



Brussels, 5.7.2016
SWD(2016) 210 final

COMMISSION STAFF WORKING DOCUMENT

**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)**

Accompanying the document

Commission Decision

**on the signing of a contractual arrangement on a public-private partnership for
cybersecurity industrial research and innovation between the European Union,
represented by the Commission, and the stakeholder organisation**

{C(2016) 4400 final}
{SWD(2016) 215 final}
{SWD(2016) 216 final}

Table of Contents

1. EXECUTIVE SUMMARY	3
2. INTRODUCTION	4
3. BACKGROUND TO THE INITIATIVE.....	5
4. DEVELOPED TRUST AND CYBERSECURITY COMPETENCES IN THE PROGRAMME.....	9
5. METHOD	11
6. IMPLEMENTATION STATE OF PLAY.....	12
7. ASSESSMENT OF IMPLEMENTATION AND PARTICIPATION	18
7.1. Cooperation between Research organisations and Industry	18
7.2. Improved coordination of research activities.....	19
7.3. Make critical infrastructures secure	20
7.4. Make cloud and mobile services Cybersecure.....	21
7.5. Make digital authentication a reality.....	21
7.6. Ensure human rights in the cyber world	22
7.7. Standards and certification.....	22
7.8. Ensure cybersecurity knowledge take-up	22
7.9. Improved European industrial competitiveness.....	23
8. CONCLUSIONS	28
8.1. Strong outcomes.....	28
8.2. Weaknesses of the FP7 cooperation and the CIP programme	29
9. ANNEXES.....	30

1. EXECUTIVE SUMMARY

Research and innovation (R&I) form a cornerstone of EU policies to boost jobs, growth and investment. The EU Research and Development Framework Programme 7 (FP7) aimed for a first class knowledge base built on excellent science, and an environment conducive to innovation in Europe. It aimed at fostering innovation that ensures economic prosperity, quality of life and a healthy environment now and in the future. The ambition of FP7 was to create thousands of new jobs and increase Europe's GDP.

The FP7 R&D and the Competitiveness and Innovation (CIP) programme has funded trust and cybersecurity projects during the 7 year length of the programme (2007-2013). This Staff Working Document (SWD) describes what type of partners participated in FP7 cybersecurity related projects and assesses to what extent these projects have contributed to the FP7 objective of excellent science and a stronger ecosystem and clustering of cybersecurity companies, research centres and universities in Europe.

The SWD assessment finds that the trust and cybersecurity part of FP7 has mobilized many research centres, universities and organisations in Europe and beyond. This has resulted in world leading competence in Europe in domains such as cryptography. Industrial partnerships within a competence domain¹ have started to emerge. The participants reflected a broad spectrum of cybersecurity actors. Half of participants were organisations active in one of the critical sectors, as specified in the network and information security (NIS) directive or in securing the Internet infrastructure² and nearly one out of five were active in securing critical services such as cloud and e-commerce services.

But there are gaps as the detailed analyses in the SWD illustrates. Only some critical sectors participated in the programme. As an example the health sector, also a critical sector, has been largely absent in the programme.

The programme was also successful in maintaining the support for the objective to build a real-life mature environment for digital authentication across several jurisdictions with high levels of assurance. More than one out of 10 participations was in support of this objective or underlying technologies such as smart cards and biometry.

The establishment of a world class competence in the domain of encryption indicates the potential of European technologies funded by the programme in contributing to safeguarding the rights of citizens in the cyber world. In addition the competence contributes to several other objectives such as authentication, identification, eIDAS etc.

The programme assured participation of standardisation organisations, through European experts that participated in diverse international standardisation efforts. In the current setting with a new NIS directive asking for best practices, which in engineering environments translate to standards, norms, certificates and audits, a higher participation is recommendable.

¹ Partnership ATOS and Cassidian Link: http://atos.net/en-us/home/we-are/news/press-release/2015/pr-2015_09_28_01.html

² Telecom framework directive Art 13a

One out of 10 participants was a consultancy organisation that transfers knowledge to users. Two thirds of these users however could be classified as telecom organisations which leaves the question open if a better balancing over other user groups would not be desirable.

While the projects that obtained an EU grant from the programme have achieved impact in the scientific world through their deliverables and publications, it is unclear whether they produced successful outcomes that can contribute to the overall goal of EU competitiveness and growth. As an example, Europe has world class competence in cryptography but European companies do not have a market presence, within the EU and globally, that aligns with the strong technological position.

A conclusion of this assessment is that the FP7 and CIP programme has been used by the participants to increase their knowledge and to raise the state of the art in the cybersecurity domain. However, the exploitation of the accumulated competences to serve the European customers, citizens as well as organisations and governments, is weak. Cybersecurity researchers leave the EU ecosystem to join US based organisations, promising start-ups are bought by non-European incumbents, etc. The risk that Europe is not able to establish a living ecosystem of companies and organisations that deliver trust and cybersecurity technology and solutions, and will therefore miss the opportunity to fill all the job openings that result from the operational cybersecurity needs created by increasing cyber threats is real.

2. INTRODUCTION

The purpose of the SWD is to assess the implementation of and participation in the Trust and Cybersecurity projects that received funding from the FP7 R&D programme and the CIP programme during the 7 year Multiannual Financial Framework (2007-2013 when the last FP7 and CIP call addressing Trust and Cybersecurity was published).

This SWD is not a fully-fledged evaluation, since the FP7 programme and CIP programme³ has already been the object of an ex-post evaluation⁴.

The rationale for assessing the implementation of and participation under FP7 and CIP is twofold: (1) assess whether grants under these programmes have contributed to a stronger ecosystem of cybersecurity companies in Europe supporting the European citizens, organisations and governments, and (2) to map the topics that have been funded in the past against existing and future EU regulations and policy priorities, in particular the Digital Single Market Strategy, the (announced) NIS directive, and the Data Protection rules, to help identify gaps to be addressed by the cybersecurity contractual PPP.

The scope of the assessment comprehends the Cybersecurity R&D and CIP programme in FP7 that made 334 M€ in grants available for the project participants between 2007 and 2013. The concerned calls can be found under the heading "Implementation of State of Play".

³ Final evaluation of the competitiveness and Innovation programme.
http://ec.europa.eu/cip/files/cip/cip_final_evaluation_final_report_en.pdf

⁴ SWD(2016)2 final 19.1.2016 Ex-Post Evaluation of the Seventh Framework Programme

3. BACKGROUND TO THE INITIATIVE

Research and innovation (R&I) form a cornerstone of EU policies to boost jobs, growth and investment. The EU Research and Development Framework Programme 7 (FP7) aimed for a first class knowledge base built on excellent science, and an environment conducive to innovation in Europe. It aimed at fostering innovation that ensures economic prosperity, quality of life and a healthy environment now and in the future. The ambition of FP7 was to create thousands of new jobs and increase Europe's GDP.

The FP7 programme has funded many trust and cybersecurity projects during the 7 year length of the programme (2007-2013). This document assesses which projects and project partners benefited from the FP7 grants and how these grants have contributed to a stronger ecosystem of cybersecurity companies in Europe.

The following eight specific policy objectives for FP7 were identified in the Impact Assessment report (see footnote 6):

- (1) enhancing the competitiveness of European industry through joint technology initiatives;
- (2) increasing European-wide S&T collaboration and networking for sharing R&D risks and costs;
- (3) contributing to an increase in the level of research investment;
- (4) improving the coordination of European, national and regional research policies;
- (5) strengthening the scientific excellence of basic research in Europe through increasing coordination and competition at European level;
- (6) promoting the development of European research careers and making Europe more attractive to the best researchers;
- (7) providing the knowledge-base needed to support key Community policies; and
- (8) increasing availability, coordination and access in relation to top-level European scientific and technological infrastructure.

The FP7 Trust and Security Programme funded a significant number of projects that address the cybersecurity gaps in today's ICT systems. The cross-national research aimed to increase the competitiveness of European organisations in this area of research and to ensure that European cybersecurity state of the art would rise to a higher level for European citizens and businesses, in line with EU legislation.

The forthcoming **Network and Information Security (NIS) Directive**⁵ – proposed by the Commission in 2013 on which a political agreement between the European Parliament and the Council has been reached end of 2015 – aims to ensure a high common level of cybersecurity in the EU, by: Improving Member States' national cybersecurity capabilities; Improving cooperation between Member States, and between public and private sectors; Requiring companies in critical sectors – such as energy, transport, banking and health – as well as key Internet services to adopt risk management practices and report major incidents to the national authorities. The NIS Directive is expected to bring many benefits: Citizens and

⁵ <https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive>

consumers will have more trust in the technologies they rely on daily; Governments and businesses will be able to rely on digital networks and infrastructure to provide their essential services at home and across borders; and the EU economy will reap the benefits of more reliable services and a culture of systematic risk management and incident reporting – creating more equal and stable conditions for anyone trying to compete in the Digital Single Market.

The **EU Data Protection** framework ensures that personal data can only be gathered under strict conditions and for legitimate purposes. Organisations that collect and manage your personal information must also protect it from misuse and respect data subjects' rights. In 2012, the Commission proposed a major reform of the EU legal framework on the protection of personal data which resulted in the recently adopted Regulation 2016/679 (General Data Protection Regulation – GDPR) and Directive 2016/680. The new proposal strengthens individual rights and tackles the challenges of globalisation and new technologies. A political agreement was reached end of 2015 on the GDPR⁶ which entered into force on 25 May 2016 and will be applicable as of 25 May 2018.

The **ePrivacy Directive** (Directive on Privacy and Electronic communications) builds on the EU telecoms and data protection frameworks to ensure that all communications over public networks maintains a high level of privacy, regardless of the technology used. This Directive was updated in 2009 to provide clearer rules on 'users' rights to privacy. This link with data protection is important because Telecom operators and Internet Service Providers hold a huge amount of user's data, which must be kept confidential and secure. Such information must be protected, e.g. against unauthorised access or being stolen. Furthermore, under this Directive the provider must report any "personal data breach" to the national competent authority and, in certain circumstances, also notify the subscriber or individual.

The review of the ePrivacy Directive – announced in May 2015 in the Digital Single Market Strategy and made necessary with the adoption of the GDPR – is one of the key initiatives aimed at reinforcing trust and security in digital services in the EU with a focus on ensuring a high level of protection for citizens and a level playing field for all market players.

The **Telecom Framework Directive** has as one of its objectives the insurance of the integrity and security of public communications networks (Article 8, paragraph 4(c) and (f)). Specific rules are provided for in order to ensure that operators take appropriate technical and organisational measures to appropriately manage the risk posed to security of networks and services and to guarantee the integrity of their networks and thus the continuity of supply (Article 13a and Article 13b of the Framework Directive).

The eIDAS components⁷: Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 and entered into force on September 17, 2014 provides a regulatory

⁶ 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), OJ L 119, 4.5.2016, p. 1–88, which will be applicable as of 25 May 2018.

⁷ <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

Taking into account the overall eight FP7 objectives⁸ presented above and the more specific Cybersecurity objectives that have been identified in FP7 and CIP Work Programmes relevant for the calls, the list of Cybersecurity R&I themes covered were the following:

1. **Improved European industrial competitiveness** in markets of trustworthy ICT, offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.
2. **Widen take-up of research outcomes and increase the number of European start-ups in the field.**
3. **Improve security and dependability of networks and service infrastructures.**
4. **Wider use of metrics, standards, evaluation and certification⁹ methods and best practices in security** of networks, infrastructures, software and services.
5. **Make critical infrastructures, such as energy, information and communication networks, sensitive manufacturing, finance, healthcare, or transportation systems more secure and dependable.**
6. **Support to users to make informed decisions on the trustworthiness of ICT.**
7. **Security, privacy and personal data protection -preserving technical solutions in clouds, mobile services and management of cyber incidents** in compliance with privacy and personal data protection legislation.
8. Development and implementation of European strategies for internet security. **Significant contribution to making Internet a medium that can be used to exercise human rights, including in hostile environments.**
9. **Improved coordination and integration of research activities** in Europe or internationally.
10. **A real-life mature environment for digital authentication across several jurisdictions with high levels of assurance.**

⁸ SWD(2016)2 final 19.1.2016 Ex-Post Evaluation of the Seventh Framework Programme.

⁹ Certification methods are laid down under Decision 768/2008.

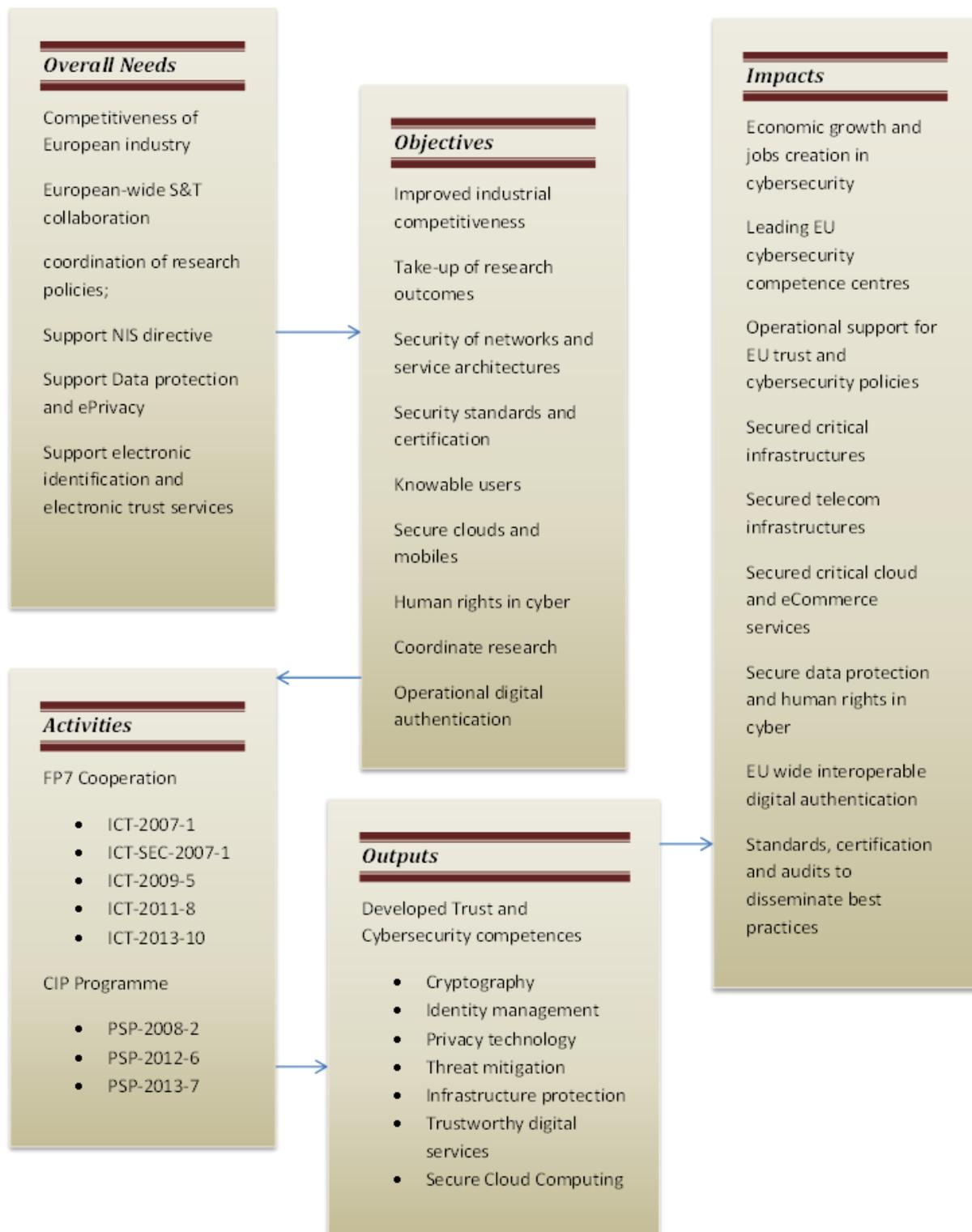


Figure 1: Intervention logic

4. DEVELOPED TRUST AND CYBERSECURITY COMPETENCES IN THE PROGRAMME

This section illustrates the research and innovation carried out by the projects in the FP7 Trust and Cybersecurity programme through qualitative examples.

An indication of the positive contribution that FP7 delivered to competence building is illustrated by the following project outcomes:

- The European Union established a name in Cryptography with FP7 projects such as the European Network of Excellence in Cryptology (Ecrypt II); Computer Aided Cryptography Engineering (CACE); Secure, Embedded Platform with advanced process isolation & Anonymity Capabilities (SEPIA); and Trusted Revocable Biometric Identities (TURBINE).
- Identity Management and Authentication, supporting eIDAS was well addressed through the FP7 programme with projects such as: Secure Identity Across Borders Linked (STORK); Authentication and Authorisation for Entrusted Unions (AU2EU); Shaping the Future of Electronic Identity (FutureID); Trusted Architecture for Securely Shared Services (TAS3); and Secure widespread identities for federated telecommunications (SWIFT).
- Privacy Enhancing Technologies was another priority of the programme to support the Data protection Directive, the e-Privacy Directive and the forthcoming GDPR. Some of the FP7 projects that retained attention are: Attribute-Based Credentials for Trust (ABC4Trust); Privacy and Identity management for community services (PICOS); Privacy and Identity Management in Europe for Life (PrimeLife); Context-aware data-centric information sharing (Consequence); and Privacy-aware Secure Monitoring (PRISM).
- The Threat Detection and Mitigation priority focused on combatting network induced threats. Projects that belong to the portfolio that address this priority are: Worldwide Observatory of Malicious Behaviours and Attack Threats (Wombat); Nippon-European Cyber-defense Oriented Multilayer threat Analysis (NECOMA); and Securing Websites through Malware Detection and Attack Prevention Technologies (SWEPT 22).
- The Critical Infrastructure Protection priority is inspired on the forthcoming Network Information Security directive and the fact that cyber-attacks in critical sectors can have devastating results. Competence building FP7 projects that supported this priority are "A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet (SYSSEC)"; a "Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures (MICIE); and a "Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security (TRESPASS).
- FP7 was also successful in maintaining the support for the objective to build a real-life mature environment for digital authentication across several jurisdictions with high levels of assurance. 12% of the participations in the programme supported this objective and made the realisation of the eIDAS possible. This stronghold in the domain is due to maintained investments in SMARTCARD and BIOMETRY related

technologies and in support for the eIDAS legislation. It found support from the FP7 projects "a Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS)"; Secure provision and Consumption in the Internet of Services (SPaCIOS); Policy and Security Configuration Management (PoSecCo); and "Holistic Approaches for Integrity of ICT-Systems (HINT)".

- Secure Cloud Computing is indispensable in cybersecurity and was supported by FP7 projects such as: Trustworthy Embedded systems for Secure Cloud Computing Applications (TRESCCA); Trustworthy Clouds – Privacy and Resilience for Internet –scale Critical Infrastructure (TLOUDS); Privacy-Preserving Computation in the Cloud (PRACTICE); Confidential and Compliant Clouds (Coco Cloud); and the "Secure Provisioning of Cloud Services based on SLA management (SPECS).

While the above takes a qualitative approach, illustrating the output of the FP7 programme through some of its projects, this document complements it with a quantitative approach. This is illustrated in Annex 9.4, which complements the qualitative examples with a graphical representation of the established links between project partners through their project participations and Annex 9.5, which illustrates participants benefitting from more than one grant under the programme and how contributes to competence clusters as described above. One competence cluster easily spotted is the Cryptology cluster for which the University of Leuven is a competence centre.

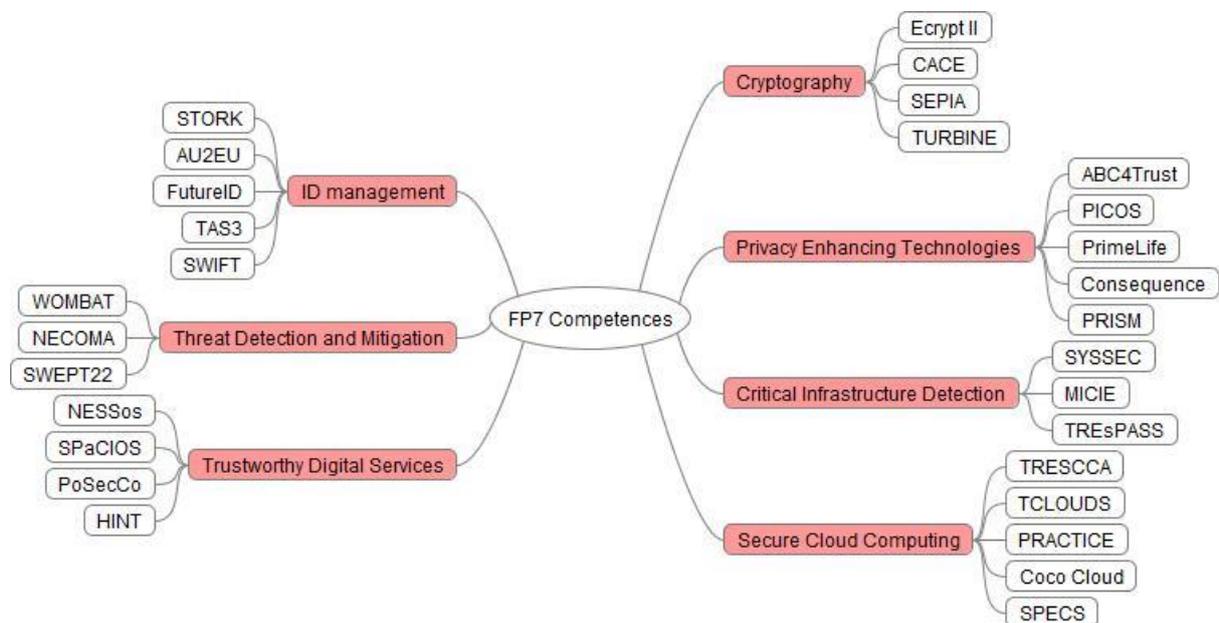


Figure 2: Developed FP7 Competences

5. METHOD

The methodology used is that of a desk top study exploring published material and internal data of the European Commission.

This SWD draws upon the findings of the report "*An Analysis on EU Security and Trust R&D Projects*"¹⁰, one of the deliverables of the SECCORD FP7 project and an annex of the "Research and Innovation Yearbook 2015" of the same project, and on analysis conducted by ENISA. More information can be obtained from the authors of this yearbook¹¹.

The statistics on the EU grant data come from the FP7 data held in the EU – DG CONNECT internal project data database. The period covered by the statistics is grants paid throughout the lifetime of these projects (2007 – 2016).

In this report the proxy used to analyse the achievement of objectives was the type and number of participants in the projects that received grants through the FP7 programme and the size of these grants. Retrievable indicators used throughout the assessment are: the nature of participants - large and small; different sectors; the geographical distribution of R&I efforts across the EU; contribution to EU added value and clustering; relevance of funded themes for EU legislative and policy objectives; and the strengthening of EU competitiveness.

To ensure a level of consistency the SWD complements and cross checks the material obtained through the different reports with the grant and participations data available from its internal MIS database.

The section on "Implementation state of play" investigates the characteristics of the partners in the FP7 calls that address trust and cybersecurity (Call 1, 5, 8 and 10) and the CIP calls and analyses the constituencies. It also assesses the participants in FP7 against the objectives defined throughout the FP7 trust and security research programme. The section 7 "Assessment of implementation and participation" analyses the FP7 project participations that successfully have been completed under the rules defined for FP7. It provides the reader with information on the characteristics of successful partners in the FP7 cybersecurity research programmes.

Partial data on patents and publications from the projects ongoing in the years 2007 -2013 come from the study "*Analysis of publications and patents of ICT research in FP7*"¹².

This assessment cannot and does not present a complete picture of FP7 results and impacts. The first reason (1) is that this assessment builds to an important extent on the data and graphs that have been collected from a report that was not commissioned with the purpose to deliver an assessment of the outcome of the framework programme. In addition (2), research

¹⁰ By Martina de Gramatica, Fabio Massacci and Woohyun Shim University of Trento on October 2015

¹¹ Department of Information Engineering and Computer Science, University of Trento. Martina de Gramatica, Prof. Fabio Massacci, Dr. Woohyun Shim

¹² SMART 2011/0039 which main results are published in: Jacob, J., Sanditov, B., Smirnov, E., Wintjes, R., Surpatean, A., Notten, A., & Sasso, S.. Brussels, European Commission.

projects take time to produce societal impacts: it takes years before the new knowledge generated within the scope of a single project or a portfolio of projects is valorised in the form of new products, processes, services and economic, social and environmental impacts¹³.

6. IMPLEMENTATION STATE OF PLAY

In order to realise the objectives outlined in section 2, the FP7 **cooperation** specific programme defined 5 calls addressing Cybersecurity R&D and the PSP (CIP) programme had 3 specific calls: " Biometrics + Identity Management", "Fighting Botnets" and "Website Security and Biometrics".

The total amount of EU grants distributed to participants in these funded projects amounts to € 334 million.

The FP7 'Cooperation' Specific Programme¹⁴ for Trust and Cybersecurity supported trans-national cooperation on policy-defined key scientific and technological themes. Across all these themes, support for trans-national cooperation was implemented through collaborative research and international cooperation. The Trust and Cybersecurity FP7 Cooperation Calls which have been analysed are:

- FP7-ICT-2007-1 (Identity management and privacy enhancing tools; Security and resilience in network infrastructures; Security and trust in dynamic and reconfigurable service architectures; Trusted computing infrastructures),
- FP7-ICT-SEC-2007-1 (Critical Infrastructure Protection),
- FP7-ICT-2009-5 (Technology & Tools, Mobile Devices and Smartphones; Trustworthy Network Infrastructures; Cloud Security; Trustworthy Service infrastructures; Privacy Management),
- FP7-ICT-2011-8 (Data policy, governance and socio-economic ecosystems; Heterogeneous networked, service and computing environments; Trust, e-identity and privacy management infrastructure),
- FP7-ICT-2013-10 (Security and privacy in cloud computing; Security and privacy in mobile services; Development, demonstration and innovation in cyber security) and

The Competitiveness and Innovation Framework Programme (CIP) running from 2007-2013 had the following objectives: (1) to foster the competitiveness of enterprises, in particular of SMEs; (2) to promote all forms of innovation including eco-innovation; (3) to accelerate the development of a sustainable, competitive, innovative and inclusive information society; and to promote energy efficiency and new and renewable energy sources in all sectors, including transport.

¹³ See also the conclusions of the SWD(2016)2 final 19.1.2016 Ex-Post Evaluation of the Seventh Framework Programme

¹⁴ More details, including call texts can be found on the www.cordis.europa.eu website. Most projects had a duration of around 3 years.

The CIP programme consists of three ‘pillars’: The Entrepreneurship and Innovation Programme (EIP), the Information Communication Technologies Policy Support Programme (ICT-PSP) and the Intelligent Energy Europe Programme (IEE). Within the Trust and Cybersecurity work programme ICT-PSP calls addressing the topic have been used:

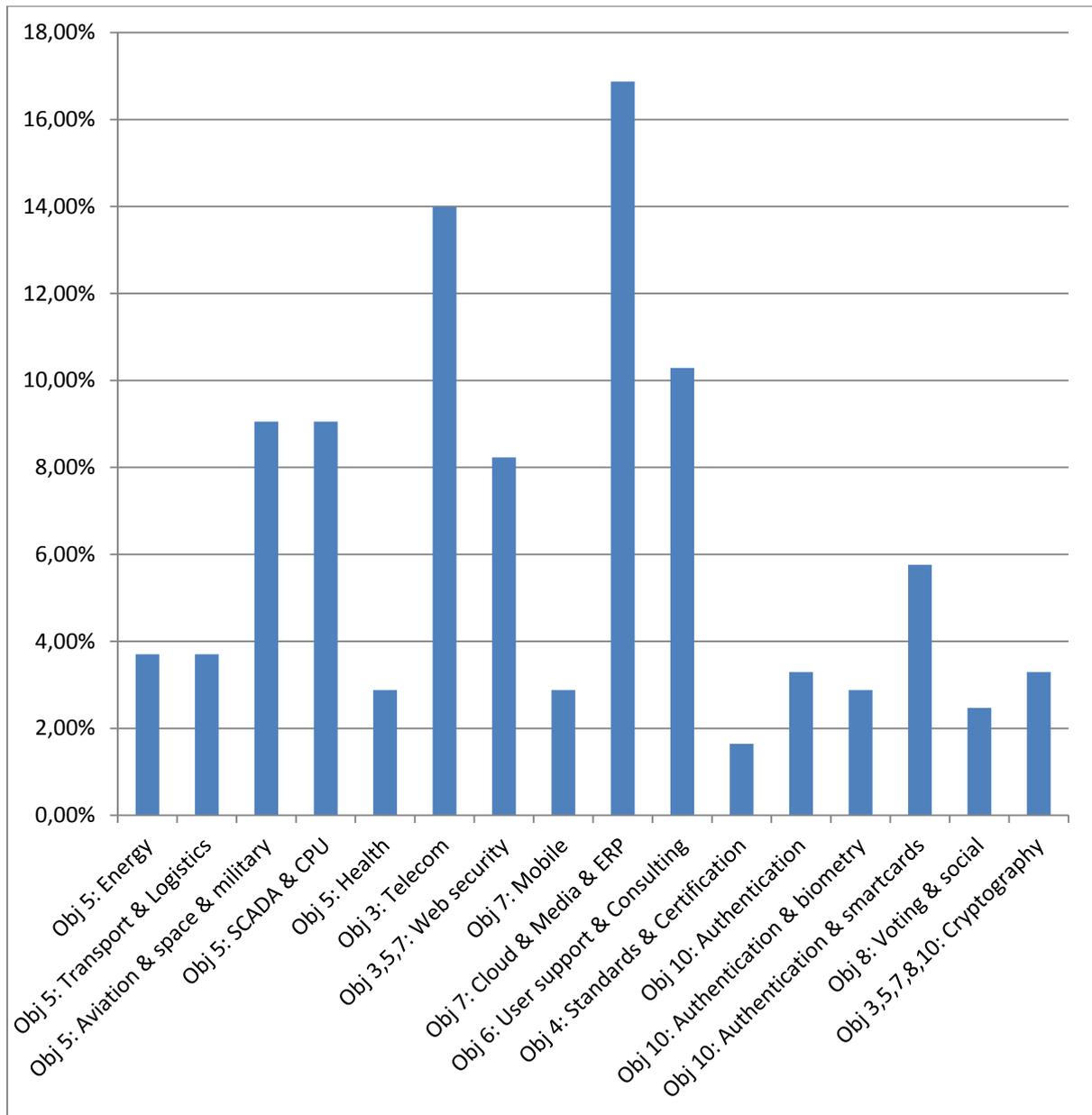
- CIP-ICT-PSP-2008-2 (Biometrics + Identity Management),
- CIP-ICT-PSP-2012-6 (Fighting Botnets),
- CIP-ICT-PSP-2013-7 (Website Security and Biometrics).

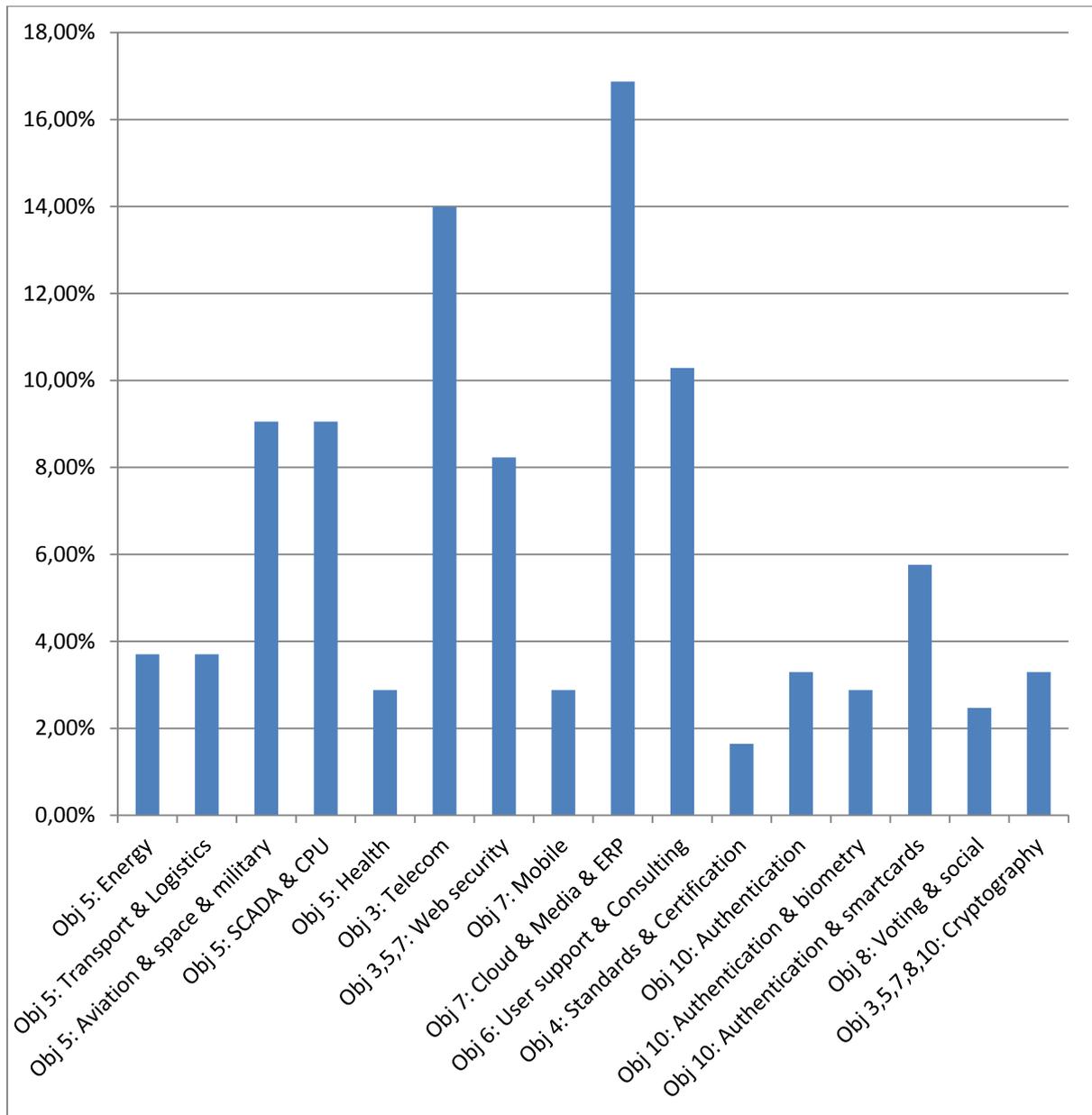
The resulting activities co-funded by EU grants have been executed by successful bidders (and their project partners) to the competitive calls described under this heading. The same holds for the collaborative research network built by academic, industrial and use case partners over the considered period.

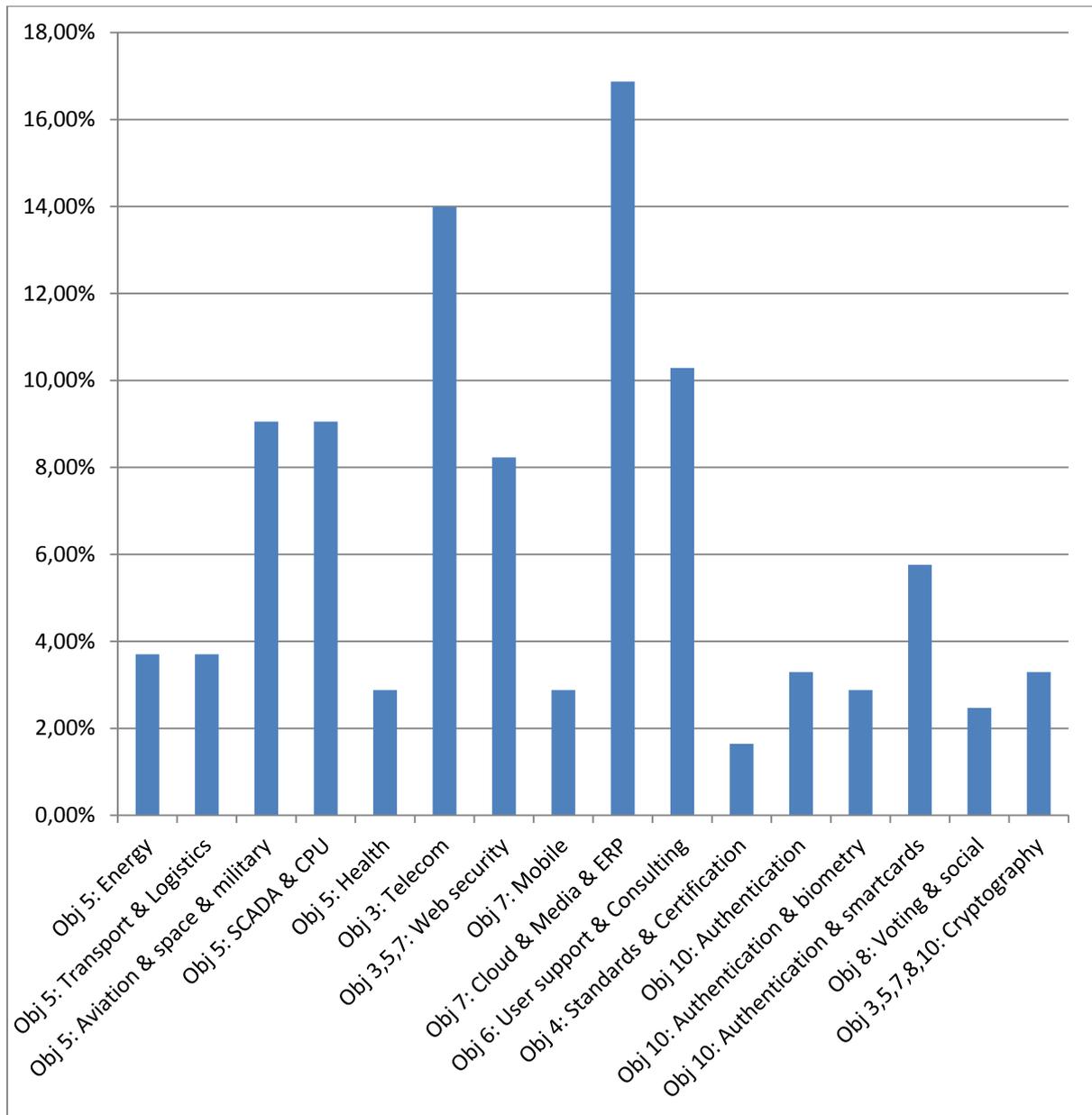
Table 1: Contribution to programme objectives

Main category	Partner	Sub category	Partner	Supports objective
Industry		Technological		1
		Consulting		6
		Cloud & mobile		7
Research		University		2,8,9
		Research Centres		2,9
		Innovation institutes		2
Others		Government		10
		Non Commercial		
		Standard		4
Users		Telecom		3
		Energy		5
		Water		5
		Transport & Logistics		5
		Automotive		5

To be able to assess how far FP7 and CIP have realized the objectives put forward under the heading "3.Background of the Initiative" the beneficiaries were classified in different categories. Table 1 illustrates how the different types of participants contribute to the different objectives. In the table and included graphs, tables and texts in the SWD the convention used is: "Industry" stands for technological, consulting and cloud/mobile companies, the "Research" group contains the universities and research centres and innovation institutes; the "Others" category contains government agencies, non-commercial and standard organisations, and users contain telecom, energy, water and others.







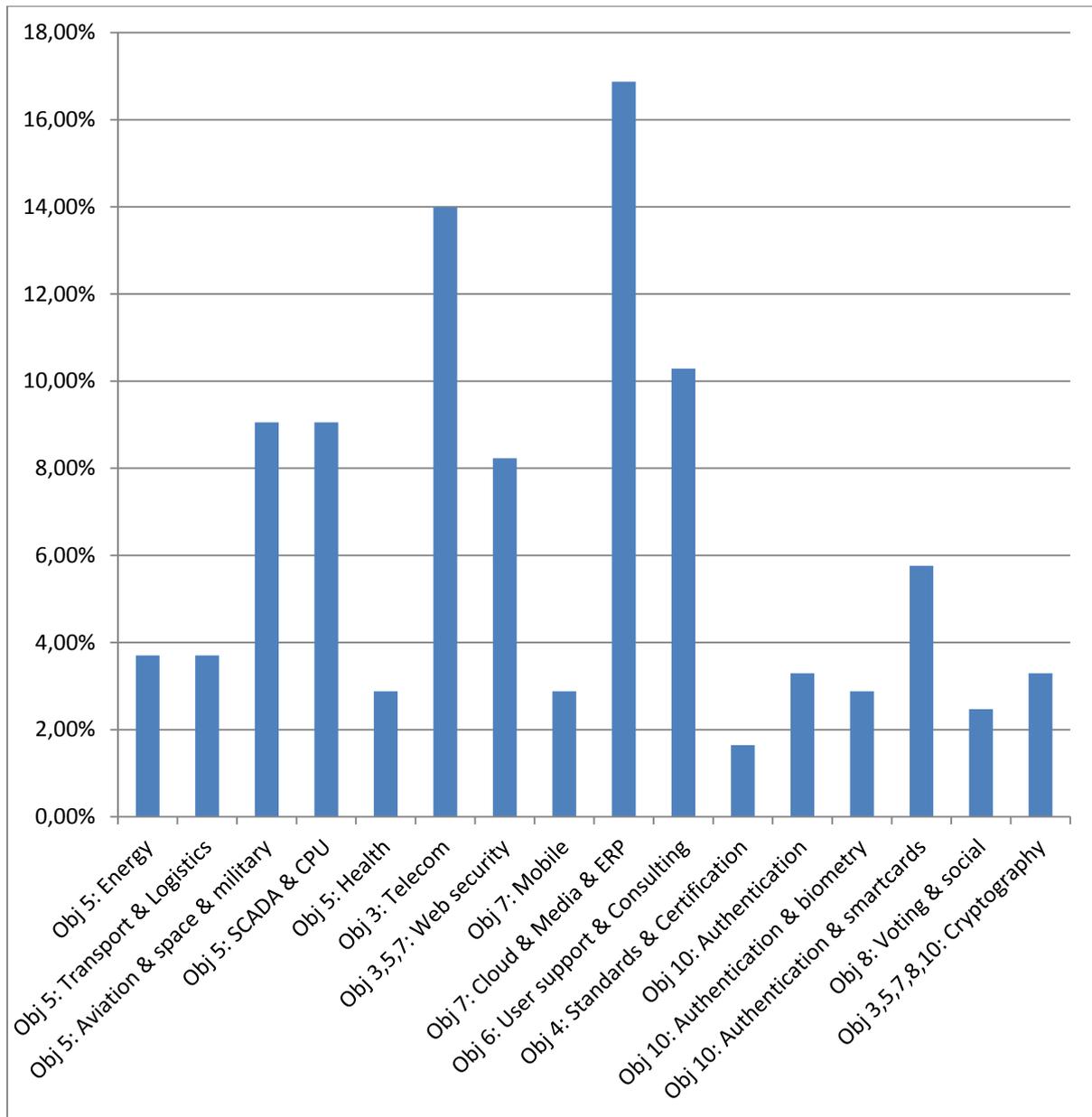


Figure 3: Organisational Participation by Objective

To indicate the **effectiveness** of the FP7 programme **for the objectives formulated in the trust and cybersecurity FP7 call headings** the table 9.1 in Annex has been populated with the number of participants of the corresponding category in the projects that received grants. Participants (company, organisation, consultant or user of the technology) having benefitted from one or two grants have been characterised as low participation, of three grants as medium, and of four or more grants as high participation in the programme. The graph resulting from this table can be found in Figure 3.

7. ASSESSMENT OF IMPLEMENTATION AND PARTICIPATION

FP7 and earlier RTD Framework Programmes have established collaborations at the European level. An analysis of the results of these collaborations is useful for the assessment of the **effectiveness** and **efficiency** of the programmes and could serve to indicate in which direction Cybersecurity R&I policies in the EU should develop.

Over the period 2007-2013, the 101 cybersecurity projects funded produced a total of 16 patents and 201 publications¹⁵, 0.8 patents per EUR 10 million and 54 publications per EUR 10 million. As a comparison, the 2,448 FP7 ICT funded projects analysed in the FP7 ex-post evaluation of ICT research resulted in a total of 289 patents, with a very skewed distribution: in general (only 139 projects resulted in at least one patent) and 18,169 publications¹⁶.

The analysis shows that roughly 10% of the participants in the projects were cybersecurity Small and Medium sized Enterprises (SME's). This ratio is lower than the ratio of SME's that exist in the cybersecurity domain and below the targets set for SME participation in FP7. The rate of SME participation in FP7 security was slightly higher, but encompasses SMEs providing administration or services but not doing R&I.

In CIP projects, the SME rate was above 15% (e.g. project SWEPT, with 5 SMEs out of 11 partners, benefiting from 41% of budget), but the volume of CIP projects in the digital security area (5) may not be statistically significant. In FP7, a number of projects had above 15% rate of SME participation (e.g. Euro-Mils at 41% of budget going to SMEs, with 5 SMEs out of 15 partners; Trespass at 21% or ABC4TRUST at 20%), but this was otherwise generally below FP7 target. Cybernetica, an Estonian SME, developing ICT-based security solutions, participated in 3 projects totalising EUR 1.2 million of EC funding. This example was however rather an exception, though showed the possible attractiveness of such European programme for industrial SMEs.

While the projects that obtained an EU grant from the programme have achieved impact in the scientific world through their deliverables and publications, it is unclear whether they produced successful outcomes that can contribute to the main objective and overall goal formulated before. As an example: Europe is the world leader, by far, in cryptography but the answer on the question "*are European cybersecurity companies exploiting this technological advantage?*" is not at all evident.

Figure 3 that represents the content of table 9.1 in Annex offers the possibility to analyse how effective (as described in the methodology section) the **FP7 and CIP Trust and Cybersecurity programme has been in realizing the objectives** as identified in section 2.

¹⁵ These data are however partial as they were based on a survey of project coordinators covering ongoing projects.

¹⁶ See Ex-post Evaluation of ICT research in the Seventh Framework Programme, Final Report prepared by DG CONNECT, January 2015

7.1. Cooperation between Research organisations and Industry

To assess the second objective (2) "**Widen take up of research outcomes and increase the number of spin-offs in the field**" the editors of the SWD used the proxy "**ratio of research centres and university participations** against participation of organisations (of any kind) in the FP7 Trust and Cybersecurity projects".

Table 9.1 in Annex, which describes the proportion of participation of different types of beneficiaries (universities, Network Infrastructure providers, Internet and web services,...) illustrates that the FP7 trust and security research programme has created an effective way to engage cooperation between universities, research centres and organisations.

A more detailed analysis of the Industry and Research cooperation can be found in the graphs presented in figure 9.4 in Annex and in the figure 9.5 in Annex regarding participants that had more than 2 participations in FP7 projects.

Figure 9.4 in Annex indicates in detail the participation by research centres and universities, industrial companies and consultancies and other partners such as government agencies. The figure shows the active cooperation between organisations and universities and research centres that was the result of the FP7 research and innovation programme. The cooperation between the different partners is indicated by lines between the nodes.

Figure 9.5 in Annex only retains beneficiaries with a more frequent participation in the programme, gives a less cluttered overview and a more precise indication of the size, in number of project participations, of the participation of the beneficiary. The red rectangles indicate industrial partners and the size of the rectangle is proportional to the number of project grants this participant was able to obtain from the programme. From the diagram on the figure in annexe 9.4 we deduced the table in annexe 9.2 with the size, in number of project participations of each participant in the programme, of industrial participations. The figure in annexe 9.4 indicates (roughly) the competence clusters that have been built as a result of the framework research programmes.

7.2. Improved coordination of research activities

To have an indication of how effective objective (9) "**Improved coordination and integration of research activities in Europe or internationally**" has been the SWD includes a graph illustrating the participation in the programme by EU Member State.

The table 9.3 in Annex and Figure 7 represent the participation by category of participant and country. Participants that cooperate over member state borders are more active in networking, which is a necessary step in the build-up of an effective cybersecure ecosystem that supports the Digital Single Market priority. Figure 7 illustrates that Germany, France, Italy and Spain are the EU countries with the most consistent participation in the programme. France, Germany and Italy have a balanced participation of Industry, Research and Others while Spain provided more Users in the programme and Greece more Research partners. For the

eastern European countries, we observe only small participations although recent statistics¹⁷ illustrate that cyber-attacks are occurring frequently in these countries (see figure 4).

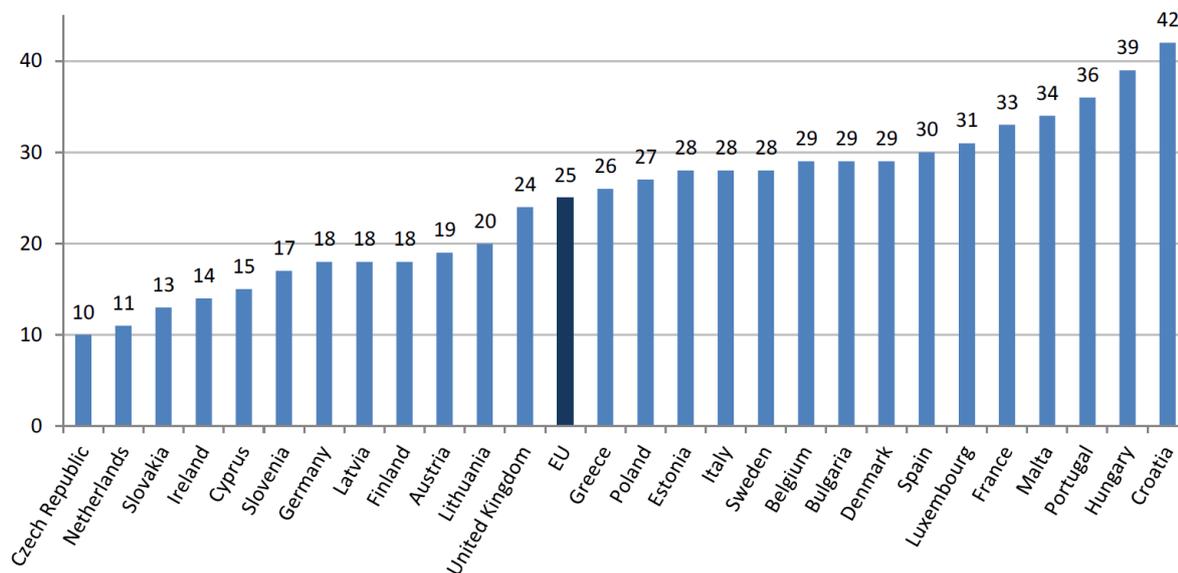


Figure 4: Experienced Cybersecurity problems for private Internet users

7.3. Make critical infrastructures secure

Two of the objectives formulated in the FP7 calls address the security of critical infrastructures: Objective (3) **"Improve security and dependability of networks and service infrastructures"** and objective (5) **"Make critical infrastructures, such as energy, information and communication networks, sensitive manufacturing, finance, healthcare, or transportation systems more secure and dependable"**.

These objectives also relate to the overall ex-post impact assessment of FP7 that calls for a closer coupling between research, innovation and EU policy. In the context of trust and cybersecurity these objectives link to the forthcoming **Network Information Security (NIS) Directive** that will require Member States to ensure a higher cybersecurity readiness of their critical infrastructures.

Table 9.1 in Annex illustrates that 28.4% of the organisations that received grants from the FP7 trust & security programme belong to one of the user categories that manage critical infrastructures (as defined in the forthcoming NIS Directive): Energy, Transport including aviation and Logistics, Health and SCADA and Central Processing Unit (such as found in mobiles, tables and personal computers) manufacturing companies.

¹⁷ Source: Eurostat, share of internet users who experienced security related problems in the EU Member States, 2015 (% of individuals who used the internet within last year). Link to Eurostat news release 9 February 2016, Safer Internet Day: <http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef>

Table 9.1 also illustrates that Network and Information Security organisations and Internet and web security companies took up 22.2% of the number of company participations in FP7.

In conclusion 50.6% of the number of project participations came from organisations that had to do with critical services or critical network services as defined in the NIS Directive, a participation ratio that justifies the statement that the FP7 trust and cybersecurity programme grants went effectively to critical service providers and critical network service providers.

7.4. Make cloud and mobile services secure

One of the objectives formulated in the FP7 calls address cloud security: **(7) "Secure and privacy-preserving technical solutions in clouds, mobile services and management of cyber incidents in compliance with privacy legislation"**.

The forthcoming Network Information Security directive identifies cloud services as critical services therefore the participations of companies that develop solutions to secure the cloud directly address this policy directive. Table in annexe 9.1 indicates that 16.87% of the number of organisational participations address cloud security in organisational (Enterprise Resource Management, Customer Relationship Management, Business Cloud applications) or personal settings. Within the programme SAP, the top ranked cloud service provider in Europe¹⁸, was one of the most active participants in the cloud cybersecurity services call. In conclusion the participation of cloud service providers in the FP7 trust and security programme was effective in attracting European ICT companies that are active in the domain.

The call objectives formulated in the call also include mobile security. Telecom services and the network become more and more mobile and therefore mobile services are as important as fixed line and broadband networks. The table in 9.1 indicates that 2.88% of the organisations in the trust and security programme had an activity in mobile security.

The low number of participations of companies active in mobile technologies is in line with the diminishing number of European technology providers that can maintain a foothold in these markets.

7.5. Make digital authentication a reality

One of the objectives formulated in the FP7 calls was: **(10) "A real-life mature environment for digital authentication across several jurisdictions with high levels of assurance"**.

This objective relates to the eIDAS Regulation that requires EU Member States to have interoperable authentication systems. Within the FP7 trust and security participations the organisations that do research and innovate in the domain of Smartcards, Biometry and

¹⁸ SAP, T-Systems, SmartFocus, Unit 4 and Cegid, are in order the top 5 European Public Cloud Vendors. IDC study "Uptake of Cloud in Europe" (SMART 2013/0043 report). Web link: <https://ec.europa.eu/digital-single-market/en/news/final-report-study-smart-20130043-uptake-cloud-europe>

Digital Authentication have been labelled as contributors to this objective. These organisations account for 11.93% of the total number of organisations participating in the trust and security FP7 calls.

In conclusion the FP7 Trust and Cybersecurity programme has been able to attract the technology organisations (e.g. smartcard etc...) that could provide an effective support for the eIDAS legislation.

7.6. Ensure human rights in the cyber world

Objective (8) formulated in the FP7 calls for a **(8) Significant contribution to making Internet a medium that can be used to exercise human rights, including in hostile environments.**

Exploring the organisations that participated in the FP7 Trust and Security programme indicates that 2.47% of these organisations claim to develop solutions that support this objective. They develop solutions that support e-voting and secure social networking. Another group of organisations invest in enabling technologies, such as encryption, that support many objectives. If we would add the innovation in encryption participations as adding to the preservation of human rights in the cyber world, the total number of organisation in the FP7 trust and security programme totals to 5.76%.

In conclusion, the FP7 Trust and Security programme supported the objective to preserve the citizens' rights also in the cyber world. The world-class competence developed in the encryption domain for instance provides evidence that the FP7 Trust and Security programme has been efficient toward preserving citizens' rights.

7.7. Standards and certification

Objective (4) formulated in the FP7 calls for a **"Wider use of metrics, standards, evaluation and certification methods and best practices in security of networks, infrastructures, software and services"**.

The NIS directive will call for best practices that make it possible to reduce cybersecurity risks for all the stakeholders, users as well as product and service providers. It is believed that standards, evaluation and certification methods are instrumental to make such best practices applied throughout the industry and organisations. Objective 4 supports this objective. The number of participations of standardisation organisations, private as well as public, in the FP7 trust and security programme is 1.65%, which is higher than the ratio of standardisation and certification organisations versus other ICT organisations in Europe. The FP7 Trust and Cybersecurity programme has thus assured an effective participation of these standardisation organisations although in the current setting with the forthcoming NIS Directive requirement for best practices, which in engineering environments translates to standards, norms, certificates and audits, might justify a higher level of participation from such organisations.

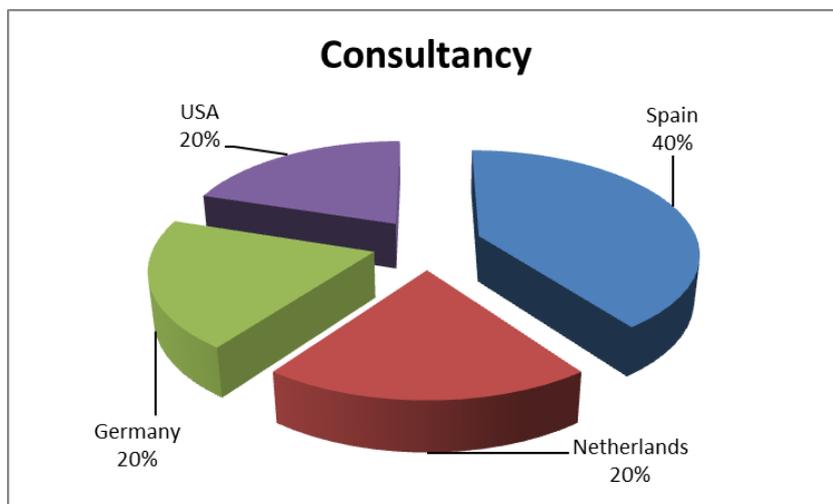
7.8. Ensure cybersecurity knowledge take-up

Objective (6) formulated in the FP7 calls for **"Support to users to make informed decisions on the trustworthiness of ICT"**.

In the analysis this request has been translated in the proxy factor "number of participations of consultancy organisations" in the FP7 Trust and Security calls. It will be the consultancy

organisations that implement the solutions at the user's premises and that provide the first line of knowledge dissemination.

Consultancy organisations that group the different types of management consultants and system integrators (e.g. companies that make cybersecurity solutions operational in a user organisation) are in numbers rather limited in the programme. Only five industrial partners have been identified as consultants. Of course it is not always easy to classify an industrial organisation as a software integrator (consultant) or a software and service researcher or developer. Some of the software integrators also develop sometimes original applications or services. Figure 5 shows the country of origin of the consultants in the FP7 funded Trust and Cybersecurity projects. In conclusion 10.29% of the number of participations came from consultancy companies. An effective participation of consultancy organisations although the distribution of these organisations throughout the European Union can put in question the efficiency of the FP7 Trust and Security programme for this objective.



Another way of analysing the question "*Ensure cybersecurity take-up*" can be done using the user perspective. The question would then become "*In which European countries are the users based that received EU grants from the FP7 Trust and Security programme?*"

Within the scope of this note "User organisations" that try out the prototypes developed by the

Figure 5: RTD participations by consultancy companies

technology partners are another smaller group of participants in the FP7 trust and cybersecurity RTD programme. Eight organisations have been labelled as Users that participated in the programme. This includes the big telecom companies such as France Telecom, Deutsche Telecom, Telecom Italia, T-systems and Telefonica. A more detailed analysis of the content of the individual projects should possibly reveal that some of their work in the programme could also be qualified as cybersecurity technology development. **The Telecom companies are with 16 participations out of 23 user organisations by far the biggest user group in the research programme.** France was most successful in engaging users in the Trust and Cybersecurity programme, followed by Germany as a distant second and Italy as third country. Analysing the user perspective shows that the participation throughout the European Union is a little more dispersed than the consultancy organisations although the user base remains limited to the larger telecom organisations that receive aid from the FP7 Trust and security programme.

7.9. Improved European industrial competitiveness

Objective (1) formulated in the FP7 calls for **Improved European industrial competitiveness** in markets of trustworthy ICT, offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.

If the FP7 Trust and Security programme had shown one priority ambition then this would be the ambition to develop knowledge and take-up of this knowledge by European state of the art technology organisations. Europe is without doubt a leader in academic and applied research on cybersecurity and data protection. However when we analyse the industrial participations in the FP7 trust and cybersecurity research and development programme we get a different message. Figure 6 shows that IT companies with headquarters in the US receive 21% of the research grants. Japan had a modest 3% participation and Israel 2%. France (27%) and Germany (26%) had the biggest industrial participation in the FP7 Trust and Security programme on number of project participants over the whole programme.

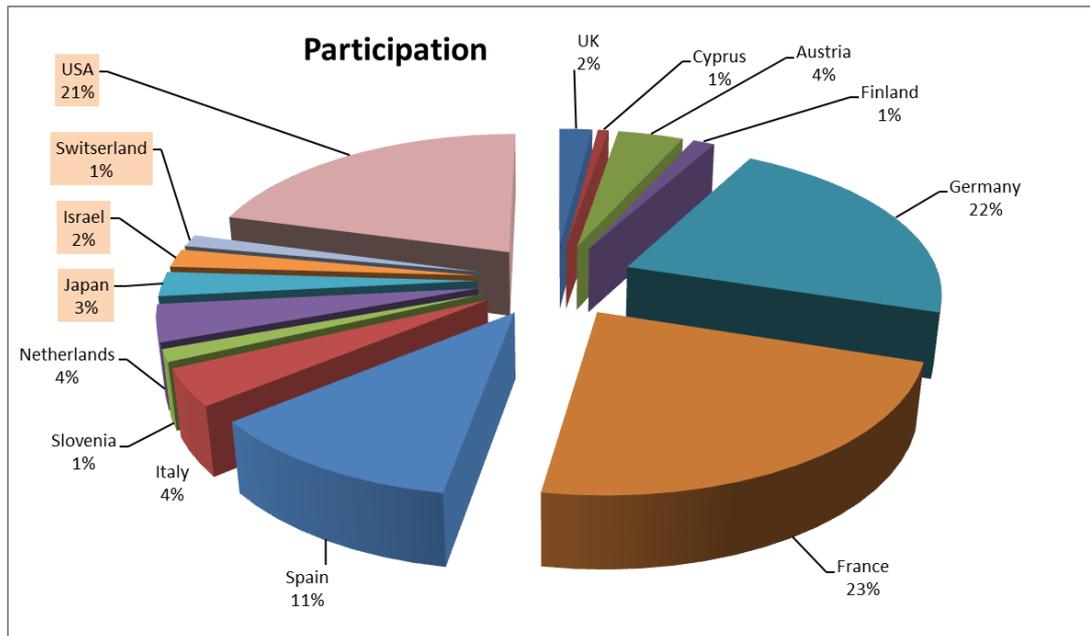


Figure 6: Technology companies in the FP7 Trust & Cybersecurity programme

The figure in annexe 9.5 shows a detailed view and is drawn from the received grants by the beneficiaries of the FP7 programme that can be qualified as technology companies that develop cybersecurity solutions in the research programme (Table 2). The data is extracted from the MIS database¹⁹ that contains the data of the funded projects.

Table 2: Participation technology companies in FP7 Trust & Cybersecurity programme

Company	Country	Participations	Grant (€)
KeyLemon	CH	1	176.460
Biometry	CH	1	106.875
Primetal	CY	1	186.060

¹⁹ EU internal project database

TECHNICON	AT	6	3.009.212
G DATA	DE	1	110.267
SAP	DE	14	9.344.364
IT objects	DE	1	277.380
MORPHO CARDS	DE	1	313.577
NOKIA solutions	DE	2	666.327
SIRRIX	DE	1	892.555
Software AG	DE	1	507.495
INFINEON	DE	10	3.909.714
SYSGO	DE	2	1.240.538
NOKIA	FI	2	74.880
AIRBUS	FR	5	1.067.011
Cassidian	FR	3	640.273
GEMALTO	FR	5	1.082.190
MORPHO	FR	2	681.095
Opentrust	FR	1	129.219
STM	FR	2	523.733
THALES	FR	15	4.232.144
Trusted labs	FR	1	129.219
Israel Aerospace	Il	1	120.845
AFCON	Il	1	324000
OS new Horizon	Il	1	498.000
Engineering	IT	5	1.411.862
TXT	IT	1	88.795
Fujitsu	JP	1	478.000
NEC	JP	3	1.119.222
NXP	NL	2	542.496
Philips	NL	4	1.343.498
ATOS	SE	17	5.447.480
XLAB	SI	2	492207
ARM	UK	1	1.999.991
BAE	UK	1	174.303
Epsilon	UK	1	396.310
AMS	US	2	10.694.162
CISCO	US	1	0
EMC2	US	1	227.040
IBM	US	9	6793517
HP	US	7	25.084.851
INTEL	US	2	221.806
MICROSOFT	US	5	92565
Alien Vault	US	1	333.292
STARLAB	US	1	312.337
SYMANTEC	US	1	367.041

Verizon	US	1	165.000
---------	----	---	---------

The table 2 and annexe 9.5 illustrate that Germany and France receive the bulk of the available grants (22 and 23%) followed very close by Technology companies that have their headquarters in the USA who receive 21% of the total of grants. The figure in annexe 9.6 represent graphically the received grant / technology participant.

In summary the participation of **technology providers based in the European Union** rounds up to a total grant of 88.029.208 € while the total grant distributed to cybersecurity projects in FP7 is 230.637.778 €. Therefore the industrial participation in FP7 ratio is 38.2% for the technology companies. This participation ratio can be compared to other participation ratio's such as in contractual Public Private Partnerships (cPPP's) funded through the FP7 programme that cumulate an industrial participation of 57% to obtain an indication of effectiveness of the FP7 programme to attract industry.

Table 3: FP7 objectives and impact

Objective	Relevance	Effectiveness	Efficiency	EU added value
Cooperation of Research and Industry	Relevant policy objective of FP7	Yes, 49% Research and 51% organisations	Yes ²⁰	Yes ²¹ , a core EU Science policy
Improved coordination of research activities	Relevant policy objective of FP7	Yes, but participation of East EU member states is low	Yes ²²	Yes ²³ , a core EU Science policy
Make critical infrastructure cyber secure	Relevant NIS linked objective	Yes, 50.62% of the organisations are active in securing critical infrastructures and/or the information network	Qualitative evidence provided by the ACDC project	Yes, cybersecurity is a priority for the Digital Single Market
Make cloud and mobile services cybersecure	Relevant NIS linked objective	Yes, 19.75% of the participations are linked to securing the cloud and mobile	Qualitative evidence provided by TRESCCA, TLOUDS, PRACTICE etc...	Yes, cloud security, and online business security are required by the NIS directive
Make digital	Relevant	Yes, 11.93% of the	Quantitative	Yes, interoperable

²⁰ SWD(2016)2 final "Ex-Post Evaluation of the Seventh Framework Programme" provides substantial evidence

²¹ SWD(2016)2 final "Ex-Post Evaluation of the Seventh Framework Programme" provides substantial evidence

²² SWD(2016)2 final "Ex-Post Evaluation of the Seventh Framework Programme" provides substantial evidence

²³ SWD(2016)2 final "Ex-Post Evaluation of the Seventh Framework Programme" provides substantial evidence

authentication a reality	eIDAS linked objective	participations are linked to digital authentication	evidence by NESSoS, SPaCIOS etc...	digital authentication solutions are needed to fulfil EIDAS requirements
Ensure human rights in the cyberworld	Relevant to protect fundamental right of EU citizens	Yes, 5.76% of the participations are linked to technology and solutions that make it easier to support human rights	The establishment of a world class competence in the domain of cybersecurity indicates efficiency of the programme	Yes, it is an enabler to ensure EU citizens rights in the future.
Standards and certification of products, services and processes	Relevant. The NIS calls for the introduction of best practices.	Yes, 1.65% of the programme participations is by standardisation and certifications organisations	Quantitative evidence from the EU Trust and Cybersecurity project database.	Yes, EU standards and certification procedures will prohibit possible barriers for the Digital Single Market easier
Improved European industrial competitiveness	Relevant for the FP7 RTD programme and the recovery targets of FP7	No. (1) Part of the generated IPR belongs to organisations with headquarter in the USA, the third largest beneficiary of the programme after Germany and France. (2) The programme fails to give evidence that the grants resulted in final product and services. Capacity building mainly remained mainly on the component level such as encryption.	38.17% of the EU grants have been made available to EU technology companies	The objective remains highly relevant for Europe and even more given the new NIS directive and the relevance to have the ability to protect EU citizens fundamental rights and the IPR of organisations and security of critical sectors and services.

Table 3 summarizes the findings of the previous paragraph. The FP7 Trust and Security programme scores relatively well against the policy objectives formulated in the call heading with the exception of the most important priority: *Ensure competitiveness of European organisations in the domain, stimulate innovation and the creation of jobs and take up in Europe.*

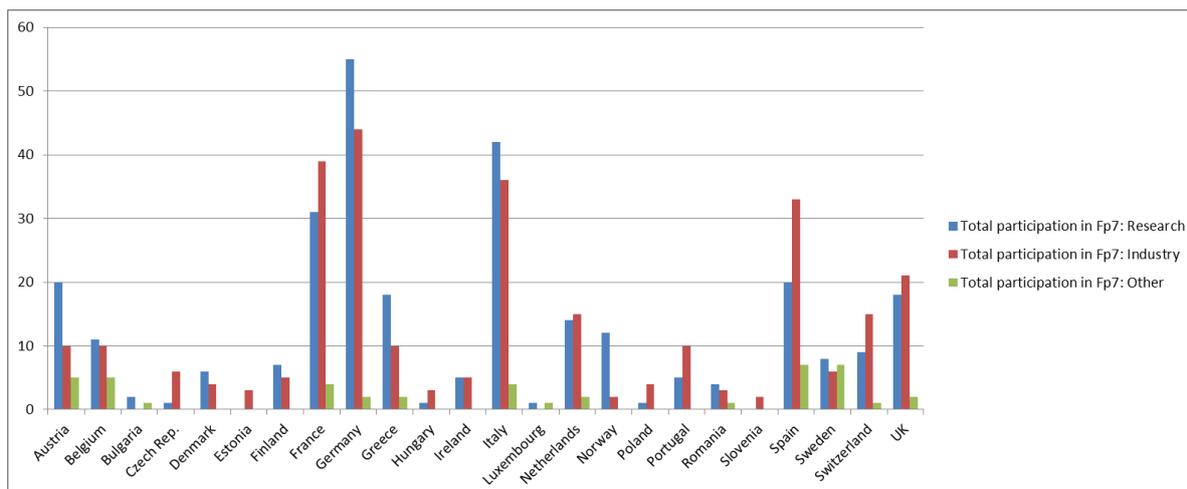


Figure 7: Number of project participations by country

8. CONCLUSIONS

This evaluation provides a quick glance on the objectives outlined in the introduction which were: (1) to assess whether grants under these programmes have contributed to a stronger ecosystem of cybersecurity companies in Europe supporting the European citizens, organisations and governments and (2) to map the topics that have been funded in the past against existing and future EU regulations and policy priorities, in particular the Digital Single Market Strategy, the (announced) NIS directive, and the Data Protection rules, to help identify gaps to be addressed by the cybersecurity contractual PPP.

8.1. Strong outcomes

On the positive side we can conclude that the FP7 and CIP trust and cybersecurity research and development programme has mobilized many research centres, universities and organisations in Europe and beyond. This resulted in world leading competence in some domains such as cryptography. Examples of this world leading competence can be found in encryption solutions we use every day when doing online payments, or using smart cards to get money from ATM machines. The establishment of a world class competence in the domain of encryption indicates also efficiency of the programme in safeguarding the rights of EU citizens in the cyber world. In addition the encryption competence contributes to several other objectives such as authentication, identification, eIDAS etc that use encryption as an enabling technology.

The analysis presented in this evaluation indicates also the important positive contribution of the FP7 programme to competence building in the Trust and Cybersecurity domain.

Cybersecurity is a complex challenge to address due to the multiple facets of cyber threats and vulnerabilities. The FP7 and CIP programmes have helped to structure cybersecurity research and innovation, by breaking down the broader challenge of cybersecurity into identifiable and complementary domains of investigation. It has enabled to bring together key

industrial and research stakeholders in each of these domains and foster their cooperation. The network analysis of stakeholders over the different FP7 calls has shown that the cooperation started in the first calls appears to sustain over time.

Through FP7 and CIP programme, cybersecurity research and innovation became structured into specific topics, such as secure network infrastructures, threat detection, resilience, critical infrastructure protection, biometrics, identify management, authentication, privacy, trustworthy service infrastructures, secure software engineering, cryptography, cloud security, mobile security, embedded systems, certification... A number of these areas have a clear connection to legislation and policies that were developed in parallel, like the NIS Directive or the EU cybersecurity strategy.

8.2. Weaknesses of the FP7 cooperation and the CIP programme

While strong competences have been developed by the FP7 and CIP programme, some less solid outcomes have also been identified in this SWD.

Germany, France, Italy and Spain are the EU countries with the most consistent participation in the programme. France, Germany and Italy have a balanced participation of Industry, Research and Others while Spain provided more Users in the programme and Greece more Research partners although **the report finds a smaller participation of Eastern European countries than what could be expected.**

The fact that 50% of the project participants were by organisations active in the domain of securing one of the critical sectors as specified in the NIS Directive or in securing the Internet infrastructure is encouraging although that detailed analysis informs that while air transport had a fair share in the programme **some critical sectors such as health have been largely absent.**

A similar conclusion can be made for the effort that went into securing European, mainly enterprise linked, cloud services with a participation ratio of 18%. However, the **cloud service security budget went mainly in securing enterprise cloud applications and less to securing general purpose digital applications accessible to EU citizens.**

The FP7 Trust and Cybersecurity programme has assured an effective participation of standardisation organisations (1.65%) although in the current setting with a new NIS directive asking for best practices, which in engineering environments translate to standards, norms, certificates and audits, **a higher level of participation of standardisation and certification organisations could be appropriate.**

A fair amount of participants (10%) were consultancy organisations that disseminate knowledge to users. **Two thirds of these users however could be classified as telecom organisations which leaves the question open if a better balancing over other user groups would not be desirable.**

The detailed analysis of the industrial participation informs that **one third of the participants are companies that have their headquarters outside Europe.**

Despite the high number of innovative SMEs in cybersecurity across Europe²⁴, the low participation of industrial SMEs in the FP7 and CIP programme shows the difficulty of this type of companies to engage in European R&I programme (unless they are a consultancy or are already part of the value chain of a larger enterprise). The new instruments brought by Horizon 2020 (such as the SME instrument) offer new venues to foster the participation of SMEs in future cybersecurity R&I.

One of the limitations of the approach taken in FP7 and CIP is to have fragmented the topics. If this enabled to address more specific and achievable scientific challenges, this has also defined specialty areas among which interaction and cross-fertilisation needs to be enhanced. Assurance, joint security and privacy by design, identity, access and trust management, data security and encryption, ICT infrastructure cybersecurity (threats management, system security, end-to-end security, etc.), cybersecurity services (auditing, compliance and certification, risk Management, cybersecurity operation centres) all appear like promising areas building on the previous activities. Multidisciplinary research should prevail in these activities, addressing technical and non-technical aspects such as economics and law, but also ethics, political science, behavioural science...

²⁴ See SWD(2016)216

9. ANNEXES

9.1. No of participations by objective defined in the call

Programme objective	By participation	No EU participations	Participation in % points
Industrial competitiveness	Organisations	243	
Take up Research	University	234	
Coordinate Research	University	234	
Critical infrastructure Security	Obj 5: Energy	9	3,70%
Critical infrastructure Security	Obj 5: Transport & Logistics	9	3,70%
Critical infrastructure Security	Obj 5: Aviation & space & military	22	9,05%
Critical infrastructure Security	Obj 5: SCADA & CPU	22	9,05%
Critical infrastructure Security	Obj 5: Health	7	2,88%
Network Infrastructure Security	Obj 3: Telecom	34	13,99%
Internet and web security	Obj 3,5,7: Web security	20	8,23%
Secure Mobile	Obj 7: Mobile	7	2,88%
Secure Cloud	Obj 7: Cloud & Media & ERP	41	16,87%
User Support	Obj 6: User support & Consulting	25	10,29%
Standards and Certification	Obj 4: Standards & Certification	4	1,65%
Digital Authentication	Obj 10: Authentication	8	3,29%
Digital authentication & biometry	Obj 10: Authentication & biometry	7	2,88%
Digital authentication & smartcards	Obj 10: Authentication & smartcards	14	5,76%
Human Rights	Obj 8: Voting & social	6	2,47%
Cryptography	Obj 3,5,7,8,10: Cryptography	8	3,29%

9.2. Number of participations in the FP7 R&D programme

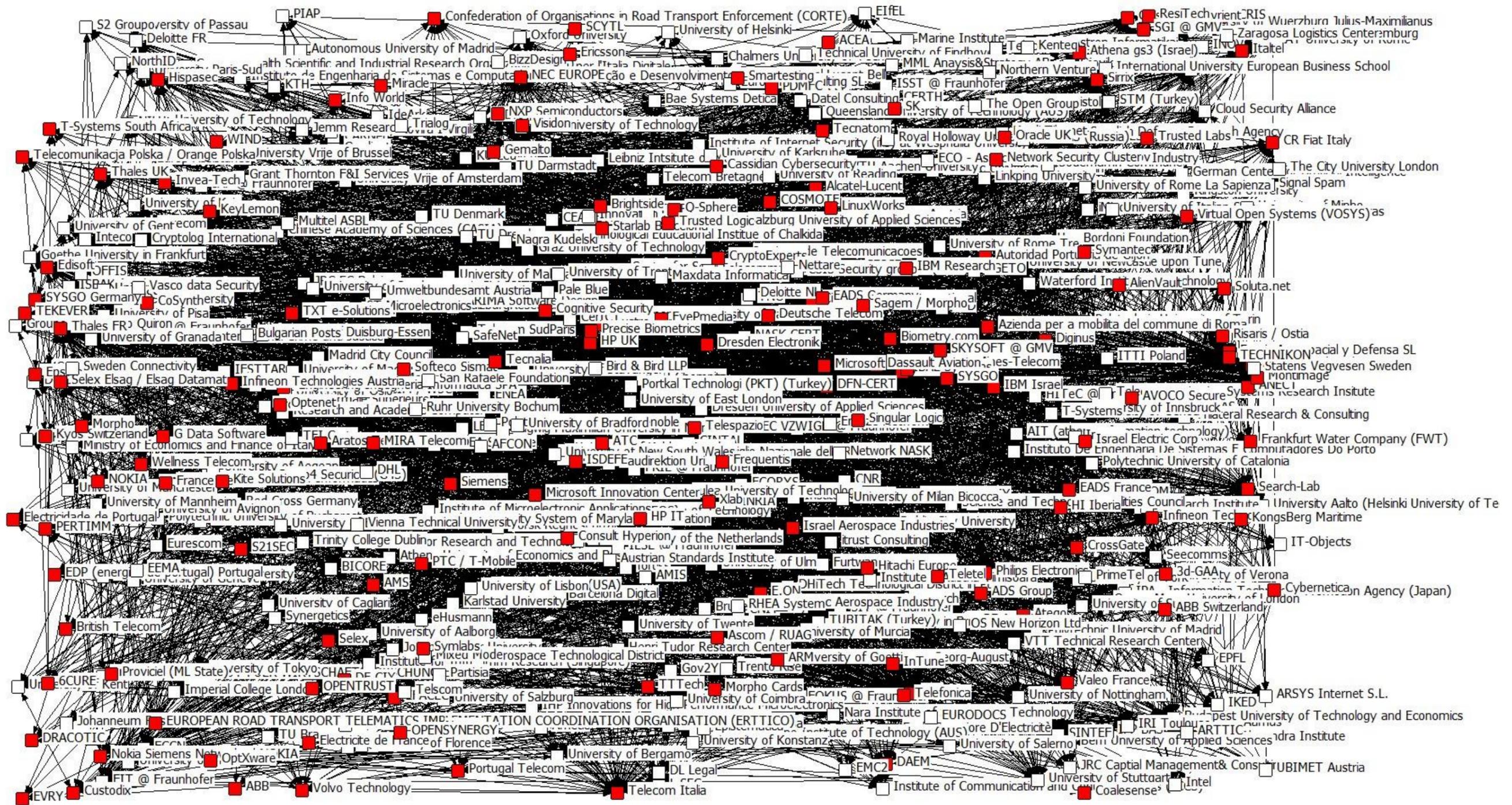
	Country HQ	Industry	Low (1-2 participations)	Medium (2-3 participations)	High (>3 participations)
Afcon	Israel	Technology	X		
Alien Vault	US	Technology	X		
AMS	US	Technology	X		
BAE systems	UK	Technology	X		
Biometry	Swiss	Technology	X		

Cassidian	France	Technology		X	
Cybernetica	Estonia	Technology	X		
CoSynth	Germany	Technology	X		
Deutsche Telecom	Germany	User	X		
Engineering	Italy	Technology	X		
Energies de Portugal	Portugal	User	X		
Epsilon	UK	Technology	X		
Frankfurt water	Germany	User	X		
G Data software	Germany	Technology	X		
Gemalto	France	Technology	X		
IBM	US	Technology		X	
Inteco	Spain	Consultant	X		
Intel	US	Technology	X		
IT-objects	Germany	Consultant	X		
HP	US	Technology			X
KeyLemon	Swiss	Technology	X		
Maxdata	US	Technology	X		
Microsoft	US	Technology			X
Miracle	US	Consultant	X		
Montimage	France	User		X	
Morpho	France	Technology	X		
NEC Europe	Japan	Technology		X	
Nokia	Finland	Technology			X
Opentrust	France	Technology	X		
OS new horizon	Israel	Technology	X		
Primetel	CY	Technology	X		
SAP	Germany	Technology			X
Search-Lab	Hungary	Technology		X	
Siemens	Germany	Technology	X		
Sirrix	Germany	Technology	X		
Starlab Barcelone	US	Technology	X		
ST Microelectronics	Italy	Technology	X		
Technaton	Netherlands	Consultant	X		
TXT e-solutions	Italy	Consultant	X		
T-systems	South Africa	User	X		
Telecom Italia	Italy	User		X	
Telefonica	Spain	User		X	
Thales	France	Technology			X
Vosys	France	Technology	X		
Wellness Telecom	Spain	Consultant	X		
Xlab	Slovenia	Technology	X		
IBM research	US	Technology		X	
EMC2	US	Technology	X		
ATOS	Spain	Technology			X
France Telecom	France	User			X

9.3. Number of project participations by country

	Total participation in FP7			Call 1			Call 5			Call 8			Call 10		
	Research	Industry	Other	Research	Industry	Other	Research	Industry	Other	Research	Industry	Other	Research	Industry	Other
Austria	20	10	5	8	2	2	8	2	2	2	3	1	2	3	0
Belgium	11	10	5	3	3	0	3	3	0	3	1	4	2	3	1
Bulgaria	2	0	1	1	0	0	1	0	0	0	0	1	0	0	0
Czech Rep.	1	6	0		2	0		2	0	0	2	0	1	0	0
Denmark	6	4	0	1	1	0	1	1	0	2	0	0	2	2	0
Estonia	0	3	0	0	0	0	0	0	0	0	2	0	0	1	0
Finland	7	5	0	3	2	0	3	2	0	0	1	0	1	0	0
France	31	39	4	9	10	1	9	10	1	8	13	2	5	6	0
Germany	55	44	2	16	13	0	16	13	0	18	15	1	5	3	1
Greece	18	10	2	7	4	1	7	4	1	3	2	0	1	0	0
Hungary	1	3	0	0	1	0	0	1	0	1	1	0	0	0	0
Ireland	5	5	0	2	2	0	2	2	0	1	0	0	0	1	0
Italy	42	36	4	14	12	2	14	12	2	6	6	0	8	6	0
Luxembourg	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0
Netherlands	14	15	2	3	4	1	3	4	1	5	5	0	3	2	0
Norway	12	2	0	3	0	0	3	0	0	4	2	0	2	0	0
Poland	1	4	0	0	1	0	0	1	0	0	1	0	1	1	0
Portugal	5	10	0	1	3	0	1	3	0	1	3	0	2	1	0
Romania	4	3	1	2	1	0	2	1	0	0	1	1	0	0	0
Slovenia	0	2	0	0	0	0	0	0	0	0	0	0	0	2	0
Spain	20	33	7	5	8	3	5	8	3	6	8	1	4	9	0
Sweden	8	6	7	4	2	3	4	2	3	0	2	1	0	0	0
Switzerland	9	15	1	4	6	0	4	6	0	0	1	1	1	2	0
UK	18	21	2	4	5	0	4	5	0	7	6	1	3	5	1

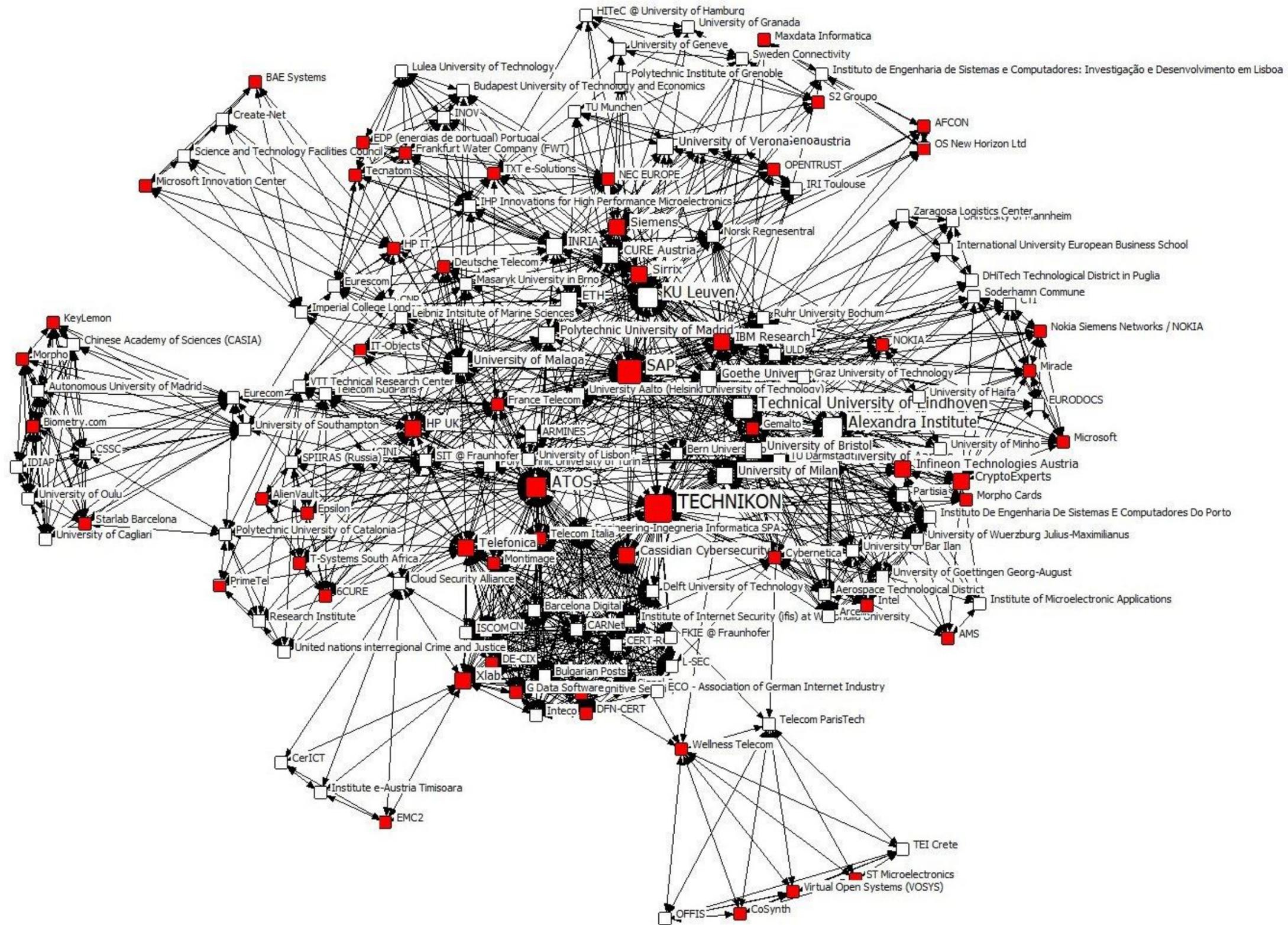
9.4. Detailed FP7 participations in FP7 Trust and Cybersecurity programme



Participations and links in FP7 Trust and Cybersecurity programme

In the figure the colour red is used to indicate industrial and consultancy organisations. Industrial partners can be technology providers, integrators and users of cybersecurity solutions. The cooperation between the different partners is indicated by lines between the nodes.

9.5. Detailed FP7 project participations (>2) in FP7 Trust and Cybersecurity programme



The red rectangles indicate industrial partners and the size of the rectangle is proportional to the number of project grants this participant was able to obtain from the programme.

[This page was left blank intentionally]