ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State’s local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact
For queries in relation to this document, please use wg2_secretariat@ecs-org.eu

Classification and Distribution
This document is classified as internal to ECSO for discussion with the EC.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources including external websites referenced in this publication.

Disclaimer

This document has been prepared by the European Cyber Security Organisation and it reflects the views only of its authors.

Copyright Notice

Reproduction is not authorised.
# VERSION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status</th>
<th>Editor(s)</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>2018 05 07</td>
<td>Draft to the EC for review</td>
<td>ECSO Secretariat – approved by the Monitoring Task Force</td>
<td>Extended perimeter of EC investment (DS-07-2017, DS-08-2017 and 50% of CIP-01-2016-17), updated figure of KPI 3 and KPI 5</td>
</tr>
<tr>
<td>2.</td>
<td>2018 06 05</td>
<td>Draft to the EC after 3rd PB</td>
<td>ECSO Secretariat</td>
<td></td>
</tr>
<tr>
<td>2.1.</td>
<td>2018 07 04</td>
<td>Draft to the EC after meeting 26.06 with CNECT and 10.07 with RTD</td>
<td>ECSO Secretariat</td>
<td>Formal changes to be in line with the contract, new figures from market analysis (including an update of the leveraging factor), and additional information on the survey (response rate).</td>
</tr>
<tr>
<td>3</td>
<td>2018 08 27</td>
<td>Final Draft to the European Commission</td>
<td>ECSO Secretariat</td>
<td>Executive summary, update of H2020 projects description in 2.1 Section and formal changes</td>
</tr>
<tr>
<td>4</td>
<td>2018 10 08</td>
<td>Final Draft to the European Commission after the feedback from CNECT on 25.09</td>
<td>ECSO Secretariat</td>
<td>Changes according to the EC comments on 1) Survey assessment methodology, 2) Market analysis 3) Collection of EC data</td>
</tr>
<tr>
<td>5</td>
<td>2018 10 10</td>
<td>Final Draft V5</td>
<td>ECSO Secretariat</td>
<td>Changes on wording related to the Survey assessment methodology</td>
</tr>
<tr>
<td>6</td>
<td>2018 10 29</td>
<td>Final Version</td>
<td>ECSO Secretariat</td>
<td>Disclaimer added as suggested by RTD</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The contractual Public-Private Partnership (cPPP) on cyber security was initially funded in July 2016 through the European Union’s Horizon 2020 Framework Programme for R&I. This initiative aims to be the industrial policy hub dedicated to fostering the competitiveness of European solutions. Thanks to 218 members across 28 countries (by the end 2017), European Cyber Security Organisation (ECSO) builds solid bridges between academic research communities, large corporates as well as SMEs, national and local public administrations, and end-users. Such a global approach enables to envision solutions that includes the sustainability of the most important government processes, the provision of vital services and the day-to-day role of European citizens.

The cPPP on cyber security has its roots in the 2013 European Cyber security Strategy adopted by the European Commission (EC) to provide a strategic framework for the EU initiatives on cyber security and cybercrime. It emphasises the need to develop industrial and technological resources for cyber security in the EU. The Digital Single Market Strategy for Europe published by the EC in 2016 acknowledges the existing specific gaps in the fast-moving area of cyber security technologies. In this context, there is a need for a more coordinated approach to step up the supply of more secure solutions by European industry and to stimulate their take-up by enterprises, public authorities, and citizens. In addition, the Commission Communication Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cyber security Industry reaffirmed the need to adopt a comprehensive approach to cyber-resilience and cyber security industrial policy, which would include research and innovation.

In July 2016, the EC signed a contract with the European Cyber Security Organisation (ECSO) ASBL establishing a contractual Public-Private Partnership (cPPP) on cyber security. The objectives of the cPPP are the following:

- Boosting European cyber security research, development, innovation and use of European cyber security solutions as means to support and protect the development of the Digital Single Market in Europe;

- Fostering European cyber security leadership for job creation and prosperity;

- Accelerating Europe’s innovation process and raise the competitiveness of cyber security industry in the EU on the global market.

The first Monitoring Report conducted by ECSO covers the period from July 2016 to December 2017. It lays out ECSO’s vision for the future of the cyber security sector in Europe and provides an analysis of R&D areas covered by the cPPP’s operations. Our methodology includes trend analysis and yearly surveys. These regular surveys were answered by ECSO members and H2020 beneficiaries and allowed to gather data and information on R&D investments and the creation of jobs in the European cyber security sector.

3 Contractual arrangement setting up a public-private partnership in the area of cyber security industrial research and innovation between the European Union and the European Cyber Security Organisation, 5 July 2016.
Please find below a few outcomes of the report:

- **Membership and Governance**: the European Cyber Security Organisation (ECSO) has continued to grow - from 132 members in 2016 to 218 at end 2017. In parallel, ECSO has designed and implemented an efficient governance model which is based on three main bodies: a Board of Directors, a National Public Authority Representatives Committee, and a Partnership Board.

- **R&D activities**: in the context of the cPPP on cyber security, the first H2020 projects were launched. The first step was in December 2016 with the delivery of the first official version of the Strategic Research and Innovation Agenda (SRIA), which was shared with the EC services and Member States representatives at the Programme Committees. The ECSO SRIA report is the result of extensive discussions conducted among ECSO’s members and involving more than 300 experts. In 2017 the European Commission has funded the first 19 cPPP projects through the H2020 programme (€67.45 Million) and divided in four topics (DS-06-2017, DS-07-2017, DS-08-2017 and CIP-01-2016-17 limited to 2017).

- **Private investments**: the ECSO’s stakeholder community is currently achieving, and actually exceeding, the expected planned level of investment for the cPPP in cyber security since it was signed in July 2016. The results of the analysed data show that, apart from the H2020 funding, the total R&I investment of the European cyber security industry in 2017 and within the SRIA perimeter could be estimated at € 522 Million.

- **Job creation**: in order to sustainably support the growth of the European cyber security industry, one must first make sure that an increasing workforce is available in Europe. Until now, it has been very challenging to determine the estimation of the overall number of employees in the cyber security sector, namely the baseline workforce in cyber security. However, the first Public Monitoring Report shows the positive trend of the jobs market within the entire value chain of the industry and among SMEs which have experienced an important increase (+ 80%) of employment in the 2016-2017 period.

- **The role of the SMEs**: SMEs are considered as the backbone of the European economy by the development of R&D that enhance global competitiveness. For this reason, ECSO established a specific Working Group in which the number of 55 SMEs (+23 comparing to 2016) cover the complete cyber security value chain. This specific Working Group gives them the opportunity to collaborate for developing their place in the market. In this regard, the inclusion of a dedicated support to SMEs in the Work Programme has been considered as a significant achievement. Unfortunately, this has not increased yet the participation of SMEs to the first cPPP projects as it was originally expected. More efforts will be required to promote and empower the role of SMEs. A range of specific measures are under elaboration to achieve this, such as for instance the creation of a SME Hub Platform.

It is important to emphasize that due to the fast digitalisation of several sectors of European economy, the need for a comprehensive approach to cyber security has also gained the strategic importance for the European society as whole. Hence, the SRIA sets out a number of societal challenges which go beyond the type of collaborative research efforts that may normally be supported through H2020 or by industry acting alone. These actions address the wider context of the R&I environment that are important. Firstly, the objective is to develop new enhanced technologies and services adapted to consumer needs that will respect security and integrity of
data and ensure the protection of personal data in a way compliant with the new General Data Protection Regulation. Secondly, the development and implementation of education programme as well as raising awareness solutions and campaigns on cyber security for society at large, including companies (especially SMEs) and citizens is of major importance.

Looking at the evaluation of the KPIs agreed with the European Commission, after 18 months of operations for the cyber security PPP Contractual Arrangement, we can say that the programme is positively progressing. For instance, ECSO is even exceeding its target on the leverage effect in the field of R&D investment.

If the EU wants to position itself as a global market player in an inter-connected world, mastered by technologies, more challenges remain to be overcome. In this context, the cPPP on cyber security and ECSO itself distinguish themselves on the European stage. Since the beginning, these innovative initiatives have considered the need to develop a solid European cyber security ecosystem. Beyond R&D issues, ECSO tackles fundamental industry policy aspects for market deployment and economic competitiveness. For instance, this includes certification, public and private investments, local aspects, education and training. In 2017, ECSO developed and is still developing key elements for the growth and harmonisation of the European cyber security Community and Ecosystem. To tackle the challenges the European cyber security industrial policy faces today, various activities have been launched through an integrated set of five additional working groups. The Annex IV of this report summarizes these additional activities (Certification, Market deployment & Private Investment, Sectoral demand, Support to SMEs, Education, training and raising awareness).

The 2017 EU’s Cybersecurity Joint Communication on strengthening Europe’s cyber resilience system\(^4\) recalls the need for a more comprehensive approach, such as for instance with the Cybersecurity Act. This announcement sets out the range of measure that the EU needs to take. The work conducted by ECSO will follow the same path for an effective development of the European cyber security ecosystem. In the context of the post H2020, the creation of a European Cybersecurity Network and cybersecurity Competence and Research Centre at its heart, and a reinforced ENISA, a boosted configuration of the current cybersecurity system is being discussed by ECSO in close cooperation with the EC and a solid involvement of all its public and private members.

**Disclaimer**
This document has been prepared by the European Cyber Security Organisation and it reflects the views only of its authors.

# TABLE OF CONTENT

## ABOUT ECSO

---

## EXECUTIVE SUMMARY

---

## 1. INTRODUCTION

---

## 2. MAIN ACTIVITIES AND ACHIEVEMENTS 2016 – 2017

### 2.1. Implementation of the relevant 2017 calls for proposals

---

### 2.2. Mobilisation of stakeholders, outreach, success stories

---

### 2.3. ECSO governance

---

## 3. MONITORING OF THE OVERALL PROGRESS SINCE THE LAUNCH OF THE CPPP

### 3.1. Achievement of the goals of the cPPP

---

### 3.2. Progress achieved on KPIs

---

### 3.3. Evolution over the years

---

## 4. OUTLOOK AND LESSONS LEARNT

---

## Annex I – Common Priority Key Performance Indicators

---

## Annex II – Specific Key Performance Indicators for the cPPP

---

## Annex III – Contribution to Programme-Level KPI's (to be provided by the EC)

---

## Annex IV – Report on industrial policy activities
1. INTRODUCTION

From the *WannaCry* virus and *NotPetya* malware to revelations about election interference in Europe and worldwide, 2017 provided nearly constant reminders about the challenge and importance of building a robust and secure industrial base for the digital age. The past year also marked an important phase in the implementation of the cyber security contractual Public-Private Partnership (cPPP), as the first cyber security H2020 projects in the context of the cyber security cPPP have been launched and the European Cyber Security Organisation (ECSO) have continued to grow and put additional building blocks in place to support the European cyber security community.

The youngest cPPP launched by the EU has its roots in the Cybersecurity Strategy of the European Union adopted by the Commission in 2013 to provide the overall strategic framework for the EU initiatives on cyber security and cyber crime. The 2013 document emphasises the need to develop industrial and technological resources for cyber security in the EU. In its COM (2015) 192, the EU recognised that the specific gaps still exist in the fast-moving area of cyber security technologies and that a more comprehensive approach is needed in order to stimulate European cyber security industry. In addition, the COM (2016) 410 highlighted the need for a comprehensive approach to cyber-resilience and cyber security industrial policy, including research and innovation.

**Goals and Budget**

In July 2016, EU signed a contract with the European Cyber Security Organisation (ECSO) ASBL establishing a cPPP on cyber security. While the focus of the ECS cPPP is – like other “traditional cPPPs” – on R&I, the objectives defined in the cPPP are much broader:

- boost European cyber security research, development, innovation and the use of European cyber security solutions as means to support and protect the development of the Digital Single Market in Europe,
- foster European cyber security leadership for a job creation and prosperity,
- accelerate innovation processes at European level and raise the competitiveness of the European cyber security industry in the global market.

According to the established cPPP, the EU has committed to invest up to 450 million euros under its research and innovation (R&I) programme *Horizon2020* over the period 2017-2020. ECSO’s stakeholder community is planning to invest three times more, bringing the total amount of investment in European cyber security ecosystem up to 1,8 billion euros.

---

7 Commission Communication Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry COM (2016) 410
8 Contractual arrangement setting up a public-private partnership in the area of cyber security industrial research and innovation between the European Union and the European Cyber Security Organisation, 5 July 2016.
**Strategic Research and Innovation Agenda (SRIA)**

In order to achieve the above-mentioned objectives, the first formal version of the Strategic Research and Innovation Agenda (SRIA) was finalised in December 2016 and shared with the European Commission. The ECSO SRIA document⁹ is a result of the extensive analysis and discussions within ECSO Working Group 6 (WG6), involving more than 300 experts. It highlights the cyber security sectors which are strategic to Europe, in order to link the demand with the supply side and determine research priorities in a top down approach – by identifying the main requirements from the vertical application domains and users’ needs, and by defining large transversal infrastructures (applicable to several domains) while leveraging upon basic components, all in an improved ecosystem able to understand the challenges and use of innovative solutions. Accordingly, the document is organised in four thematic areas – *ecosystem, vertical sectors, transversal infrastructures, technological components*. Drawing on the inputs of ECSO members, the Strategic Research and Innovation Agenda is revised and updated on an annual basis.

Following the successful drafting and approval of the strategic document, the first cPPP projects were launched in 2017. During the first year, 67.45 million euros were invested under the H2020 programme. The investments were allocated to four strategic areas – DS-06-2017, DS-07-2017, DS-08-2017 and CIP-01-2016-17 (this last call is limited to 2017 and funded by DG CNECT, 50% and by DG HOME, 50%). This report presents the results from the first year of SRIA implementation and demonstrates the positive effects of the private investments in the area covered by the cPPP SRIA.

**Cyber Security Industrial Policy**

While establishing a roadmap for the future R&I activities, ECSO also works to tackle other important cyber security industrial policy issues. In parallel with WG6, related to the R&I and the main cPPP counterpart, ECSO has established five other working groups (WGs) in order to address European cyber security issues in a holistic approach and cover such topics as innovation development and market deployment, cyber security industry development and standardisation, as well as cyber awareness and training. The achievements of the five WGs, designed to interlink with WG6, and their input in supporting the implementation of the R&I strategy of the WG6 are summarized in the Annex IV of this report.

The increased recognition of the cyber domain can be considered as one of the most significant changes since the EU establishment of the cPPP on cyber security. After being a niche area for a long time, cyber security has recently emerged as a major societal concern – from scientists to business, to governments, to individuals, and to society as a whole. Issues surrounding espionage and data protection, disruptive business models, privacy, information operations up to warfare and of course around the Internet of Things (IoT) and Artificial Intelligence (AI) have become central to the way corporate, people and public administration

---

⁹ ECSO SRIA can be accessed here: [https://www.ecs-org.eu/working-groups/wg6-strategic-research-and-innovation-agenda-ria](https://www.ecs-org.eu/working-groups/wg6-strategic-research-and-innovation-agenda-ria)
think about and implement what it means to be cyber secure. In the timeframe of our cPPP (until 2020), we expect even more attention to these important issues and we will continue to focus industry support to face such important challenges. In this regard, we estimate that the size of the European cyber security industry between 2016 and 2017 has grown at a rate of 8.3% - from 25 billion euros in 2016 to 27 billion euros in 2017.10

As the implementation of the cPPP has just begun, we can only assess the first projects and actions carried out under H2020 programme, while the report on the innovation outcomes will be carried out in the upcoming years. However, the monitoring of the first 18 months has been crucial establishing baselines and Key Performance Indicators (KPIs), as well as identifying private investment patterns and jobs market trends, which will serve as a reference point for the next years.

We remain convinced that having a robust European cyber security industry is essential for securing Europe’s digital future and protecting EU citizens against cyber threats. Such political and economic developments as the proposed European Cybersecurity Act and the implementation of Digital Single Market strategy shows the urgent need for consistent action towards further enhancing European cyber industry. As a “multiscale ecosystem builder” which is capable to address concerns of the R&I activities, industrial development and cyber policies at the local, national and European levels, we will continue towards the successful implementation of the cPPP on cyber security.

The first progress monitoring report (PMR) provides an assessment of the implementation of the cPPP since its launch in July 2016, indicates the main accomplishments, as well as provides recommendations for the further stages of its implementation.

**cPPP on Cyber Security at a Glance – 1st Period**

**Investment in R&I**
- 481,5 million euros in 2016 and 522 million euros in 2017 were invested by the European cyber security market players in topics related to the ECSO SRIA perimeter
- 67,45 million euros in 2017 were invested by the European Commission under its H2020 programme

**ECSO Market Estimation (based on 10 different market studies – refers to footnote 10)**
- In 2016, European cyber security market amounted to 25 billion euros
- European market accounted for 27% of the global market in 2016 estimated 90 billion €
- Total number of cyber security companies in Europe in 2016 was of the order of 11,000.

**Cyber Security Industry Employment**
- Cyber security sector employed around 180 000 – 200 000 workers in 2016
- By 2017, employment in cyber security sector has grown 10% in large companies, 80% in SMEs and 45% in RTOs

---

10 The market analysis we have performed is based on 10 different market studies published recently on the web (Cybersecurity Ventures Orbis research, Alliedmarket research, Gartner, Markets&Market, Reportbuyer, Zion Market Research, Mordor Intelligence, Research Beam, Market Research Future, PWC and AGC). These sources have been analysed to determine an estimate of the global cybersecurity market in Europe and the relative growth.
2. MAIN ACTIVITIES AND ACHIEVEMENTS 2016 – 2017

2.1. Implementation of the relevant 2017 calls for proposals

The first calls – pertaining to the activities of the ECS cPPP and being a part of the 450 million euros investment of EU under its H2020 programme – were closed on 25 April 2017 and 24 August 2017. The evaluation of the proposals for the first call (DS-06-2017) were completed in 2017 and of the other three calls completed in 2018. There are four main calls for proposals that can be attributed to the cPPP activities:

- DS-06-2017: Cyber security PPP: Cryptography (four projects)
- DS-07-2017: Cyber security PPP: Addressing Advanced Cyber Security Threats and Threat Actors (five projects, one of which starts in September 2018)
- DS-08-2017: Cyber security PPP: Privacy, Data Protection, Digital Identities (seven projects, one of which starts in September 2018)
- CIP-01-2016-17: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe (topic funded 50% by DG CNECT and 50% by DG Home) (three projects funded under the 2017 call)

Projects under the call DS-06-2017 started on 1 January 2018, and those under the call CIP-01-2016-17 have already been selected with the starting dates ranging from May to September 2018. The list and information of the selected projects under the calls DS-07-2017 and DS-08-2017 have just been published on CORDIS (July 2018), allowing to include a quick analysis of them in this report.

The successful launch of the first H2020 projects allowed to advance the R&I goals defined in the ECSO SRIA document. The analysis presented herein is solely based on the topics that will be addressed by the projects, as well as their potential impact on strengthening European cyber security ecosystem. The ESCO SRIA v1.2 includes the areas and the priorities of the calls indicated in the European Commission Working Programme for 2016 – 2017, because they were defined before the creation of ECSO and the signature of the ECS cPPP, even if the precise domains and foreseen solutions of these projects were not known yet. In the following paragraphs we will present the analysis of both ongoing and just retained projects, which were funded under ECS cPPP framework. We will also assess their relevance to the ECSO SRIA strategy.

The call CIP-01-2016-17 is dedicated to the protection of critical infrastructure, covering both the physical and cyber dimensions of security. The call also covers the period before cPPP on cyber security was signed. After the establishment of cPPP on cyber security, three projects – Resisto, Safecare and Finsec – have been retained for funding in 2017. RESISTO aims to develop a platform for Communication Critical Infrastructures holistic situation awareness and enhanced resilience. SAFECARE seeks to provide solutions which aims to improve physical and cyber security in health sector by developing and promoting new technologies to enhance threat prevention, threat detection, incident response and mitigation of impact. FINSEC aims to provide a mature implementation of the reference architecture (RA), based on the enhancement and
integration of the novel solutions from the partners (e.g. Anomaly Detection, AI CCTV Analytics, Risk Assessment Engines, Collaborative Risk Analysis & Management, Compliance), in order to strengthen the security of the financial sector.

The ECSO SRIA identifies the need to invest and focus on the protection of the critical infrastructure. For this, we need the analysis of the risk aspects of the evolving technology in relation to legacy systems, as it will help to achieve an adequate level of protection and risk management. The ever-increasing use of IoT and Cyber-Physical Systems (CPS) to achieve a higher degree of automation exposes critical infrastructures to new types of attacks. Thus, monitoring and threat detection tools become of primary importance when reacting quickly to threats with a strong degree of automation, in order to enhance the resilience and high availability of the systems and critical infrastructures.

The call DS-06-2017 primarily focuses on the Cryptographic solutions which go beyond already existing techniques such as homomorphic encryption (for processed data), anonymisation and obfuscation (including the measurement of the information leakage), lightweight crypto for tiny battery powered devices, implementation of hardware and software crypto and its usage, token-based authentication mechanisms for payment schemes, privacy preserving mechanisms and post quantum cryptography. FENTEC addresses functional cryptography to allow the processing of the encrypted data, addressing privacy preserving mechanisms, statistical computation and analytics over encrypted data, and IoT-specific use cases. PRIViLEDGE project focuses on the blockchain and distributed ledger technologies supporting privacy, anonymity and decentralised consensus. Recently launched (January 2018) PROMOTHEUS and FutureTPM projects focus on the post-quantum computing. The former aims to design new security primitives and protocols, while the latter aims to design and develop a quantum-resistant trusted platform module with provably-secure algorithms.

The ECSO SRIA identifies the need to invest and focus on both software and hardware crypto solutions which are affordable (in terms of complexity and cost) and have wide applicability in several industrial sectors, including the protection of the privacy of the citizens, e.g. homomorphic crypto solutions of dedicated crypto hardware. In addition, the ECSO SRIA strategy indicates the importance of designing quantum resistant crypto technologies with a smaller cyber innovation cycle, enabling to meet the challenges of future threats and market opportunities in Europe.

Regarding blockchain and distributed ledger technology (DLT), the ECSO SRIA strategy highlights the need to improve the cyber resilience of the finance sector – from bringing more trust and auditability to reducing the costs associated with the usage of intermediaries. Many challenges (e.g. throughput in number of transactions, scalability, latency, capacity, etc.) still need to be addressed to make the technology usable in different applications where automated process, involving devices, could be set up without the need for a centralised infrastructure.

The call DS-07-2017 focuses primarily on cyber security threats and its management, both in terms of raising awareness and collecting evidence, and in terms of simulation environments and training materials to counter advanced cyber attacks. SPEAR project aims to define new technologies for the Smart Grids, which helps to detect threats and develop appropriate security solutions, including the collection of the forensic information to provide evidence of the possible attacks. ASTRID project focuses on the microservice architectures and virtualised services with the aim to develop new opportunities in situational awareness. CYBERWISER.EU project seeks develop an educational, collaborative, real-time civil cyber range platform, while CYBER-TRUST seeks to address the security of IoT devices with the intent to develop a cyber intelligence platform. REACT
project focuses on the proactive measures to identify and reach to potential attacks and on the fortification solutions to the potential targets with passive and active defence approaches.

The ECSO SRIA indicates the importance of developing new cyber ranges and simulation techniques, including a strict focus on education and training. These actions are necessary if we want to empower individuals and organisations for situational awareness and cyber-threat detection.

The call DS-08-2017 indicates the need for the new solutions and tools to support the fundamental rights in digital society and, specifically, to increase trust in Europe’s digital economy. Three areas have been identified and addressed by the funded projects: privacy-enhancing techniques (PETs), GDPR in practice and, finally, secure digital identities. Most of the funded research activities in the nearest future will focus on GDPR and its application in practice. SMOOTH project focuses on creating GDPR awareness to micro-enterprises and assisting them in becoming fully compliant with the regulation. DEFeND project seeks to develop a platform to test GDPR compliance of the organisations. BR4GDPR project seeks to create the end-to-end, GDPR compliant, intra- and inter-organisational, ICT-enabled processes at various scales, to investigate PETs, and, ultimately, to provide the Compliance-as-a-Service (CaaS) solution. PDP4E projects plans to integrate privacy and data protection techniques into the existing software tools so that the final products would be GDPR compliant. PoSeID project seeks to develop a dashboard for the monitoring of the personal data protection and for the controlling the privacy settings, with the ultimate goal to support GDPR compliance of the services and products. PAPAYA project focuses on untrusted third-party data processors and the related privacy concerns. Finally, OLYMPUS seeks to address secure digital identities – Intrusion Detection and Prevention Systems (IDPs) in particular – to allow users to maintain unlinkable identities with different service providers and to achieve a secure and interoperable European identity management framework.

Although ECSO SRIA strategy indicates the importance of developing a new privacy enhancing techniques, especially in e-governance and public administration, the funded projects limitedly cover these aspects and mainly focus on providing relevant tools to test GDPR compliance and developing new data protection awareness services. Nevertheless, the implementation of these projects will help to strengthen European market and guarantee the fundamental rights of the EU citizens.

2.2. Mobilisation of stakeholders, outreach, success stories

ECSO – a unique pan-European cyber security organisation

The nature of ECSO reflects the very peculiarity of the cyber security domain. While cyber security can be described as a vertical/industrial industry, it is also (and most importantly) an operational domain of non-specialized players, such as public authorities, infrastructure operators and corporations. Because of this, research and innovation (R&I) activities are led not only by traditional players as research and technology organisations (RTOs) and specialized companies but also by a multitude of technology end-users, ranging from industrial integrators and infrastructure operators to financial organisations (e.g. insurance), to clusters, to public administration and regional authorities.
The involvement of a broad range of stakeholders in the ECS cPPP and ECSO association to support the development of European cyber security ecosystem is a very important and unique precedent. ECSO already had 132 members when the cPPP on cyber security was signed on 5th July 2016. Eventually, 86 news members joined ECSO community and by the 5th December 2017 ECSO was already counting 218 members from 28 different countries. Regarding the profiles of the new members, they were representing users & operators, national public administrations, research centres and SMEs.

![ECSO Members as of 5 December 2017](image)

**Figure 1. E COS members by category**

Since its launch in July 2016, ECSO has been developing its communication strategy. The strategy is structured around three key objectives:

- establishing a pan-European stakeholder awareness on the importance of cyber security and its implications to our economies and societies;
- promoting the cPPP on cyber security, as well as its activities and achievements in addressing cyber security issues;
- promoting ECSO messages stemming from deliverables, position papers and reports prepared by its six working groups and approved by its Board of Directors.

To achieve these objectives, ECSO and its members have participated in a more than 97 events (see KPI6) throughout the reporting period of July 2016 – December 2017.

On the 7th July 2016, during ECSO Extraordinary General Assembly its Board of Directors was elected, according to specific rules described in the ECSO Bylaws (see section 2.3). On 20th June 2017, ECSO held its first General Assembly in Brussels, Belgium, attended by 150

---

11 As the Board of Director is in charge of the official approval, those figures don’t take in account the members applications got after the Board of Direction of 5th December.

12 ECSO countries include: Member States, EEA/EFTA countries, H2020 associated countries.

participants representing ECSO members. The General Assembly provided an opportunity to gather the entire ECSO community to discuss the management of the association. The General Assembly was followed by a public event open to ECSO members and potential new members, as well as non-ECSO members from European institutions, agencies and associations. During the event, ECSO Secretariat presented the evolution of the cPPP on cyber security, its achievements and the strategic outlook for the upcoming year.

Throughout 2017 ECSO implemented a wide range of activities to promote collaboration among European organisations and institutions to effectively address the issues related to cyber security industrial policy. Due to these activities, ECSO not only became known as European ‘ecosystem builder’, but also raised the awareness of the strategic importance of cyber security for the European industry. ECSO has established strong relationships and collaborations with many European Union agencies and bodies (ENISA, EUROPOL, EASA, CEN/CENELEC, ETSI, EDA, EIT Digital, EIB, etc), some of which are now moving towards a more formalised collaborations with ECSO, based on the memorandums of understanding (MoUs).

ECSO has also established important synergies with other cPPPs, including Factories of the Future, Big Data Value, 5G IA, euRobotics, Energy-efficient Buildings etc., with the aim to address cyber security challenges and investigate possible cooperation opportunities with other cPPPs for a comprehensive and effective implementation of European cyber security strategy. The cooperation with other cPPPs is implemented at two levels – the strategic level and the technical level. While the former includes close cooperation between cPPPs and ECSO Secretariat, the latter involves close coordination between cPPPs and ECSO members. The goal of this two-level cooperation is to jointly coordinate and define European cyber security R&I priorities, embracing vertical sectors and other technologies.

The presence of the common members in other cPPPs and related EU initiatives, as well as the continuous dialogue at the ECSO Secretariat level help to guide the external collaboration. Three external collaborations were initiated in 2017 (with a few more planned in 2018, e.g. with euRobotics):

- **BDVA.** A first roundtable discussion with Big Data Value Association has been organised on 20th June 2017 and a second open meeting on 23rd November 2017. The outcome is a list of shared topics and areas of collaboration between the two cPPPs, which will have an impact on ECSO SRIA.

- **EFFRA.** ECSO gave a presentation at European Factories of the Future Research Association event in September 2017 with the aim to investigate the requirements and cyber security challenges facing digitising industries. The roundtable discussion on this topic is planned for 2018.

- **5G IA.** Both ECSO and 5G Infrastructure Association identified the need to work on a common cyber security strategy addressing encompassing vertical sectors (ex. transport), standards and research priorities.
2.3. ECSO governance

The ECSO governance model, extensively presented in the Industrial Vision document\textsuperscript{14}, is based on the three bodies: Board of Directors, National Public Authority Representatives Committee and Partnership Board (see the scheme below).

\textbf{ECSO Board of Directors}

ECSO Board of Directors manages ECSO and steers the cyber security industrial policy issues. Its activities are supported by the Coordination / Strategy Committee, which is coordinating the activities of the different Working Groups and Task Forces. ECSO Board of Directors is composed of representatives from each membership category/constituency, namely large companies, SMEs, RTO/Universities, users & operators, national public administrations, regions and clusters. During the Extraordinary General Assembly, ECSO members elected the Board, composed by the First Directors (mandate for 3 years) and Directors (mandate for 1 year). Such mandate system allows

\textsuperscript{14} http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf
ECSO to ensure both the continuity in its management and the opportunity for the new members to be elected and actively participate in ECSO governance.

*The National Public Authority Representatives Committee (NAPAC)*

ECSO also established the National Public Authority Representatives Committee (NAPAC), which consists of the representatives from the national public authorities. As (cyber) security is a national prerogative, the participation of the national governments in cPPP implementation is of fundamental importance. Instead of traditional “mirror groups”, the NAPAC has been designed to allow national representatives to have their own forum for dialogue and discussion, while closely working with ECSO members and governing bodies. The national representatives participate in NAPAC on their professional capacities as technical experts and policy officers\(^\text{15}\), but not as the formal representatives of the Member States as it is the case in the Programme Committees and European Council.

The aim of the NAPAC is (a) to participate in the discussions and activities of the ECSO Working Groups and Task Forces, as well as to bring a governmental perspective and operational needs; (b) to support the development and implementation of the ECSO SRIA and ECSO Multiannual Roadmap into the R&I Work Programme; (c) to exchange the best practices and promote the national / regional research programmes on cyber security.

The initial conference calls were organised between July and December 2016 among several public administrations and ECSO Secretariat, with the aim to exchange the information and to define the Working Terms of the NAPAC. The NAPAC Secretariat is managed by the European Network and Information Security Agency (ENISA) with the support of the ECSO Secretariat.

*ECSO Partnership Board*

Partnership Board is a formal communication channel between the European Commission and ECSO in order to discuss the Horizon 2020 Work Programme relevant to the implementation of the cPPP on cyber security, the implementation of the overall R&I programme related initiatives and the monitoring of the key progress indicators (KPIs). Partnership Board is composed of the representatives of the European Commission and ECSO members (with an exception of the national public administrations). Due to its nature, Partnership Board allows to have an open dialogue between ECSO members and European Commission and ECSO and provides oversight of the cPPP implementation by monitoring, advising, providing support etc.

The European Commission called for the first Partnership Board on 6th October 2016. The Board discussed the rules of procedures as well as the first inputs of ESCO to the Commission’s Horizon2020 Working Programme 2018-2020. During the second (26th April 2017) and the third (27th October 2017) meetings of the Partnership Board discussion concentrated on the contract monitoring, the rules of the R&I agenda implementation and the demand side inclusion in the cPPP. The agreement on the monitoring methodology is a particularly important achievement of the Partnership Board\(^\text{16}\).

---

\(^{15}\) E.g. the National Authority for Cyberdefence and Network and Information Security -ANSSI- for France or the Ministry of Economic Development for Italy.

\(^{16}\) The document is available on the ECSO Portal. However, the access to the ECSO portal is restricted to the ECSO members. The EC-ECSO arrangement on monitoring mechanism is available to non-ECSO members upon request to secretariat@ecs-org.eu
3. MONITORING OF THE OVERALL PROGRESS SINCE THE LAUNCH OF THE CPPP

The monitoring and assessment of the progress in achieving the desired effects and expected impact of the CPPP on cyber security is important for the whole European cyber security community. For ECSO, it helps to track the progress of the CPPP implementation and to measure the impact of the activities. For ECSO members, it helps to understand and follow the major trends of the EU cyber security market. Finally, for the EC and national public authorities, monitoring is necessary to have a better understanding of the industrial ecosystems, as well as it advantages and limitations.

In its initial European cyber security industry proposal, ECSO provided a list of KPIs to describe in detail what would be needed to achieve a better understanding of the market trends. Through the consultation process, which took into consideration numerous inputs – including the experience of the other CPPPs and the outcomes of the mid-term evaluation exercise led by the EC’s Directorate-General for Research and Innovation (DG-RTD)\(^\text{17}\) – the initial proposal was modified, leading to a more focused and measurable set of KPIs to measure the CPPP on cyber security. The DG RTD-led review of the CPPP monitoring, the dialogue with the European Commission during the first year of the partnership and the extremely useful discussion during the second Partnership Board (26\(^\text{th}\) April 2017) helped to identify seven KPIs to monitor the impact of CPPP implementation in the future and to agree with the EC on the monitoring methodology.

In the following paragraphs, we introduce the impact analysis of the seven KPIs, which include indicators specific to the CPPP on cyber security market as well as indicators relevant to all CPPPs.

3.1. Achievement of the goals of the CPPP

In this section we focus on the first ECSO objective – to boost European cyber security research, development, innovation. The research projects under the cyber security calls (see section 2.1) are expected to produce the preliminary results in terms of technological solutions only in 2018, because by the end of 2017 they have been active only for a few months. It is still not possible to evaluate the potential market innovation of these projects at this stage. However, the ECS CPPP has already started to engage with the Coordination Support Action funded projects (e.g. EUNITY, AEGIS and Cyberwatching.eu) in order to understand the level of preparedness and coverage of the research priorities identified by ECSO, which aims to support the implementation of the Digital Single Market. The expected set of project activities carried out with the public investments under

the H2020 Work Programme will complement the industrial strategic priorities indicated in the ECSO SRIA v1.2.

Since the projects in the EC’s Working Programme 2018-2020 would likely deliver the results between 2021-2023 (keeping in mind the average period of three-years for the full implementation), the SRIA focuses on the short to mid- and long-term research priorities. Keeping into account the evolution of technologies, cyber threats and the changing market conditions, the specific guidelines are applied:

1. Allocating the funding to the applied research and innovation by focussing resources on fields that could maximise European competitiveness in the cyber security market.

2. Concentrating the research funding efforts on cyber security sectors strategic to Europe, such as healthcare, energy, transport, finance, and Industry 4.0.

3. Linking the demand and supply sides, as it helps to: (i) identify the main requirements from the vertical application domains / users’ needs, also useful to define large transversal infrastructures applicable to several domains, (ii) leverage upon basic components, all in an improved ecosystem able to understand the challenges and (iii) apply the most innovative solutions.

4. Evaluating the benefits of the available cyber security technologies from the previous projects through the main demonstrators and possibly based on European cyber security large transversal infrastructures.

5. Fostering continuous innovation through further research on basic technologies and components and anticipating the possibly disruptive technologies in order to keep the medium and long-term competitiveness of the products and services and foster European digital autonomy.
### Pilots and validation of solutions in INFRASTRUCTURE (for use in all sectors) & APPLICATIONS (specific verticals)

<table>
<thead>
<tr>
<th>Infrastructure Solutions</th>
<th>Applications/Specific Verticals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry 4.0 and ICS</td>
<td>Public Services / eGovernment</td>
</tr>
<tr>
<td>Energy</td>
<td>Healthcare</td>
</tr>
<tr>
<td>Transportation</td>
<td>Smart cities &amp; smart buildings</td>
</tr>
<tr>
<td>Finance and Insurance</td>
<td>Telecom, Media, and Content</td>
</tr>
</tbody>
</table>

---

### CYBERSEC TECHNOLOGIES & SERVICES to protect Infrastructure / Applications and citizens’ privacy

- Encryption (key management, homomorphic, post quantum, ...)
- ID and DLT (blockchain, ...) security
- AAA: Authentication; Authorisation; Accounting
- Security / Resilience & Privacy by Design (GDPR, ...)
- PET: Privacy Enhancing Technologies
- Information Sharing, Threat Detection and Intelligence (incl. sensors / probes for ICS, SIEMs and SOCs), Artificial Intelligence and Analytics
- Protection of innovative ICT infrastructure
- Risk Management, Response and Recovery
- Tamperproof communication protocols

---

### CYBER ECOSYSTEM: preparing the market to introduce and use innovations

<table>
<thead>
<tr>
<th>Standardisation</th>
<th>Legislation &amp; Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation / Labelling / Certification</td>
<td>Investments – Funds / Economics - Business models / Insurances</td>
</tr>
<tr>
<td>Trusted management of the supply chain: Assurance</td>
<td>Support to SMEs</td>
</tr>
<tr>
<td>Education (cyber-Erasmus)</td>
<td>Regional / local aspects</td>
</tr>
<tr>
<td>Training / simulation (certification of experts)</td>
<td>Awareness of citizens, users (Cyber Hygiene) and decision makers (procurement, implementation and use)</td>
</tr>
</tbody>
</table>

---

**Figure 3. A strategic view for the SRIA**

The core technologies at the backbone of the cyber security ecosystem are fundamental to ensure the creation of the cyber security supportive ecosystem and citizens’ participation in the digital world (see the bottom section of the Figure 3). Moreover, these core technologies are essential in protecting the infrastructure and applications to sustain the digital transformation in key economic areas and ensuring Europe leadership in these sectors (see the top section of the Figure 3). The development of the core technologies will be assured by a set of priorities and actions in critical areas to increase skills in risk management, to increase data security for data-driven applications and services, and to ensure the resilient and user-friendly architectures and tools for trusted cyber solutions and services.

**Development of innovative cyber security technologies and services**

The European technology capabilities in encryption, ID management, data protection as well as privacy should be continuously developed to face the changing cyber threats. For example, past investments have ensured Europe a leading position in digitalisation, but there is still a need for an ambitious strategy to meet the challenges of quantum computing and related cyber threats, as well as distributed approaches to ensure better authentication and authorisation schemes to increase trust in new cyber security solutions.
The privacy and security requirements for applications and data management (both at rest and in motion) are increasing, as citizens and governments become more and more concerned with data security and protection. The increased demand for security is related with the introduction of the user-friendly security mechanisms and specific risk management solutions. In Europe, there is an increased need to establish technologies and platforms which can help to ensure better risk management of infrastructure and more secure key applications, complying with European legislation, to address cyber threats (predict-prevent-detect-respond). To achieve innovation in cyber security technologies and to increase data security for data-driven applications and services, key priorities have been identified in ECS SRIA¹⁸.

European cyber security market has a strong position in several ICT technologies, however it is not always able to provide technological solutions to protect those ICT technologies. Because of this, non-European solutions are often used even if they might lack sufficient security validation. Such situation in European cyber security market emerged due to the weak investment models or due to the existing difficulties in defining the targeted business models.

To develop strong European solutions and innovative services, in particular for SMEs, it is vital to have a better understanding of the market needs and dynamics. This will also enable Europe to validate the trustworthiness of the supply chains and to have new methods for developing resilient systems out of potentially insecure components. The resilient and user-friendly architectures and tools for trusted solutions and services can be achieved by addressing the following priorities:

- **Security and privacy by design** → increased trust in solutions and services by both developers, using the components, and end-users; market stimulus for secure / privacy-friendly by-design solutions;
- **Trusted supply chain** → increased trust along the supply chain and improved market opportunities for security component suppliers;
- **Security services** → dynamic and innovative European market in cyber security services.

**Cyber ecosystem: preparing the market to introduce and use innovations**

Due to the digitalisation of the industry and the pervasiveness of ICT solutions and services at all levels, the sustainable growth of the European economy and the further implementation of the Digital Single Market strategy will become increasingly dependent on Europe’s ability to protect itself against cyber threats. Even if European countries have cyber strategies and preparedness trainings for business and citizens, they have different approaches and their maturity level to effectively address cyber threats is still considerably low. Hence, it remains important to raise cyber security awareness, to support education and training at local and European level, as well as to increase coordination and cyber security industrial policy harmonisation across countries, which will help to increase cyber hygiene among European population and to stimulate cyber security labour market.

In addition to education and training, Europe also needs a harmonised certification scheme, which would allow to have a trust in innovative cyber security solutions and secure procurement. This is particularly important for SMEs, because very often innovations come from them, but they are not sufficiently supported with market-specific instruments of standardisation. The fragmented

¹⁸ For more details see the SRIA document available on ECSO website.
approach to security assurance certification needs to be addressed, because it harms European cyber industry and precludes Europe from developing a strong cyber security ecosystem.

**Pilots and validation of solutions in infrastructures and applications**

Europe is the world leader in several industrial applications, the conventional key infrastructures and economic sectors. However, the available security solutions are not sufficiently tested for the specific applications (or not known by users) and very often are not validated or certified for the use of the specific applications.

The SRIA strategy focuses on key vertical markets where cyber security solutions need to be tested and their application validated. The key vertical markets which are highly dependent on innovations include Industry 4.0 and ICS; Energy and Smart Grids; Transportation; Finance and Insurance; Healthcare; Telecommunications and Media; Smart Cities and Smart Buildings; Public Services, eGovernment and Digital Citizenship. The implementation of the pilot projects can help to test the applicability and usefulness of the cyber security innovations to address the specific security needs of the verticals. Tested cyber security solutions will not only help to protect the critical infrastructure, the operation of services, and the competitiveness of the economic sector, but also to promote European innovative solutions.

**Sample of areas under development**

In terms of the SRIA implementation roadmap, industrial investments are mainly driven by the market needs and by the vertical applications, which have a direct impact on the growth of the European economy. This trend is apparent in the preliminary data analysis – the survey on the success stories and market studies indicates that industry is willing and planning to invest not only in the areas proposed by the cPPP R&I plan, but in a much wider spectrum of areas identified by ECS SRIA. The collected data allows us to identify the three main areas of investment:

- Technology development;
- Technology implementation and market deployment;
- Technology use in the different applications / verticals.

The primary focus areas of investment – in addition to the areas already mentioned in the Section 2.1, which are partially covered by public funding – are Risk Management, Detection, Response and Recovery, including Information Sharing and Threat Detection. In order to achieve practically applicable solutions to the protection of critical infrastructure, the research and development works have to be extended to another domains, such as Authentication to Encryption, As previously indicated, the main driving force are industrial applications in the vertical markets covered by the ECSO SRIA, including Industry 4.0, Finance, and Energy sectors among many others.

The analysis of the implementation of the ECS SRIA roadmap demonstrates only the initial results. The wider effects of the cPPP on cyber security will become more tangible in 2018, when the real impact of the private and public investment will be visible through new technological solutions available on the market and increased cyber resilience.
3.2. Progress achieved on KPIs

KPI 1 – Assessing the cyber security R&I investment leverage factor

Community commitment

Following the guidelines presented in the ECS SRIA, which reflects the needs of the European cyber security industry, ECSO stakeholder community has committed to increase the level of EU funding allocated to R&I in cyber security by a leverage factor of 3. As ECSO Monitoring Task Force analysis indicates, ECSO community is achieving and starting to exceed the amount of investments foreseen when cPPP on cyber security was established in July 2016.

Assessment methodology used

Progress monitoring methodology is composed of four steps, including:

1) Survey. To gather the data on R&I investments and the progress of the cPPP objectives implementation, 218 ECSO members and 44 beneficiaries of the H2020 project (DS-06-2017) were invited to participate in the monitoring survey. After 7 weeks of data collection, 81 responses (70 – from ECSO members, 11 – from H2020 beneficiaries) were received. The 30% response rate can be considered sufficient for this first analysis. However, when collecting the data for the next year’s monitoring report, ECSO Secretariat will be more ambitious and will seek to significantly improve the response rate. The detailed strategy is indicated in the OUTLOOK AND LESSONS LEARNT chapter.

2) Data analysis. The received survey responses have been organised in clusters corresponding to the ECSO membership categories. The analysis of the cumulative data for the different categories revealed the presence of potential outliers. Hence, to reduce the impact of the potential biases (e.g. over- or under-assessment of the private expenditure in research) to the final results of the analysis, we have inferred the average amount of investment for each type of organisation by computing the percentiles (5-th-95th; 10-th-90th; 15-th-85th; 25-th-75th). To highlight the potential outliers for the largest populations, the extreme values were eliminated from further analysis if an extreme deviation from the indicated investment average was found. Then, the average investment has been recomputed and multiplied by the number of survey participants belonging to that category.

3) Yearly estimation of the private investments. The collected data indicates the total amount of investment for the period between July 2016 – December 2017. To estimate the 2016 baseline, calculated on an annual basis, we have considered the total investment under the period of observation and then considered a growth of 8.3% from 2016 to 2017 to estimate the investment in 2016 and in 2017. Simulations for the other growth rates identified in the market analysis have been done as well.

4) Qualitative data collection. The last step of the progress monitoring methodology is the qualitative data collection, based on the analysis of the organisations’ success stories and the real impact of investment on R&I projects.
The main biases from the methodology and presented figures

When conducting data analysis, we assume the presence of the significant methodology biases, which can affect the results. The biases, such as the already discussed presence of potential outliers, can easily alter the estimations of the private investment in R&I and the final calculations of the leveraging factor.

There are several reasons for such biases to emerge. Firstly, R&I figures are often treated by companies as a confidential information, which is especially the case when dealing with the private R&I investments in cyber security. Unwillingness to share the specific data, even if it is an anonymous survey, reduces the response rates. Among ECSO members, the highest response rate is from the Regions (67%), which is the smallest category with only 3 members, and from the RTO & Academia (44%). The response rate of the remaining categories – Large Companies, Associations, SMEs and Public Administrations – is 30% on average.

Secondly, ECSO membership categories contains many companies and organisations, which are different in size of cyber security R&I, as well as in types of business, ranging from B2B to B2C, to B2G cyber security solution providers. Because of these differences, the estimated averages of investments per category cannot be compared. In some cases, it might be difficult to differentiate between the general R&I investments and cyber security specific R&I investments, or the investments allocated to both business development and R&I units (especially in the case of SMEs).

Figure 4. The size of the private investment by different types of organization (July 2016 -- December 2017). The size of the data points indicates the number of answers received per value. The median is represented by the horizontal line.

Even if the response rate of the survey is considered as sufficient by statistic approach, some answers do not meet the general assumptions and can be regarded as the underestimation of investments received by the organisation. Figure 4 shows (in logarithmic scale) the distribution of the answers from each category and the median using all data points available. Only the companies
belonging to ‘Large companies’, ‘SMEs’ and ‘RTO’ categories have a significant number of responses to plot the percentiles.

To reduce the potential bias in the estimation of the average, which is used to compute the 2016 baseline and 2017 leverage factor, the outliers are removed for the three above-mentioned categories based on the plotted percentiles. The average private investments injected into cyber security market per category in 2016 (starting from the launch of the cPPP) and in 2017 is estimated (see Figure 5) keeping into account the different values of percentiles to identify the outliers. We have also considered the 8.3% market growth rate, which has been identified by our internal market analysis.

![Figure 5. Estimated private investment in 2016 (left) and in 2017 (right), keeping into account the 8.3% market growth](image)

In order to be conservative in terms of private investment and to limit the impact of the potential biases inferred by the available data to compute the leverage factor, we consider the 15th and 85th percentiles as the valid points in our analysis and the impact market growth rate on the estimation of the 2016 baseline and 2017 private investment (see Figure 6).

![Figure 6. Private investment estimation for 2016 and 2017 by varying growth rate of the market](image)
The market growth rate influences the distribution of the investments for 2016 and 2017. However, the private investment is above the leverage factor in all cases (see the yellow line in Figure 7). For the estimation of the leverage factor, we have identified 8.3% market growth rate by analysing the consolidated data from ten independent and publicly available market studies\(^\text{10}\). To have most precise information about the investments into cyber security market, we have also estimated private investment for 2016 and 2017 by using the corrected averages, calculated after the elimination of the outliers (see Figure 7). As the reporting perimeter is expected to remain the same, for the following years, we will be able to compare the values from the first period with the results from the upcoming reporting periods.

![Figure 7. Estimated private investment for 2016 and 2017 with corrected averages](image)

**The leverage factor assessment for 2017**

The investment into the R&I, provided by the European cyber security industry in 2017 is estimated to be 522 million euros (see Figure 6). The public investment from H2020 programmes related to cyber security, namely DS-06, DS-07 and DS-08 and 50% of CIP-01-2016-17, counts to 67.45 million euros. Given the amount of investments from the private and public sectors and the minimum target of the leverage factor of 3, the total amount of investments reaches about 202 million euros by the end of 2017. As expected, the main contribution (almost 65% of the total investments) comes from the large companies, followed by the end-users and operators, and RTOs. The relatively high amount of target investment from the operators could be explained by the increased awareness of cyber security risks and the increased demand for the customised cyber security solutions for the vertical markets.

The estimated leverage factor is higher than the one foreseen at the signature of the cPPP on cyber security. Given the growing awareness of cyber threats, we expect that the private investments in cyber security technologies and services will continue to grow in the upcoming years. The recent cyber attacks have significantly raised the interest in cyber security among society, business and politicians at the national, European and international levels. The damaging effects of the cyber attacks have also demonstrated the need to design and develop the appropriate cyber security solutions. We will be able to assess better the potential investment growth in 2018,
as we will be able to use the current estimation as baseline to determine the potential market growth and the available market studies to validate the data.

**Conclusions on the leverage factor for 2016**

The analysis indicates that the private investment is estimated to be 522 million euros in 2017, which represent the 38% of the total investment indicted in the contract. This result is a valuable indication to confidently estimate that ECSO stakeholder community invests in cyber security, leveraging the public investment ratio, as well as creates new market opportunities and strengthens European cyber security market.

**Success Stories**

Because the quantitative data tells us only half of the story, we asked our members to share their success stories and provide a qualitative assessment on the R&I investment: mainly, how the cPPP has benefited in creating the cyber security ecosystem and facilitating market development. This section provides information about the concrete initiatives taken by our members, which serve as a strong example of how ECSO stakeholder community contributes to the development of a competitive European cyber security technology ecosystem.

In terms of cyber security technology, ECSO members initiated several highly relevant projects. **F-Secure**, one of the main European pure cyber security players, launched in the beginning of 2017 an internal R&D project which aims to develop an early detection service for advanced attacks in traditional endpoints and provide guidance for appropriate response actions. The project will use several components developed earlier partially within another Finnish national research collaboration project, named Cyber Trust and supported by the local Finnish funding provided by Tekes / Business Finland national funding agency. The foreseen impact to the market will be quite relevant as it should introduce a competitive European solution in the Endpoint Detection and Response segment for mid-size (500 – 5000 seats) organizations.

Among the RTO category, it is worth mentioning the project led by **Eurecat Technology Centre**, based Catalonia, Spain. In the context of Living Utilities, the project involves large companies from different sectors (water, energy, telecommunications, and transport), Spanish SMEs, universities and research centres. The project aims to develop a toolkit for the effective protection, prevention, detection and management of cyber threats and attacks. Furthermore, **French Institute for Research in Computer Science and Automation (INRIA)** is involved in an international R&I project with Microsoft Corporation (UK, USA, India), and Carnegie Mellon University to develop a High Assurance Cryptographic Library (HACL*) written in the F* formal verification language to guarantee provably secure code for all modern crypto primitives. The verified code from HACL* has been already integrated into the Firefox web browser and WireGuard VPN. It is being integrated into the Everest verified https stack and the Riot IoT operating system, which is expected to have a large impact in the future. **TECNALIA Research & Innovation** works on a project dedicated to the creation of a business-oriented blockchain solutions that will allow consortium companies and their customers to adopt blockchain technology in their business environments and to take into account national and international regulatory requirements such as GDPR and the right to be forgotten. Another application areas of the blockchain solutions are digital identity, traceability of digital goods and smart contracts. Some ECSO members have launched pilot R&I projects or the project dedicated to the validation of the solutions in infrastructures and vertical markets. For example, **innogy SE**, a Germany-based energy company, has launched several projects with the aim to develop cyber security solutions for the energy sector. One of the projects, developed in
cooperation with a world-famous European industrial cyber security provider, aims to develop an Intrusion Detection Solution in SCADA environment.

There are several important projects focusing on the development of the cyber security ecosystem at the regional level. Brittany region (France) and the Basque country (Spain) are among the most active regions which have made cyber security a strategic investment priority for their regions. **Brittany region**, represented by the Regional Council of Brittany, decided to allocate 12 million euros in cyber security for the 2014-2020 period. Regarding the research-related activities on cyber security, 6 million euros are planned to be invested during the 2014-2020 period, with 4.1 million euros being invested already. Together with the French Ministry of Defence, INRIA and Centrale Supélec – a French institute of research and higher education in engineering and science, Brittany Region has developed a Joint High Security Laboratory (Laboratoire de Haute Sécurité - LHS) in the city of Rennes. LHS has a strong links with industry and an open platform for viruses and security evaluation. The laboratory has peer-to-peer collaborative network, which is capable to include civilian and military sectors, public and private partnership, as well as to address cyber defence and cyber security topics. The main aim of the initiative is to facilitate the cyber security research and technology transfer in cyber security at the regional level.

**Basque region**, represented by the Basque Regional Government and Basque Cyber Security Centre, is another example of the strong regional commitment to invest in R&I. (SPRI-Basque Business Development Agency) has launched different programs (e.g. Hazitek and Elkartek) to promote R&I in a wide range of areas of expertise and technology application. The projects also intended to enhance specific use cases of smart specialization sectors regarding cyber security. For instance, the SecureGrid project (2016-2018) focuses on the security of electrical substations in the high and medium voltage network, as well as the electronic equipment and Intelligent Electronic Devices (IEDs), as their electronic features and remote communication through communication networks represent one of the most vulnerable points of the Smart Grids. The main goal of the project is to develop of the centralised security management system at substations which is able to integrate the capacities of different IEDs and to research the security capacity in a set of IEDs. 1.7 million euros investment has been made for the creation of cyber security facility ‘BCST-4P3 – Basque Cyber Security Testbed for Public Private Partnership’ with four specialised laboratories, including Smart Grid Cyber security lab, Automotive Cyber security Lab, Industrial Blockchain Lab and Cyber-Ranges lab.

**KPI 2 - New skills and job profiles**

To ensure a sustainable growth of the European cyber security ecosystem in the long term, we need to ensure the supply of a highly skilled cyber security professionals at all level of technology development – from the initial R&I phases to the pilot projects, to the market deployment and sales – if Europe want to be competitive at the global level.

The education and training in cyber technology is already a very important issue and will become even more important in the future. It is estimated that by 2022 there will be a shortage of 350 000
professionals\textsuperscript{19}. The education and training has already been recognised as a top priority by to the European Commission, which started to address the cyber security technology skills gap through several programs, including the ‘New Skills Agenda for Europe: Working together to strengthen human capital, employability and competitiveness’, adopted in June 2016\textsuperscript{20}. A skilled cyber security workforce is an important matter for the private sector as well. If private companies operating in cyber security market wants to maintain their market share or grow to the new markets, they need to invest in education and training of cyber security professionals, as well as in cyber security awareness.

Since its establishment, ECSO has been working on education, training, awareness and cyber ranges in one of its established working groups. One of the main achievements in 2017 was the creation of the European Human Resources Network for Cyber Security (EHR4CYBER), dedicated to building a network of universities, training academies and HR departments, which will help to foster skill and create jobs in cyber security. For cyber security professionals recruitment, EHR4CYBER works on a common benchmarking system and seeks to implement a matchmaking platform to advertise vacancies and job fairs, as well as training programmes, national and European initiatives, events and hackathons (for more details see Annex IV).

In order to collect the primary data on the creation of new jobs and skill in the context of the cPPP, a survey was distributed for ECSO members and non-ECSO members, in which they were asked to provide an estimation on the existing workforce. Here, a main bias from the first version of the survey should be underlined. After having the data collected, we have noticed that the questions and the provided answer options could have been misconceived. In many cases, the answer option ‘\textgreater 100 employees’ have not been considered, most likely because of the indefinite spectrum of number of employees. One of the possible reasons, is that many private companies have more than 1000 employees specialized in cyber security but they preferred to select the answer option ‘\textgreater 100’ rather than specifying the exact number. In order to improve the data collection and have more precise information, ECSO is planning to rephrase the questions in its forthcoming surveys.

For this report, we have selected 188 000 employees as a baseline, identified by the results of our market analysis. For calculating the manpower, we assume that the typical costs of a person working in cyber security area is 125k euros per job. This value is the result of the ratio between company’s turnover and the number of employees of the purely European cyber security market players. Similar model can be applied to the global market, where values need to be estimated for the companies with 660 000 – 990 000 employees.

ECSO survey on the creation of the new skills and job profiles in 2017 highlights some positive trends. While the overall number of the employees in cyber security sector (baseline workforce in cyber security) is impossible to estimate due to the above-mentioned problem related with the question on the number of employees, survey results provides us enough information to estimate the growth of the employment rate from the beginning of the cPPP (June 2016) till the end 2017. The collected data shows that companies from the three main ECSO categories have experienced an important growth of employment in the given period, which is +10% for large companies, +80% for SMEs and +45% for RTOs.

\textsuperscript{19} 2017 Global Information Security Workforce Study released by Information Security Certification (ICS)2 and based on a survey of 19,000 cyber security professionals around the world, including nearly 3,700 respondents in Europe.

Keeping in mind the estimation – 10% annual growth in the cyber security market as target for the KPI2 – made in ECSO industry proposal in 2016, the data from the 2017 survey allows us to indicate a positive trend in cyber security job market within the entire value chain of the stakeholders’ part of the cPPP. Due to the improved progress monitoring methodology and data collection, ECSO will be able to collect more precise data and provide even more precise estimations and forecast for the next years.

### KPI 3 – The participation of SMEs in R&D projects

Small and medium-sized enterprises (SMEs) have a twofold role within the cyber security ecosystem. Due to the fast changing cyber security technology, only the SMEs, which are agile and flexible, can provide a cutting-edge technology solutions to remain competitive in the technology market. However, while the United States (US) already have the largest technology market, the specific regulatory framework (e.g. the Small Business Act) and the Silicon Valley ecosystem, Israel – a strong military-academic-industry partnership, EU is still looking for an appropriate business models for the European SMEs.

A lack of the competitive solutions tailored to the needs of SMEs is an important barrier, which precludes Europe from building an efficient global security policy. SMEs make up to 99.8% of the European enterprises. However, most of them are barely prepared to face cyberattacks, because they management still often underestimate the threat posed by cybercrime. SMEs are becoming the weak link – the unpreparedness of the SMEs to fed against cyber attacks weakens the security of the large corporations, with which they work.

SMEs should be a backbone of the European economy, as they are capable of developing R&D projects, which enhances EU global competitiveness and provides the market with innovative cyber security solutions. For these reasons, the cPPP on cyber security indicated the support to SMEs players as one of the priorities and established a Working Group 4 (WG4) – Support to SME’s,
coordination with countries in East EU and regions\textsuperscript{21}. WG4 unites 55 SMEs (from which 23 joined in 2017) coming from 19 countries and completely covering cyber security value chain. Participation in WG4 activities provides SMEs with an opportunity to collaborate and establish their place in the market. During the meeting such topics as investment models, access to the new markets, participation to H2020 calls are discussed.

In this regard, a significant achievement is the inclusion in the Work Programme of a dedicated support to SMEs. The ECSO SRIA recognises the SMEs as one of the innovation drivers in Europe, thus the importance to define and develop a cost-effective framework composed of specific cyber security tool-kit to support SMEs with a limited background on cyber security and a restricted budget. Moreover, SMEs are embracing different sectors and have different needs requiring the design of customised and versatile cyber security solutions that can be adjusted dynamically to their business in order to reduce their exposure to cyber incidents, minimise the risk of a cyber attack, and promote the usage of cyber security best practices. The ECSO SRIA will build upon these solutions and has already identified the need to complement them with dedicated support to SMEs for cyber range to increase the level of cyber resilience and certification schemes for SMEs identified as additional relevant priorities.

As the baseline of SMEs participation in H2020 calls is about 18% of total beneficiaries\textsuperscript{22}, the cPPP on cyber security has a strategic objective (which is one of the KPIs) – to ensure that at least 20% of the unique participants involved in cyber security calls funded under cPPP framework are SMEs, start-ups or high-growth (50+% increase in annual revenue) companies specialized in cyber security. For that reason we don’t take in account the SMEs specialized in consultancy, marketing and communication, or coordination of R&D project.

\textsuperscript{21} For more details see Annex IV.

\textsuperscript{22} Data source: \textsc{Horizon 2020 Dashboard} for cyber-relevant topics under H2020 2014-2016. We count a total of 14 topics under the title of DS and with two further topics ICT-32-2014 and CIP-01-2016-17 (funded 50% by CNECT and 50% by HOME). The 12 topics under DS include: DS-01-2014, DS-01-20146, DS-02-2014, DS-02-2016, DS-03-2015, DS-06-2016, DS-04-2015, DS-04-2016, DS-05-2015, DS-05-2016, DS-06-2014, DS-06-2015. In order to calculate only the relevant SME players (ICT companies, cyber security providers and users) we disaggregated the total number of SME unique participants (147 of total 505) by two categories: consultancy or project management companies (56) and relevant SMEs (91). In terms of percentage of funding going to SMEs, the latter category benefits 14% of H2020 net EU contribution (31,5 million € of 223,5 million €).
Figure 9. KPI 3 – Participation of cyber security SMEs in H2020

Figure 9 shows that the first projects funded under four topics, despite the efforts of ECSO to facilitate and push SMEs (among its members and beyond) in stronger participation for these projects, are going in the opposite direction respect of the objective of increasing the participation of SMEs in H2020 projects. This could also be attributed to the kind of topics that has been tackled by the specific calls.

Given the complicated market situation to which SMEs are exposed, WG4 has decided to design and establish the SME Hub – a publicly accessible European register for cyber SMEs where they can register their company, services and products. This platform allows SMEs to advertise their solutions and significantly increases the opportunities to access the market. Even if WG4 has initiated the discussion on technical specifications of the SME HUB in 2017, the first phase of implementation is expected by end of 2018.

Private sector success stories

**NSR s.r.l.** is an Italian SME working on a R&D project, which aims to develop a real-time fraud detection solution with high performance and low latency in order to superimpose a layer of advanced analysis to the modern Complex Event Processing (C.E.P.). Due to the demand of financial institutions looking for long-term fraud management solutions, the expected outcome of this project is an integrated software, which provides a reduce latency, millisecond risk analysis for transactions, flexibility for integration with transaction processing systems for instantaneous blocks, manages simultaneous analysis of tens of thousands of events per second, as well as manages repository for transaction history aggregated by relevance.

**S2 Grupo** is a Spanish SME and a founding member of ECSO. Among its recent R&D activities, S2 Grupo is coordinating two large projects focusing on cyber security of electricity network, Industry 4.0 and IoT environments. In particular the project on Smart Grid aims to develop a reference architecture and a model for deploying cyber security in the Smart Grid and non-intrusive data traffic analysis algorithms based on stream analytics techniques, while the other project is focusing on delivering monitoring toolchain for cyber security monitoring in Industry 4.0 environment and cyber security testbed. From a general point of view, being involved in ECSO has several advantages for S2 Grupo. First, it is a good way for a SME to get to know first hand of the
ongoing discussions about the most relevant issues in our field, such as certification frameworks, professional qualifications and, of course, R&D strategies. Second, ECSO meetings and events constitute a very good place to initiate and maintain a network of international contacts with other players in Europe, large companies, SMEs and Research Institutions, what also helps when building consortia for H2020 projects. In fact, in the afore mentioned smart grid project, the process of framing the consortium was initiated after contact established in one of the ECSO WG meetings.

**CyberServices** is a Hungarian SME and a founding member of ECSO, which actively participates in ECSO’s activities and leads several sub-WGs. During the last two years, CyberServices not only participated in several SRIA-driven H2020 calls, but also managed to leverage its international partnership via ECSO network. CyberServices boosted its export activities and successfully bridged the cooperation gap between academia and industry by actively collaborating with Higher Education Institutions on capacity building solutions and providing their know-how.

### KPI 4 – Significant innovation

Regarding innovations, the first reporting period cannot provide a full picture due to the nature of the topic and the time span between the granted calls and deliverables of the innovations. The first H2020 projects falling under the scope of the cPPPs on cyber security have started their activities only in mid-2017 and thus their results in terms of the significant innovations are not yet available. To evaluate the significance of the innovation, we rely on the methodology used for the Innovation Radar which is based on two indicators: the innovation potential and capacity. The former measures the commercial development of the innovation and its readiness to enter the market, while the latter measures the capacity behind the innovations. Because the Innovation Radar methodology provides a general framework, it can also be applied to analyse the results of the cyber security solutions and project.

We also measure the significance of the innovation in terms of its impact to strengthen European cyber security ecosystem. The qualitative analysis demonstrates the importance and the impact of the technology market in the short term, but also provide insights, even if less precise, on its disruptive potential in the future (e.g. the impact of the innovations in a new cryptographic library or secure protocol for communication). The report also takes into account not only tangible but also intangible assets. The intangible assets do not have an immediate innovation on the market, but they are relevant to understand how the know-how can be leveraged and exploited towards further developing cyber security innovation and solutions.

Table 1 (see below) provides a template to determine the qualitative impact of the ECS cPPP. The methodology leverages the analysis of the existing cyber security ecosystem before the the launch of the cPPP (pre-cPPP analysis). Then the impact of the cPPP projects funded under the H2020 framework, will be assessed qualitatively to estimate the potential innovation of the project. Only the projects for the call DS-06-2017 are analysed in the Table 1 to show how we will conduct the analysis of the cPPP after its implementation. The table will be updated in line with the information provided by the EC (see Annex III of the periodic activity report template), when the results of the cPPP calls will be available.
### cPPP Topic

<table>
<thead>
<tr>
<th>Name Project</th>
<th>EU Contribution</th>
<th>Summary Project</th>
<th>Expected Outcome</th>
<th>Innovation results</th>
</tr>
</thead>
<tbody>
<tr>
<td>FENTEC</td>
<td>4.223.141,25 €</td>
<td>FENTEC will address functional cryptography to allow processing of encrypted data to obtain a partial view of the message plaintext.</td>
<td>The functional encryption paradigms deployed in the project will be evaluated in 3 use cases: privacy-preserving digital currency; anonymous data analytics enabling computation of statistics over encrypted data; secure key and content distribution communication protocols for IOT devices.</td>
<td>To be provided when available</td>
</tr>
<tr>
<td>PROMOTHEUS</td>
<td>5.496.968,75 €</td>
<td>PROMOTHEUS focuses on the design of new security and privacy-preserving primitives and protocols for post-quantum computing.</td>
<td>New tools leading to the design of practical advanced protocols, like anonymous credentials, digital cash or electronic voting, that maintain users’ privacy against quantum adversaries.</td>
<td>To be provided when available</td>
</tr>
<tr>
<td>PRIVILEGE</td>
<td>4.527.917,50 €</td>
<td>PRIVILEGE project will focus on blockchain and distributed ledger technologies supporting privacy (protection of sensitive data such as trade secrets and personal information), anonymity and decentralised consensus.</td>
<td>Blockchain and distributed ledger technology will be demonstrated through four ledger-based solutions: (1) verifiable online voting; (2) contract validation and execution for insurance; (3) university diploma record ledger; and (4) update mechanism for stake-based ledgers.</td>
<td>To be provided when available</td>
</tr>
<tr>
<td>Future TPM</td>
<td>4.868.890,00 €</td>
<td>Future TPM will design and develop a quantum-resistant trusted platform module with provably-secure algorithms. The validation will be performed in online banking environments.</td>
<td>The expected outcome of Future TPM are: robust and provably-secure TPM algorithms for TPMs and contribution to standardisation effort at EU level.</td>
<td>To be provided when available</td>
</tr>
</tbody>
</table>

**Table 1. KPI 4 – The analysis of significant innovations**
KPI 5 – End-users participation

Another crucial element to assess the efficiency of a sustainable ecosystem is the involvement of end-users in the R&D projects. While European market is still fragmented by the absence of the common European approaches and regulatory framework, European cyber security sector also suffers from fragmentation in both the supply-side (industry) and the demand-side (users). Despite fragmentation, European cyber security market is strong due to the market leadership in several core industrial segments (e.g. aerospace, automotive, chemical, food etc). The cPPP on cyber security provides an opportunity-window to bring together representatives from different sectors, who have a capacity to collect the information and feedback from various user groups, which helps to better specify the demand-side and to include the offers and the operational requirements from the users & operators, as well as procurement bodies.

One of the main aims of the cPPP on cyber security is to promote the deeper involvement of the end-users in cPPP projects and thus to increase their participation by 15% in H2020 projects. For this purpose, ECSO has established a Working Group 3 - Sectoral Demand, dealing with the market applications according to the eight sectoral demands. The analysis of the end-users participation enables to have a complete view of the key stakeholders in R&I ecosystem.

ECSO has successfully involved the end-users in the discussion on the SRIA-related topics, allowing different sectors and market players to express their specific needs and to contribute to the development of the European cyber security ecosystem. In 2017, WG3 held three sector-specific workshops dedicated to energy, transport and financial sector. The aim was to bring together ECSO members, sectoral associations, end-users and utilities, as well as relevant European Commission’s policy departments (Directorates-General) to discuss the main priorities and actions and to collect a feedback from a wide range of sectors.

WG3 workshops have shown the importance of engaging with sectoral associations and European Commission Directorates-General to ensure an inclusion of a wide-ranging spectrum of cyber security stakeholders and their valuable inputs, as well as to avoid the duplication of actions and limited-impact initiatives. For example, since its first workshop in 2016, WG3 sub-working group on energy, has established an ongoing dialogue with The Directorate-General for Energy (DG ENER) which liaise with ECSO on the main R&D and industrial policy in the energy sector. Such established cooperation ensures a convergence on European policy objectives and research topics (i.e. 2017 call for projects have co-funded by DG ENER and by the Directorate-General for Communications Networks, Content and Technology (DG CNECT)).

Fixing the baseline for the end-users participation for the pre-cPPP period has been one of the biggest challenges. The main problem faced during the Monitoring exercise is a lack of data targeting the end-users participation from the publicly available H2020 Dashboard. As the categorization of the H2020 participants is limited to few categories (public administration, research centres, education institutes, private company), the baseline is fixed according to the estimation based on the 505 unique participants in pre-cPPP projects (12% of the total). This assessment, even if based only on our estimation, will be used as current estimation of the baseline.
The preliminary information about 19 projects funded under the cPPP framework shows that 25 end-users are among the 249 unique participants of cPPP H2020 projects (10% of the total) with at least one end-user on average representing different sector. These finding only confirms the need to raise awareness among end-users and to promote the participation opportunities in R&D projects. One of the recommendations for the European Commission would be to introduce an additional category in the H2020 Dashboard which would allow to collect more data and provide a more in-depth analysis.

KPI 6 – Dissemination and Communication

The establishment of ECSO association, the launch of the cPPP on cyber security and the creation of the six working groups have been the major events for which a targeted communication strategy was design (see Section 2.2). During the reporting period (June 2016 – December 2017), ECSO and its members participated in 97 events – ranging from summits, to national conferences, to regional workshops, to roundtables – in 19 countries across three continents, including Austria, Germany, France, The Netherlands, Italy, Israel, USA, Cyprus, Greece, Saudi Arabia, Belgium, Spain, Turkey, Norway, Finland, Estonia, Slovakia, Poland, Luxembourg. Due to their knowledge and insights on cyber security, ECSO Secretariat and ECSO members were invited to participate in various panel discussions, debates and workshops. ECSO objective was the creation of meaningful cooperation between various entities, ranging from European agencies and bodies to sectoral agencies, to international standardisation bodies, to international organisations, to regional and European initiatives. Another important goal has been the promotion of ECSO among the companies and governments, leading to the ever-growing and strong ECSO community.

During the reporting period, ECSO appeared in the media for 53 times, no including the appearances in press releases. The support of the organisation of brokerage events for H2020 calls increased ECSO visibility. With its targeted communication strategy and continuous efforts to
raise awareness about its work on cyber security industrial policy and cPPP, ECSO has considerably increased its membership base since June 2016 (see Section 2.2.)

KPI 7 – Openness

European Commission has funded 19 cyber security cPPP projects under the H2020 framework by the end of December 2017. The amount of investments injected counts to 67 million euros. The overview of the approved projects shows that about 70% of the H2020 programme beneficiaries are non-ECSO members and 50% of the project funded are coordinated by the non-ECSO members.

Figure 11. KPI 7 – Openness

Given the current situation, a reasonable target for the future could be a ratio of 50% ECSO and 50% non-ECSO members. In order to have a diverse audience of beneficiaries and to provide a support to different sectors, ECSO sets a goal to monitor the H2020 beneficiaries and provide an opportunity to become ECSO members.

Figure 12. EU Contribution to cPPP participants (2016-2017)

Within the framework of 19 cPPP projects funded by the European Commission, the financial support received by ECSO members seeks about 40% with regards to the 28% of ECSO members in projects, which can be explained by fact that some ECSO members are one of the largest and most influential companies in cyber security sector.
The implementation of the cPPP on cyber is in its initial stage (see Figure 13). According to the information provided by the Commission, European Commission has invested slightly less than 15% of the total amount of investment envisaged to be allocated to cPPP by H2020 programme throughout the period of four years 2017-2020.

In this context, it is important to highlight the need to continue the coordination among the projects funded under the call ‘DS-05-2016’ aiming to establish the EU-wide cooperation and international dialogues in cyber security research and innovation at the national levels (cyberwatching.eu) as well as international cooperation with third countries, including Japan (EUNITY) and US (AEGIS). All three Coordination and Support Actions (CSA) projects are well aligned with the strategic agenda of ECSO which was made possible due to the large presence of ECSO members in the consortium of these projects and the established dialogue. The goal is to gather the feedback, which will prove valuable when defining research roadmaps and contributing to the dialogue between the industry and policy-makers.

3.3. Evolution over the years

The cPPP on cyber security founds its origins in the discussions with now ex-European Commissioner Neelie Kroes. The initiative was launched by Günther Oettinger, who served as a Commissioner for Digital Economy and Society between 2014-2016. Currently, the cPPP is supported by the current Digital Commissioner Mariya Gabriel. From 2011 until now, we have seen a growing interest in cyber security and ECS-cPPP at all levels - from local, to national, to European. The first meeting on cyber security was organised by DG CNECT on 20 January 2016 can be regarded as a starting point of the cPPP on cyber security. The meeting gathered two delegates from each EU Member State, representing both private and public sector. The participants of this meeting set the scene for an ambitious challenge – the creation of cPPP on cyber security. The initiative had to be launched in the period of four months, in order to meet the timeline of the midterm review budget. The newly established association – European Cyber Security Organisation (ECSO) – was supposed to gather the stakeholders from the private sector.

ECSO was successful in this endeavour – the cPPP between European Commission and ECSO was signed in European Parliament in Strasbourg. At that time, ECSO already had 132 members
from private and public sectors. One peculiarity of this cPPP is that public sector is represented not only by the European Commission but also by the national or regional public administrations, which are ECSO members and the association a unique ‘industrial counter-part’. Another peculiarity of this cPPP and ECSO is the fact that since its establishment, it was clearly recognized that the ambitious R&I targets for the cPPP cannot be set without developing strong European cyber security ecosystem. Only by working on such issues as standardisation, certification, investments, SMEs, regional policy aspects, education, training and awareness first, we will be able to implement the solutions and services developed by R&I projects under the H2020 investment framework. The topics identified in the adopted cyber security package and Joint Communication, released on 13 September 2017, calls for a comprehensive approach to cyber security.

The initial industry proposal and SRIA strategy, as well as the legacy of work done by the NIS Platform, set the initial vision and objectives. Already by the end of 2016, there was a massive recognition that Europe needs stronger cyber security measures at all levels – political, economic and societal. The ransomware attacks in 2017 and the more recent exposure of hardware vulnerabilities in the ‘Spectre’ and ‘Meltdown’ cases made cyber security one of the most pressing challenges for Europe and international community. The growing awareness of the scope of impact that the billions of IoT devices will have on our society resulted in the increased demand for protection against cyber attacks. Such issues as encryption, security of 5G, high performance computing and artificial intelligence have contributed to the growing understanding of the digital environment and its potential threats.

4. OUTLOOK AND LESSONS LEARNT

In the ECS-cPPP we have well anticipated these (market and threats) evolutions and we have indicated R&I priorities to cover (at least partially) such needs. Our SRIA is in continuous evolution and ECSO is constantly monitoring, also in liaison with other cPPPs, the need for new developments and evolution of the cPPP targets.

A confirmation of the high growth in interest in cyber security and the good definition of the SRIA perimeter (and hence of the cPPP objectives) is given by the important investments made by ECSO and non ECSO members in the first years, as indicated in this report, well beyond the initial expected leverage factor.

We have to continue to provide decision makers with a good analysis of the market evolution and with future priorities for R&I as well as for investments for implementation of cyber security in key infrastructures, also as support of EU legislations (e.g. NIS Directive).

CHANGES FORESEEN TO IMPROVE THE SURVEY

In order to improve market analysis and data collection, ECSO Secretariat seeks to improve the sample data of the survey. The questions, especially question #1 on the estimation of investment in R&D project in Europe and question #2 on the estimation of the number of employees working in cyber security, will be rephrased. In order to deliver a more detailed picture of the private investment in R&D, the question #1 will be focused on gathering the qualitative information. Question #2 will be rephrased to improve measurement of the KPI 2. The established EHR4CYBER will help ECSO to monitor the KPI 2 and to deliver a fine-grained insights on the emerging job profiles as requested by the European Commission during the cPPP monitoring review.
In order to receive more survey responses from ECSO community, ECSO plans to implement a tailored strategy with the aim to improve the survey response rate. Firstly, the survey will be launched ten weeks in advance to provide ECSO members a sufficient amount of time to provide information. Secondly, constant reminders about the yearly survey and its importance will be communicated to ECSO members. Thirdly, ECSO will have integrated sessions during its working group meetings to present the survey and to remind ECSO members about their commitment to the implement of the cPPP on cybersecurity. This three-step strategy should help to significantly improve the next PMR.

ECSO WG6 will update the SRIA strategy for the last call in 2020 and will evaluate the evolution of the needs in different sectors of technology and applications from the upcoming period of 2021-2027, which, in turn, will provide valuable input for the setup of the European Commission research project FP9 priorities and investments. This goes along with the work of the other WGs which contributes to the development of the European cyber security ecosystem, towards an enhanced configuration (we call it enhanced PPP) that we are discussing with the European Commission and with all our public and private members, that could take place after 2020, and that will include the Network of cyber security competence centres, the European Research Centre and a renewed (ENISA).

Among many things, one aspect of the first phase of the ECS-cPPP implementation has been especially challenging – the difficulty to converge different visions from the public and private bodies into a common strategic view. This happens mainly because private bodies represent different sectors with different interests and different levels of maturity. This took time and continuous improvement in governance and will still evolve with the progressive understanding of specific needs. Another important challenge is a strong interest from the European industry to have higher competitiveness supported by the cPPP and its future configuration. In H2020 programme, cyber security falls under the security (societal challenges) category and part under the ICT in Leadership in Enabling and Industrial Technologies (LEIT-ICT), covering competition topics. To enhance the competitiveness of European industries in the global markets and increase European digital autonomy, a more strategic approach, which is currently being discussed with different stakeholders, is needed.
### Annex I – Common Priority Key Performance Indicators

<table>
<thead>
<tr>
<th>Key Performance Indicator (KPI)</th>
<th>Value in [2017]</th>
<th>Baseline at the start of H2020 (latest available)</th>
<th>Target (for the cPPP) by the end of H2020</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 Mobilised Private Investments</td>
<td>522 million €</td>
<td>482 € million</td>
<td>1.8 billion €</td>
<td></td>
</tr>
<tr>
<td>#2 New skills and/or job profiles</td>
<td>+ 10% for large companies +80% for SMEs % 45 for RTOs</td>
<td>188.000</td>
<td>+ 10% growth rate market</td>
<td></td>
</tr>
<tr>
<td>#3 Impact of a cPPP on SMEs</td>
<td>14% of participants of H2020 projects are SMEs specialized in cybers security</td>
<td>18% of participants of H2020 projects are SMEs specialized in cybers security</td>
<td>At least 20% of participants of the cyber security calls funded are SMEs, start-ups or high growth companies (50+% increase in annual revenue) specialized in cyber/ICT or users</td>
<td></td>
</tr>
<tr>
<td>#4 Significant Innovations</td>
<td>0 (still lack of critical post-2017 results)</td>
<td>2 pending patent applications; 1 utility model awarded</td>
<td></td>
<td>See the methodology for future comparison (p 30)</td>
</tr>
</tbody>
</table>
### Annex II – Specific Key Performance Indicators for the cPPP

<table>
<thead>
<tr>
<th>KPI domain</th>
<th>Key Performance Indicator (KPI)</th>
<th>Value in (2017)</th>
<th>Baseline at the start of H2020 (latest available)</th>
<th>Target (for the cPPP) at the end of H2020</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>#5 User participation</td>
<td>Monitor the participations of users in R&amp;I activities</td>
<td>10%</td>
<td>12%</td>
<td></td>
<td>at least 15% of users / operators participating in cyber security projects funded by H2020.</td>
</tr>
<tr>
<td>#6 Dissemination and Communication</td>
<td>Number of dissemination and information actions for promoting the PPP activities to a broad range of public and private stakeholders.</td>
<td>80</td>
<td>17 events attended by the ECSO Secretariat and members in 2016 (estimation made by the ECSO secretariat)</td>
<td></td>
<td>30 events per year</td>
</tr>
<tr>
<td>#7 Openness</td>
<td>Share of participation of ECSO members / non ECSO members in H2020 projects</td>
<td>28% of unique participants are ECSO members</td>
<td>30%</td>
<td></td>
<td>50% of ECSO members vs 50% non ECSO members</td>
</tr>
</tbody>
</table>
### Annexe III – Contribution to Programme-Level KPI's (provided by the EC)

<table>
<thead>
<tr>
<th>Key Performance Indicator</th>
<th>Definition/Responding to question</th>
<th>Type of data required</th>
<th>Data [European Commission]</th>
<th>Baseline at the start of H2020 (latest available)</th>
<th>Target (for the cPPP) at the end of H2020</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Patents</td>
<td>Number of patent applications. Number of patents awarded</td>
<td></td>
<td>2 patent applications 1 utility model awarded</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Standardisation activities (project level) Contributions to new standards (PPP level)</td>
<td>Number of activities leading to standardisation Number of working items in European Standardisation Bodies. Number of pre-normative research files – prEN - under consultation in ESBs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Operational performance</td>
<td>Time-to-grant</td>
<td></td>
<td>2017: 237.5 days 2014: 257.7 days 2015: 238 days 2016: 247.8 days</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 H2020 - LEIT - Number of joint public-private publications</td>
<td>Number and share of joint public-private publications out of all LEIT publications. Properly flagged publications data (DOI) from LEIT funded projects</td>
<td></td>
<td>Total 376 Public-private pub :97 of which 8 are peer-reviewed Peer-reviewed pub 50 Useable knowledge : 286</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex IV – Report on industrial policy activities

The purpose of our cyber security cPPP is not only to address the most complex technological challenges of today’s socio-technical cyber security environment, but also to grapple with the broader challenges of the industrial policy. For doing that, 5 WGs with the participation of more than 1500 experts from 218 organisations are exploring new ways to facilitate the development of the European market.

Below is the summary of achievements by WG1 to WG5 that were recognised in 2017.

**WG1 Standardisation, certification and labelling WG1**

**WG breakdown**

WG1 has been segmented into 4 different sub WGs:

- SWG 1.1 Manufacturing of Subcomponents, Components, Devices and Products
- SWG 1.2 ICT infrastructure providers and other cloud based services
- SWG 1.3 IT Integrators, Critical Infrastructure Operators, End Users and Supply Chain Management
- SWG 1.4 Base Layer

No. of members subscribe to WG1: 135 organisations (289 experts/individuals)

WG meetings held: 7 in 2017 (2 phone conference calls) and 1 in 2016. SWGs meetings were co-located at each WG Face to Face meeting.

**Main activities**

**Challenges of the industry**

The first of WG1 in 2017 was to collect the Challenges of the Industry (COTI) using existing certification schemes and standards. The document is designed to be a compilation of problems (more than 290 inputs), to be used to understand the main driving topics that can be considered as common challenges. This input addresses a large variety of anticipated problems with the rise of Internet of Things and with the need to cover products/systems to be deployed in the field for many years. A preliminary analysis of the challenges reported by WG1 members reveal that the most recurrent topics include harmonisation, privacy, patching & updating, connected devices, time to market & innovation speed, base line, trusted products and brand protection. The document is considered internal and a living one as it is updated with new problems and challenges. The scope is to have a consistent view of the current challenges in cyber security certification to define and refine the ECSO meta-scheme approach to address the market needs.

**State of the Art (SOTA)**

The second document produced by ECSO WG1 is the State of the Art Syllabus (SOTA), which exists in two public versions (June 2017 and December 2017). The SOTA lists all standards and specifications related to Cyber security known to and deemed relevant by the authors at the moment of writing. "Relevant" here means that a standard can (potentially) be used for assessing the security strength of an item. The SOTA document gives a good overview of cyber security standards, initiatives and certification schemes, both at the European and international level (including national elements), for assessment and certification of items.
The SOTA is a living document, i.e. it will be extended regularly with new identified gaps, new standards or schemes published.

Meta-scheme approach

The two first documents (COTI and SOTA) are as a good basis to understand the challenges ahead as well as the state-of-the art to identify gaps towards a harmonised European certification framework. To not reinvent the wheel, the ECSO WG1 has also defined a Meta-Schema Approach towards European Cyber Security Certification, published in December 2017, to allow combining existing schemes efficiently or to allow creation of new schemes when required.

This meta-scheme encompasses many of the existing certification schemes (e.g. component certification, process certification, service certification, etc.). It will do so by evaluating the level of confidence in the security strength of a product, system, solution, service or organisation that results from a scheme used, and map this onto a harmonised set of levels defined by ECSO. These levels represent the level of confidence and the scope of security functionality of the item certified. The latter allows to clearly specify the security required. Each level is mapped to a single symbol that can be used for a label. The meta-frame work is based on the concept of technical groups defining the attack potential and attack method to make sure that the products are resistant to potential attacks.

The ECSO Meta-scheme approach is the response to the fact that several certification schemes exist, but there is no “one size fits all” or silver bullet solution for a Harmonised European Certification Framework. Moreover, the fragmentation in several markets requires a certain level of harmonization. A composition of existing schemes can be a pragmatic way to combine their advantages while not having to reinvent the wheel.

Engagement with other entities

European Standard Organisations: WG1 has seen the need to engage with the European Standards Developing Organisations to work together towards a common objective of strengthening cyber security in Europe. Towards this objective, ECSO has worked on establishing Memorandum of Understanding with ETSI and CEN-CENELEC (under definition) to establish important synergies to provide the lesson learnt in case there is a current gap in standardisation as identified by the exercise to map the existing certification schemes and standards with the challenges identified by the industry. ECSO WG1 has been regularly invited to contribute to the workshops and events organised by CEN-CENELEC in 2017.

Multi-stakeholder platform: The activities of ECSO WG1 have been presented to the MSP in June 2017, in particular the discussion has focused on the State of the Art document that represents an important step for establishing a common ground in Europe. ECSO was also invited to participate to the MSP meeting in December 2017.

DG-CNECT: Bilateral meetings have been organised to present the current status of the activities. ECSO has also contributed to the workshop organised on April 26\(^{th}\), 2017 to present the view on the European Certification Framework.

ENISA: A running dialogue has been established with ENISA to avoid duplication of work on certification and to reinforce cooperation and maximise resources for future actions and events.

**WG2 Market deployment / investments / international collaboration**

The objective of the WG 2 is to provide ECSO members with a market knowledge, to propose and foster an EU model for investments in EU cyber security for technology, and to establish a dialogue with the main countries (US and Japan) and initialise a dialogue with developing countries. The same WG will oversee the cPPP monitoring.
**WG breakdown**

WG2 has been segmented into 4 different sub WGs:

- SWG 2.1 Market knowledge: market, products and stakeholders update
- SWG 2.2 Investments, innovative business models
- SWG 2.3 International cooperation, global competitiveness and support to export
- SWG 2.4 Dissemination & awareness; KPI monitoring

No. of members subscribed to WG2: 81 organisations (153 experts/individuals)

WG meetings held: 2 in 2017 (2 phone conference calls).

**Main activities**

**Market Analysis**

The aim of the WG2 is not to start from scratch another market study, but to develop a common analysis of the market moves – mainly in Europe. For doing that, ECSO has supported the CIMA led by PWC and LSEC in organising national workshop with ECSO members. In addition, WG2 jointly with WG4 has developed a common taxonomy of market in order to design and deliver a market radar of the existing cyber security solutions which should provide inputs to WG6 on technological gap analysis as well as investors on market opportunities.

**Monitoring methodology**

WG2 has first elaborated and then presented and discussed the monitoring methodology at the 3rd Partnership Board on 27th October 2017. In particular, a detailed discussion took place between the EC services and the cPPPs since January 2017. Following the need to align the monitoring of the cPPP in cyber security with the forthcoming guidelines, ECSO Secretariat will refine, if needed, the proposed methodology based on further information provided by the EC on the review of the cPPPs under H2020.

**WG3 Sectoral Demand (market applications)**

**WG breakdown**

WG3 has been segmented into 8 different sectors, each represented by its own sub WG:

- SWG 3.1 Industry 4.0 and ICS
- SWG 3.2 Energy Networks and Smart Grids
- SWG 3.3 Transportation (road, rail, air, sea, and space)
- SWG 3.4 Finance, ePayments, and Insurance
- SWG 3.5 Public Services, eGovernment, and Digital Citizenship
- SWG 3.6 Healthcare, eHealth
- SWG 3.7 Smart Cities and Smart Buildings (convergence of digital services for citizens) and other Utilities

No. of members subscribed to WG3: 123 organisations (269 experts/individuals)

WG meetings held: 3 in 2017 (1 in 2016)

SWG meetings held: 3 in 2017 (1 in 2016)

**Main activities**
State of the Art (SOTA) exercise

One of the main tasks of WG3 in 2017 was to perform the first part of a SOTA exercise, drafting a sector report for each SWG to assess the needs from the sectors across four aspects: landscape, user engagement, sector specificities, and market study. The second part of the SOTA exercise will focus on assessing relevant materials, EU legislations and regulations, and providing user-driven recommendations for research needs (beyond H2020), trials (i.e. pre-commercial trials), standardisation and certification, and education, training, awareness and cyber ranges.

The sector reports, which will be publicly released and updated yearly (or as needed), aim to provide a view from ECSO members on what are the essential cyber security needs and requirements from the demand side with recommendations on how to reflect these in the overall ecosystem, and future policies and operationally-driven activities at European level.

Sector-specific workshops

In 2017, WG3 held 3 sector-specific workshops: one for energy, one for finance, and one for transportation. The aim of these workshops is to bring together ECSO members and users, utilities, sectoral associations and relevant DG’s to discuss the main priorities and actions for the sector in question and to elicit feedback from external parties on the needs and requirements expressed by ECSO members in the sector reports.

These workshops have shown the importance of engaging beyond ECSO membership with sectoral associations and relevant DG’s to ensure sufficient coverage of input from the main stakeholders in each sector and to avoid duplication on needed actions. As an example, since its first workshop in 2016, the energy SWG has established a running dialogue with DG ENER which serves to liaise on the main R&D and industrial policy activities for the energy sector, leading to a convergence on policy objectives and research topics (i.e. 2017 call topic co-funded by DG ENER and DG CNECT).

User engagement

User engagement and outreach is an important task for WG3 as this WG aims to provide demand-driven requirements to other ECSO WG’s and externally via relevant policy channels. In 2017, this was done through:

- Bilateral meetings with sectoral associations
- Building an internal database (excel) with the main users and associations for each sector
- Drafting a business development strategy and outreach document aimed at users
- Presenting ECSO at events and conferences with users as the main audience

ISAC survey

In 2017, ECSO WG3 members have discussed the topic of European sector-specific ISAC’s and what should be done with respect to these in terms of their setup, what they should achieve, and how to improve their efficiency.

European ISAC’s do not currently exist for each sector but each one needs a body where information can be shared in a trusted way. ECSO members believe that ISAC’s are needed that can provide information in the right model and with some added value that can put the intelligence between the ISAC and the final user. ISAC’s are also important in the context of the implementation of the NIS Directive.

A survey was therefore conducted internally to analyse ECSO members’ assessment of the needs and priorities for a European ISAC within their sector. The results of this survey are still being consolidated and will be synthesised in a position paper, considering also the release of the ENISA
study “Information Sharing and Analysis Center (ISACs) - Cooperative models” released in February 2018.

Exchange with ENISA

ENISA were regularly invited to WG3 meetings and bilateral meetings were held in 2017 to liaise on content related to the main sectors of activity shared by both entities: ICS, Smart Grids, Finance, and Health. A running dialogue has been established with ENISA to avoid duplication of work on these topics and to reinforce cooperation and maximise resources for future actions and events.

WG4 Support to SMEs and regions

The objective of WG4 is to focus on the following issues:

- Support the development of SMEs, start-ups and high growth companies
- Develop coordinated activities between clusters (both business oriented and triple helix), Regions and local bodies (for local implementation of solutions / educations)
- Development of East and Central EU public and private sectors dealing with cyber security.

Segmentation:

- SWG4.1: SMEs, start-ups and high growth companies -
- SWG4.2: Coordination with activities in EU countries and regions -
- SWG4.3: Support to East and Central EU Members

No. of members subscribed to WG4: 80 organisations (141 experts/individuals)

WG meetings held: 2 in 2017 (1 in 2016)

Main activities:

Support to SMEs

The kick off meeting for WG4 was held on 9th November 2016 in Helsinki and was attended by 31 people. The chairs and segmentation were approved, and particular attention was given to SWG 4.1 on SME’s. It was agreed that the next meeting should focus more on the cooperation with regions, clusters, and associations. Input to WG6 on the SRIA was also discussed. Then, WG4 has elaborated a position paper where we propose the establishment of European cyber security SMEs HUB as platform that allows small companies first to get to know each other, then to develop integrated solution and harmonize offering and thus get access to digital EU market. Government procurement at national level is an opportunity for EU SMEs. However, cyber security is often only a part of a larger public tender, making difficult for SMEs to apply. In fact, SMEs with innovative and potentially disruptive technologies are not well equipped to work with major infrastructure service providers, large enterprise clients and on large government contracts. Problems include lack of resources to carry through the implementations, including high business risk of ramping up the capabilities, but also inadequate experience in dealing with large customer processes in general. In this context, a HUB could facilitate the participation of SMEs to tender because structured cooperation among SMEs can drive wider SMEs engagement in the market, reduce transition costs and the fragmentation of the offer, and finally support integrated offer in wider bids-in particular for public procurement. A concrete solution to be developed by such HUB could be the proposal of an EU harmonized form for SMEs that wish to apply for public procurement in different countries.

Support to regional Ecosystems/Smart specialization on cyber security
Since its launch, ECSO has put a lot of effort to bring regions and regional players as key stakeholders. In March 2017, WG4 organise the kick-off of its activities with 11 regions, 4 DGs (REGIO, CNECT, GROW, JRC), 5 national public administrations and 2 industrial associations. The discussion revealed different regional approaches to cyber security and different level of maturity in the implication of local players in the cyber security ecosystem. Some best practices can be shared through a bottom-up approach. According to official EU data, some regions are already working on ICT/cyber with EU structural funds and some of them are investigating the option to launch specific activities of cooperation (e.g. INTERREG). There is a clear need of partnership: the debate was beneficial to identify common challenges. The problem is not the lack of EU investments: there are many funds available, but they are not well known among the stakeholders. First, the priority is to raise the awareness about the opportunities already available. Then, we could design and foster an operational cooperation among regions.

WG5 Education, training, exercise, raising awareness

WG breakdown

WG5 is segmented into three sub WG’s:

- SWG 5.1 Cyber Ranges and Technical Environments
- SWG 5.2 Education & Training
- SWG 5.3 Awareness

A Task Force has also been set up, linked to SWG 5.2, for the development of a European Human Resources Network for Cyber (EHR4CYBER)

No. of members subscribed to WG5: 101 organisations (207 experts/individuals)

WG meetings held: 2 in 2017 (1 in 2016)

Main activities

Setup of EHR4CYBER Task Force

In 2017, a high priority emerged for WG5 and all of ECSO: the creation of a European Human Resources Network for Cyber Security (EHR4CYBER) to build a network of universities, training academies and HR departments of ECSO in order to foster job creation in the area of cyber security.

EHR4CYBER will aim to create awareness among decision makers (private companies, regional / local administrations, national / EU administrations) about the need to develop education and training measures which will support job creation in the cyber security field. It will work to increase public and private funding that will support the increase of such education and training.

The network will also discuss and work on a common benchmarking system in cyber security recruitment, foster collaboration through the exchange of best practices, look towards harmonisation of education and training procedures across Europe, develop and harmonise certification for diplomas and specialties, as well as facilitate the recruitment process of cyber security specialists.

As part of its first tasks, the EHR4CYBER Task Force collaborated with SWG 5.2 on drafting a position paper on gaps in education and professional training and started drafting a white paper on information and cyber security professional certification, with recommendations for a combined EU approach and framework with respect to the certification of cyber security professionals. EHR4CYBER has also been working on mapping existing cyber security education, trainings, and best practices across Europe, as well as exchanging ideas for a suitable cyber security job exchange platform for Europe.
Cyber range survey

In 2017, an internal study was launched to understand and map existing cyber range platforms and activities (technology focused) of ECSO members. The initial responses were used to develop a follow up questionnaire to assess attitudes and motivations with regards to those cyber ranges. With this, ECSO is trying to build up a large database on what is available on the market, and to explore how to further build the European cyber range landscape and capacity building efforts.

School of the Future

In 2017, as part of its WG5 activities, ECSO joined the School of the Future Initiative’s Board of Trustees. This is a creative, local Belgian initiative focused on educating school children on the importance of cyber security, digital skills, etc. through short videos & discussions at schools, leveraging also on educational materials produced by ENISA.

https://www.slashprod.eu/side/smartrevolution/schoolofthefuture.html

Digital Opportunity Scheme

In 2017, WG5 has started a collaboration with DG CNECT on the Digital Skills & Jobs Coalition, namely the Digital Opportunity Scheme which aims to link trainees (through Erasmus+) with companies and DG CNECT will support through an Erasmus internal platform where companies can post their offers and students can post their CV’s. The pilot scheme was launched by Commissioner Mariya Gabriel at the Digital Skills and Jobs Coalition Conference on 7th December 2017, where she also presented the first offers for traineeships received from companies. Prior to the event, 5 ECSO members had already provided traineeship offers or support to the scheme. The dialogue between ECSO and DG CNECT on this topic is ongoing.
