure 14

Figure 5. High-level overview of the concepts and vocabularies emerged from the analysis 25

Figure 6. High Level view of the Cybersecurity Taxonomy 27

List of tables

Table 1. European Projects Catalogue dimensions 9
Table 2. ACM Classification System Categories 10
Table 3. Cybersecurity Topic Clustering (NIST Computer Security Resource Center) 11
Table 4. ETSI TC-Cyber working group domains 12
Table 5. IFIP WG 11 Research sub-groups 16
Table 6. List of Standards taken into consideration 17
Table 7. Sources contributions to the Cybersecurity Taxonomy 24

Annex 6: Pilot Project: Work Programme Text and Timeline

Extract from

EN

Annex 6

Horizon 2020

Work Programme 2018-2020

5.i. Information and Communication Technologies

Important notice on the Horizon 2020 Work Programme

This Work Programme covers 2018, 2019 and 2020. The parts that relate to 2019 and 2020 are provided at this stage on an indicative basis. Such Work Programme parts will be decided during 2018 and/or 2019.

(European Commission Decision C(2017)7124 of 27 October 2017)

SU-ICT-03-2018: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

Specific Challenge: EU's strategic interest is to ensure that the EU retains and develops essential capacities to secure its digital economy, infrastructures, society, and democracy. Europe's cybersecurity research, competences and investments are spread across Europe with too little alignment. There is an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities. Europe has to master the relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software. European industries need to be supported and equipped with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks. This should contribute inter alia to achieve the objective of European strategic autonomy.

The Public Private Partnership on Cybersecurity[20] created in 2016 was an important first step aiming at triggering up to EUR 1.8 billion of investment. However, the scale of the investment under way in other parts of the world suggests that the EU needs to do more in terms of investment and overcome the fragmentation of capacities spread across the EU. In this context in a recent Joint Communication[21] the Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

Scope: The objective of this topic is to scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable. For this, participants should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub. Projects under this topic will help build and strengthen cybersecurity capacities across the EU as well as provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre as mentioned by the Joint Communication.

To achieve the above, support will go to consortia of competence centres in cybersecurity to engage together in:

- Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing);

[20] C(2016) 440 final

[21] Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN (2017) 450 final

- Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;
- Supporting certification authorities with testing and validation labs equipped with state of the art technologies and expertise.

Each proposal should bring together cybersecurity R&D&I centres in Europe (e.g. university labs/public or private non-profit research centres) to create synergies and scale up existing competences and demonstrated strengths to the European level. Proposals should take into consideration relevant active digital ecosystems and public-private cooperation models and focus on solving technological and industrial challenges. The centres within the proposal should aim to collectively develop and implement a Cybersecurity Roadmap covering the above and addressing multiple and complementary cybersecurity disciplines (e.g. cryptography, network security, application security, IoT/cloud security, data integrity and privacy, secure digital identities, security/crisis management, forensic technologies, security investigation, cyber psychology, bio-security). When developing the Roadmap the results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda, will serve as a starting point. Consideration should also be given to the relevant work of ENISA, Europol and other EU agencies and bodies.

The Roadmap should include targets to be achieved with deliverables by the end of the project (typically three to four years) that constitute clear milestones in its implementation, as well as priorities to be addressed in the future by the Cybersecurity Competence Network.

To implement this Roadmap, partners in the proposal(s) are expected to set up a functional network of centres of expertise with a coordinating "competence centre" (this role should be undertaken by one of the partners in the network, with the necessary capacity, resources and experience). Work includes the assessment of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry. Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people) and will be implemented, tested and validated in the demonstration cases (see below) involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure.

Projects will demonstrate the effectiveness of their selected governance structure by providing collaborative solutions to enhance cybersecurity capacities of the network and develop cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).

Projects should ensure outreach, to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, and to spread the developed expertise.

Projects should also include industrial partners and their cybersecurity research collaborators to create synergies and: (a) collaboratively identify and analyse

scalable (short/mid/long term[22]) cybersecurity industrial challenges in the selected sectors and (b) demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases.

These demonstration cases will constitute the core part of the work to be done within the project. They will be based on a specific research & development roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.

Projects under this topic are implemented as a programme through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied. Proposals shall therefore foresee resources for clustering activities with other projects funded under this topic to identify synergies, best practices and kick-off the process of creating the network involving the sub-networks already created by awarded projects. This task will contribute to the actual set-up of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage.

A proposal must involve distinct cybersecurity R&D&I excellence centres in Europe (e.g. university labs, public or private non-profit research centres, taking into consideration public-private cooperation models and the ecosystems around them), with complementary expertise, from at least 9 Member States or Associated Countries. With the aim of reinforcing technology and industrial capacity as widely as possible across Europe, proposals should include a substantial representation of the most relevant RD&I excellences centres in Europe, with a widespread European coverage and good geographical balance of activities as regards the scope of work. This will ensure the proposals meeting the policy goals of the initiative of supporting the establishment of the future Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre of the European Union.

The consortium in a proposal must involve at least 20 partners.

A proposal should also include industrial partners from various (not less than 3) sectors (e.g. telecom, finance, transport, eGovernment, health, space, defence, manufacturing) that will be involved in the demonstration cases.

The support and involvement of the relevant governmental bodies and authorities (e.g. for monitoring and assessing the projects' results during their life-cycles) will be considered as an asset.

The Commission considers that proposals requesting a contribution of up to EUR 16 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

---

[22] *Short term*: referring to cybersecurity challenges in existing industrial products that can be addressed by the research and computational capabilities of the Network, *medium term*: referring to cybersecurity challenges in upcoming products that can be addressed by the research and computational capabilities of the Network and the Center and *long term*: high risk research for challenges that will shape new policies for long-term innovation capabilities requiring computational and research capacities beyond the existing ones by the Network.

For grants awarded under this topic the Commission may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

Under this call topic, the beneficiaries nominated as project coordinators cannot, in this capacity, be awarded more than one grant from the European Union budget. In case an applicant organisation appears as coordinator in more than one proposal, only the last submitted proposal will be considered for evaluation. This approach should allow different governance models to be tested through this topic and provide a wide range of complementary outcomes, including lessons learnt, for the future set-up.

Expected Impact:

- Cybersecurity solutions, products or services for the identified critical challenges, increasing the cybersecurity of the Digital Single Market, in particular for sectors from which stakeholders are involved;
- A feasible, sustainable governance model for the Cybersecurity Competence Network developed and tested through successful pilot projects addressing selected industrial challenges;
- Clearly demonstrated strengthening of Member States' research and innovation competence and cybersecurity capacities, also within their national cybersecurity ecosystems, to meet the increasing cybersecurity challenges;
- Synergies between experts from various cybersecurity domains demonstrated;
- Bridges built between the network and industrial communities;
- Research and Development programme with a common Research and Innovation Roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing;
- A cybersecurity skills framework model developed, which can be used as a reference by education providers to develop appropriate curricula; by employers, to help assess their cybersecurity workforce, and improve job descriptions; by citizens to reskill themselves;
- Establishment of foundations for pooling and streamlining the development and deployment of cybersecurity technology and strengthening industrial capabilities to secure EU's digital economy, society, democracy, space and infrastructures.

Type of Action: Research and Innovation action

1 PILOT PROJECT: TIMELINE