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

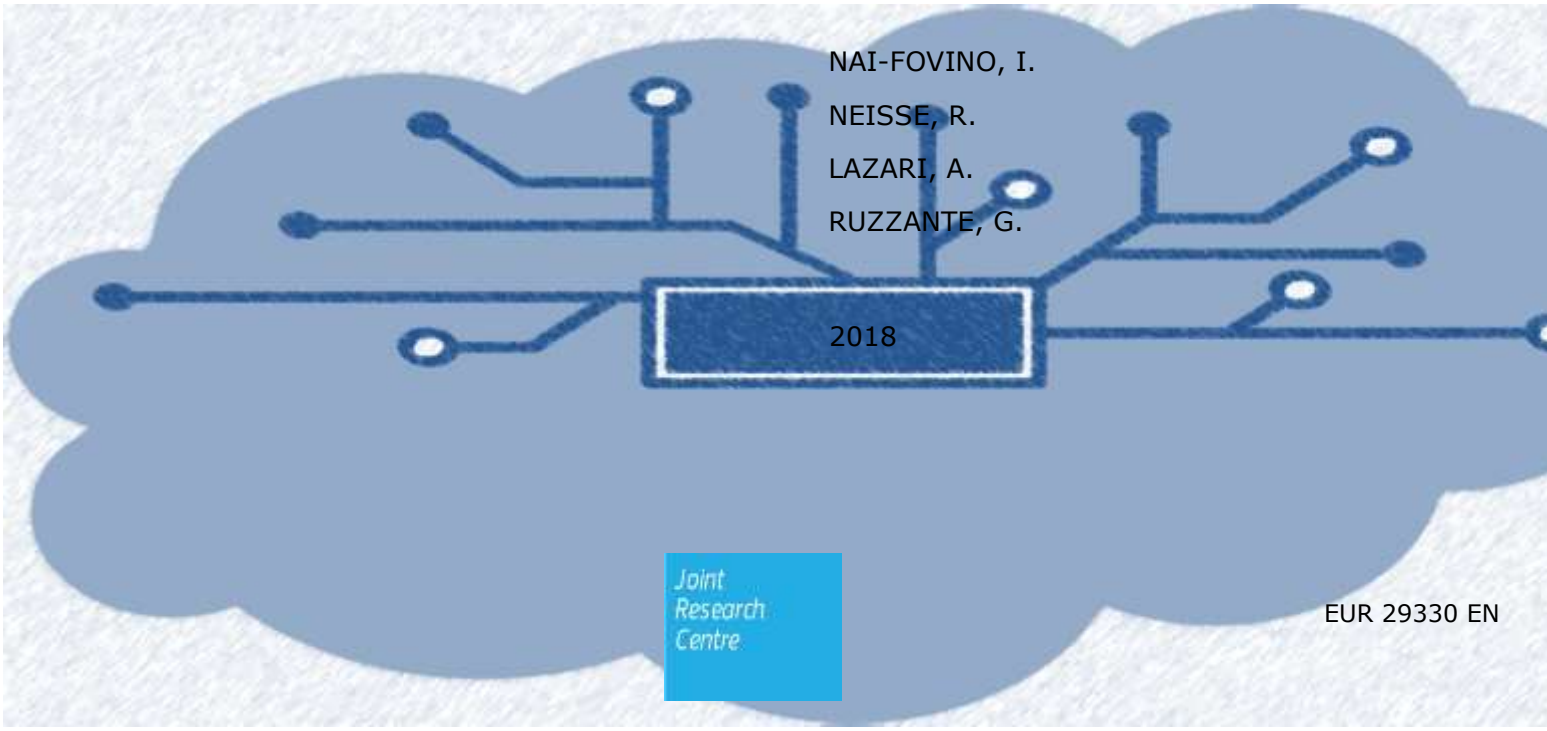
{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 404 final}

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

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:

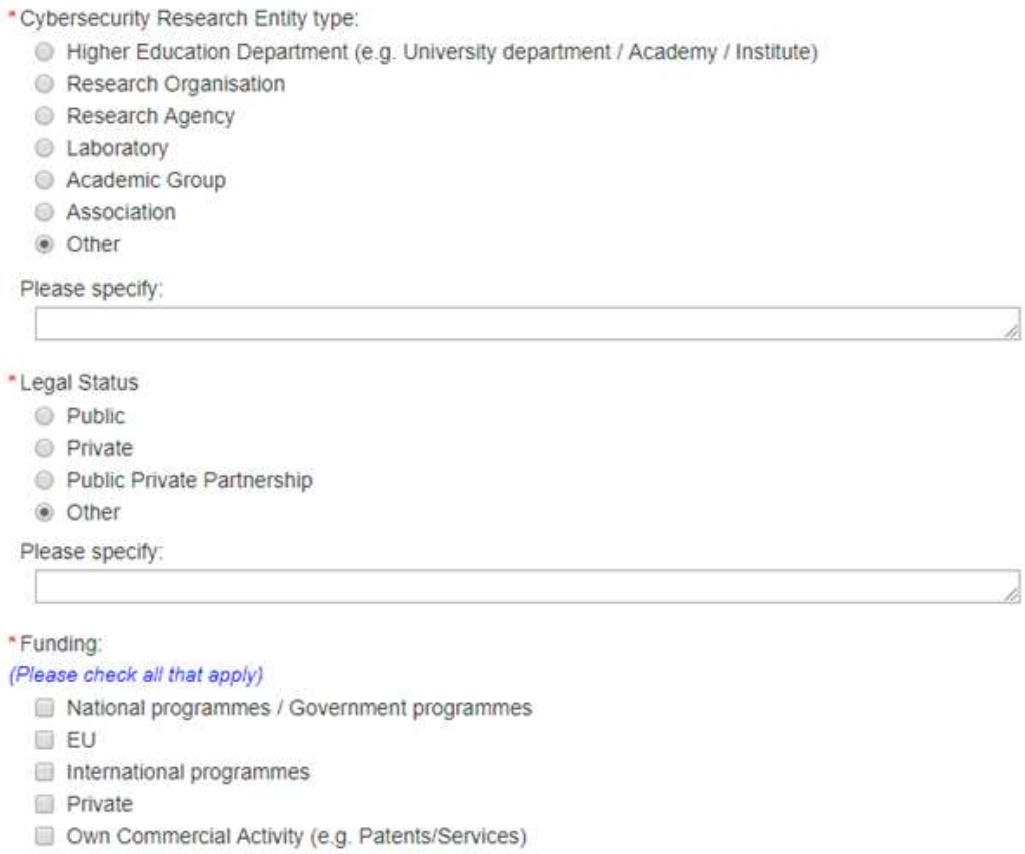


Figure 1. Entity type, legal status, and funding types.

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.

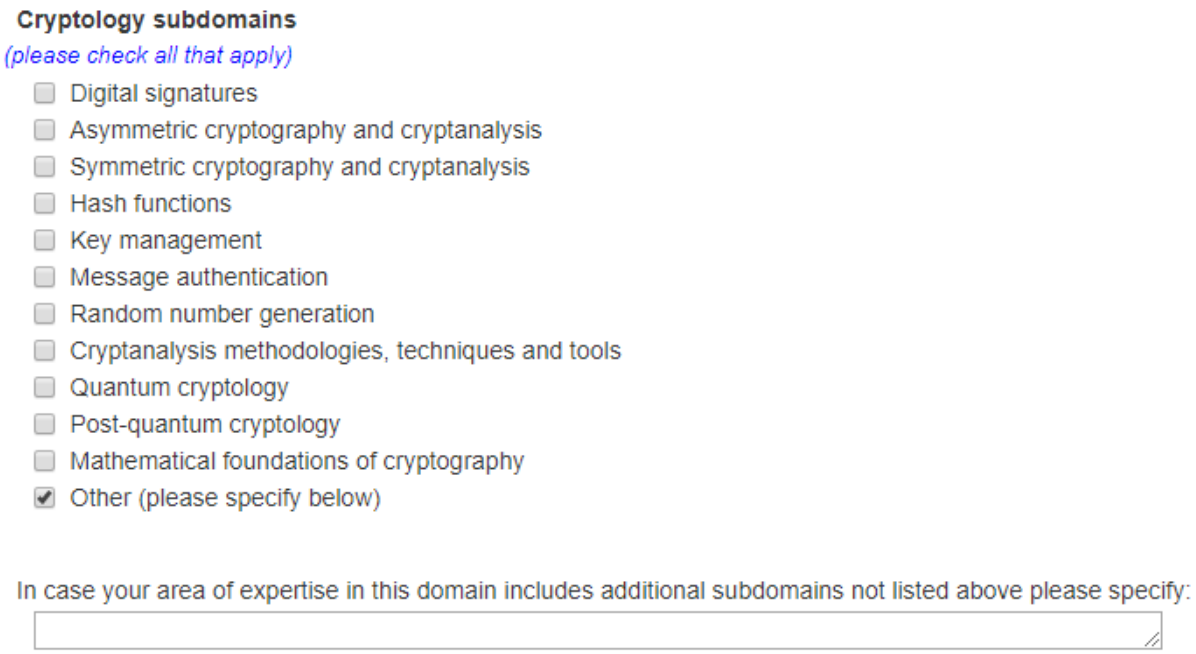


Figure 3. Cryptology subdomains.

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.

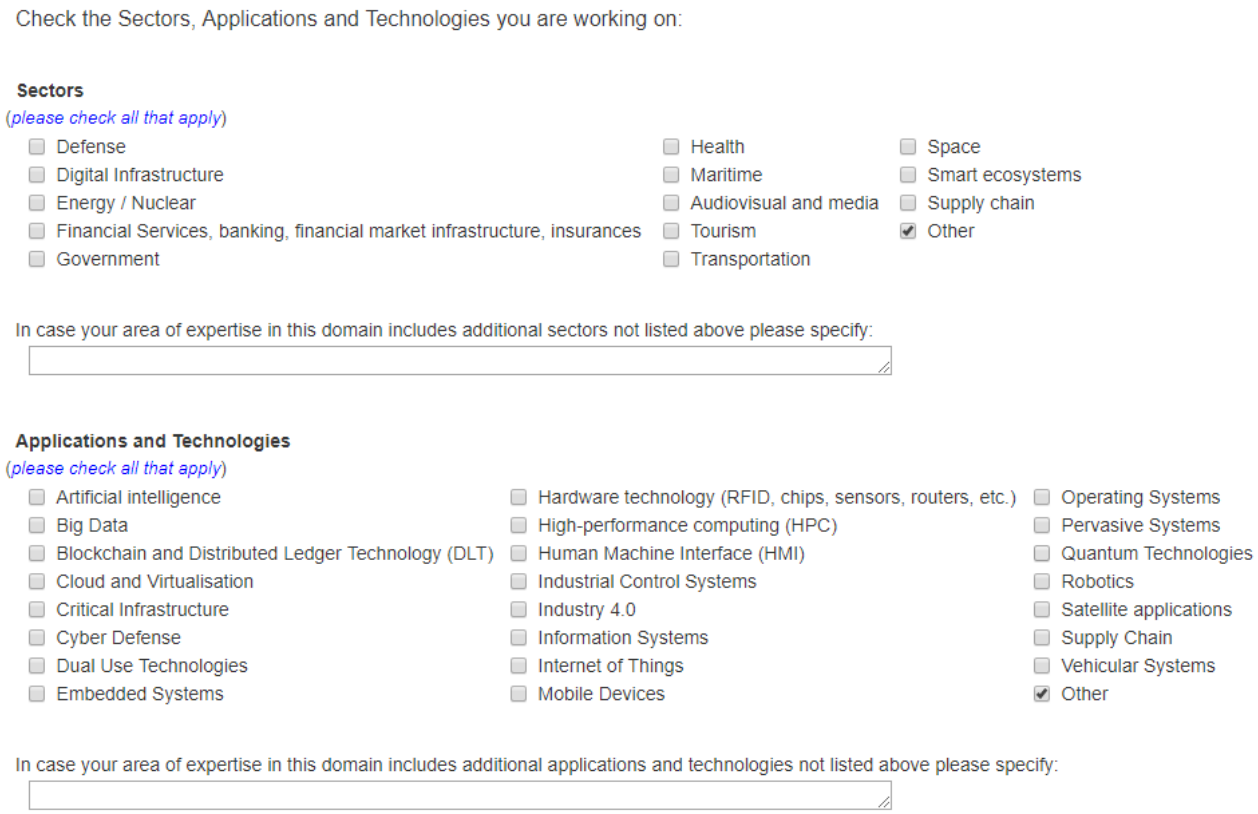


Figure 4. Sectors, applications, and technologies.

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.

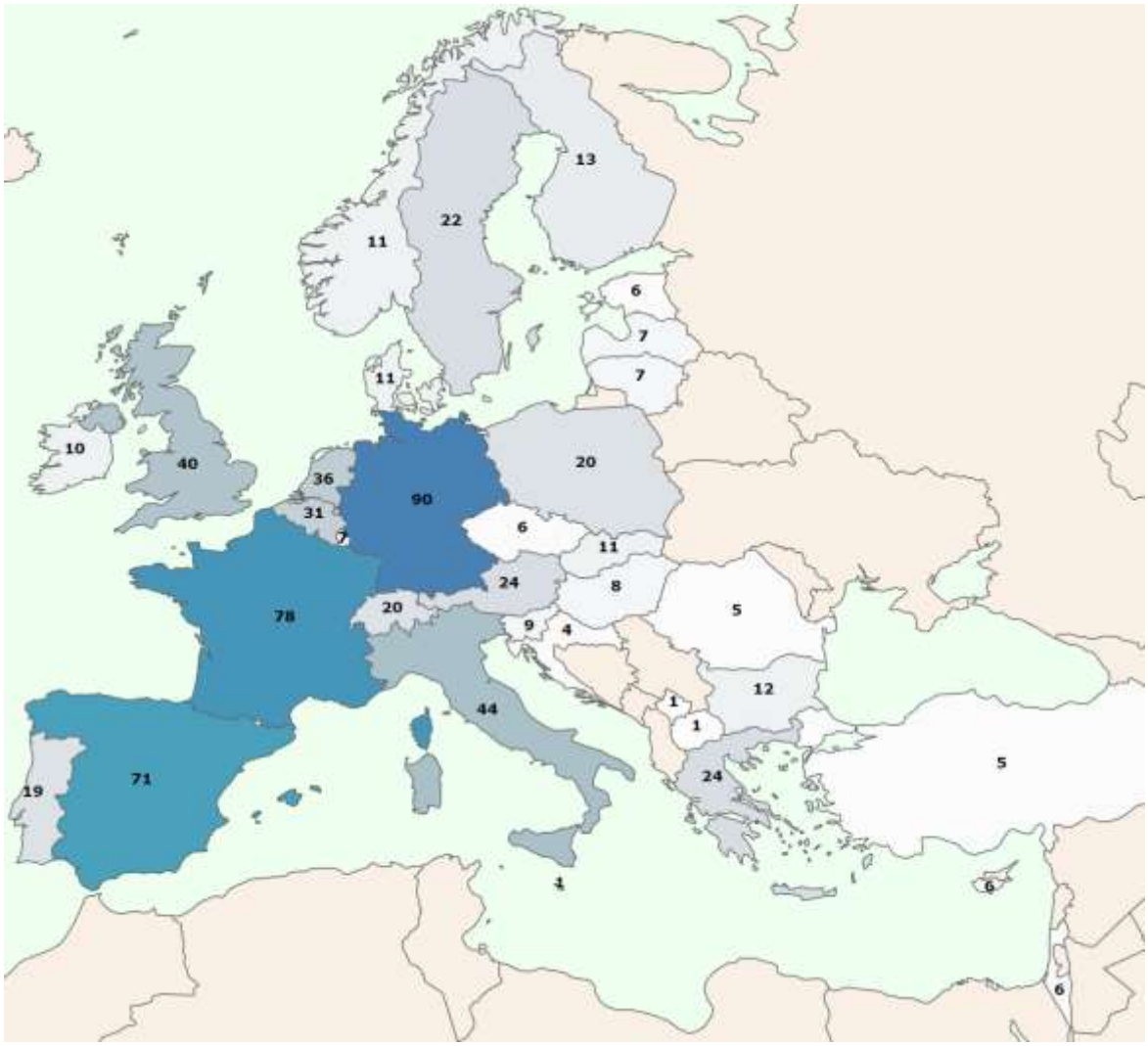


Figure 5. Geographical distribution of number of survey participants per country with a color legend indicating with darker blue color countries with a higher number.

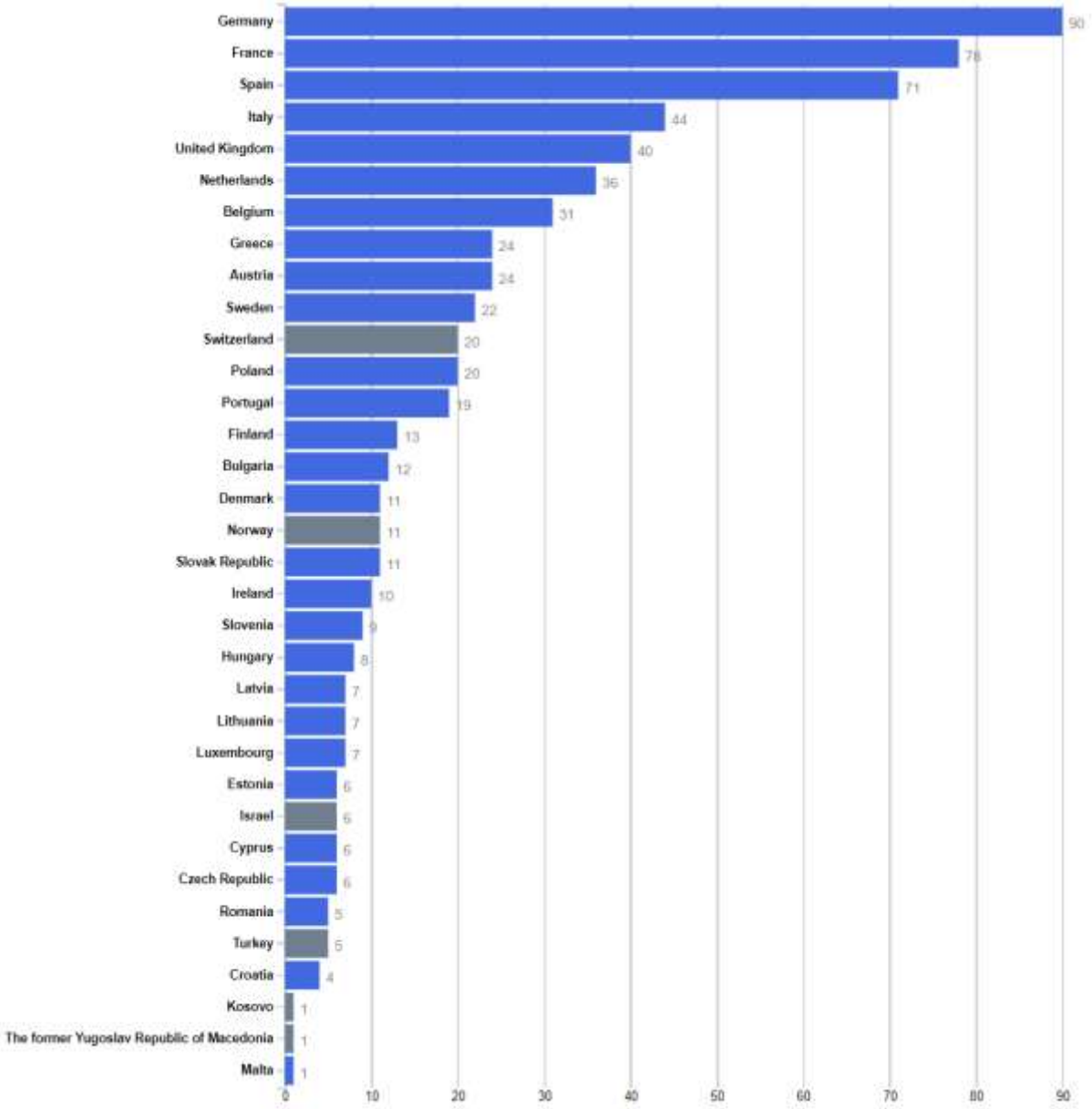


Figure 6. Number of survey participants per country. Non-EU participants are highlighted in in grey.

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.

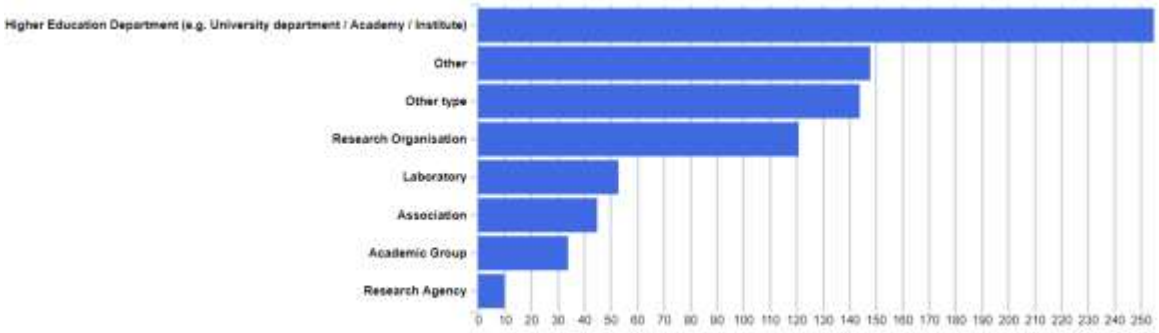


Figure 7. Distribution of participants according to their entity type.

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).

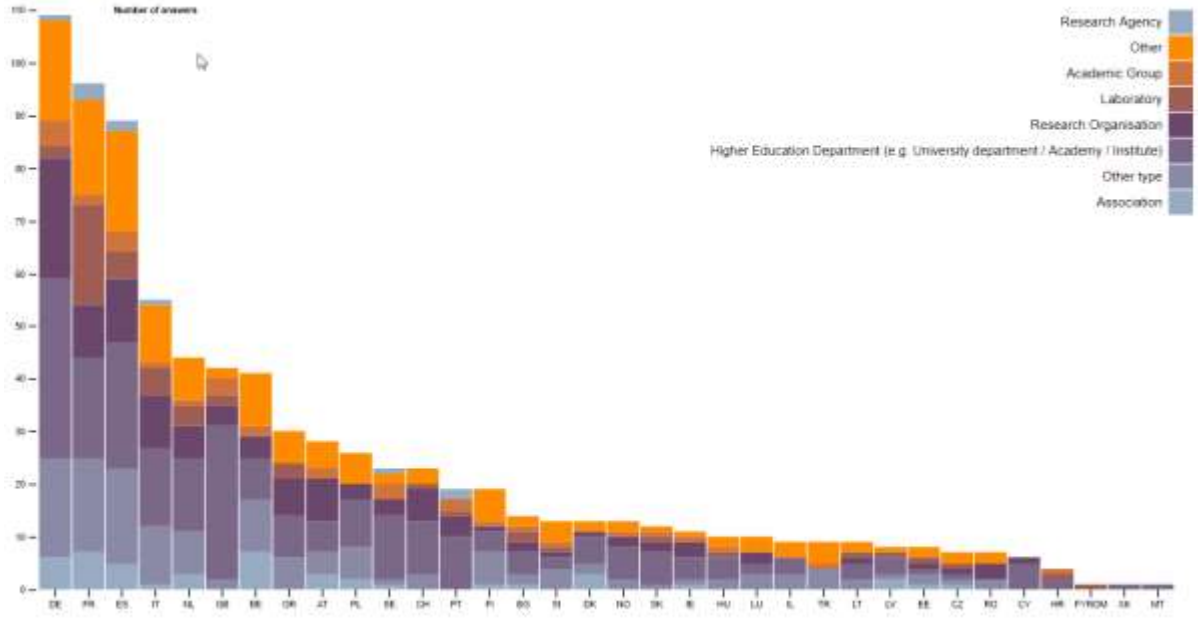


Figure 8. Distribution of entity types per country.

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).

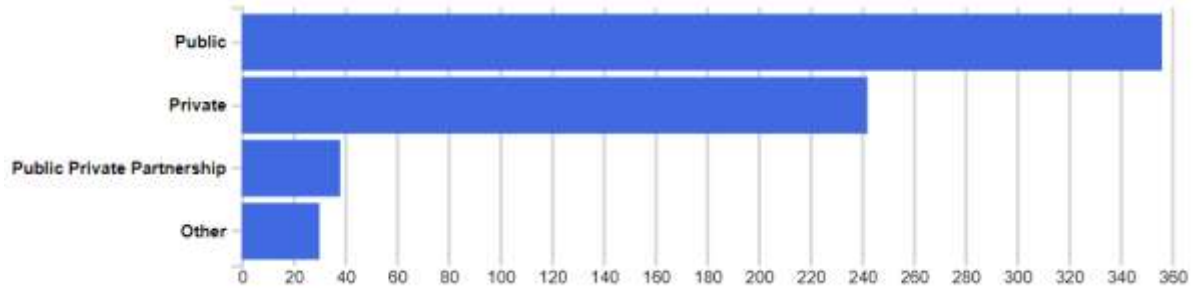


Figure 9. Distribution of participants according to their legal status.

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.

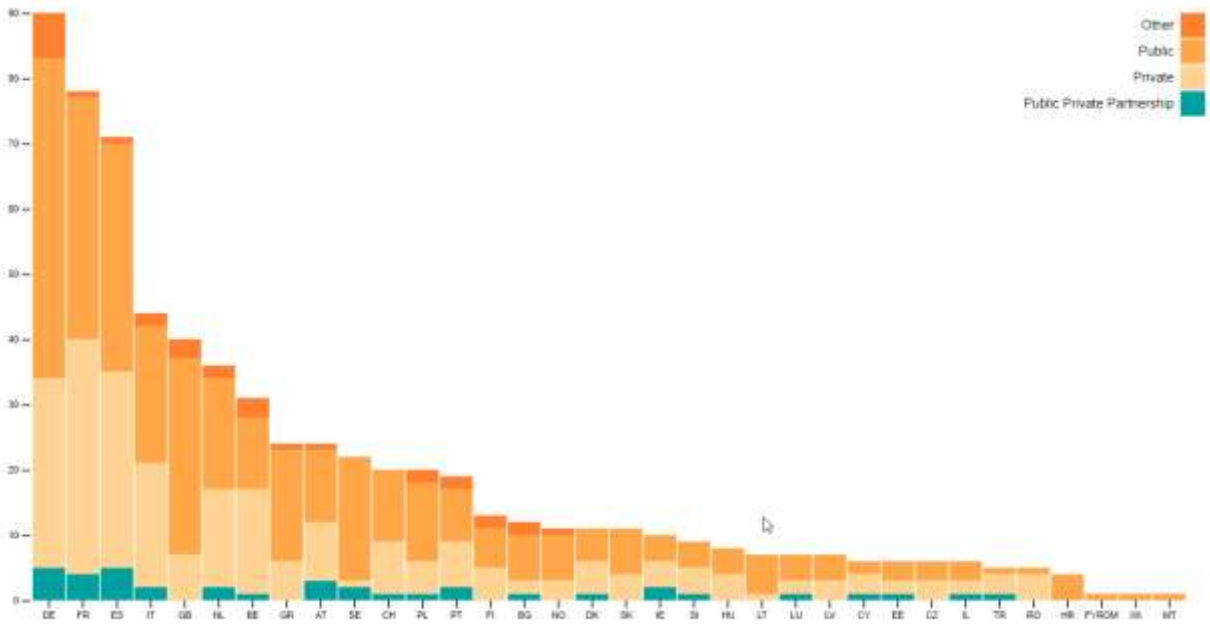


Figure 10. Distribution of entities per country according to their legal status.

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.

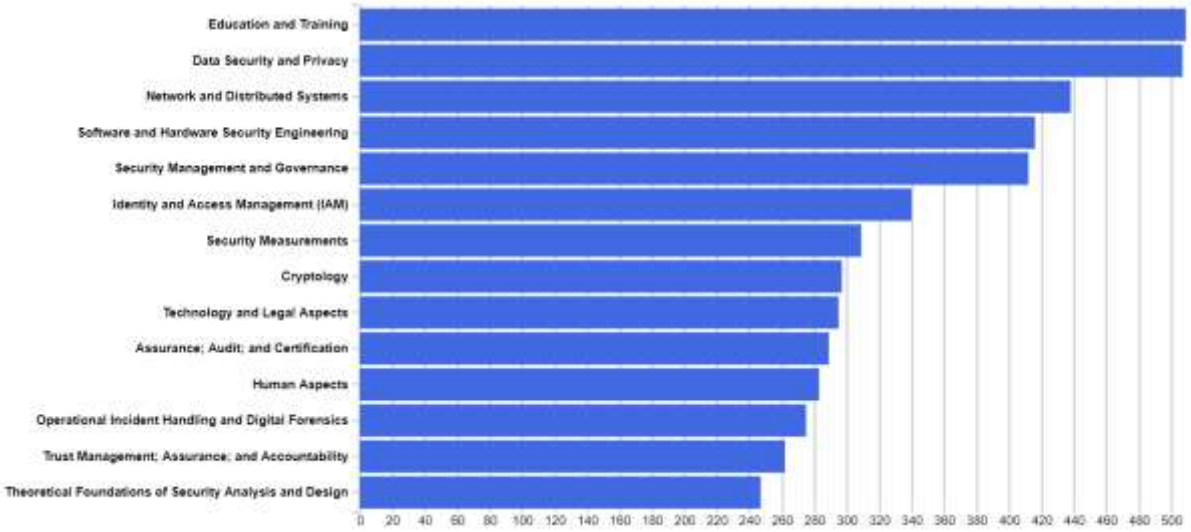


Figure 11. Distribution of participants according to their expertise in the cybersecurity domains.

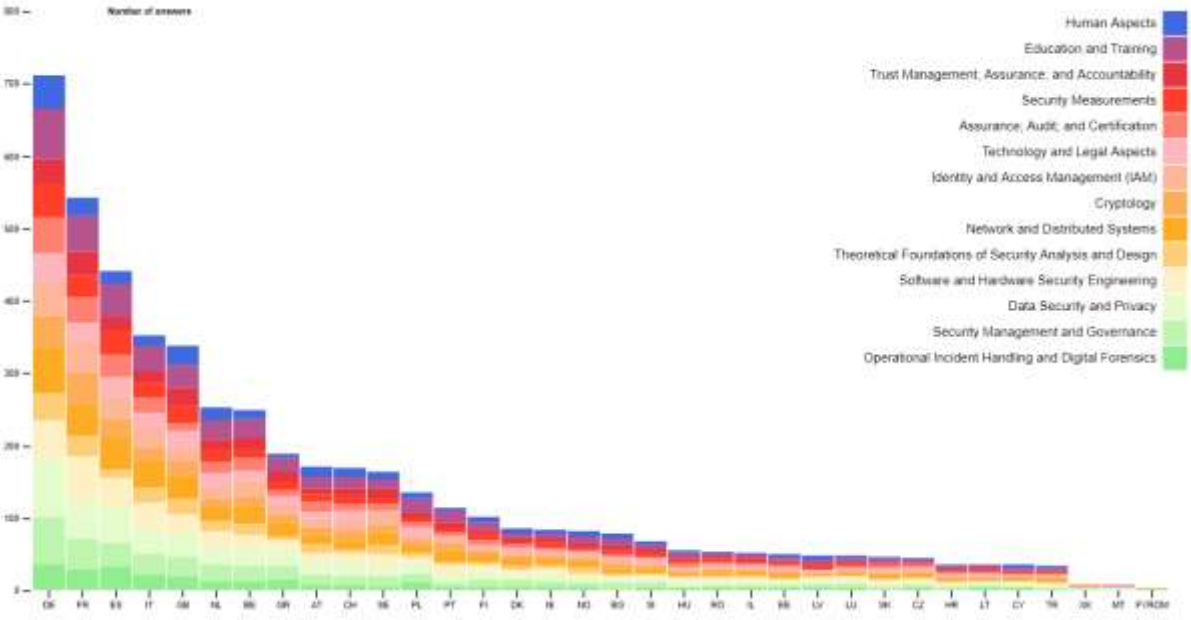


Figure 12. Distribution of domains per country using stacked columns showing total of replies per country and partition per domain.

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.

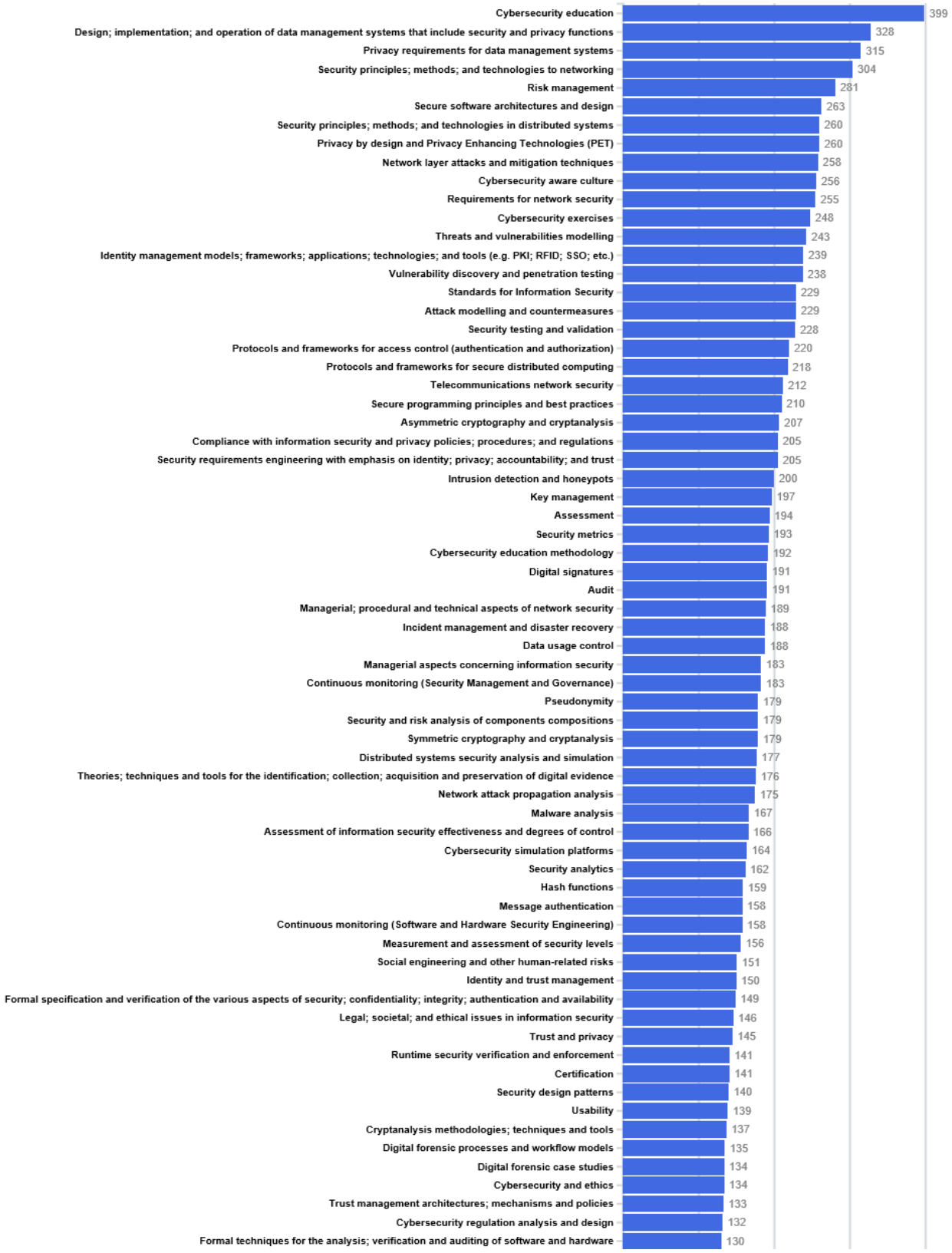


Figure 13. Distribution of participants according to their expertise in the cybersecurity subdomains, first half.

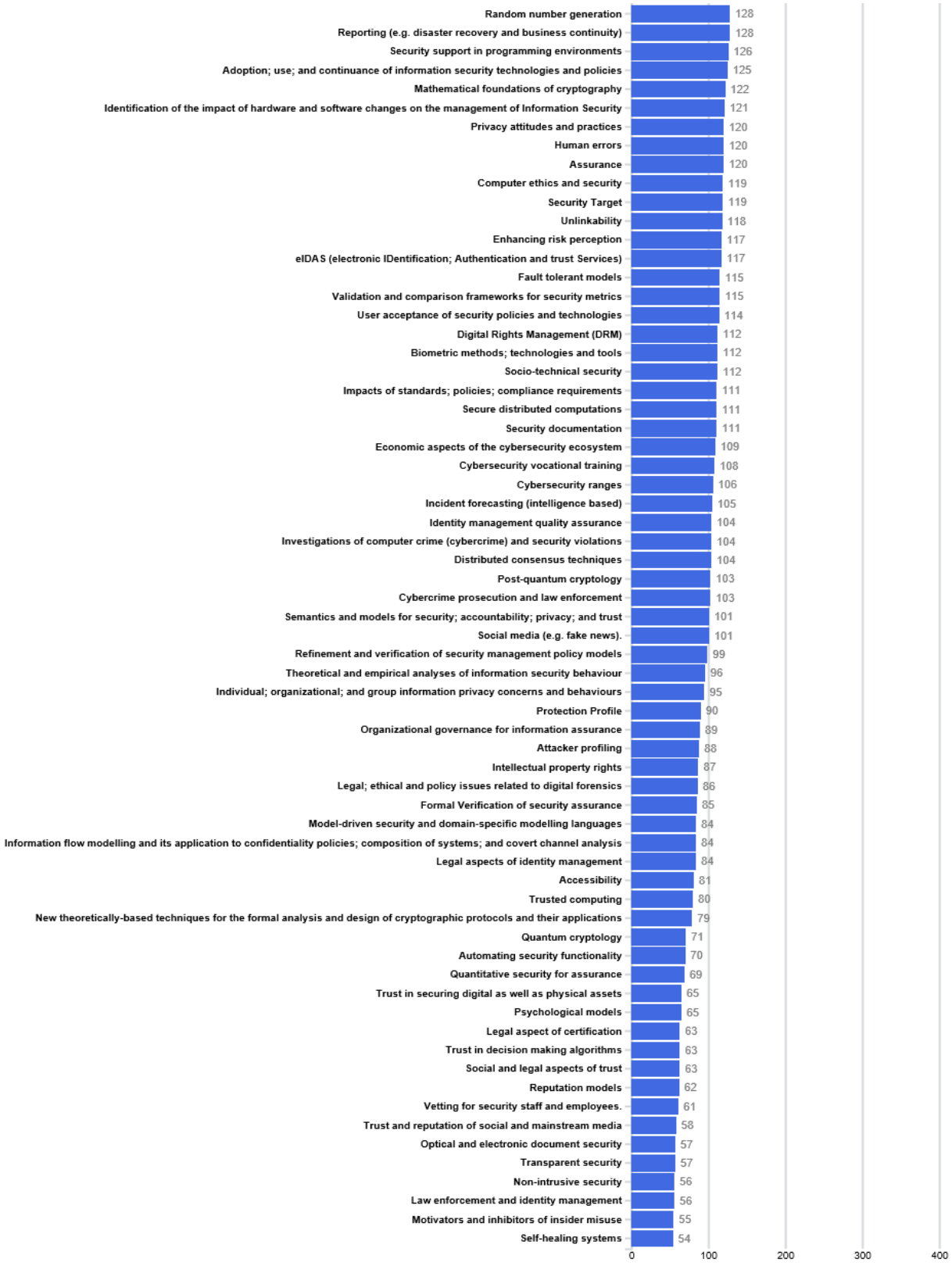


Figure 14. Distribution of participants according to their expertise in the cybersecurity subdomains, second half.

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.

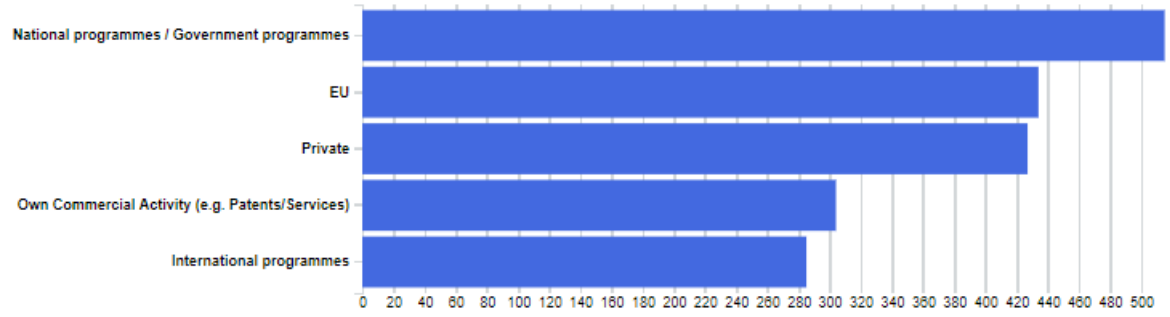


Figure 15. Distribution of funding sources.

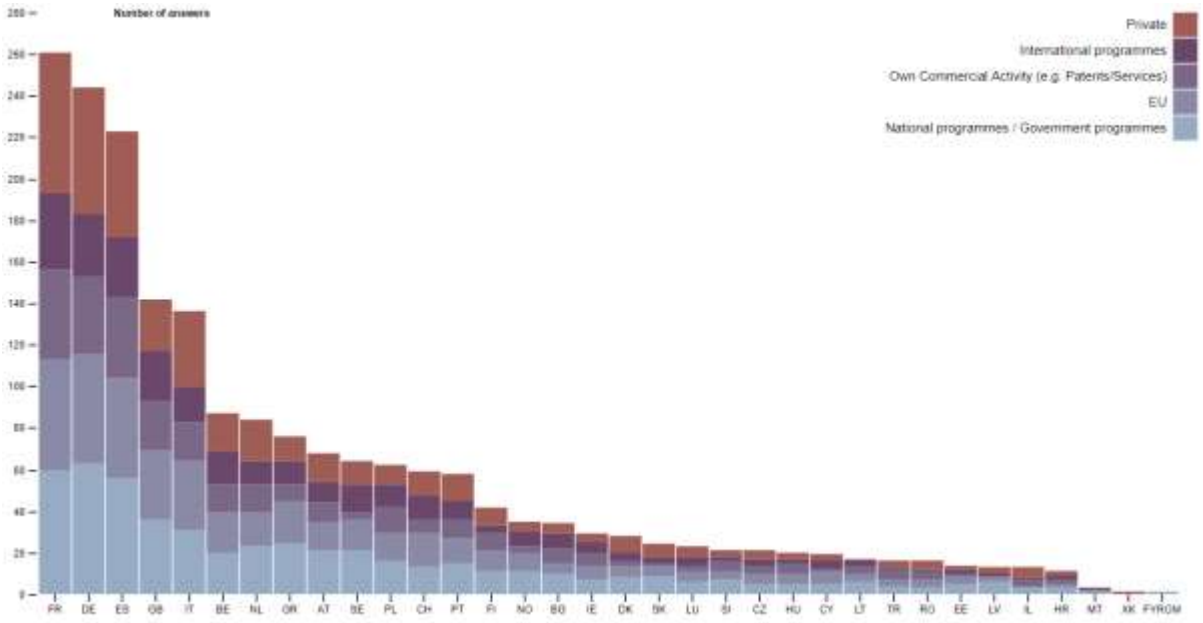


Figure 16. Distribution of funding sources per country.

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).

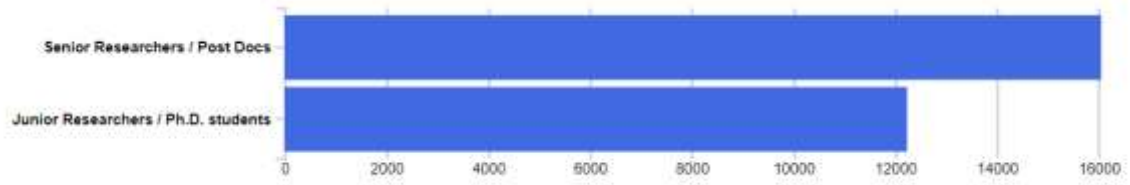


Figure 17. Overall distribution of FTE declared to be working on cybersecurity be all survey participants.

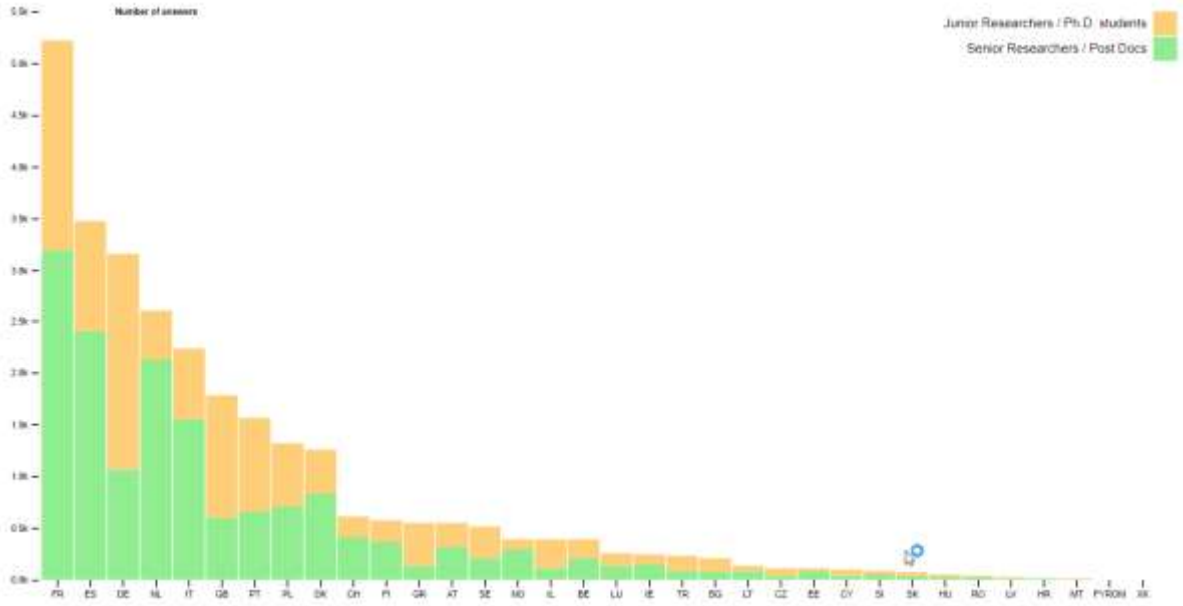


Figure 18. Distribution of FTE working on cybersecurity per country.

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.

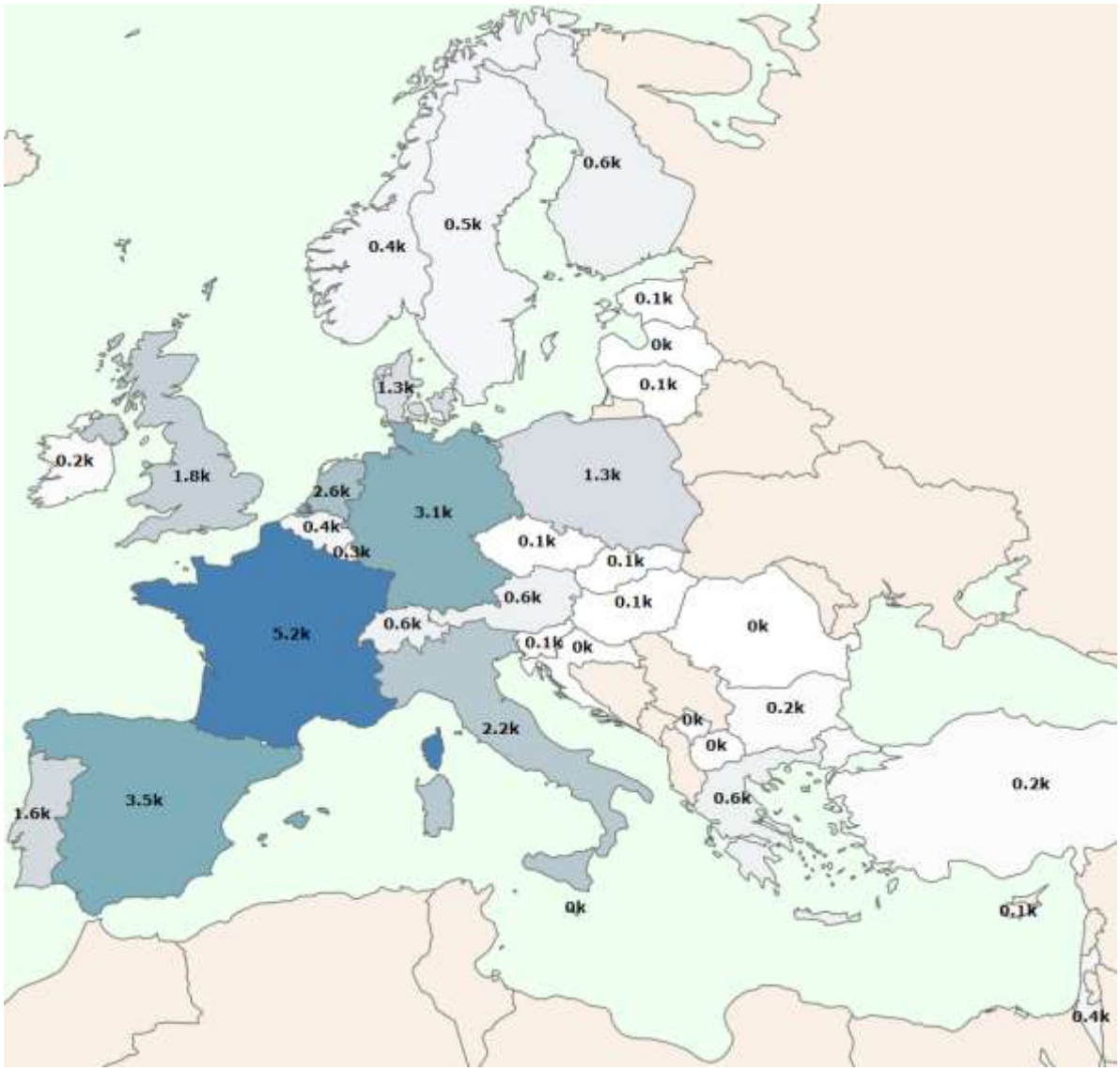


Figure 19. Geographical distribution of FTE working per country showing number of thousands (k) FTE with a color legend indicating with darker blue color countries with a higher number.

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.

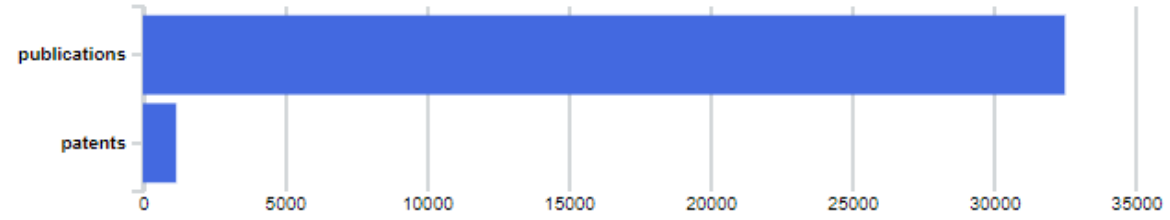


Figure 20. Total number of declared publications.

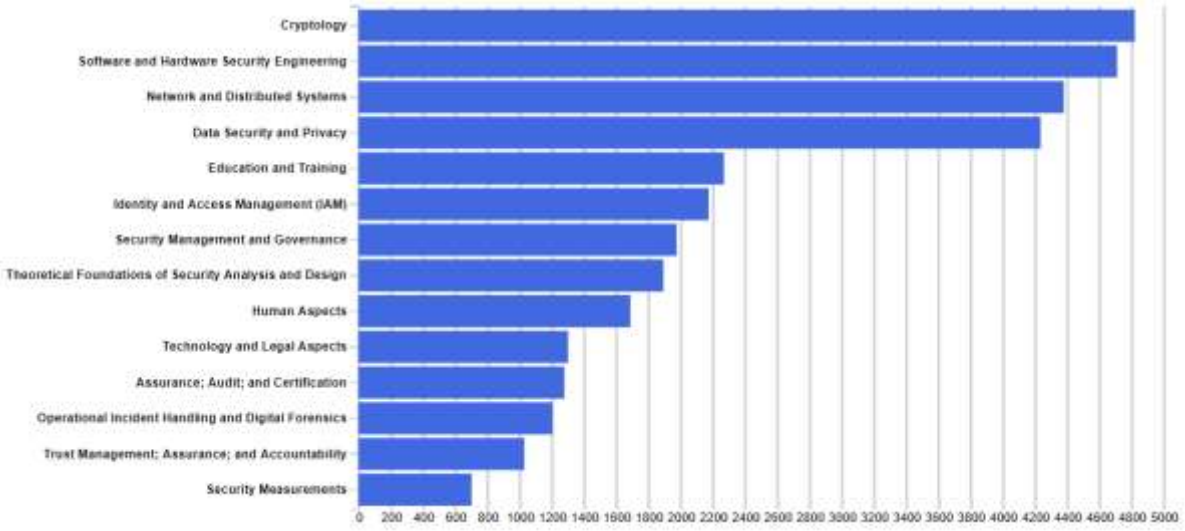


Figure 21. Number of publications reported for each cybersecurity domain.

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.

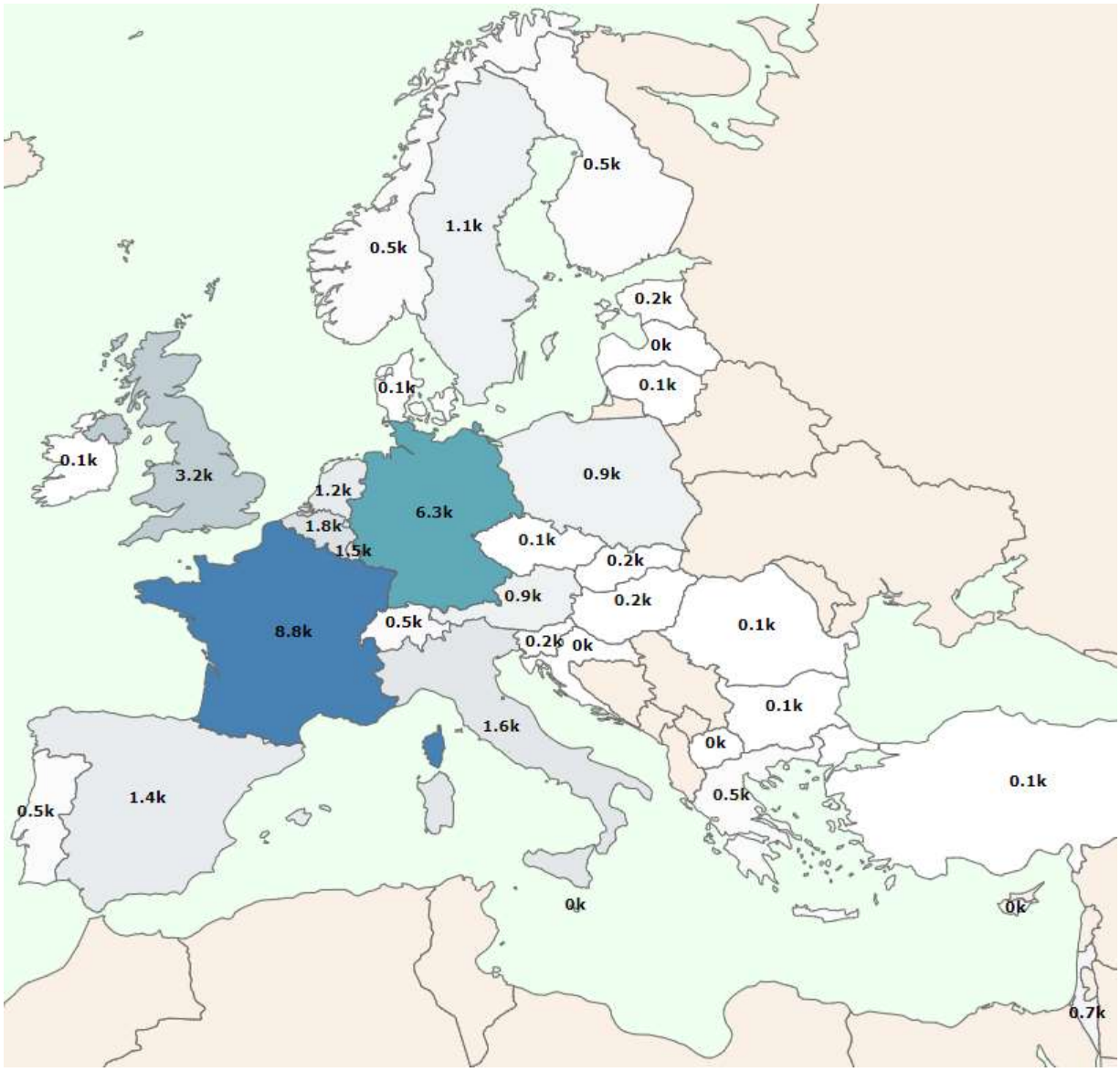


Figure 22. Geographical distribution of total number of publications per country showing number of thousands (k) publications with a color legend indicating with darker blue color countries with a higher number.

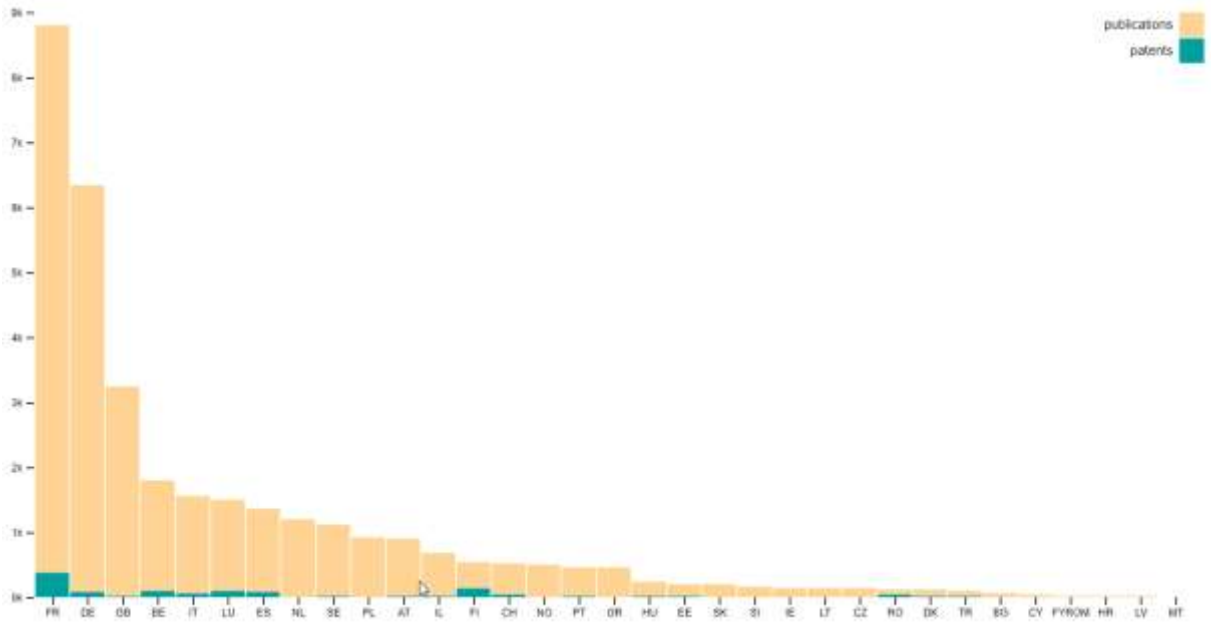


Figure 23. Number of publications per country.

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.

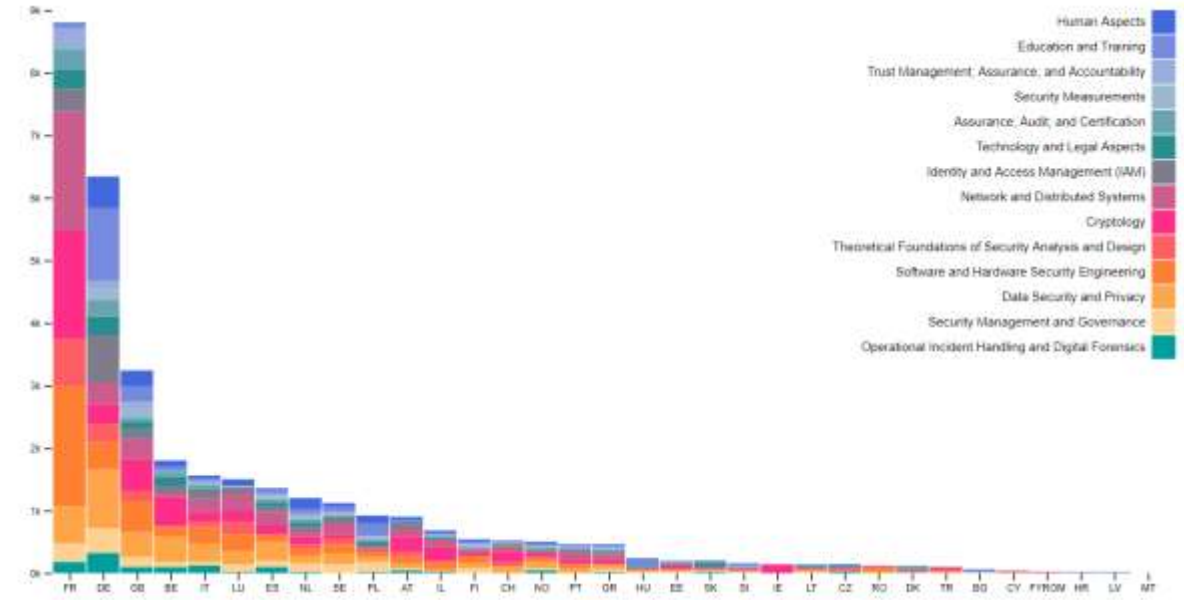


Figure 24. Number of publications for each cybersecurity domain per country.

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.

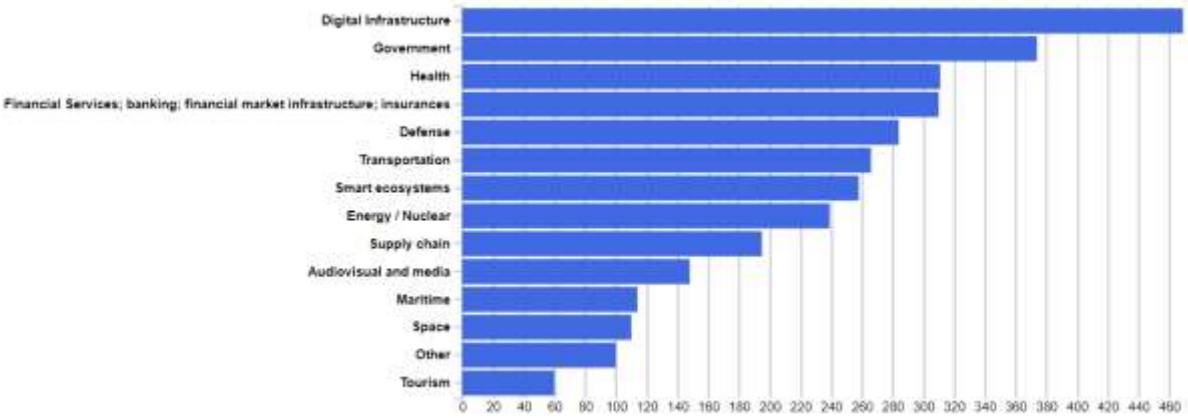


Figure 25. Overall distribution of sectors.

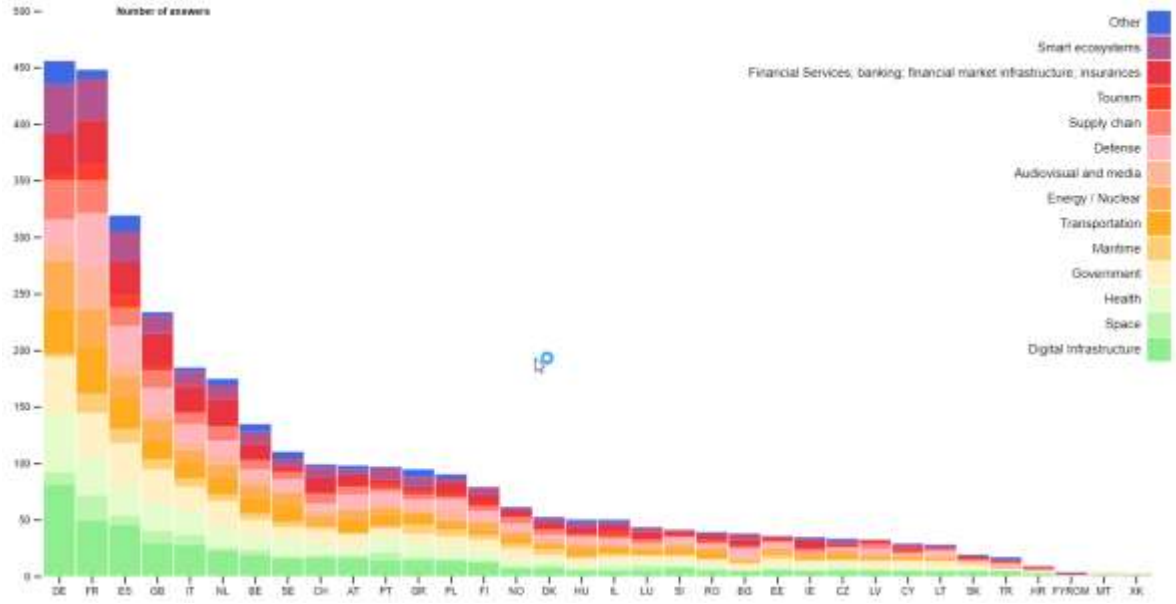


Figure 26. Distribution of sectors per country.

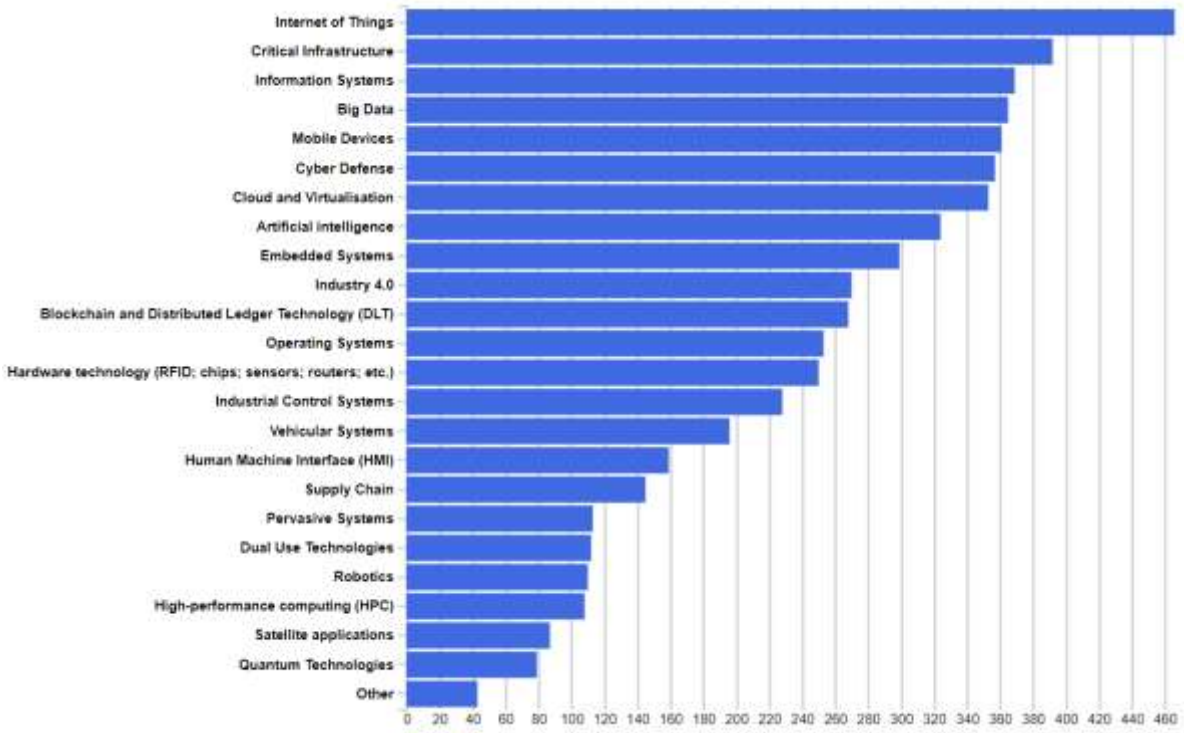


Figure 27. Overall distribution of applications and technologies.

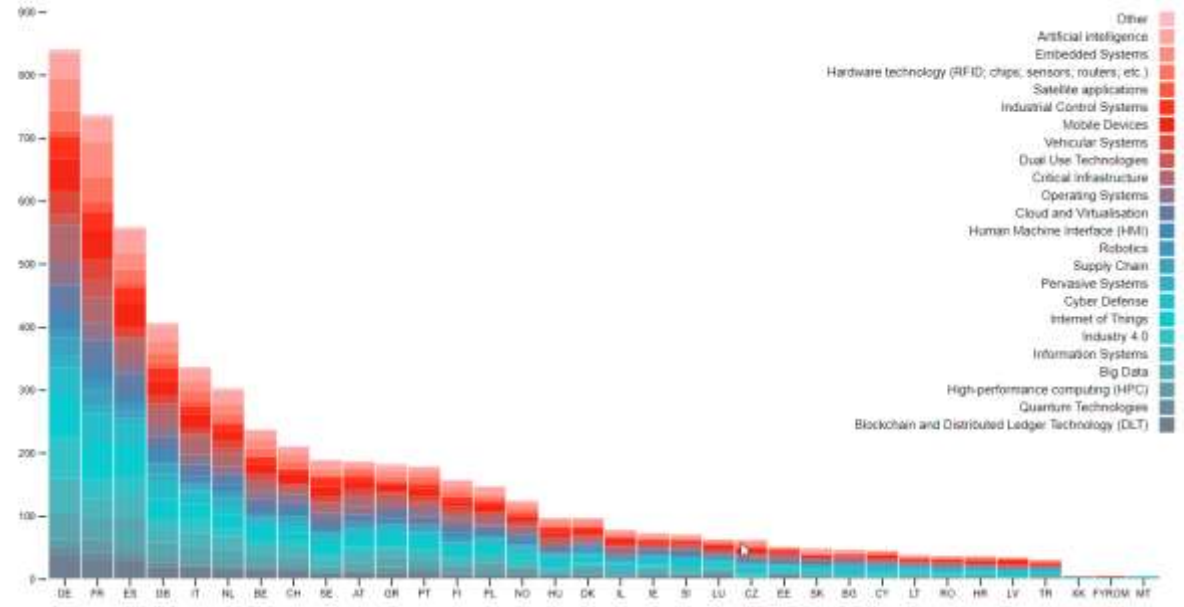


Figure 28. Distribution of applications and technologies per country.

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.

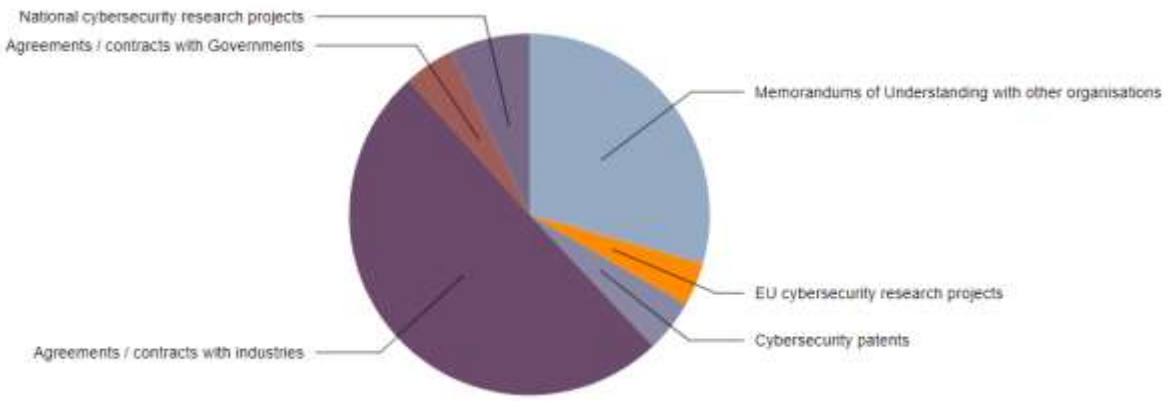


Figure 29. Overall distribution of number of international collaborations or joint programs declared by survey participants.

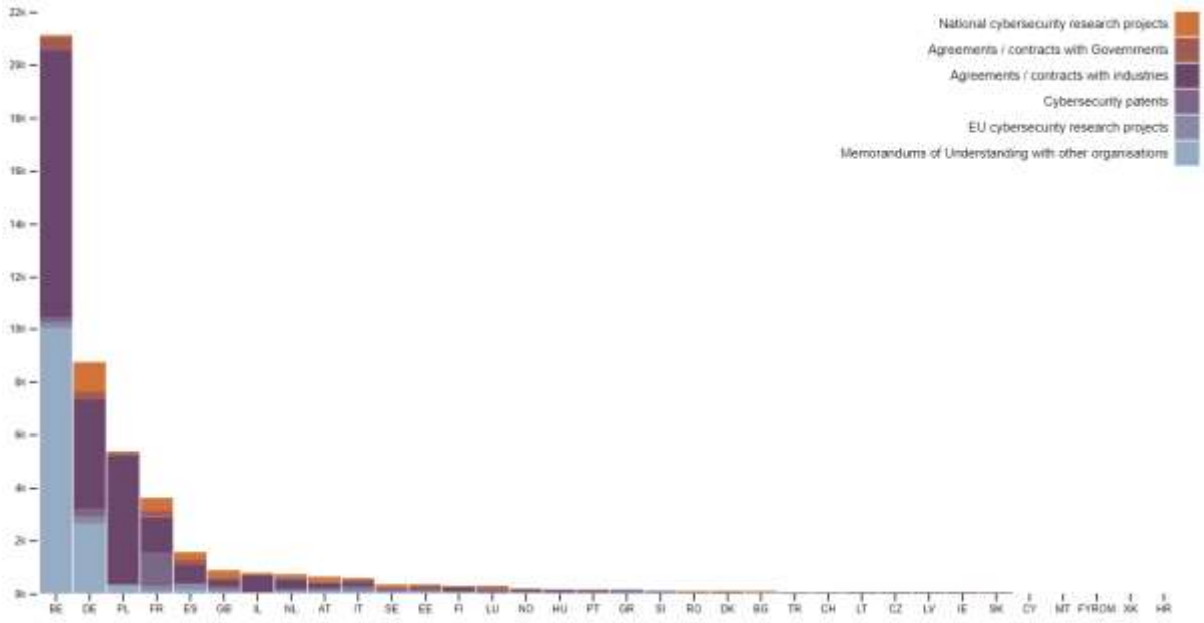


Figure 30. Distribution of number of international collaborations or joint programs declared by survey participants for each country

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;

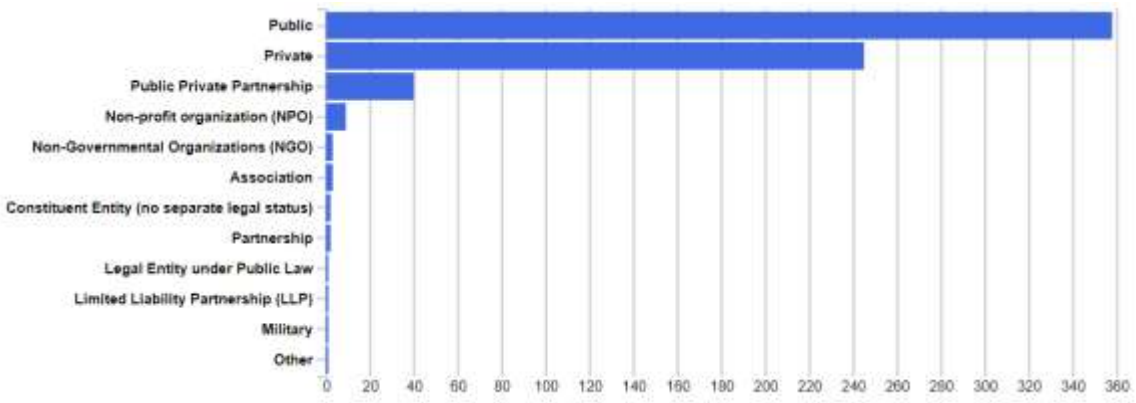


Figure 31. Distribution of participants according to their legal status after manual correction.

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).

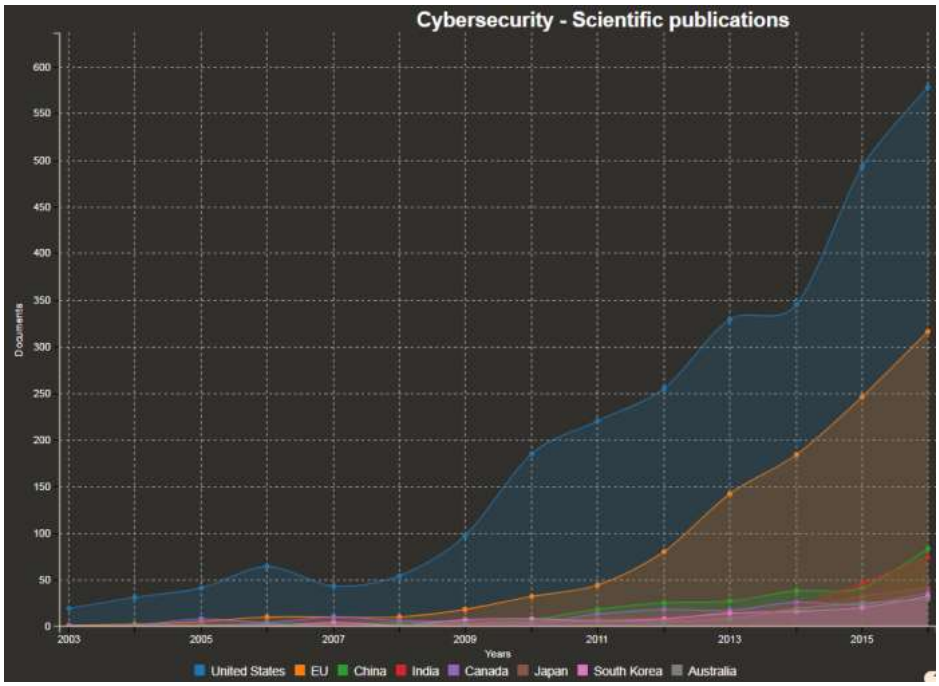


Figure 32. Scientific publications in Cybersecurity per country (Europe = orange).

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**).

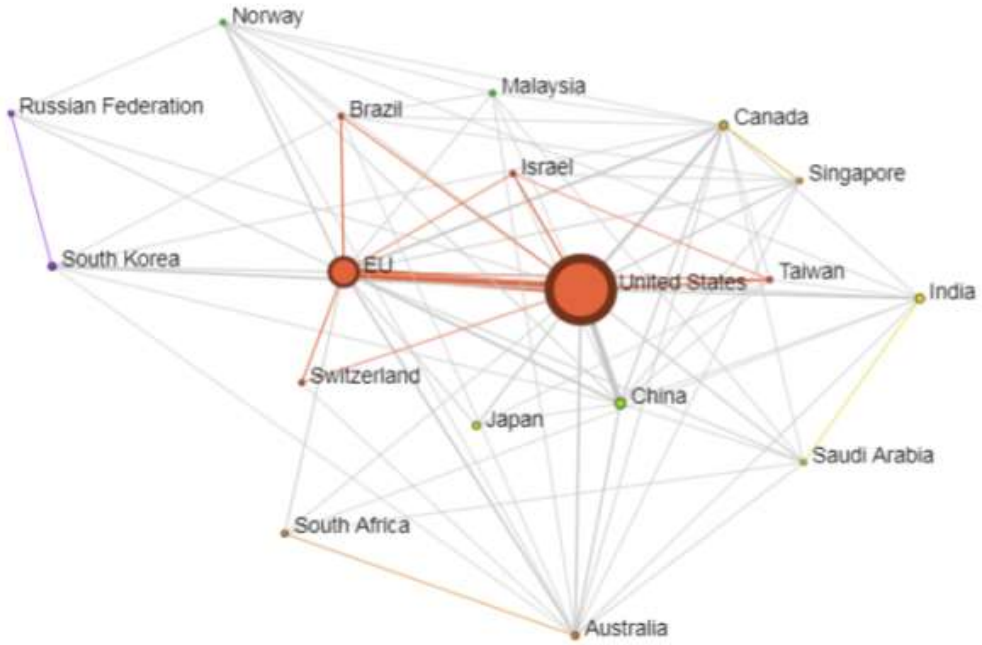


Figure 33. Size of node = Country share of scientific publications in Cybersecurity (size of nodes = number project, edge between nodes = project(s) in common, colours identify communities of countries collaborating more often together).

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**)

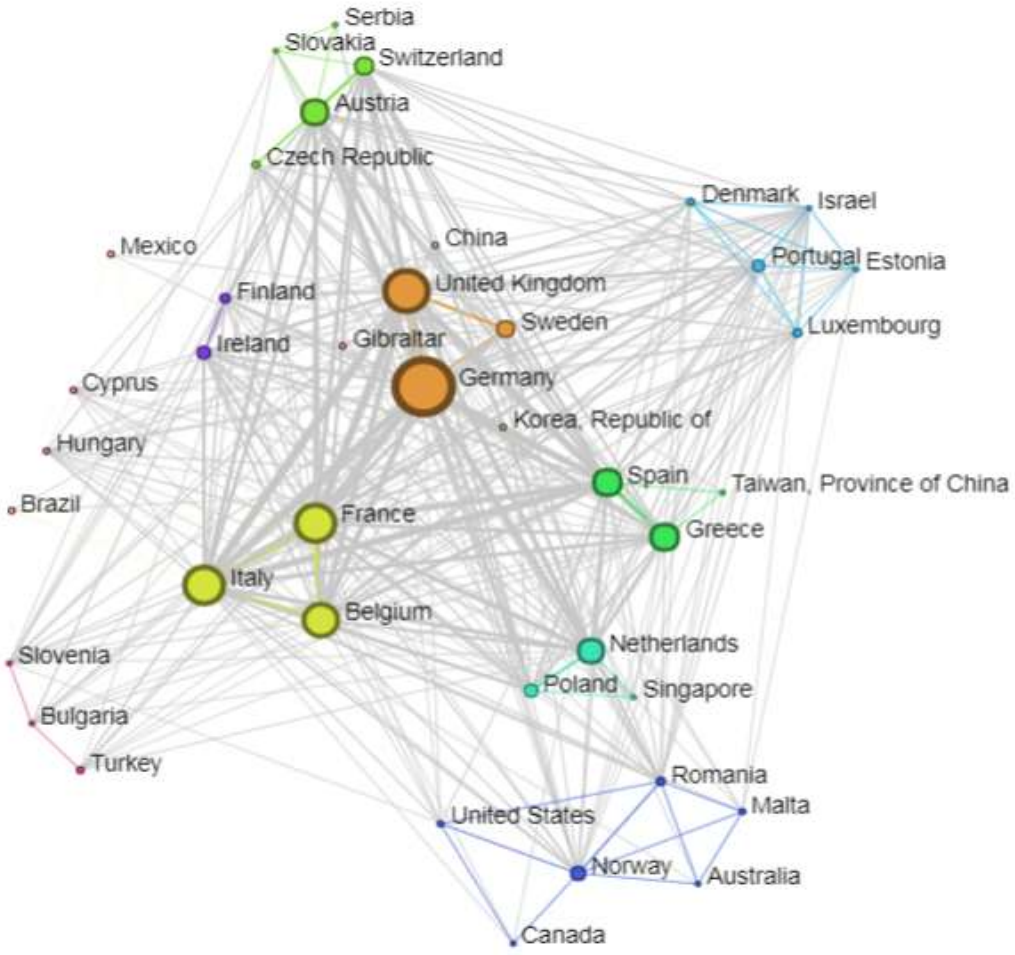


Figure 34. Participants in H2020 Cyber-Security related projects (academic partners).

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.

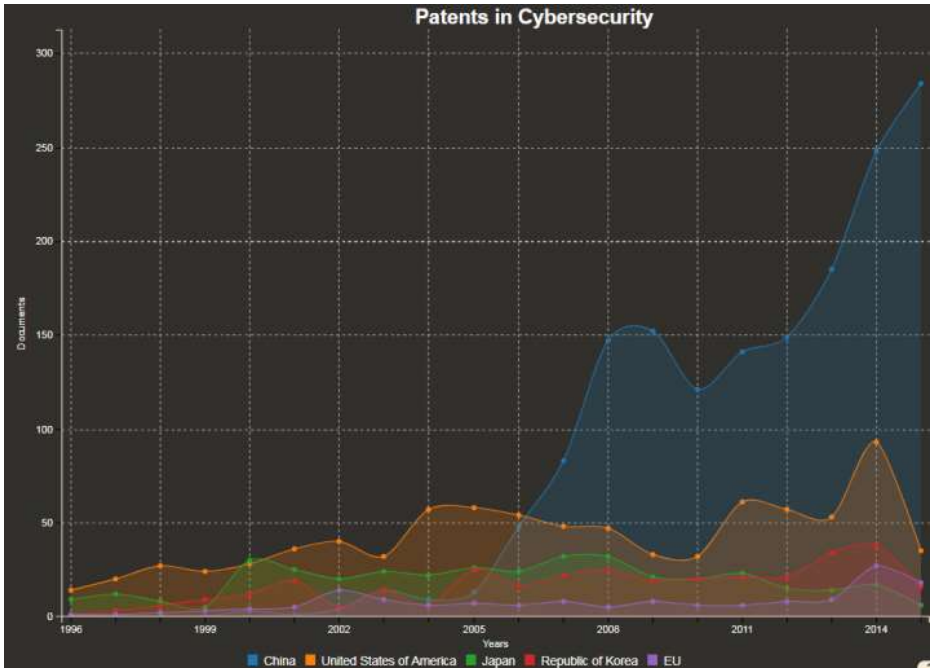


Figure 35. Patents in Cybersecurity per country (Europe = pink)

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%).

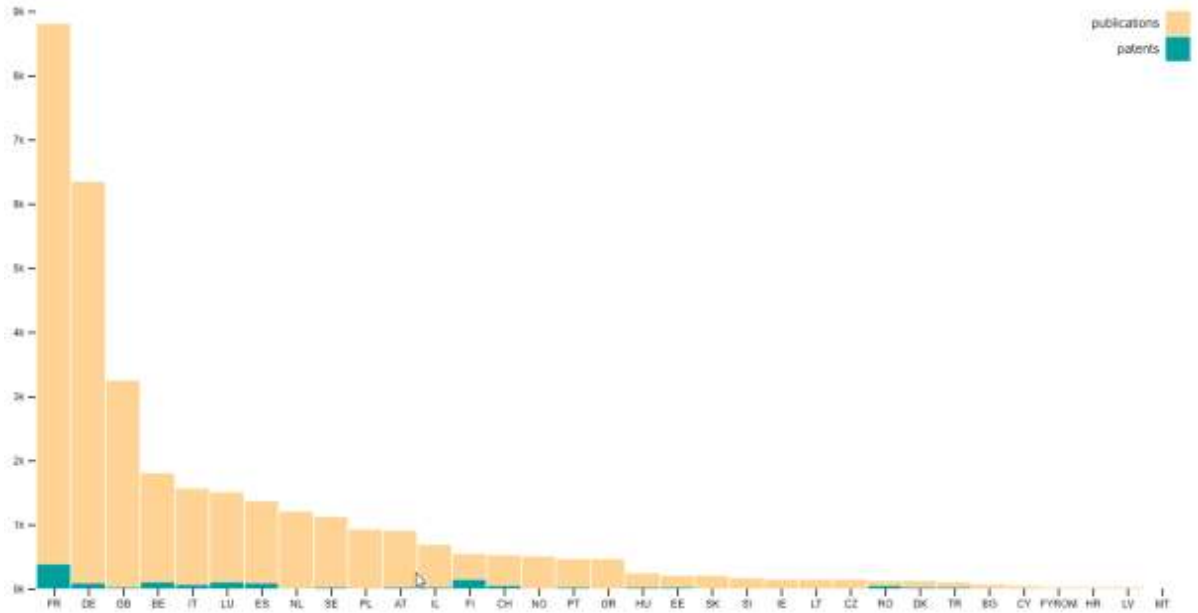


Figure 36. Cybersecurity Publications/Patent ratio per country

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.

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
- [x] 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
- [x] 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

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

Publications Office