European Cybersecurity Industry Proposal for a contractual Public-Private Partnership
Disclaimer: The following document represents solely the views of its authors from industry, research and technical organisations and cannot in any circumstances be regarded as the official position of the European Commission.
European Cybersecurity Industry Proposal for a contractual Public-Private-Partnership

June 2016
1 Preamble

Cybersecurity is one of the fastest growing ICT sub-domains as the critical processes in the society are becoming increasingly dependent on IT solutions. The sustainability of most important government processes, provision of vital services and even day-to-day actions of all the citizens rely more and more on well-working and secure ICT solutions.

The cybersecurity landscape is changing, risks are becoming more and more serious and potential impacts of cyber-attacks can affect a large number of applications and various sectors either directly or through cascade effects.

Creating a unified Digital Single Market (DSM) is one of the most relevant strategic goals of European Union and to support that goal, cybersecurity has been recognised as one of the vital fields that needs immediate actions at European level. Having strong European based cybersecurity offerings and solutions in place to build trust, is one of the key prerequisites of the implementation of Digital Single Market actions.

Yet, Europe is far from being at the right level of preparedness to counter the rapidly evolving cyber threats. The European Digital Single Market strategy points out cybersecurity as one of the relevant pillars. The interconnection of networks and systems which is key for the full implementation of an European Digital Single Market, calls for more coordination at the European level with a clearly identified industrial vision to counter potential cyber threats.

The ever increasing digital dependencies of critical processes and services, and the changes in the cyber threat landscape are circumstances that one cannot afford to ignore. The number and severity of cyber-attacks is a growing year-by-year and the cost to society is on a significant level. It is estimated that cyber-attacks are costing the global economy billions of euros every year\(^1\).

Changes in the last years have created a situation where the expectations towards information system resilience have radically evolved. Cyber threat of today is completely different from what we had to consider 10 or more years ago.

Various challenges need to be overcome in the cybersecurity and ICT security fields. It is urgent to act!

We should take advantage of the opportunities created by H2020, the European Cybersecurity Strategy and the Digital Single Market Policy, focussing resources and creating a synergy among the different EC budgets already from 2017.

We should respond to the political need and provide our users with trusted solutions according to European values, laws and procedures.

We should tackle the urgent requirement of industry in Europe to develop innovative solutions responding to competitive and societal issues, as part of a global strategy to protect our society, our economy and our industry.

As Europeans, we must aim high and mobilise stakeholders in society, industry, academia and research, to deliver first class products, services, technologies, highly skilled cybersecurity specialists, scientists and practitioners along the entire cybersecurity value chain, help to solve societal challenges in the cyber environment, grow cybersecurity sector, create high value-added jobs in Europe, and raise the general awareness of the population.

Important regulatory initiatives, like the Network and Information Security (NIS) Directive and eIDAS Regulation to support building trust in Europe are going to be implemented soon. Both of those regulations are important first steps, but many follow-up actions are needed, also with the possible support of cPPP projects, to actually implement the requirements on a practical level.

This proposal presents the vision and the tactical plan to support reaching those goals. For better coordination of the needed actions, we propose a contractual Public Private Partnership (cPPP) on cybersecurity and ICT security as one of the first crucial steps towards achieving these goals supported by a dedicated Association: the European Cybersecurity Organisation– ECSO.

\(^1\) N. ELIS (2014), Can Big Data prevent the next Cyber Attack?
2 Executive Summary

The rapid development in the digitalisation of economic activities and societies, the emergence of new technologies and the rise in digital connectivity and interconnectedness are matched by a corresponding acceleration of needs for technologies and solutions to provide security, ensure privacy and maintain trust in digital systems and networks. These needs are reinforced by the increasing prevalence and changing nature of cyber threats, and modes of attack and forms of malicious behaviour. These developments are not delimited by national borders and, specifically in the context of the DSM, require a response at a European-level.

Building on the fast digitalisation of several sectors of the European economy, the need for a comprehensive, pan-European approach on cybersecurity is gaining strategic importance for the European society and industry as a whole.

Cyber security is an essential enabling factor for the development and exploitation of digital technologies and innovation and is, therefore, inextricably linked to future prospects for growth, job creation and Europe’s response to environmental and societal goals. Specifically, Europe’s ambitions to develop or reinforce its leadership in key economic areas (e.g. health, energy, transport, finance, communications, Industry 4.0, and public services) must be accompanied by cybersecurity solutions that meet the needs of emerging digital markets.

The European cybersecurity market is about 25% (i.e. about €17bln) of the world market (estimated at €70bln in 2015), with an average yearly growth slightly larger than 6%, when the world market is growing at more than 8%/year. Also for this reason, it is urgent for Europe to boost its growth in the cybersecurity / IT security sector.

A recent study compiled by European cybersecurity industry leaders\(^2\) pointed out that Europe is in danger of falling behind in the international digital economy field. The study report also emphasised an important strength: the fact that Europe is the most trusted area in the world when it comes to ensuring high level of data security and privacy. This competitive advantage needs to be maintained and built upon. To improve the situation, we need to build on our strengths and tackle the weaknesses taking advantage from the many opportunities the dynamic digital market is offering.

The ECS cPPP has its roots in the convergence of the Secure Societies priorities of Horizon 2020 and the ICT Industrial and Technological Leadership. This convergence has contributed to the definition of the main strategic objectives to be achieved by the ECS cPPP.

The proposed cPPP should provide an important component to delivering this response, bringing together actors throughout Europe and across the diverse segments of the economy and society implicated in the development of a secure and trusted digital market (e.g. technology and solution suppliers and service providers, public and private sector customers and users, policy makers and public administrations) in pursuit of an agreed and coordinated strategy and policy actions aimed at:

- Protecting the (growth of the) European Digital Single Market from cyber threats;
- Structuring, consolidating and strengthening the European cybersecurity market with trustworthy and privacy aware technologies, products services and solutions;
- Supporting the development of European capabilities to develop and bring to market innovative cybersecurity technologies and, thereby, building a strong, resilient and globally competitive European cybersecurity industry with a strong European-based offering and an equal level playing field.

The objective of the following Industry Proposal is to bridge the gap between capacity building and the deployment of trusted European cybersecurity and ICT solutions on European and international markets. Therefore, creating new business opportunities for European industry while addressing the challenges faced by Europe and defending its stance on safeguarding the privacy of citizens.

This objective substantiates the intention to build a sustainable cybersecurity and strong trustworthy ICT industry in Europe, even beyond the scope of the ECS cPPP, by setting up a long term industrial strategy to reach expected impacts monitored through Key Performance Indicators (KPIs).

It should be noted that this proposal should be aligned with the establishment of a shared ecosystem and the support of cybersecurity and ICT industrial activities fostering the exchange of experiences, competences, pooling of resources, raising general awareness, setting up general education / specific training programmes etc.

Based on an analysis of the current nature and evolution of cyber threats in Europe supplemented by a detailed SWOT and market analysis, the proposal suggests to build this long term industrial strategy upon the strategic priority areas (both technical and non-technical) identified in the SRIA (Strategic Research & Innovation Agenda).

The technical priority areas of the SRIA are:

- Assurance and security / privacy by design
- Identity, access and trust management (Identity and Access Management, Trust Management)
- Data protection
- Protection of the ICT Infrastructure (Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
- Security services (Auditing, compliance and certification, risk Management, cybersecurity operation, security training services)

Other non-technical aspects identified in the SRIA are:

- Education, training, skills development
- Fostering innovation in cybersecurity: development of a cybersecurity ecosystem
- Define the cybersecurity value chain
- Boosting SMEs
- Bottom-up Track for Cybersecurity Innovation
- Standardisation, regulation and certification
- Societal aspects

These priorities would set the path for the development of innovative solutions and services in strategic areas of the European economy, leading to products that can be implemented transversally in different applications, such as Industrial Control Systems, Energy Networks and Smart Grids, Transport, Financial Services, Public Administration: Vital Services / eGovernment, Healthcare / eHealth, Smart & Secure Cities.

The commitment of stakeholders, for project activities running in the context of the ECS cPPP, is targeted to add a leverage factor of 3 in addition to the European Commission (EC) contributions under Horizon 2020 instruments. Therefore, the economic and industrial relevance of the scope of the cybersecurity cPPP coupled to relevant activities for market development, will facilitate Research and Innovation (R&I) investments in addition to and beyond the engagement of the EC in this partnership.

Having strong offering in the cybersecurity domain is also a crucial part in increasing the European digital autonomy for sensitive applications. Another relevant aspect is that there are many new emerging technological realities that are still in the early adoption phase and need the cybersecurity offering to be developed to match their specific needs. As these new areas (e.g. IoT, Big Data, Quantum Computing, Cloud, Mobile and embedded systems, smart grids etc.) are still emerging and escalating, then everybody has an equal chance to provide necessary cybersecurity products and services.

European cybersecurity industry and ICT should take advantage of these opportunities, particularly in those economic sectors and applications where Europe is leader. In some field, several cPPPs have already been brought to life. In these areas, collaboration with those other cPPPs is foreseen in the current proposal.

The proposal recommends the creation of an international non-profit association called ECSO with a governance model structuring the work and activities of actors engaged in the ECS cPPP. This Association will allow open
participation of all legal entities established in the countries participating in H2020. As security is a national prerogative, the participation of representatives from the national administrations is expected as well.

While the ECS cPPP will focus on R&I, the ECSO Association will tackle also other industry policy aspects for market and industrial / economic development.

The link between the SRIA priorities with its R&I priorities - which are the target of the ECS cPPP - and the policy support activities - which are one of the main targets of the ECSO Association - is essential to get the commitment of the private sector and reach a satisfying leverage factor as envisaged in the cPPP H2020 rules.
3 Table of Contents

1 Preamble .................................................................................................................. 4
2 Executive Summary ................................................................................................. 5
3 Table of Contents ..................................................................................................... 8
4 Vision ...................................................................................................................... 10
  4.1 Scene Setter ......................................................................................................... 10
  4.1.1 The evolving nature of the cyber threat .......................................................... 10
  4.1.2 Overview of the current situation in Europe .................................................... 12
  4.1.3 The strengths, weaknesses, opportunities and threats .................................... 16
4.2 Market Analysis .................................................................................................... 20
  4.2.1 Global cybersecurity Market ........................................................................... 20
  4.2.2 Market Size and Growth by NIS Product, Solution Category ....................... 22
  4.2.3 Characteristics of the European NIS market .................................................. 25
4.3 Impact of cybersecurity on strategic market sectors ........................................... 26
  4.3.1 Industrial Systems vs Information System ....................................................... 26
  4.3.2 Governance of information security for citizens ........................................... 27
  4.3.3 Vertical analysis (applications) .................................................................... 28
4.4 Needs for action .................................................................................................... 39
  4.4.1 Factors motivating the need for European action ............................................ 39
  4.4.2 Challenges and objectives ............................................................................ 41
4.5 Overall long term vision of the PPP ................................................................... 42
4.6 Strategic and Specific Objectives of the PPP ....................................................... 43
4.7 Added Value of actions at European Union Level .............................................. 47
  4.7.1 Rationale for a European approach ............................................................... 49
4.8 Added value of implementation via a contractual PPP ........................................ 50
4.9 Actors behind this proposal ................................................................................ 53
5 Research and Innovation Strategy .......................................................................... 55
  5.1 Introduction: Cybersecurity products and services ........................................... 55
  5.2 Mechanisms for SRIA implementation ............................................................... 56
5.3 Technical Priorities .............................................................................................. 56
  5.3.1 Identification and analysis of technical priority areas ..................................... 56
  5.3.2 Assurance / risk management and security/privacy by design ....................... 56
  5.3.3 Identity, Access and Trust Management ......................................................... 57
  5.3.4 Data security ................................................................................................ 58
  5.3.5 Protecting the ICT Infrastructure .................................................................. 59
  5.3.6 Cybersecurity Services .................................................................................. 60
5.4 Non-Technical Aspects and Supporting Actions ................................................. 62
  5.4.1 Education, training, and skills development ................................................... 62
  5.4.2 Fostering innovation in cybersecurity ............................................................. 63
  5.4.3 Define the cybersecurity value chain .............................................................. 65
  5.4.4 Boosting SMEs .............................................................................................. 68
  5.4.5 Bottom-up track for Cybersecurity Innovation ............................................. 69
  5.4.6 Standardisation, regulation and certification ................................................. 69
  5.4.7 Societal aspects .............................................................................................. 71
5.5 Estimated budget ........................................................................................................ 72

6 Expected Impact .............................................................................................................. 75
6.1 Expected impact on strategic objectives ........................................................................ 75
6.2 Description of Industry commitment .......................................................................... 76
6.3 Ability to Leverage Additional Investments .................................................................. 77
6.3.1 The leverage factor for industrial investments ...................................................... 79
6.4 Monitoring: KPIs ......................................................................................................... 81
   Industrial Competitiveness .......................................................................................... 82
   Socio-Economic Security .......................................................................................... 82
   Implementation and operational aspects of the cPPP ................................................. 83
   Industrial Competitiveness ........................................................................................ 83
   Socio-Economic Security .......................................................................................... 84
   Implementation and operational aspects of the cPPP ................................................. 90
   Industrial Competitiveness ........................................................................................ 92
   Socio-Economic Security .......................................................................................... 94
6.5 Proposed methodology for monitoring the commitments ........................................... 96
6.6 Risks ........................................................................................................................... 97

7 Governance .................................................................................................................... 101
7.1 Overview of the governance model ............................................................................ 101
   7.1.1 Overview ............................................................................................................ 101
   7.1.2 Structure .......................................................................................................... 101
   (a) Participate in the discussions and activities of the ECSO Working Groups and Task Forces to bring a governmental perspective and operational needs from the public administrations; ................... 102
   (b) Support the definition and implementation of the ECSO Strategic Research and Innovation Agenda and of the ECSO Multiannual Roadmap into the R&I Work Programme; ......................................................... 102
   (c) Exchange best practice and promote cybersecurity and national / regional research programmes. 102
7.2 R&I priorities definition process .............................................................................. 104
7.3 Agreements linked to the ECS cPPP or ECSO ........................................................... 105
7.4 IPR Principles .......................................................................................................... 106
7.5 Association Statutes and Modus Operandi of the Association .................................. 107
   7.5.1 Objectives and Principles ................................................................................ 107
   7.5.2 Statues of the Association .............................................................................. 110

8 ANNEX 1 ......................................................................................................................... 114
8.1 Simulations of investments ....................................................................................... 114
4 Vision

4.1 Scene Setter

4.1.1 The evolving nature of the cyber threat

Modern organisations are becoming increasingly dependent on IT systems since automating processes with digital tools is one of the few ways of providing services to the customers in an efficient way, increasing volumes of information is exchanged machine-to-machine etc. Using more and more IT solutions to provide services also increases the risks related to using cyber tools and these need to be kept in mind in order to keep the trust towards digital services.

Cyber threats are often latent by nature and in many cases ignored until it is too late. As the digital dependencies have already exceeded the critical levels, these threats need to be acknowledged and dealt with before serious consequences will happen. This is a strategic concern since more than 65% of European trade is intra-communitarian and the attack of a company or a European country can have serious consequences for the rest of the ecosystem, pointing out the need for European solidarity on this issue.

Even threats that rely on lacking very basic hygiene methods like regular back-uping are having major impact on critical services. One of the most relevant examples here is the increasing frequency of ransomware attacks, including attacks on hospitals\(^3\), several medical service providers have declared a state of emergency due to having relevant files decrypted paralysing the capability to take care of patients. To save lives, hospitals have been forced to shift critical patients to other hospitals\(^4\). Also other critical service providers, government organisations and even common citizens are under heavy attack. Just one of the most “popular” ransomware tools Locky is, according to Forbes, affecting 90 000 PC across the world per day\(^5\). In US, FBI registered 1838 complaints about ransomware and estimated the losses of victims to 23,7 million dollars, in 2015 the number of complaints grew to 2453, and the damage was estimated to be 24,2 million dollars\(^6\). These simple tools, harvesting very primitive attack vectors showcase the vulnerability and also make it clear that the awareness and basic cybersecurity hygiene skills of everyone are very important.

The world is changing rapidly, new emerging technologies also impact cybersecurity, introducing new vulnerabilities. Lewis\(^7\) has named the situation where there are new vulnerabilities related to digital dependency of critical services the *electronic Achilles’ heel*, suggesting that adopting new technologies and not being able to think through all possible new weaknesses is a reality that we need to acknowledge and constantly deal with.

The variety and the number of personal digital devices have increased enormously. Same trend has happened in other connected smart devices (e.g. grid devices, sensors, domestic devices etc.). The number of mobile phone users is expected to reach 5 billion by 2019, and 26 billion IoT devices are expected to be in use by 2020. At economic level, IoT market numbers indicate an expected growth from 1.9 Trillion US $ in 2013 to 7.1 Trillion US $ by 2020. Since every connected device is a potential target for hackers. For instance, the rapid emergence of Internet of Things (IoT) has created many new challenges that need to be tackled in a very large scale, across platforms and considering very different usage patterns.

Statistics show that also the number of cybersecurity incidence as well as the severity of their impact is increasing year by year\(^8\). In today’s world we also need to consider that the IT systems are not only threatened by human

\(^3\) http://www.cnbc.com/2016/02/16/the-hospital-held-hostage-by-hackers.html
\(^5\) http://www.forbes.com/forbes/welcome/
\(^6\) http://www.geekwire.com/2016/fbi-investigating-growing-number-ransomware-cases-report-says/
\(^8\) N. ELIS (2014), Can Big Data prevent the next Cyber Attack?
mistakes or recreational attackers, but also politically motivated cyber-attacks are becoming a reality, making it even more important to make sure our critical ICT solution are well protected.

The risk factors that need to be taken into account in the cyber room today are completely different of those we had to consider 20, or even 10 years ago. The technologies have changed, new methods of cyber-attacks have emerged. Today huge technical capacities are available at rather low cost, the web is full of tutorials teaching how to attack different IT systems and due to that, even people with limited technical skills can cause lot of trouble.

Critical infrastructures are vital in modern society and economy. Most of the critical infrastructures (e.g. water supply, electricity, healthcare, and telecommunication) highly depend on Industrial Control Systems (ICS) that manage key functions of the infrastructures. As these systems increasingly consist of (interconnected) networks, these systems have become more vulnerable for threats from outside the infrastructure, such as malware, botnets or denial of service attacks. ICS manage large-scale physical systems (e.g. nuclear power plants) and an attack on an ICS may have serious financial but also societal consequences (e.g. production loss, safety risks, information theft, disruption of key utilities).

Many outdated ICT solutions for ICS are still in use that were not built following security by design ideology, and even if they were – the cyber threat landscape has changed beyond recognition within last decades. E.g. many SCADA systems that were built in 1970-s or 1980-s are still in operation today, making them over 30-40 years old! These were designed with the focus on availability and personnel safety, not on IT system security, and are thus now vulnerable to malicious attacks like sniffing and tampering. Years ago this was not a problem because SCADA systems were often operated in dedicated, proprietary networks, but these systems are more and more opened up to internet protocols to exchange data with central information systems in head offices to provide real-time production data to support operational business decisions etc. In addition, industrial companies started to make use of off-the-shelf IT solutions that are more vulnerable to malware than in-house developed IT, which can affect the availability of ICSs. These developments enlarged the vulnerability of the systems to potential cyber disruptions from outside the company.

Higher connectivity is a reality that cannot be denied, but it also opens doors to many security risks that are not well managed. There are no policies currently in Europe to systematically fight against outdated legacy technologies and even if such no legacy policies emerge, it will take years (decades) to implement them. In the mean while new generation of cybersecurity tools are needed to monitor and maintain the data, network and system integrity, security etc.

Lewis also concludes in his study that conducting a cyber-attack is in many cases much cheaper than attack in a physical world, making this an attractive tool to use in modern warfare. There are already many examples of so called “hired guns” being involved in supporting the malicious intentions of certain groups in implementing their criminal activities. Teams of high-skilled hackers are employed by terrorists and criminal organisations, to break important information systems (Tsang and Smith, 2008). Often attacks in cyber world are part of a hybrid war scenario. Cyberattacks can potentially be part of a wider ‘hybrid strategy’ targeting several sectors. While lacking a conventional military component, cyberattacks can deliver subversion, disinformation and cyber-weaponry in a

---

13 SCADA — Supervisory Control and Data Acquisition systems are real-time process control systems that monitor and control local or geographically remote devices (Tsang and Smith, 2008).
14 No Legacy Policy – a set of guidelines that aim to support getting rid of existing IT legacy and help to avoid the build-up of legacy systems in the long run. One of the core principal suggested by Estonian is that there should not be any important IT systems in use in the public sector that are older than 13 years (Aet Rahe, Master’s Thesis “Modern governments need No Legacy Policy to keep ICT cost under control”, 2016, Tallin Technical University)
15 Hybrid threats comprise a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

European Cybersecurity cPPP – ECS cPPP – Industry Proposal

11
coordinated manner, which may challenge a country's police force, political institutions and financial sector simultaneously. Examples here are the attacks against U.S. military computer networks during operations in Kosovo (Lewis, 2002) or the attacks against Estonia in 2007 and Georgia in 2008 (Beidleman, 2009), many others have followed over the years (Crimea etc.).

Another way to use cyber world for malicious causes is virtual espionage. In a situation where majority of data is available in electronic format, this poses an additional risk that the potential victim often is not even aware of. In that case it is not the perpetrators interest to cause direct damage by listening in, but rather to collect information he can use against the victim when the time is right (Lewis).

The described changes have created a situation where the expectations towards information system resilience have radically changed. Cyber threat of today is completely different from what we had to consider 10 or more years ago. Today cyberspace has become one additional setting for war on par with land, sea, air, and space.

In summary, we can group the mentioned threats or challenges into three broad areas:

1. Threats to fundamental security
   i. cyber-attacks as a form of modern warfare
   ii. politically motivated disruption of major elements of infrastructure
   iii. invasion of personal privacy

2. Financial / property crimes
   iv. financial theft and other financial crimes such as ransomware
   v. theft of commercially valuable intellectual property from European companies

3. Threats to European business competitiveness
   vi. European Cyber Security providers having a small share of the world Cybersecurity market and, therefore, little market power
   vii. European companies being behind the other global companies in making economic use of the mass of data being generated.

We could rank these threats / challenges according to societal, economic, political priorities and use this ranking for the investments foreseen in this cPPP. Yet, the priority ranking will be different according to those who will establish the ranking. Establishment of priorities to threats and hence on investments is maybe the most challenging exercise of this cPPP and will condition the success of this initiative. We provide an initial quite global view of the different priorities and possible activities but only with the more structured dialogue at European level, between public and private stakeholders across the different sectors we will be able to refine the priorities and make a better common choice.

4.1.2 Overview of the current situation in Europe

4.1.2.1 Cybersecurity challenges in Europe

We can describe the current challenges and characteristics of cybersecurity in Europe as follows:

- **Global cybersecurity and ICT market dominated by global suppliers from North America.** Our estimation of the 2015 value of the global cybersecurity market is €70 billion with roughly an 8% average yearly growth, a large portion of which (more than 40%) is made up of the North American market. The enterprise market is largely dominated by global suppliers such as Microsoft, IBM, CISCO, Symantec, etc. Beyond these suppliers companies, we could mention also those companies managing (and thus controlling) a large number of data

like Google and Facebook, that can have an impact on our privacy and security at large. Main expert IT consultants are also originating from the US: market studies and advices have often an American pitch.

- **Mature commodity market.** Most IT hardware and software products are built outside the European Union. The market in “commodity protection” products, close to the ICT mass markets (firewalls, antivirus, IDS\(^\text{18}\) software etc.) is already reaching maturity and is therefore more costly and complex to enter.

- **Market fragmentation.** The EU’s 28 Member States have different regulations and approaches towards cybersecurity as well as data privacy concerns, also originating from past local needs and sovereignty issues which created “trusted companies”, competitive at national level. This ultimately leads to the development of different specific solutions not necessarily competitive in a global scale. More coordination in requirements would bring better interoperability, thus increasing the market size and creating larger opportunities for industry while decreasing development costs.

- **Innovation led by imported ICT products.** The pervasiveness of ICT in our everyday lives is growing rapidly through the increased use of different products and services such as electronic banking, e-commerce platforms, big data, cloud computing, e-supply chain, smart devices and internet of things among others. Many innovations in products and services are driven by ICT products that are not designed and manufactured in Europe and as a consequence they might not have a recognised certification and do not necessarily provide the privacy and trustworthiness expectations of European customers. The downside to becoming dependent on ICT is that we are increasingly vulnerable to the risks posed by cyber threats. The service based approach in which Europe has demonstrated strengths could be the one in which Europe can better compete.

- **Innovation** is strong in Europe, emanating from ICT labs, SMEs and large players, but not always properly funded due to a lack of a consistent transnational approach. Results of Research and Innovation are hardly reaching the market. There is still a lack of strategy in European research: the several ongoing projects and the NIS-P WG3 efforts have identified technology and societal gaps but the proposed R&I priorities have not seen sufficiently in a wider economic perspective to bring the European industry to a global competitive level. There is a need to better identify areas where Europe is well positioned to be a global leader, what are the strategic products and services and assist in defining long-term plans for building up these competencies.

- **Financial.** Weak entrepreneurial culture, lack of venture capital, and seed money calls for other ways to support innovation with the relevant financial effort and awarding mechanisms efficient enough to keep up with the pace of cyber threats.

- **European industrial policies not yet addressing specific cybersecurity issues.** Whilst the European Security Industrial Policy\(^\text{19}\) and the Communication for a European Industrial Renaissance\(^\text{20}\) set out the main roadmap for the development of a more competitive European security industry, they did not specifically stress them as main problems in the domain of cybersecurity.

- **Human factor.** The human factor plays a key role in cybersecurity. The time for creating a national cybersecurity culture metric is long overdue. For Europe, a deeper understanding about a cybersecurity culture is of utmost importance as it touches upon some of the most profound questions for development. Not only does digitalization help businesses make smart use of information technology and data, it ensures citizens benefit from the digital age and it underpins economic growth. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cybersecurity culture is shaped and how it affects the digitalization in businesses, sectors and on a national level. Understanding of the cybersecurity culture, as well as the mechanisms that forms it, is important in order to develop ICT policy and politics. For businesses, it presents them with a method for evaluating the effectiveness of their cybersecurity policies, education and measures.

---

\(^{18}\) Intrusion Detection System


\(^{20}\) COM (2014) 14/2 Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions For a European Industrial Renaissance
• **Sovereignty.** The current market fragmentation is partly due to the fact that security in general, and cybersecurity in particular – especially as a component of critical infrastructures and national assets protection – remains, within the European treaties, a national responsibility. From the industrial point of view, Cybersecurity include sensitive domains (e.g. cryptography), which would need to continue developing, at least to a certain extent, country-specific solutions. Hence, there is a strong link between cybersecurity solutions and sovereignty matters for the Member States that can result in a lack of cooperation and lead to increased market fragmentation.

• **Strategic supply chain dependency.** Europe is heavily dependent on non-European technologies in many domains in the ICT and cybersecurity field. Whilst this is not necessarily an issue for commodity hardware and software solutions, it can become a major problem when considering devices for critical applications manufactured by suppliers outside of Europe’s legal frameworks and without full confidence that the devices do not include, for instance, built-in backdoors or are applying the same level of quality requirements. As acknowledged in the joint European Communication on ‘Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’ “There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its frontiers. It is vital to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure, and guarantee the protection of personal data”.

From this analysis, it is clear that we are far from being at the right level of preparedness and that the interconnection of networks and systems which is at the key to the full implementation of an EU Digital Single Market calls for more coordination at the European level with a clearly identified industrial vision.

4.1.2.2 A cyber-opportunity window for Europe?

In Europe, a number of actions have been undertaken, ranging from the European Cybersecurity strategy in 2013, the NIS directive (political agreement reached in 2015), the updated General Data Protection Regulation and the Communication for a Digital Single Market. Together with the proposal of creating a Public-Private partnership (PPP) on cybersecurity, all these actions constitute steps in the right direction.

Europe is specific in its sensitiveness to privacy issues: European institutions are becoming increasingly demanding towards security measures in all innovative technologies.

• **Protecting critical infrastructures from cyber threats.** Whilst we are focusing on critical infrastructure and data protection, we are not addressing the cybersecurity challenges introduced by the many parallel infrastructures currently being deployed. These are creating new entry doors whose security, privacy and data management are only partially addressed through either of these communications and regulations.

In 2014, Google purchased NEST, an intelligent thermostat maker for 3.2 Billion $. Since September 2014, NEST was made available for installation in European homes through utility providers in Belgium, France, Ireland and The Netherlands. Interestingly, NEST thermostats were also originally sold through Apple stores, and were removed in 2015 when Apple started selling its own home automation kit. In practice, all these initiatives are creating a direct path into European homes, without any regulations or communications related to the level of security. Whilst the first level features are of course attractive in terms of giving home owners increased (remote and local) control over their consumption, this should not come at the price of security or privacy.

In the farming sector, John Deere, the US manufacturer of tractors, is revolutionizing farming with big data. Using data collected from the tractors and advanced sensors, the data is used to support better analysis of crops, production etc. Whilst again the first level impact is of course of relevance to all farmers, the security and usage of the data flows are not being addressed by European regulations; nor is the ownership of these data flows clearly understood by all farmers.

• **Use of massive data collection to increase overall security.** The concept of critical infrastructures has been expanded to align to the digital world that we know, but have yet to take into account the current revolution

21 https://datafloq.com/read/john-deere-revolutionizing-farming-big-data/511
brought on by the massive collection of data taking place from many different sources, including the important machine to machine communications.

With the use of the latest technologies (e.g. big data) it is possible to retrieve and structure data to create added value and intelligence which, when made at country or organisation level, can lead to political, societal and economic advantage (not necessarily European advantage).

But how much can Europe control its data when it is not even controlling its complete ICT infrastructure and services? What is really at stake when we hear requests for an increased European digital autonomy? Is it to have all our solutions and services sourced in Europe?

This is not a reasonable or even valid approach – today, not a single company, nor even a single region, can provide all the expertise and the resources necessary to address the multiplicity of challenges of the cyber-world.

- **Increased European digital autonomy.** An increased European digital autonomy or maybe less supply chain dependency can be considered for specific sensitive applications and should also giving control and creating transparency so that citizens and businesses are empowered to become actors of their own levels of cybersecurity and privacy.

Cyber-security services and solutions will increasingly be built through advanced integration of technologies from multiple providers both within and outside of Europe. There are no country borders in the cyber-domain: cyber solutions will continue to be sourced at world-wide level. What is important for Europe is to, of course, be at the forefront of innovative solutions, but first and foremost to be able to drive the delivery of solutions that address its own needs. For instance, today, cyber-threat intelligence is often based on data purchased from US providers. This is an issue, both in terms of autonomy and in terms of adequacy, as this data does not sufficiently address the reality of interconnected infrastructures, cultural diversity and legal variations across the European Member States and the other countries participating in the cPPP.

- **Security and trust of the whole supply chain.** Another dimension in the integration of several solutions is to ensure that when multiple solutions are combined into a single platform, their combination does not create new cybersecurity threats, do not create new entry points into the core of an enterprise; that customers are fully knowledgeable about the core components that are assembled. We should therefore support innovation through shared and agreed interoperable paths, that include security, transparency and accountability in the way these platforms are created.

Having emphasised the importance of retaining Europe’s capability and innovation to manage its data, to ensure security levels of new infrastructures, the European grown technologies in Europe, we should also recognise the importance of collaboration with global solution and service providers. We cannot and do not want to reinvent the wheel and invest massive amounts of money to build all the IT components and services in Europe. If we want to protect from cyber threats the growth of a European Digital Single Market, cooperation with non-European originated companies is and will be needed. What is important now is finding the right balance between using non-European originated technologies and developing (and using) European solutions, in order to control our data and not voluntarily, or involuntarily, offer competitive advantages to non-European organisations / countries.

Key in this process will be the creation of trusted supply chains, composed of validated and trusted non-European components as well as elements produced by trusted European companies.

If Europe has lagged behind in certain mature ICT domains and applications, there is still time to enter and become leader in emerging applications such as the Internet of Things, Quantum Computing, Big Data, Cloud computing, Mobile and Cyber Physical Systems, data integrity, strong electronic identity and digital signature management etc. But for this, important and strategic investments are needed in research and piloting, to effectively bring innovation to the market.

- **Investments in areas where Europe has a clear leadership.** Europe has also to ensure in this world-wide approach that it not retains but expands on the key innovations where it has clear leadership; for instance, European companies are at the very leading edge in the block-chain-based technologies and their applications. But this strength could be at risk due to the difference of investments in this domain. For instance, 1 billion $ of investments have been channelled into block-chain commercialisation by US venture capital last year alone.
- **Leveraging upon the potential of SMEs.** 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, from both business and operational angles.

- **Increase competitiveness.** Today, security is tackled in the European research programme H2020 as a societal issue, yet there is an urgent need to better consider competitive issues and support Europe in the development of a genuine cybersecurity industry and the creation of those global champions that can also better assure data management following European interests and cultural needs. To reach this goal, the European cybersecurity cPPP is a major opportunity to build a stronger technology base, leveraging upon an industrial strategy to effectively meet the interests of Europe, merging the societal with the competitiveness issues.

### 4.1.3 The strengths, weaknesses, opportunities and threats

Following is the overview of the existing strengths, weaknesses, opportunities and threats of European cybersecurity domain.

This SWOT analysis shows how Europe has many weaknesses in the cybersecurity / ICT security domain, but has also many opportunities to respond to needs. In this cPPP we will have to face those weaknesses and leverage upon our strengths to get those opportunities.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>European aspects:</strong></td>
<td><strong>European Aspects:</strong></td>
</tr>
<tr>
<td>- Europe is known and valued for a high level of data security and privacy. This is currently seen as competitive advantage compared to other regions (supported by the General Data Protection regulation and the NIS directive)</td>
<td>- Fragmentation of cybersecurity strategies across Member States as well as the other counties participating in the cPPP</td>
</tr>
<tr>
<td>- Tailored solutions that address specific European requirements</td>
<td>- Diversity of operational authorities across Member States and in the other counties participating in the cPPP</td>
</tr>
<tr>
<td>- Large number of existing companies that provide cybersecurity solutions and services, thus there are European capacities with growth potential</td>
<td>- Limitations to cooperation and effective data sharing due to Member State sovereignty barriers</td>
</tr>
<tr>
<td><strong>Market and Business:</strong></td>
<td>- Limited amount of large companies, many niche players (very large number of SMEs) without critical mass that need nurturing</td>
</tr>
<tr>
<td>- Large internal market in Europe (EU28: 500 million consumers)</td>
<td><strong>Market and Business:</strong></td>
</tr>
<tr>
<td>- Highly diversified cybersecurity SME industry serving local markets / needs</td>
<td>- Fragmentation of market needs with lack of a minimum agreed set of requirements for security and privacy for devices (IoT, mobile) and solutions</td>
</tr>
<tr>
<td>- Strong relationship of national trusted companies with local governments</td>
<td>- Lack of structure due to fragmentation of capabilities across a few large private industries and a high number of small to very small niche players</td>
</tr>
<tr>
<td>- Europe is among market leaders in encryption, blockchain, eIDs, digital signature technologies etc.</td>
<td>- Lack of commonly agreed industrial strategy for European funding across the complete value chain: early development phases, growth phases (limited access to European-based venture capital, less attractive Venture Capital ecosystem in Europe vs USA)</td>
</tr>
<tr>
<td>- Growing interest and awareness in ICT and cybersecurity at national and European level</td>
<td>- Lack of mass-market offering</td>
</tr>
<tr>
<td>- 33 European companies rated in the top 250 CyberSecurity ranking22; Europe has a demonstrated cyber related innovation capability</td>
<td>- Global market dominated by global suppliers from North America for software, Asia for hardware</td>
</tr>
<tr>
<td><strong>R&amp;I and Technical:</strong></td>
<td>- Lack of too few global competitive European companies positioned on emerging subjects</td>
</tr>
<tr>
<td>- European wide networking effective at research level; deployed operationally at national level for cybersecurity</td>
<td></td>
</tr>
<tr>
<td>- Innovation uptake mechanisms in place in the IT sector</td>
<td></td>
</tr>
</tbody>
</table>

---

| (EIT Digital, FIWARE) | • Huge academic competence gathered from EC projects |
| • Growing initiatives in universities or private institutes, companies for professional training |
| • Cybersecurity training programmes emerging in university level |
| • Many cyber range environments have been built to enable cyber exercises and practical, hands-on trainings for specialists: cyber exercises run at European level (ENISA, Cyber awareness month, Locked Shields, Cyber Coalition etc.) |

**Policy and Legal:**

- Europe has a reliable and trusted legal framework with long track record from analogue world
- Privacy regulation fostering trust; legal and regulatory framework supporting free and open cyberspace
- The European Union promotes free and open processes
- eIDAS regulation in place to foster cross-border secure authentication and mutual trust
- NIS directive to ensure high common level of cybersecurity in Europe

**R&I and Technical:**

- Insufficient level of European and national funding coordination to support emergence of European solutions in strategic sectors
- Industry driven innovation lacks support in Horizon 2020: Bottom-up instruments as Fast Track to Innovation need substantial funding for cybersecurity
- Europe heavily dependent on non-European technologies in many domains in the ICT and cybersecurity field
- Vulnerable (outdated) critical infrastructures with low resilience levels with respect to current digital threats, insufficient impact of policies for systematic upgrades (policies agreed at reporting levels but not at investment, evolution levels)
- Long cycles from innovative ideation to commercial products: slow innovation process and lack of significantly sized demonstration and commercialisation actions to accelerate transfer from laboratory to market
- Lack of awareness of market developments within Europe
- Insufficient testing / testbed facilities
- Stronger and more advanced innovation ecosystems exist around the defence/military sectors in other regions, leading to more advanced R&D and better innovation outcomes in NIS (US and Israel in particular)
- Lack of tools, solutions and services to keep up with the increasing cyber-threats (ensure systems’ resilience, data integrity etc.)

**Education and Skills:**

- Shortage of the right skills: long-term lack of sufficient skilled personnel in ICT / cybersecurity
- Low general awareness of the cyber-threats among the population
- Lack of cybersecurity education and awareness programmes for all levels in schools
- Very limited cybersecurity awareness raising efforts targeted to general population
- Low situational awareness of cyber-threats among vital service providers, policy makers and other relevant stakeholders
- No wide-scale ecosystem exists to enable hands on competence building, awareness raising, experience exchange, products testing etc.
### Opportunities

**European Aspects:**
- Wide business opportunities due to the size of the European market
- Wide SME base, potential to increase collaboration for finding synergies
- Leverage European market development upon cybersecurity needs for vital service providers / important European and national infrastructure and services, limiting procurement, when possible / needed for high security reasons, to genuine European solutions
- Use and leverage upon specific European cultural assets
- The existence of different cybersecurity needs and best practice examples in different European countries, high potential for finding synergies
- Strengthening the European market, by consolidating SMEs and key industries
- Investment in the entire supply chain, beyond basic research, using European and national funds

**Market and Business:**
- Growing the European market leveraging upon the existing European Cybersecurity industry
- Boost the go-to-market actions of innovation leaders and SMEs with high growth potential would eliminate the need to sell these technologies to buyers outside Europe at the early stage in the business development process
- Implementing disruptive innovation funding instruments for accelerators and SME clusters / associations would enable a wider range of SMEs, start-ups and high growth potential companies to get funding in the early stage of business development, as companies at that stage are unable to manage the administrative burden of European funding processes. This burden can partly be taken on the shoulders of accelerators, clusters and / or associations
- Fast growing market place
- Fast changing threat landscape, increase of digital dependencies, wide use of data and emerging technological realities create a need for new products and services – equal chance for innovation for European providers
- Export opportunities, particularly in emerging markets, due to good reputation of European products
- Creation of cybersecurity clusters at national / regional level can drive wider SMEs engagement in the market
- Increased need for specific and tailored security solutions for European Industries - in particular for SMEs on emerging markets
- European policies in leading European markets

### Threats

**European Aspects:**
- Massive cyber-attacks in different European / national sectors could create major damages to the society and economic loss also across countries
- The solutions non originated in Europe need to be validated according to European criteria for trustful use in sensitive applications
- Europe lacking a strong cybersecurity investment culture

**Market and Business:**
- Low-cost off-shore manufacturing, in particular for services
- There are several barriers to market entry or growth for SMEs in the internal market as well as accessing markets outside Europe
- Largest cybersecurity firms are located overseas, creating dependability on solutions
- Majority of SMEs are too small to cope with long and costly cross-border sales cycles
- Lack of European-based venture capital that is realistically available for SMEs
- Increasing digital dependency of critical processes in the society

**R&I and Technical:**
- Threats to information systems are becoming more complex and traditional cyber defence mechanisms are less effective
- Level of integration required to effectively combat cyber-threats is increasing (no single company can provide a complete solution)

**Education and Skills:**
- Lack of skilled professionals and graduates
- Many skilled professionals leave Europe to work in other regions; there is a risk of a “Brain Drain” in Europe
- Low general awareness of key stakeholders

**Policy and Legal:**
- Regulatory and certification requirements in emerging markets
- Increasing regulatory burden
- Ethical and privacy issues could cause loss of competitiveness if not imposed by regulation or supported financially
**Supporting application of cybersecurity solutions**

- Competitive advantage in creating cybersecurity solutions for markets where Europe is leader: energy, transport (automotive, aeronautic), financial services, retail, telecommunications, leisure, consumer goods etc.

**R&I and Technical:**

- Implementation and strengthening of mutual trust building tools like certificates, labels etc. to tackle the market fragmentation challenges
- Secure interoperability tools and standards will facilitate data exchange
- Potential to capitalise on innovation from EC funded projects
- Smarter use of research funding to support innovation and taking this innovation to market

**Education and Skills:**

- Higher involvement of students in research activities to give them practical skills
- Cybersecurity training modules should be integrated into school programs on all levels to raise a cyber-threat-aware generation in Europe. Joint and shared ecosystem helps to scale the effect and reduce collective costs.
- Stronger collaboration between existing educational programmes as well as between industry and education providers to strengthen the formal education of cybersecurity: collaboration between industry and educational sector to compile high-quality educational modules and programmes for all school levels
- Increase the number of cybersecurity trainings and the number of students in those training programmes to grow the resource pool
- Integrate cybersecurity training modules to the training programmes of other industries (especially critical services industries, policy making, legal training) to grow a generation of cyber-threat-aware key stakeholders
- Strong technical exercises ranges exist that could be scaled to serve wider range of stakeholders (SMEs, critical infrastructure providers, universities, policy makers etc.).
- Creating network of integrated ecosystems to support awareness raising and technical as well as strategic trainings of stakeholders and specialists
- Web-based training programs can be brought to life to grow the resource pool and provide additional training opportunities to specialists in other fields (e.g. critical infrastructure operators, SMEs etc.). Web based programs would enable to scale the awareness raising and competence building of wide user-base

**Policy and Legal:**

- Creation and implementation of an European cybersecurity industrial policy
- Some of the regulatory frameworks are in place to build cross-border trust and collaboration in internal market (NIS directive, eIDAS act).
- Increase European Strategic Autonomy for sensitive applications to boost references and competitiveness
• European Digital Single Market Strategy to facilitate introduction of cybersecurity solutions
• European Cybersecurity Strategy
• Harmonisation of policies within Member States as well, if possible, with the other counties participating in the cPPP, would create level playing field on internal market of Europe
• European standardisations and certifications as processes to protect the security of European governments, citizens and businesses
• Harmonisation of certification processes to lower the market fragmentation and make it easier for start-ups and SMEs to enter other countries within Europe. Similarly to mutually accepting each other eIDs (as regulated by eIDAS), there is a potential to build trust towards certificates issued by other Member States and some other counties participating in the cPPP, instead of every country within European demanding their own

4.2 Market Analysis

4.2.1 Global cybersecurity Market

In the recent years, there has been a strong growth of the cybersecurity market, as part of the wider IT market. Cybersecurity constitutes today, on average, about 2.3% of the IT spending which is expected to be about €3100 bln (source: Gartner) in 2015.

Digital security is at the beginning of its maturity cycle, if we refer to the “hype curve”\(^\text{23}\), with a plateau reached in 5 to 10 years. The Hype Cycle for Emerging Technologies report is the longest-running annual Hype Cycle, providing a cross-industry perspective on the technologies and trends that business strategists, chief innovation officers, R&D leaders, entrepreneurs, global market developers and emerging technology teams should consider in developing emerging-technology portfolios.

\(^{23}\) [http://www.gartner.com/newsroom/id/2819918]
Due to the differences in defining the cybersecurity market and the scope of available market studies, the global market size for network and information security (NIS) “civilian” products and services has been difficult to estimate, ranging from €46.9-€76.3bn according to the EU NIS-P.\textsuperscript{24} We have actually found market studies extending the expected market value for 2015 up to $120 bln, which seems quite excessive to justify.

According to the market study made in the F7 project IPACSO the European civil cybersecurity market reached the level of €18.8 bln in 2014 (yet, including Russia). It is forecasted to grow at an annual rate of 7.4% reaching the level of €26.7 bln (including Russia) in 2019. The European market is however smaller than the US market which is estimated to be around €26 bln in 2014. The UK, Germany and France constitute the biggest market sub segments and about 60% of the European market and estimated to achieve growth rates of between 5-6%.

![Market Size by region (and market share in brackets), Source: IPACSO - 2014](image)

As seen in the figure above, the two biggest regional markets for cybersecurity products are the North America and Europe, composing about a half of the global market.

It is estimated (e.g. Gartner, Visiongain)\textsuperscript{25}, that the cybersecurity market in 2015 was of about €70 billion, with an average yearly growth higher than 8% (about 6% in Europe). The adoption of mobile, cloud, social and information will be the main drivers for the use of new security technology and services in the near future.

Combining elements from the different mentioned sources, the European cybersecurity market is about 25% of the world cybersecurity market (i.e. about 17bln € - not including Russia – hence the difference with IPACSO) with an average yearly growth slightly larger than 6% (giving an EU market larger than € 22 bln in 2020), as presented in the following table.

<table>
<thead>
<tr>
<th>CYBERSECURITY NATIONAL MARKETS</th>
<th>2014 € bln</th>
<th>Market %</th>
<th>Average growth in the next 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>26</td>
<td>39,0%</td>
<td>4%</td>
</tr>
<tr>
<td>P.R. China</td>
<td>5.5</td>
<td>8,2%</td>
<td>higher than 10%</td>
</tr>
<tr>
<td>Japan</td>
<td>5</td>
<td>7,5%</td>
<td>5%</td>
</tr>
<tr>
<td>Germany</td>
<td>4.3</td>
<td>6,4%</td>
<td>5%</td>
</tr>
<tr>
<td>UK</td>
<td>3.7</td>
<td>5,5%</td>
<td>5%</td>
</tr>
<tr>
<td>Russia</td>
<td>3.1</td>
<td>4,6%</td>
<td>6%</td>
</tr>
<tr>
<td>France</td>
<td>3</td>
<td>4,5%</td>
<td>5%</td>
</tr>
<tr>
<td>South Korea</td>
<td>2.6</td>
<td>3,9%</td>
<td>5%</td>
</tr>
</tbody>
</table>


\textsuperscript{25} \url{http://cybersecurityventures.com/cybersecurity-market-report/}
The main difficulty is the evaluation of the percentage of the world market secured by companies having their origin in Europe (not being European subsidiaries or European HQ of external companies). A rough estimation, gives a value of about 6 bln €, corresponding only to 35% of the European market and 8,5% of the world market (a value close to an estimation given by Gartner specific to “system and network security software” sector), thus showing the progress that the European cybersecurity industry can make! The corresponding number of highly skilled experts in European cybersecurity industry is suggesting a figure of about 100.000 direct jobs.

4.2.2 Market Size and Growth by NIS Product, Solution Category

Combining elements from the different mentioned sources, figures according to the different class of market products can be provided[26].

<table>
<thead>
<tr>
<th>MARKET BREAKDOWN BY SOLUTIONS / SERVICES</th>
<th>2014 € bln</th>
<th>Market %</th>
<th>Average growth in the next 10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance, vulnerability and cybersecurity management</td>
<td>2,7</td>
<td>4,0%</td>
<td>11%</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>7,3</td>
<td>11,0%</td>
<td>10%</td>
</tr>
<tr>
<td>Data security</td>
<td>11,3</td>
<td>17,0%</td>
<td>6%</td>
</tr>
<tr>
<td>Cloud Security</td>
<td>2,7</td>
<td>4,0%</td>
<td>12%</td>
</tr>
<tr>
<td>Applications security</td>
<td>2,7</td>
<td>4,0%</td>
<td>7%</td>
</tr>
<tr>
<td>Network systems security</td>
<td>14,7</td>
<td>22,0%</td>
<td>5%</td>
</tr>
<tr>
<td>Hardware (device/endpoint) security</td>
<td>4,0</td>
<td>6,0%</td>
<td>6%</td>
</tr>
<tr>
<td>Audit, planning and advisory services</td>
<td>9,3</td>
<td>14,0%</td>
<td>6%</td>
</tr>
<tr>
<td>Management and operations services</td>
<td>2,0</td>
<td>3,0%</td>
<td>7%</td>
</tr>
<tr>
<td>Managed security services - MSS</td>
<td>9,3</td>
<td>14,0%</td>
<td>15%</td>
</tr>
<tr>
<td>Security training services</td>
<td>0,7</td>
<td>1,0%</td>
<td>10%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>66,7</td>
<td>100,0%</td>
<td>higher than 8%</td>
</tr>
</tbody>
</table>

Allocation of cybersecurity budget as a percent of cybersecurity spend (2014)

This “averaged” growth estimation (also supported by data from Morgan Stanley and Indra) is yet different from the one given by Forrester in their 2014 survey of security decision makers[27] which gives for certain sectors (like network

---

26 EOS - CYBERSECURITY FOR A TRUSTED EU SINGLE DIGITAL MARKET - Market Study for a Cybersecurity Flagship Programme - December 2015
system security) a short term growth of 15% (maybe a problem of perimeter definition, but also to be considered that this is a more mature and larger market).

In the following graphic we can better appreciate the solutions / services having a larger growth, like Cloud Security and MSS.

An interesting market view is also obtained by multiplying the market size for each solution / service area with its percentage growth. In this case, we obtain, as shown hereafter in a normalized - over the largest value – view, a perception of the market dynamics linked to the market size: this shows the interest for entering certain markets (most attractive for their size and growth).

A different market view is recalled in the Business cases deliverable of the NIS-P WG3 study28.

Current market sizes by NIS solution sub-segments (source: IPACSO / adapted from McAfee)

The increasing fragmentation and diversity of available NIS technologies is reflected in the “Other” Categories segment where a high growth rate (YOO = Year Over Year) of 14.2% exists.

An interesting view of the technology evolution is also given by the Ponemon study29. Big shifts in new technologies are expected towards big data analytics, forensics and intelligence based cyber solutions. The following technologies will gain the most in importance over the next 3 years: encryption for data at rest, big data analytics, SIEM and cybersecurity intelligence, automated forensics tools, encryption for data in motion, next generation firewalls, web application firewalls, threat intelligence feeds and sandboxing or isolation tools. In the following figure we can see the percentage net changes in importance ratings for 25 enabling security technologies for the consolidated sample. Here, a positive net change percentage indicates that the importance of a given technology is projected to increase over the next three years. A negative percentage indicates the importance of the technology is projected to decrease. The technologies that achieve the highest percentage net change are: encryption for data at rest, big data analytics, forensics (automated tools), next generation firewalls, SIEM, threat intelligence feeds, web application firewalls, sandboxing or isolation tools and encryption for data in motion. Technologies that are projected to become less important over time include anti-virus tools and data loss prevention systems.

As it can be seen in the presented elements, apart from the difficulties to compare similar topics (due to the different segmentation in the different market studies, maybe not sufficiently independent) the values are considerably different.

### 4.2.3 Characteristics of the European NIS market

The European market can be divided into three parts: high grade, low grade and mid-grade cybersecurity.

**High grade** is a niche market for companies originating from the defence sector. Given restrictions on public procurement, a protected and high-level European offer has been developed.

The **low-grade** cybersecurity market is largely dependent on non-European companies. As the offer for the general public, Business-to-Consumer (B2C), is mainly based outside Europe, new European companies entering the market are often acquired by non-European actors.

The **mid-grade** European cybersecurity offer catering to critical infrastructures and public authorities is quite dispersed. There are thousand European companies. The large majority of them are SMEs having a turnover under 5 million Euros and less than 50 persons. They are specialized in one area of activities and do not offer the whole range of cybersecurity products, hence they are not in a position to offer a comprehensive cybersecurity solution to critical infrastructure companies.

For the high grade, national administrations have always asked for a certain level of protection. For the low grade, consumers have always looked for anti-viruses, firewalls, anti-malware etc. The demand in these sectors has actually grown progressively. In the medium grade sector, the demand has deepened following attacks from viruses like Stuxnet and indeed following Snowden.

An additional problem is that there is no public or private mechanism that would provide information over the services provided by the many SMEs in Europe which offer cybersecurity, so that contracts are given to non-European companies even in cases when European offers exist. The promising SMEs are also vulnerable to acquisitions by foreign companies at prices that European companies cannot match.

European cybersecurity start-ups and SMEs face funding problems and have great difficulty in raising the necessary funds for their technological and commercial development. Several innovative companies were acquired by foreign companies, such as Stonesoft (FI) acquired by McAfee, Secusmart (DE) acquired by Blackberry or Anubis Networks (PT) bought by BitSight. Despite having identified the issue, there is not yet a strategy for consolidation in Europe. In addition, cooperation across SMEs and large companies in Europe is still at infancy stage.

The current competition and merger policy in Europe does not foster the European-wide pooling of resources. The fragmentation of the European market has enhanced the dominance of US-players in particular, not only from the competition perspective but also in the fields of data protection and cybersecurity. A level playing field in terms of privacy and security between Europe and United States is needed.

Many SMEs lack the knowledge of international markets they need to operate effectively overseas. Some have exported very successfully but even those who are exporting successfully would welcome better intelligence on countries, opportunities and competitors overseas. However this information can be hard (or expensive) to acquire. Meantime particular niches in the domestic market are relatively small. US firms in particular have a much wider domestic market to target before they need to think about international expansion. SMEs do not have the resources to monitor the developments in their big competitors. One of the biggest problem SMEs have in their propositions is that they do not have sufficient competitive intelligence to understand where their product sits in the market.

There are a few initiatives at European level to support SMEs when dealing with cybersecurity issues: COSTAR, ATALANTA, FI-PPP and FIWARE Accelerator[^30] as well as the Business Development accelerator of the EIT ICT Labs[^31].

The overall objective of the ATALANTA project is to drive innovation, facilitate technology transfer and to support entrepreneurship on a transnational European level to contribute to the exploitation of more innovative products.

[^30]: https://www.fiware.org/fiware-accelerator-programme/
[^31]: https://www.eitdigital.eu/innovation-entrepreneurship/business-development-accelerator/
and services coming from European R&D projects and to support the creation of more successful ICT start-ups in Europe. The project supports groups of leading accelerators for delivering cross border services to innovative SMEs and entrepreneurs.

Similarly, FI-PPP FIWARE delivers, and links these groups with knowledge creators and education organisations (i.e. mentors, trainers, service providers and partners) on one side and to investors (i.e. venture capital organisations) and the business world (i.e. potential clients, partners, suppliers and venture capitalists) on the other.

4.3 Impact of cybersecurity on strategic market sectors

4.3.1 Industrial Systems vs Information System

An important factor in the choice of priorities for supporting the growth European cybersecurity industry is the area of application of the solutions/services. Even if the different solutions are in general applicable to all kind of system, specific customers and applications could need more specific solutions having an important impact on the security and resilience of the system/critical service itself.

A first major distinction can be made between Industrial Systems and Information Systems. A critical differentiator between industrial systems and information systems is that industrial systems control real world physical processes that relate to nuclear power, water, electric, gas and other critical infrastructures. Therefore, targeted attacks on industrial systems such as disruption to nuclear reactors or to the electrical power grid ecosystem can have real world consequences on human lives and the environment. For the most part, the same cannot be said of the information systems domain where the consequences of, for example, a disrupted online banking or retail service has such profound and critical impact on society.

Information Systems, linked to Business Services, Media Entertainment and Leisure (e.g. tourism, gaming, culture), as well as Retail and Wholesale, are less “critical” for the society, but have a considerable economic weight and should be protected as well from cyber-attacks.

Industrial systems concerns domains where Europe is among the world leader and for this reason they deserve special attention when establishing cybersecurity / ICT security investment priorities in Europe.

Industrial systems are ubiquitous within a wide cohort of industry domains where Europe is among the world leader, such as pharmaceutical, and manufacturing (e.g. automotive, food production ...), buildings infrastructure (e.g. Heating Ventilating & Air Conditioning, elevator transportation and physical access control to and within buildings) or industrial system of societal/vital importance, such as water treatment, oil and gas, transportation, electric power. Industrial systems include Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) that form a complex interconnected real-time heterogeneous ecosystem.

In the past industrial systems bore little resemblance to traditional cyber information systems, in that they were using for the most part proprietary (unsecure) protocols and were largely considered isolated from cyber information networks (i.e. the Intranet and Internet). However, with the explosion of the Internet of Things (IoT), the increasing usage of wireless devices and cheap Internet Protocol (IP) based devices, the industrial systems market is seeing a strong demand for such technologies. As a consequence, the introduction of these new IP enabled devices significantly reduces the isolation these industrial ecosystems once had. This creates major security challenges to secure both the new and especially the legacy (non-secure) industrial systems from internal and external threats.

Industrial systems are undergoing a paradigm shift from isolated ecosystems to IoT-style ecosystems where isolated islands are interconnected to other Intranets and Internets. This results in a number of unique security challenges that need to be overcome within the industrial system domain. For example, developing new and advanced security mechanisms to protect unsecure legacy proprietary industrial systems that where never designed to be connected to the Internet. Another example is the introduction of off-the-shelf information systems devices into the industrial systems ecosystem means that new security and privacy mechanisms that harden the security generic operating systems such as Microsoft and Linux are required. That is the information systems paradigm of ‘good enough security’ must become ‘real-time resilient security’ with respect to industrial systems domain.
The security challenges are not just limited to securing legacy industrial systems and adapting information systems for the industrial environment. The key security challenge will be to develop next generation security aware embedded networks and IoT based ecosystems for the industrial systems domain.

While currently the cybersecurity initiatives in Europe are mainly focusing on SCADA systems for critical infrastructures, there is a real need to broaden the scope to consider other types of control systems and application domains. This is particularly relevant when considering that end user are increasingly demanding for more secure product in all application domains, including manufacturing processes (see later Industry 4.0), such as automotive, and buildings infrastructure such as Heating Ventilating & Air Conditioning (HVAC). This is due to the increasing connectivity to enable more functionalities, e.g. remote maintenance and the adoption of emerging technologies like cloud and IoT to enable smarter and more integrated systems. Finally, while these industrial systems are not always used as part of critical infrastructure, if they are tampered with, there could catastrophic consequence, e.g. HVAC control indoor environment during a festival.

In summary, there is a high demand, not just from a traditional cybersecurity perspective, but also from a regulatory compliance and economic perspective to provide new standards, mechanisms, frameworks and tool suites that provide automated resilient security and privacy controls within the industrial system domain.

A higher-level category that is gathering elements from Information Systems and Industrial Systems are the Cyber-Physical Systems (CPS). As CPS we can recognize Smart Grids, mobile devices, IoT etc., all sensitive to cyber-attacks and needing advanced cybersecurity.

Cyber-Physical Systems are integration of computation, networking, and physical processes. A CPS is a system of collaborating computational elements controlling physical entities. Today, a precursor generation of cyber-physical systems can be found in areas as diverse as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances. This generation is often referred to as embedded systems. In embedded systems, the emphasis tends to be more on the computational elements, and less on an intense link between the computational and physical elements. CPS integrates the dynamics of the physical processes with those of the software and networking, providing abstractions and modelling, design, and analysis techniques for the integrated whole.

Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. The notion is closely tied to concepts of robotics and sensor networks with intelligence mechanisms proper of computational intelligence leading the pathway. Ongoing advances in science and engineering will improve the link between computational and physical elements by means of intelligent mechanisms, dramatically increasing the adaptability, autonomy, efficiency, functionality, reliability, safety, and usability of cyber-physical systems. This will broaden the potential of cyber-physical systems in several dimensions, including: intervention (e.g. collision avoidance); precision (e.g. robotic surgery and nano-level manufacturing); operation in dangerous or inaccessible environments (e.g. search and rescue, firefighting, and deep-sea exploration); coordination (e.g. air traffic control); efficiency (e.g. zero-net energy buildings); and augmentation of human capabilities (e.g. healthcare monitoring and delivery).

Mobile cyber physical systems, in which the physical system in question has inherent mobility, are a prominent subcategory of cyber-physical systems. Examples of mobile physical systems include mobile robotics and electronics transported by humans or animals. Common applications of CPS typically fall under sensor-based communication-enabled autonomous systems. For example, many wireless sensor networks monitor some aspect of the environment and relay the processed information to a central node. Other types of CPS include smart grid, autonomous automotive systems, medical monitoring, process control systems, distributed robotics, and automatic pilot avionics. In industry domain, the Cyber-Physical Systems empowered by Cloud technologies lead to new approaches that pave the path to Industry 4.0.

### 4.3.2 Governance of information security for citizens

The governance aspect of information security could be one of the most important innovation to be developed in this cPPP.

Information security and cybersecurity are known as socio-technical subjects and governments are in a good position to coordinate all social aspects.
From citizen perspective, they are in a weak position to counter cyberattack. A new governance design should take more responsibility to coordinate the capability and resource to cope with security incidents. Nowadays citizens basically feel no existence of government service in terms of protecting them against cyberattacks. As we are facing an IoT and “Internet-of-Body” future, the needs of security and privacy will penetrate the life just like the need of healthcare. We need some governance mechanisms to tell the citizens, for instance, what is your security health status, what could be the risk you are facing, which aspect and to which degree can you compromise your privacy for better security and trust (or vice versa), how can you get real-time security (free or paid) service from authorized and trusted security contractors, and how citizen can act as a knot of a national / EU security sensor network, etc. We may learn some experience from the healthcare industry or the public health field.

Thus, the governance needs the “analog-to-digital” evolution as well. Managers, officials, politicians, etc., need evidence-based and statistics-based reasoning and decision making. Governance structure design needs corresponding innovations as well based on analytics to assist in achieving security goals.

New governance models (e.g., more personalized and individualized on some social aspects or a digital “social contract” concept) may be promising to better harmonize the stress nowadays between national security and citizen privacy we are not short of real needs if looking at the Apple-FBI, PRISM, etc.

Governance in terms of security needs substantial involvement of other social workers, e.g., to mind the culture and language gaps between lawyers and security workers (referring back years ago how we felt it difficult to convince lawyers that transformed / protected biometrics templates are not necessarily containing personal information).

A new governance concept design in security should consider a lot of such cross-sectorial challenges again taking healthcare sector as an example, the government is not a doctor but via it citizens enjoy a fair and good-quality healthcare service today.

Facing IoT, IoB, and machine intelligence driven future, it may have some chance information and cybersecurity become a fundamental right to citizens (like healthcare and physical security which had been coordinated by government for already hundreds/thousands years in the forms of hospital and police/army).

This innovation in governance may cause cost models change in security service delivering with the development of new interesting business solutions.

4.3.3 Vertical analysis (applications)

Each vertical sector deals with information security issues: some sectors have developed superior experiences, others have improved their approach.

In these last years, the increased digitisation has produced new conditions for cooperation between sectors, and fostered new business models. The interconnected nature of critical infrastructure systems has introduced a host of new vulnerabilities, leading to complete review of security approaches. All of these factors have influenced the shift from the information security to the cybersecurity.

4.3.3.1 Industrial Control Systems

Industrial Control Systems (ICSs) are vital for the well-functioning of industrial processes as they monitor and manage these processes. They are also vital for the well-functioning of industrial products such as automobiles, trains, planes and ships, as these assets can integrate electromechanical systems that are managed by these ICS. They are maybe less visible and glamour than cyber applications for consumers and the wide ICT market, providing only “indirect” benefits, yet they are fundamental for the efficiency and resilience of all our society.

ICSs are typically applied to control critical processes such as the production and distribution of electricity, water treatment and rail electrification. Most ICSs consist of supervisory software installed on (a network of) servers, which acquire real-time data from remote devices that control local operations. These supervisory data generally encompass indicators on product, process and environmental conditions (e.g. meter readings) and are displayed to an operator on (a) central PC(s), often called the control centre. Based on the data retrieved from network devices the control centre sends automated or operator-driven supervisory commands to network devices. These feedback and feed forward loops enable the ICS and operator to supervise the industrial process and to take action when needed.
As regard the security of ICSs, several sources (e.g. RISI, the US ICS-CERT) report a substantial increase in cyber threats in the last decade. From 2006 to 2012, the number of cyber incidents reported to the US ICS-CERT increased with 782%. This proliferation is caused by more companies reporting, but it is also caused by a substantial growth in vulnerabilities and numbers of attacks. According to the RISI, increased use of collaborative networks has made systems more susceptible to attacks. Approximately 65% of the facilities registered in the RISI database allow remote access to their ICSs and around 35% of the ICS security incidents in 2011 were initiated through remote access. In line with this, Bologna et al. (2013:4) found that in 2012 the number of vulnerabilities in SCADA systems detected between 2010 and 2012 was twenty times higher compared to the 2005-2010 period.

Industrial Control Systems, as used in Water, Food, Nuclear and Chemical operations, form a diverse ecosystem with varying components and protection goal. A shared feature of those – as well as similar system in transport, electricity and manufacturing – is that the security maturity level is largely rather low, and many deployed system have no cybersecurity whatsoever. In the past, this was argued to be acceptable, as these systems where operated as separate islands with no connection to the outside world. With the increasing use of off-the-shelf components, remote maintenance and system integration, as well as increasing realisation that air-gapping rarely works in a practical system deployment, those systems are now increasingly exposed to external attacks, and data gathered from commercial companies and national CERTS show a massively increased number of targeted attacks in this domain.

When analysing the future demand for cybersecurity in industrial production, the latest initiatives in the various European Member States and in the other countries participating in the cPPP have to be looked at. An essential technological shift is taking place or at least emerging. The future of Industrial Production is characterized by the massive and consequent use of Internet technologies in order to realize networked production environments, within enterprises but also between enterprise, in combination with considering whole life cycles of production assets in both the physical and the virtual world.

On the one hand, mainly from the computer science perspective, this technological trend is defined as the application of the Internet of Things (IoT) and the Internet of Services (IoS) to industrial production. From the perspective of the mechanical engineering disciplines, this trend is defined as the rigorous application and coupling of Cyber-Physical (production) Systems on all levels, i.e., physical (production) systems including an embedded software logic, that is capable to communicate to the “cyber world”, which is usually the Internet, or at least networking domains in which Internet technology is being used as communication protocols or data model definitions.

Whatever definition is being used, there are the same technological trends behind. As part of the FP7 research programme the European Commission already launched as part of the FP7 research programme a series of calls and projects under the terms “Factory of the Future” and “Future Internet”, now being continued in H2020. European Member States and other participating countries have started national initiatives following this trend with different names.

Since 2011, Germany has launched a joint initiative entitled “Industrie 4.0” (or in the English spelling Industry 4.0) encompassing mechanical engineering, electrical engineering and computer science industry as well as the relevant research organisations, respectively. “Industrie 4.0” means the hypothesis that these technologies will launch changes that are of revolutionary nature, finally, the 4th industrial revolution. As defined by the “Platform Industrie 4.0”, an Industry 4.0 scenario is characterized by the following three main aspects:

1. A new level of organizing and controlling the entire value chain with the lifecycle of products.
2. The availability of all relevant information in real time which is achieved by interconnecting all instances that participate in the value creation
3. The creation of dynamic, real-time optimized and self-organizing cross-company value networks by the connection between humans, objects and systems.

As these statements show, the main revolution will emerge on the level of the value chains, which means, in fact, disruptive business models.
4.3.3.2 Energy Networks and Smart Grids

One of the main challenges of energy transmission networks is communication across the network, as this is still an inhomogeneous environment. In the Netherlands public telecoms infrastructures are commonly used but not power line carrier (PLC) over high voltage (HV) lines. For example, in Germany there are about 900 different system operators and public utility companies. However, they use no common protocol for communication. Moreover, the electricity market is equipped with its own private communication network. While other areas have to use facilities of the telecommunications sector, e.g., radio (mobile networks) or landlines, for communication, signals within the electricity market can be transmitted via the high-voltage lines, i.e. by using the PLC-system.

One of the most prominent initiatives for electric utility networks today is the “smart grid”. The key characteristics of the smart grid are 1) a communication infrastructure built to manage the grid, and 2) designed to flexibly integrate decentralized grid components. Generally, users within the energy sector use all kinds of telecommunications networks, which enable data transfer to collect data from any kind of sensors, for remote control systems, or for remote administration (e.g. to control smart grids and virtual power plants)\textsuperscript{32,33}.

The current situation of cybersecurity in the energy sector can be described by the following three main points:

- **The electric grid is highly vulnerable to attacks that could have major impact.**
- **Most utilities only comply with mandatory cybersecurity standards and have not or not fully implemented voluntary recommendations.**
- **Many utilities have not taken concrete steps to reduce the vulnerability of the grid.**

Additionally, the PLC systems are often only weakly protected against attacks that try to control this kind of network. This is due to the widespread opinion that these systems are protected by the nature of carrying high-voltage electricity. Another reason for this is that their SW/HW platforms and communication protocols are outdated with limited capabilities to support common security functions.

Another main issue is the security features of smart meters (see later). These may be deemed inadequate under future cybersecurity standards, and the earliest smart meters may have been developed without taking into account the NIST Guidelines for Smart Grid Cybersecurity\textsuperscript{34}.

Along with the increase of decentralised and stochastic electrical power injections and more and more extensional trading, this makes the energy system/infrastructure more vulnerable and the risks of outages more likely in the future.

Resilience has always been the prime goal for the operators in charge of the generation, transmission and distribution infrastructures. In Europe, these operators have a long track record of success in containing accidents, avoiding black outs, and mitigating the effects of natural disasters. With the Smart Grid, cybersecurity is now at the core of their efforts to provide a resilient infrastructure. In Europe and elsewhere, the electrical grid is being transitioned into the smart grid in order to increase flexibility and accommodate large-scale energy production from renewable sources. This transition involves, among other steps, the installation of new, advanced equipment – for example, the replacement of traditional domestic electrical meters with smart meters - and remote communication with devices – for example, allowing remote access to unsupervised energy production sites. Even though the integration of information and communication technologies into the traditional grid improves its adaptivity, such a change may also make the grid vulnerable to cyber-attacks.

The issues linked to cybersecurity follow from the very nature of the Smart Grid transition. It should be assumed that all software components could be compromised either because they are exposed to the Internet, or because physical security can be bypassed. It should be assumed that all components of the Smart Grid, from smart meters, to power plants, or relays could be targets for cyber-attacks, as well as the SCADA systems used to monitor these software components. As mentioned earlier, user’s privacy should be enforced, and the mechanisms of trading marketplaces should be resilient.

\textsuperscript{32} http://de.wikipedia.org/wiki/Fernwirken
\textsuperscript{33} http://en.wikipedia.org/wiki/Smart_grid
\textsuperscript{34} http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628
The fact that any components might be compromised is commonplace on the Internet. The obvious solution is to rely on encryption whenever data is transmitted or stored. The problem then is (i) to secure encryption keys, (ii) to secure encryption and decryption and (iii) to secure the computation that takes place on decrypted data. The existing hardware protection techniques (e.g., trusted execution environments or hardware secure modules) can be used to guarantee confidentiality and integrity (as the sensitive data is protected in hardware that can provide tamper-resistance and tamper-evidence), but they cannot guarantee availability (as the secure hardware is accessed from software which is potentially compromised). Sandboxing techniques can be used to contain the computations on decrypted data. Note that these techniques address the issues linked to cybersecurity as well as privacy.

This rapid change creates security challenges, especially since traditionally these domains have not prioritized security. For one, the deployed resource-constrained devices may not have sufficient resources to run traditional security mechanisms and they interface legacy systems or use protocols never built with security in mind. Many of these devices are also placed in remote locations where the physical security of the devices cannot be ensured, thus putting doubts on the validity of the remote measurements collected, where such values may be an important part when calculating grid stability. Furthermore, the life cycle of components are long from an ICT point of view and it may be impossible to immediately shut down and patch a machine that needs to run 24/7.

Given that traditional ICT environments are faced with security challenges, it is expected that also ICT components in the smart grid are vulnerable to similar attacks (memory corruption, vulnerable protocol stacks, etc.). There are also challenging new problems originating from the intersection between the electrical engineering and ICT domains, for example where a cyber-attack (buffer overflow) in turn affects properties of the electrical grid (power quality), which in turn may propagate back to the ICT domain (control loop vulnerability). An interdisciplinary approach is required to identify challenges and potential threats as well as possible solutions. Given the lifetime of the systems, it is important to be proactive before deployment.

4.3.3.3 Transport

In the transport sector, there are significant strategic challenges in which ICT can play a vital role. Among the most important challenges, it is interesting to mention:

- minimisation of CO2 emission by promoting the use of cleaner means of transport such as electric vehicles,
- increase of road safety with particular attention on reducing significantly the number of deaths caused by road accidents,
- creation of the Single European Sky, to address the forecasted 50% increase in air traffic in the next 20 year,
- increase of the capacity, speed and safety of both passengers and goods rail transport systems,
- creation of an European cross-border integrated and sustainable transportation network,
- improvement of the cross-border electronic document interchange and logistics support systems to enhance the efficiency of the freight traffic by sea.

The maritime sector, which transports more than 70% in value of the transported goods in the world, is another critical domain for which a set of targeted attacks on industrial systems could trigger economic perturbations at a global scale.

Vehicles and other means of transport will be connected to communication networks to support infotainment, safety and emergency functionalities. Transport support systems will be more easily accessible by nomadic users – this is a truly indispensable factor in the transport sector.

This new scenario will introduce new threats and risks, and more critical dependencies with risk management, prevention, infrastructures monitoring, collaboration and crisis management, user data privacy.

What makes transport vulnerable to cyber-attacks is the increasing inter-connection and inter-dependence of information systems and networks (e.g. information technology and infrastructure merging), merger of information systems (seen in the deployment of ITS systems, E-enabled transport), increased connectivity and reliance on the Internet, embedded devices, complexity and scale of the transport industry as well as intricate public-private interactions.
Transportation systems are becoming increasingly complex, incorporating numerous, intricate control systems and sub-systems working in parallel; also, they interoperate in an environment composed by a large number of diverse service providers, across several countries. A wider use of communications and information technology will increase the efficiency and functionality of transportation systems, yet, this increase in complexity, functionality and connectivity comes at the price of an increased vulnerability.

These complex infrastructures will be highly distributed and thus difficult to protect; besides, it is also important to consider that every country has its own networks and every transport operator has its own strategy regarding the protection of its infrastructure.

Some common security and resilience general challenges across the different types of transport are:

- **assess and manage risks:**
  - compliance with the requested level of security, safety, dependability and privacy, taking into account the whole perimeter of the infrastructure (including physical assets, the cyber layer, processes and services)
  - increasing threat and risk factors, including cyber, physical, process and human risks

- **prevent attacks:**
  - achieve a comprehensive and continuous situational awareness, supported by an information intelligence capability
  - support the information sharing and the effective and automatic use of exchanged data
  - tampering of field devices, roadside and infrastructure equipment
  - security (including confidentiality and availability) of the communication channels used by infrastructures, vehicles and other transport means; equipment’s mutual authentication and trust

- **monitoring and protection:**
  - Integrated monitoring, including all infrastructures layers (physical, field, network, systems and applications)

- **unauthorized data access, modification or destruction:**
  - unauthorized use of services or denial of service (DoS)

- **manage incidents:**
  - Incident real-time detection
  - automated systems self-configuration

- **privacy of users data:**
  - privacy in open and big data, distributed networked objects, passengers and vehicles geo-localisation information and mobility patterns

- **secure and precise positioning of transport means and goods:**
  - dependable and attack resilient positioning systems

The attention paid to cybersecurity across the transport sector varies widely, as might be expected with the diverse industries and technologies included in the sector. This is a consequence of several factors, including:

- The **dependency of each industry segment on cyber-technologies** (and consequently the range of cyber-assets and vulnerabilities involved)

- The **criticality of cyber-technologies to safe and efficient operation** (or, conversely, the effectiveness of manual supervision and fall-back in preventing loss)

- The **degree of centralisation** (which affects the impact of threats to individual assets)

- The **degree to which development and operation of transport systems are regulated** (for reasons other than security)
The historical impact of attacks and accidents in the sector, which have a strong influence on regulatory and public expectations (this can also vary by national interest as well as by industry segment)

These factors introduce different approaches to cybersecurity and different tolerance of various types of risk. For example:

- In civil aviation, a relatively limited number of high value assets (aircraft and airports) have been the subject of a wide variety of threats in the past, and their failure is highly visible. Regulation is also strongly enforced for safety reasons. Key elements of the system, such as air navigation service providers are inevitably centralised.

- In rail, the transport system again depends on a relatively limited number of technically sophisticated controlling assets (signalling systems) and the transport vehicles are large and relatively few. Regulation is again strong.

- In automotive transport (including passenger cars and road freight), a different model has traditionally applied. Central control is limited (although crucial to effective operation in areas of high traffic density) and individual vehicles are modest in value and are under the primary supervision of a (more-or-less) skilled operator. The regulatory regime takes these differences into account.

- In maritime transport, there are a very large number of ships that transport cargoes of high value. The ships are spread all over the world, taking a limited number of maritime routes where the ships traffic can be very dense. Central control is limited. The interfaces between the sea and the terrestrial transport are the ports, where industrial control systems are also of critical importance.

The case of automotive transport is particularly interesting for the direction in which technological change is moving – the increasing introduction of Advanced Driver Assistance Systems (ADAS) and even elements of autonomous control place increasing importance of the cyber-technologies used to realise them. Current proposals however, still do not envisage the level of central control present in other sectors.

The cost of stringent security controls is high, even by the standards industry segments that operate sophisticated centralised assets (e.g. aviation, rail and maritime). This leads to a distinction between critical operational systems (flight control systems, railway-signalling systems, air traffic management networks, ship navigation systems) and informational or supervisory systems (information & even entertainment systems). The former may be managed by industry-specific standards (e.g. EUROCAE’s ED-202 - Airworthiness Security Process Specification in aviation) while the latter are more likely to be managed via conventional commercial ICT security techniques. The evolution of technology is challenging the assumptions on which this division depends, however:

- Critical and non-critical functions are increasingly dependent on shared infrastructure and facilities (telecommunications networks, satcom links, vehicle networks) and

- The increasing complexity of operations has a tendency to make functions which were once only informational or advisory into a critical part of a system’s operation (compare the manner in which anti-lock brakes on cars become crucial when traffic densities rise and the vast majority of drivers come to rely on their function).

Further variation in the degree to which security control can be applied is introduced by the fundamental distinction between fixed infrastructure and moving assets. Mechanisms that can be applied to secure communications between highway control centres, air traffic control centres or railway operations centres may not be applicable to the wireless links with vehicles. The permissible security controls are also limited by the need for (international) interoperability (cybersecurity cannot be allowed to stop cars or trains crossing borders) and the limited control that a system operator (a railway company or highways agency) may be able to exert over transport operators that use the network (individual vehicle owners & drivers). The ownership of the assets that need to be controlled and the responsibility for the risk that may be presented are not the same.

A number of common issues for cybersecurity in transport nevertheless emerge from these diverse segments:

- Increasing connectivity, and increasing complexity, make cyber-technical elements increasingly essential for transport

- Increasing use of common technological elements (networks, software stacks, or processing elements) will make the established approach of partitioning high value information assets from lower value networks increasingly difficult to maintain
The cybersecurity risks of systems including shared infrastructure (physical or logical networks) with mobile users who must be allowed interoperable access to the infrastructure are significant. The relationship between ownership of equipment and responsibility for a risk is not clear in such cases.

The potential for system access resulting from the interoperability of transport systems exposes assets to infiltration and subsequent manipulation of sensitive operations. Assets include static field devices, dynamic transport management systems, connected vehicles and freight transport management systems.

There are two general methods an attacker can use:

- **Altering data storage** and prevent access to servers: sabotage of the system through physical alteration or destruction of system components, jamming or denial of service type of attack, infection of servers with malwares in order to make the data unusable;

- **Altering exchange of information:**
  - falsification of messages (e.g. key extraction or physically removing a vehicle’s credentials and using these credentials to create and distribute seemingly legitimate messages to neighbouring vehicles), selective dissimulation of messages, selective delay of messages, infection of the system with malware, framing attacks (e.g. an attacker makes a vehicle’s on-board equipment appear to be malfunctioning by generating false messages to contradict the target vehicle’s legitimate messages);
  - software manipulation (e.g. installing malicious software on the vehicle’s on-board unit to create messages containing arbitrary or altered information);
  - sensor manipulation (e.g. interfering with the vehicle’s sensor output to alter, inject, or suppress messages that originate from internal vehicle systems or interfering with the sensor input that directly reports vehicle behaviour or external circumstances);
  - denial of services (these attacks result in valid messages being suppressed or not received)
  - message linking (e.g. an attacker sniffs vehicle to vehicle, attempting to use information found within messages to identify a particular vehicle or a driver’s whereabouts.

The main measures that are in place are the following, although they are not applied uniformly in the transport sector and their quality greatly varies.

### 4.3.3.4 Financial Services

The term “Financial Services” can refer to a broad spectrum of organisations and services operating in different areas such as banking and insurance, and each of these could warrant its own detailed section. Focus here is on the retail banking services and related infrastructures, with some overlaps in other areas of financial services. The European financial services market can be described as having a ‘bank-based’ model, where the majority of enterprises are financed by banks, as opposed to capital markets, for example. Indicative of this is the fact that the share of banks in credit intermediation in Europe represents around 70%-75% of debt financing to households and enterprises. In the US, this number is around 20%-30%. The European financial services sector, specifically the banking sector, is the largest in the world.

The specific trends within the financial services shaping the landscape for the future of the industry include Single Euro Payments AREA (SEPA) Regulation No 260/2012 which will make all electronic payments across the euro area as easy as domestic payments within one country, new entrants to the market which are retail merchants and telecom providers leveraging on customer trust and enable weak barriers of entry, digital and mobile banking that will have to adopt mobility solutions, mobile payments, influence from online retail sector, adoption of cloud computing and the bring your own device culture (BYOD).

Common types of threats within the financial services sector include threats to online banking, threat to payment processors, threat to financial markets and securities. The main tools and techniques used by threat actors to create cyber disruption include installed malware, social engineering, targeted attacks, Advanced Persistent Threat, Denial of Service Attack and Distributed-denial-of-service Attack.

Some of the research opportunities in the financial services sector could include evaluation of existing cybersecurity solutions in order to help mitigate the impact of cyber threat, developing standards for threat and incident
information sharing practices, European cybersecurity incident management practices, and identifying and promoting awareness of the emerging threats.

Security of financial services operations relies on both robust technical and non-technical controls. The non-technical controls range from effective governance, employee and user training and awareness, disaster recovery and business continuity planning and deployment of Security Operations Centres (SOCs). Furthermore, appropriate technical measures are implemented. **Network security in financial services refers to the provisions and policies adopted by a financial institute to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.** Most commonly and widely adopted practices within the financial services include: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), design and implementation of Secure Applications, Strong authentication for online transactions (e.g. chipTAN authentication), inbound email sandboxing (used to combat phishing by deploying a solution that checks the safety of an email link when a user clicks on it and go some way to mitigating the risk of phishing) and real-time analysis and inspection of web traffic.

4.3.3.5 Public Administration: Vital Services / eGovernment

Public services are at the core of modern societies, and their availability and trustworthiness is a key enabler for economic growth and social innovation. Innovation in Public Administration is influenced by different drivers, such as the necessity to cut costs and to “do more with less”, the rising expectations of citizens with respect to participation and openness of public processes and data, the pervasive availability of mobile devices which represent an ubiquitous entry point to services, the mass usage of social media, and the obsolescence of old legacy systems versus the growing trend toward cloud-based ICT infrastructures for Governments.

4.3.3.5.1 Public Administration - Vital Services

ICT security is essential to preserve the continuity public administration services, but most attacks to services cannot be considered critical despite their severity if we take into account the classic definition of “critical infrastructure”. Indeed, only specific services such as emergency response (including medical, police, fire, and rescue), those that ensure the continuity of government (national defence and military operations), and those that support a small fraction of public administration (diplomacy, the armed forces, decision-making) are considered as “critical”. This consideration of public administration services as a “critical infrastructure” is not so clear in the European Programme for Critical Infrastructure Protection (EPCIP), which set the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity.

Actually, this concept is not specified at all in the cybersecurity market studies (mainly of American origin). We would put here more emphasis to this issue, as Europe has a fragmented political structure, with fragmented national sovereign markets, each one of them is using “trusted” suppliers to respond to cyber threats to national critical infrastructures. Following the definition used in Estonia, this is actually the first form of “cyberdefence”: i.e. the defence of national security from cyber-attacks.

It is a non negligible market and each main EU Member State has a considerable competence in the domain, but due to the sensitiveness of the issue, there are problem for exporting such solutions in other countries. Yet, this is allowing the development of competence (e.g. encryption, intelligence, data security, identification, network security, managed security services, etc.) useful for those “defence contractors” to develop technologies and offer that can be used in less sensitive civilian cybersecurity markets which are more deeply explored in this study.

It is therefore essential consider this element of the public administration cybersecurity market which constitute the basis for many of the most important technology solution providers in Europe also for the civilian market, a fundamental concept to be considered in the European cybersecurity market dynamics.

4.3.3.5.2 Public Administration: eGovernment

Governments must engage with the wider public and follow the open government principles in order to “make the services more user-friendly and effective, improve the quality of decision-making, promote greater trust in public institutions and thus enhance public value”, but at the same time they have to cope with strong economic
constraints, which require the conception of new sustainability strategies and the reuse of best practices and solutions across all governmental levels.

The key role played by ICTs in such transformation is both a fundamental enabler and a source of issues. Indeed, for example, digitalisation of public services and mobile government (mGovernment can be seen as the extension of eGovernment to mobile platforms) on the one hand help improving efficiency of the back-office and provide users with better and ubiquitous services, and on the other hand increase the attack surface and causes new security issues and privacy concerns, including distributed denial of service, identity thefts and information leakage.

Within public administration services, “e-Government”, as defined by the European Commission, is about “using the tools and systems made possible by Information and Communication Technologies (ICT) to provide better public services to citizens and businesses”. While e-Government is often thought of as "online government" or "Internet-based government," many non-internet "electronic government" technologies (instant messaging, telephone, tracking systems, smart cards and so on) can be used in this context.

The outcome of e-Government is to transform the entire relationship between the public sector and users of public sector through a creative utilisation of electronic delivery systems, in a way that strengthens a nation and increases the economy immeasurably in a more transparent, cost effective and premeditated way.

The primary delivery models of e-Government can be divided into:

- **Government-to-Citizen (G2C)**, this is the communication link between a government (mainly the public administration) and private individuals or residents to offer a variety of ICT services to citizens in an efficient and economical manner, and to strengthen the relationship between government and citizens using technology.

- **Government-to-Business (G2B)** is the online non-commercial interaction between local and central government and the commercial business sector. The Main Goal of Government to Business- is to increase productivity by giving business more access to information in a more organize manner while lowering the cost of doing business as well as the ability to cut “red tape”, save time, reduce operational cost and to create a more transparent business environment when dealing with government.

- **Government-to-Government (G2G)** is the online non-commercial interaction between different Government organisations, units, departments, and authorities at national, regional and local level among each other, as well as with foreign governments. The use of ICT can connect all parties and support processes and activities. Other objectives are to make government administration more transparent, speedy and accountable, while addressing the society's needs and expectations through efficient public services and effective interaction between the people, businesses and government.

- **Government-to-Employees (G2E)** is the online interactions through instantaneous communication tools between government units and their employees. Documents can be stored and shared with other colleagues online. G2E services also include software for maintaining personal information and records of employees.

Attacks to e-Government services are driven by different motivations that include self-benefit, political objectives or even personal recognition. They are carried out by a wide variety of actors or attackers, including cyber criminals, hacktivists, cyber terrorists, state-sponsored spies or disgruntled employees. Attacks to e-Government services can be classified by their operational impact, their nature, and their informational impact. The attack called denial of service, in particular its distributed version, is considered the major attack executed in this sector.

Future governmental cloud infrastructures are a very appealing target for malicious hacktivists, since they represent a “single point of failure”, and a successful attack can potentially give access to a high number of agencies. However, since the security countermeasures deployed in data centres are quite high, external attacks that aim at stealing sensitive data or at mounting Distributed Denial of Service are not very likely to be successful. Indeed the security level of future cloud infrastructures is likely to be much higher than the one implemented by each single Public Entity, since they will be operated by personnel highly skilled on cybersecurity, which is not the case in the vast majority of Public Administrations.

Citizens will have the means to access and manage (including grant access to any third party), from a single point, their data and to adapt public services to their specific needs and to their specific context. Moreover, since data will be managed in a unique place, it will be possible to solve problems of redundancy and scattering of information across Public Administrations, thus improving accountability of the services.
Some of the research challenges that apply in e-Government application area include **creating trust and confidence in privacy measures** by creating mutual transparency between public administration and citizens, **security (secure authentication)** and **possible adoption of common standards**.

### 4.3.3.6 Healthcare / eHealth

According to the EU, eHealth refers to tools and services using information and communication technologies (ICTs) that can improve prevention, diagnosis, treatment, monitoring and management. This includes information and data sharing between patients and health service providers, hospitals, health professionals and health information networks; electronic health records; telemedicine services; portable patient-monitoring devices, operating room scheduling software, robotized surgery and blue-sky research on the virtual physiological human. eHealth can benefit the entire community by improving access to care and quality of care and by making the health sector more efficient.

ICT has been exploited in the health care sector for several decades. However, what we now witness is the transition from the traditional model of a stand-alone Health Information Systems (HIS), that is the HIS operating within the boundaries of a single Healthcare Organisation (HO), to the **networked HIS, that is a HO’s HIS interconnected to HISs of other HOs or even of third parties, over national or international Wide Area Networks (WANs)**. Moreover, web-based and mobile e-health services are already been regularly provided and the healthcare sector has started exploiting the cloud computing paradigm. Additionally, mobile devices like laptops, PDAs and even mobile phones are being increasingly used by the healthcare sector to access, store or transmit health information within the framework of providing health services. The trend towards **seamless system and data interconnection, mobile services, smart devices and data analytics** has already started and will lead to revolutionary changes in the delivery of health care.

IT will play a relevant role enabling eHealth for citizens’ empowerment and eHealth for integrated care. Specifically, to address these two aspects which are strictly related each other, it will be necessary to move toward a complete and deep digitalisation of all the healthcare levels which is a precondition to put the citizens / patients in the position to exploit and use all the information – shared also with the healthcare and social institutions – necessary to enable the self-management of cares and preventions. All this will be possible thanks to infrastructures enabling the hosting and sharing to work on eHealth solutions enabling the realisation of a fully integrated healthcare system involving Electronic Medical / Social Record (EMR), Personal Health Record (PHR) and the Electronic Health Records (EHR) able to share the data in a coherent, compliant and reliable way.

Also, Medical devices and implants, such as pacemakers, are also becoming more connected. They suffer from not being built for security, and can real personal data about their carrier, or be targeted to malfunction with a deadly outcome.

The security of health information and the privacy of the patients is a subject well researched. A wealth of literature has been produced in the past decades. Issues that have been well investigated pertain to:

- the **perception**, the attitude and the concerns of healthcare services consumers towards the privacy of health information subjects;
- the perspective of healthcare providers of the need for compliance to existing legal and regulatory requirements regarding the **security and privacy of health information**;
- technical and organisational methods for **controlling access to health information**;
- the relationship between and the effects of **data interoperability** on health information security and privacy;
- health information security and privacy on **web-enabled healthcare provision**;
- health information security and privacy in **m-health**;
- health information security and privacy in the **cloud computing paradigm**;
- retaining health information security and protecting patient privacy when health information is disclosed to authorized parties and for research purposes;
- adverse effects of **health information integrity loss** and means for preventing it;
- financial risk and **fraud as related to health information security**;
- implications of privacy and security on healthcare practice;
- health information security risk management.

These extensive research results have been complemented by a spectrum of pertinent standards by different standardisation organisations. Still, despite the available technology, knowledge and guidance, information security remains an issue in the healthcare sector. This is likely due to the fact that, whilst everyone recognizes the need for securing health information, what is often neglected is the fact that security is more than erecting physical and electronic barriers.

Other than its attractiveness to a multitude of diverse actors, there is nothing extraordinary with personal health information that exposes it to threats different in nature than those against other types of information. What is different is the level of vulnerabilities that threats may exploit: these are usually much higher in healthcare provision environments than in other types of environments, for a variety of reasons. Similarly, the impact of a security breach of health information is frequently very high.

What is also unique to healthcare is the array of factors to be considered when assessing threats and vulnerabilities to determine the risk level. Hence, considering also the extent of research already performed in the field, new research challenges in the field primarily emerge as a result of the evolution of the healthcare system in Europe.

The healthcare system is evolving during the last years to address the new challenges deriving from the new social and economic conditions that Europe is experiencing, namely citizen aging, more and more increase of chronic diseases, overlap between health and social problems, new family models and the request for a drastic rationalisation of the healthcare costs. In this process of evolution, ICT is called upon to enable more citizen involvement in producing, using and managing health information on one hand and to provide fully integrated care on the other. At the same time, new computing paradigms and technological developments find their way into the healthcare sector. This implies that health information risks must be re-examined, from a different perspective. For example, the combination of interconnected Cyber-Physical Systems with manifold potential vulnerabilities and complex data analytics services requires revisiting our existing security and privacy policies, measures and practices, because of new threats that health information may be exposed to. A deeper understanding of factors influencing the willingness of healthcare consumers to share and disclose personal information is necessary if generalised adoption of eHealth is sought. To answer the quest for more financially efficient healthcare provision in Europe, economic aspects of health information security need to be researched in detail. The conditions under which new technological developments may be securely, effectively and safely applied in the healthcare sector need to be thoroughly investigated. Issues related to securely federating systems and services of different environments, different control domains, governed by different laws and regulations and differently managed so as to enable secure world-wide eHealth services delivery and privacy-preserving information sharing over a variety of technological platforms need to be addressed and resolved. Last but not by any means least, a significant field of research is the preservation of security and privacy levels when interconnecting systems of varying degrees of technological maturity, considering the vast amount of legacy systems that exist and operate (and will continue for quite some time to do so) in the healthcare sector.

4.3.3.7 Smart & Secure Cities\textsuperscript{35}

The term “Smart City” provides an umbrella that integrates various types of infrastructure, including traffic management, smart factories with industrial control systems (ICS), power plants, public transportation (covered by own sections) and smart buildings.

The smart city ecosystem\textsuperscript{36} is actually a broad partnership between the public and private sector. City planners and developers, non-governmental organisations, IT system integrators, software vendors, energy and utility providers, the automotive industry, and facility control providers, as well as technology providers for mobile technology, cloud computing, networking, Machine-to-Machine (M2M) and Radio-Frequency Identification (RFID), all have a role to play.

\textsuperscript{35} Source: Strategic Research Agenda. WG3 Network and Information Security (NIS) Platform - Draft v02.80
The smart city experience involves systems and objects interconnected through various technologies, like local, wide and wireless networks. The “Internet of Things” (IoT) concepts apply here in terms of multitude of devices interacting with control units and dashboards, through sensors, RFID, M2M, satellite and GPS.

The amount of data generated by these systems can reach a considerable size. Big Data will need to be appropriately and centrally stored, managed, analysed, and protected. The city operation’s centre will supervise the interaction between systems and will have to ensure continuity, integrity and resilience. With time, the interconnected and interdependent services of smart cities will evolve under a centralised governance dashboard of specialised stakeholders, responsible for setting policies and processes, managing ICT assets, services and protocols, and ultimately administering the services for constituents. ICT control and management capabilities will be crucial, to guarantee an efficient, secure and resilient governance and delivery.

The systems, disciplines and technologies involved, can include the following sectors, some of them already previously mentioned:

- Smart grids and energy efficiency
- Intelligent transportation
- Connected healthcare
- Public safety and security (including law enforcement)
- Wireless communications and hotspots
- Smart buildings

City governance should therefore ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy. In this scenario of overlapping functions, the process and information exchange in the city need to be interconnected and contextualised in a common middleware. The systems need to be standardised, interoperable and open but also secure; in order to take third-party information into consideration and ensure an overall seamless service delivery. Like any other ICT system, the smart city technological and communication environment – the network infrastructure and the Internet of Things – will present vulnerabilities to cyber-attacks. The higher complexity and heterogeneity of these environments could in fact determine an even higher exposure, and need for more sophisticated protection strategies.

City governance will need to identify the most critical areas to protect, the types of threat they could be subject to, categories of attackers and likely motivations (financial, criminal or political). City IT ecosystems will increasingly be built on public sector cloud or infrastructure virtualisation, with social and mobile computing as the primary access for applications and services.

Information management and protection systems and backup and recovery systems for mission-critical administration data should protect citizens’ privacy and identities across domains, including local tax, healthcare, education and utilities.

By definition, vulnerabilities increase when systems become connected and integrated. In particular, this occurs when an unprecedented amount of additional data (Big Data) is generated by various smart devices (like sensors, meters and cameras) and processed by connected systems. The network infrastructure, be it broadband, Wi-Fi or satellite, that connects systems and their operators, adds entry points and opportunities for security breaches or human error. For these reasons, it is important that smart city designers and planners develop solutions with robust, embedded cybersecurity and mitigation strategies in case of attack or loss of data.

4.4 Needs for action

4.4.1 Factors motivating the need for European action

- Governance / sovereignty

Security (specifically cybersecurity) remains primarily a national competence/responsibility. This has consequences for the fragmentation of cybersecurity strategies, regulatory systems and public/societal attitudes, which are primarily determined at a national level. However, the interconnectedness of digital markets and technologies
requires a coordinated and multinational approach. Notwithstanding subsidiarity/sovereignty, an EU approach provides the basis for greater convergence (or, at least, restriction of future further divergence) across national markets, through facilitation of the identification of common needs and implementation of common strategic responses.

- **Awareness / Investment**

There is a general lack of awareness of scale, scope, nature of security vulnerabilities and threats. As a consequence, there is an under investment / weak investment culture in cybersecurity (public sector, private sector, citizens). This calls for public intervention to increase awareness, thereby empowering citizens, businesses and public administrations to ‘actively’ engage in their cybersecurity and privacy and raise investment in cybersecurity. Again, the interconnectedness of digital markets and technologies requires a coordinated and multinational approach, which calls for EU-level action.

- **Innovation, entrepreneurial behaviour and financial culture**

Europe suffers, in general, from weaknesses in innovation behaviour and the commercial exploitation of R&D, which (arguably) are magnified by a weak entrepreneurial culture and poor financial support to bring innovative products and services to market. These are not specific to cybersecurity. Nonetheless, public intervention may be required to address systemic weaknesses in systems for innovation and entrepreneurship.

In the cybersecurity domain, Europe suffers from underinvestment (relative to international competitors) and fragmentation of research and innovation activities (i.e. limited/uncoordinated national level approaches). There is a need for a more ‘holistic/structured’ approach for EU-level support for research and innovation, which could improve coordination of R&I efforts and promote synergies between different initiatives, while reducing the risk of unnecessary duplication of R&I efforts.

- **Economic opportunities (growth and jobs)**

The market potential of cybersecurity – in terms of future growth and jobs prospects – is substantial, both with respect to the provision of cybersecurity products, services and solutions (supply-side) and through their utilisation (demand-side). Moreover, there are significant synergies to be achieved between cybersecurity and other EU priority areas for growth and jobs creation; especially Digital Agenda / DSM / Industry 4.0, but potential interlinkages go much wider than these.

- **Societal and political needs**

To illustrate the societal and political needs for action, we would consider the resolution largely adopted by the European Parliament on March 12th, 2014, following the report led by MEP C.Moraes “Inquiry on electronic mass surveillance of European citizens”. The report is stigmatizing the undue surveillance of European citizens, in particular linked to the PRISM affair and calls for a number of actions (including an increased digital autonomy of Europe for securing sensitive applications and the need for a revision of the Safe Harbour). More recently (October 2015) the E. Parliament issued a “Follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of European citizens” reiterating the request (topic 47 and 48) for a “legislative change in the field of procurement to enhance the IT security of the EU institutions; calls for the systematic replacement of proprietary software by auditable and verifiable open-source software in all the EU institutions, for the introduction of a mandatory ‘open-source’ selection criterion in all future ICT procurement procedures, and for efficient availability of encryption tools;” … “the development, within the framework of new initiatives such as the Digital Single Market, of a European strategy for greater IT independence and online privacy that will boost the IT industry in the EU”.

- **Digital autonomy**

Broadly speaking, ICT developments (product and service innovations) are being driven by non-EU suppliers. Europe is increasingly reliant on ‘foreign’ developed ICT products and services, the security of which is determined outside the EU and does not necessarily reflect EU requirements (level of security, specific requirements, or fundamental attitudes). Equally, European supply chain(s) increasingly reliant on ‘foreign’ developed ICT and cybersecurity technologies, opening up potential vulnerabilities to components that do not meet requirements of trustworthiness,

---


security and guaranteed protection of personal data. In this context, action is warranted to ensure European technological independence (digital autonomy), particularly in sensitive areas.

- **Structural aspects of the European cybersecurity industry**

  The European cybersecurity industry suffers a number of structural weaknesses, e.g.:
  
  o Prevalence of SMEs, lack of critical mass, gaps in supply/value chain, missing/low visibility of ecosystems, asymmetries between supply and demand (e.g. between SMEs with innovative/disruptive technologies and large-sized customers);
  
  o Shortages/deficiencies in skills and training, “brain drain”;
  
  o Low /limited investments in research and capacity building (esp. compared to US);
  
  o Absence of industrial strategy for cybersecurity

  These conditions call for public intervention to address these weaknesses, notably to strengthen the overall supply/value chain of the cybersecurity industry. Given the fragmentation of the sector, there is a need to strengthen supply/value chains that are – in so far as it is possible to ascertain – dispersed across Europe so as to integrate players from outside the main/leading economies. This calls for a European approach to simultaneously create opportunities for consolidation (economies of scale) and specialisation.

- **Market Functioning**

  There is need to develop a truly European cybersecurity market, based on principles of fair competition and providing a level playing field – e.g. equal access to products and services, independently of the provider – for all. This implies addressing market regulation, and aspects such as standardisation, certification, labelling requirements and technical concerns (e.g. interoperability). Such developments support the structuring of the market and, in turn, support investment in technology/product development by reducing uncertainty (e.g. by increasing predictability/transparency etc.) and raising customer confidence etc. A European-level approach reduces the risk of regulatory/standardisation fragmentation.

  Further, EU action should reduce the risk of *de facto* market-adoptions of non-European regulatory/standardisation approaches and raise European influence on setting of global market standards etc. By contrast, a weak EU position in the global cybersecurity sector/market is likely to diminish European influence on the development of regulatory approaches and accompanying norms and standards, both technical and operational (e.g. in terms of security, privacy and trust).

4.4.2 Challenges and objectives

Europe is developing its common cybersecurity approach on the principles laid down by the European Cybersecurity Strategy, also tackling the protection from cyber threats of growth of the European Digital Single Market (DSM). Yet Europe should still better advance in implementing strong measures to protect its Network Information Systems and avoid undesired leakage of sensitive data.

Envisaged investments on research and capacity building are still extremely limited when compared to the US. This will further widen the already critical divide that exists in ICT and ICT security.

To build a Smart & Secure Digital Europe, we have to better understand what is at stake and reconsider our future investments, focusing them towards priorities that would have a real and positive impact on Europe, for the creation of jobs and growth and the protection of our cyber space, data and values. To address these issues, we need to act immediately and the ECS cPPP will give us the opportunity to tackle main challenges:

- Clear need for systemic innovation on challenges that pose significant risks to the economic and social texture of European societies and /or to strategic new opportunities;
- Clear need for partnering: the challenge cannot be solved by any single means, organisation, sector, or domain knowledge;
- Clear need for European level action: where local, regional or national action alone is not sufficient;
- Clear prospects for European competitive advantage.
Answering to these challenges will allow to satisfy the following major objectives:

- Foster and protect from cyber threats the growth of the European Digital Single Market considering its cultural and economic ecosystem, ensuring a level playing field (access to products and services having adequate security, independently of the provider).
- Develop the European cybersecurity market and the growth of a strong, competitive European cybersecurity and ICT industry, with an increased market position.
- Develop and implement European cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.

This will allow maintaining a strategic presence in key steps of its supply chain, increasing European digital autonomy for sensitive applications for greater security, improved privacy and trusted data management.

No individual industry sector or European country has the required multi-disciplinary capability to act at such level and scale of excellence in cybersecurity.

4.5 Overall long term vision of the PPP

The ECS cPPP has its roots in the Industrial Leadership and the Secure Societies priorities of Horizon 2020. The convergence of Security with the ICT Industrial and Technological Leadership challenges has contributed to the definition of the main strategic objectives for an industry led European Cybersecurity cPPP:

- The protection from cyber threats of the growth of the European Digital Single Market
- The creation of a strong European-based offering and an equal level playing field to meet the needs of the emerging digital market with trustworthy and privacy aware solutions
- The growth and the presence of European cybersecurity industry in the global market

This approach will induce a paradigm change also at societal level – empowering each human being to become an active actor in the protection of cybersecurity, across his / her personal and professional lives.

Europe should move from its current approach of handling cyber-threats in a reactive mode – deploying too few resources, too late, focusing on damage control and reporting - towards a pro-active, pre-emptive management of risks.

This vision requires providing the knowledge, interest, services and controls to understand and manage what is at stake; providing each organisation, from the private and public sectors, the support to decide how, where and why to invest, with a focus highly based upon “Return on Investment” (yet not forgetting breakthrough developments), driven by a prioritised approach to protection.

The proposed approach would not only achieve the mentioned objectives by supporting the growth of the cybersecurity industry but also stimulating and coordinating (where possible) the “demand” for cybersecurity solutions. For example, by requiring, or subsidising higher levels of security for major elements of European infrastructure, and, in doing so, creating a larger European market for cybersecurity products and services. This larger market would also provide the impetus for a stronger European cybersecurity industry.

The cPPP expected direct or indirect impacts include:

**Market and Competitiveness**

- Support European cybersecurity global market share (at least 25%), with yearly growth up to 8%.
- Improve rating of European companies and solutions in the global market offer.
- Focussed use of resources into a commonly defined strategy for cyber / ICT security R&I and industrial policy actions.
- Increased standardisation, certification and establishment of a trust European label.
- Increased participation of users (targeting 15%) in H2020 projects to better drive R&I.
• Identification and development of strategic components / solutions to be mastered at European level to increase European digital autonomy for sensitive applications, also linked to validation of trusted supply chains, including non-European components.

• Implementation of large scale projects and pilots in European strategic sectors to validate and disseminate innovative European trusted solutions.

• Stronger participation of SMEs (targeting 20-25%) in H2020 projects and support to their development via accelerators, investment initiatives, knowledge of their offer, market outreach.

• Link between R&I and other European and national investment funds targeting common strategic objectives. Stimulation and grow of European cybersecurity capital ventures or other financing instruments to support innovation and SMEs.

• Improved knowledge of R&I project results and take up, in particular for SMEs and disruptive technologies.

• High visibility at national, European and International level of European cybersecurity policies, strategies and activities.

Socio – Economical

• Increase of employment (target: 10% annual growth) in the cyber / ICT security sector, thanks to growth of the European cybersecurity market share and to education via academies, professional training courses, certification.

• Improvement of awareness and capability to threat reaction thanks to extended exercises and training modules

• Development at Member State level of increased awareness on cybersecurity threats and solutions thanks to the participation into the cPPP activities and the creation of dedicated national associations or PPPs.

• Users better informed through a European cybersecurity centralised cyber threat intelligence facility and the development of Information Security and Analysis Centers for specific sectors.

• Information exchange of mutual horizontal threat and incident at a European level.

• Increased use of Security and Privacy by design Enhancing Technologies.

• Increased understanding of risks and adapted solution / procedures, using agreed Risk Management methodologies, coupled with insurance approaches.

• Support to the implementation of European directives (NIS) and regulations (e.g. eIDAS, PSD2 etc.) to better protect and stimulate the market.

4.6 Strategic and Specific Objectives of the PPP

Main strategic objectives for development of the European cybersecurity sector

• To protect growth of the European Digital Single Market from cyber threats.

• To create a [truly] European cybersecurity market, based on principles of fair competition and providing a level playing field – e.g. equal access to products and services, independently of the provider – for all.

• To create a strong, resilient and competitive European cybersecurity industry that is:
  o built on trusted supply chains able to provide European digital autonomy in sensitive areas;
  o capable to deliver cybersecurity solutions that meet the needs of the emerging digital market while simultaneously respecting European requirements and values (e.g. security, privacy and trustworthiness);
• capable to deliver cybersecurity solutions that support the development and use of innovative solutions for major economic and societal challenges, particularly in areas where Europe is – or has the ambition to be – a world leader.

• To establish the position of European security industry as a major presence in global (non-EU) security markets.

In the following we remind the list of objectives of the cPPP as listed in the contract with the European Commission.

STRATEGIC OBJECTIVES

The scope of the European Cybersecurity cPPP is:

• To foster cybersecurity market development, job and wealth creation in Europe through a long term investment commitment by cybersecurity industry, research and technology organisations (RTOs), academia, the European Commission, Member States' public administrations participating in the partnership as well as cybersecurity solution users;

• To support the use of innovative trusted solutions and services for major societal and economic challenges in Europe, e.g. in different essential services providers, particularly in areas where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);

• To accelerate Europe’s innovation process and time to market by addressing the full innovation and value chain of cybersecurity in different application sectors;

• To foster the development of European cybersecurity industry by creating a Europe-wide technology and application base, building up competence and competitive European cybersecurity companies, including SMEs, facilitating the acceleration of business ecosystems and appropriate business models with a particular focus on SMEs, start-ups and high growth companies;

• To mobilise and leverage public and private resources to provide contributions to the development and implementation of European cybersecurity policies, regulations and standards (e.g. contributions to European policies; support to implementing legislation like NIS Directive, eIDAS regulation; contributing to creation and updating of ETSI/CEN/CENELEC standards);

• To increase the awareness and demonstrate the value of cybersecurity solutions for businesses (including decision makers) and the public sector to accelerate the take-up, but also to improve the cybersecurity awareness among citizens and skills development of experts.

SPECIFIC OBJECTIVES of the cPPP:

In the frame of the ECS cPPP, the stakeholders will cooperate, on the basis of the Industry Proposal, to develop, implement and support a multi-annual research and innovation agenda. The Industry Proposal, including objectives and Key Performance Indicators (KPIs), have been developed in cooperation with the different stakeholders.

The Industry Proposal would provide evidence for consistency of the activities of the contractual agreement with existing European policies and initiatives. The Industry Proposal will also look how to avoid duplication with other R&D initiatives at European or national level. It will actually seek ways to find synergies between different initiatives.

The specific objectives of the Industry Proposal are as in the following. They are linked to the KPIs (see § 6.4) and are more or less impacted and supported by the cPPP.

OBJECTIVES FOR IMPROVED COMPETITIVENESS

• Support the evolution of cybersecurity revenues in the European and global market, including positioning and market share of the European industry: aiming at maintaining the European cybersecurity market share at least at 25% of the global market and attaining a yearly growth of the European market at least of 8% by 2020;
• Develop solutions leading towards the use of cybersecurity technologies in the fields of different vital infrastructure and service providers, in particular where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);

• Support activities for increased industrial competitiveness of Europe through the development and implementation of cybersecurity industrial measures (e.g. standardisation, use of testing, validation, certification infrastructures as well as trust labelling procedures, best practices and pilots for innovative elements of the supply chain, link to regulations). The development of certification activities in cybersecurity will consider Regulation 765/2008 and Decision 768/2008 and certification provisions included in the General Data Protection Regulation 2016/679;

• Stimulate existing and new alliances and the ecosystems along and across the value chain that reinforce competitive capabilities of European cybersecurity industry in existing market segments or help address new market segments;

• Support the development and link of clusters as a mechanism at local level and beyond (Regional / National) to develop the market and support SMEs and start-ups;

• Support the emergence of start-ups with products / services that effectively reach the market;

• Foster the creation of financial / investment instruments to support industry and innovation in IT and cybersecurity, helping to bring innovative solutions to full maturity as well as stabilize / develop SMEs: e.g. entrepreneurial (private fund) and venture capital (bank / financial entities) investments funds, cybersecurity bonds (corporate bonds) etc.;

• Support innovation in companies with high growth potential to achieve next level in business developments and cross-border solution delivery.

INNOVATION OBJECTIVES

• Support the widest and best market uptake of innovative cybersecurity technologies and services for professional and private use by accelerating the wide diffusion of cybersecurity technologies in many industry sectors and the emergence of new business opportunities;

• Make the innovation process more inclusive, sustainable and effective through the direct involvement of players along and across the full value chain, including those communities, like “white hackers” and “open source”, that could bring disruptive views and breakthrough innovation;

• Facilitate networking between different actors (suppliers, users, R&D centres, public actors etc.) to find synergies and decrease the effects of fragmentation in the cybersecurity field;

• Support the creation of European-wide ecosystem for networking, training, testing and experience exchange through a network of integrated technical exercises environments, also to validate technologies from a technical and business perspective;

• Contribute to activities for pre-standardisation and / or standardisation to support development and use of products and services that meet the requirements set out in relevant legislation;

• Support the development of a trusted European cybersecurity supply chain where relevant, for higher technological independence at National / European level, by creating a catalogue of trusted products and companies, and by increasing the visibility of SMEs, promoting the European cybersecurity offerings and allowing informed procurement;

• Support increased use of trusted European certified or labelled solutions introduced in the different markets / applications;

• Plan funding for disruptive innovation through accelerators and / or SME associations or clusters to improve funding opportunities for small players (start-ups, SMEs, high-growth companies).
SOCIETAL OBJECTIVES

• Develop employment in cybersecurity sectors (supply and users/operators) in the European Union.

• Develop and implement European approaches for cybersecurity, trust and privacy by design:
  o Develop new personalised and enhanced technologies, products and services adapted to consumers’ and organisations’ needs that will respect security and integrity of data and ensure the protection of personal data in a manner that is compliant with the new General Data Protection Regulation;
  o Foster trust in the data-driven economy, including through incentivizing the application of the principles of privacy and security by design as well as the cooperation with relevant authorities in case of data breaches and cyber incidents;
  o Support the implementation of eIDAS Regulation as well as the development and uptake of high-security authentication tools by citizens to protect their identity and assets in the cyber domain;
  o Address acceptance of new cybersecurity technologies by society and consumers by identifying potential barriers.

• Develop education, training and skills on cybersecurity products and safe use of IT tools in Member States for citizens individuals and professionals:
  o Support widespread know-how, education and skills in Europe through curricula to stimulate higher education;
  o Develop an ecosystem that supports the general awareness raising and basic-hygiene skills development in the cybersecurity field for citizens in Europe to help manage the risks that have come along with the ever-increasing digital dependencies of everyday actions of the citizens;
  o Foster the development of new cybersecurity training modules to be integrated into training programs in different educational levels to provide basic skills and awareness of cyber threats also in traditional educational training;
  o Support the increase of in-depth cybersecurity training and education opportunities for securing a skilled workforce for cybersecurity industry as well as provide cybersecurity experts for public sector organisations and critical infrastructure / essential service providers, in particular through the EIT Digital (European Institute of Innovation and Technology Knowledge and Innovation Community on Digital) action line on Privacy, Security & Trust.

OPERATIONAL OBJECTIVES

• Establish an open, transparent and inclusive approach to determining and updating the SRIA.

• Bring innovative results to market via systematic use of the whole set of funding tools (at European and national level; public and private), showing the benefits and the link between European / National funds, European policies and market growth.

• Facilitate, together with the public side, that at least 20% of the participants of the calls to be funded are SMEs, start-ups or high growth companies (50+% increase in annual revenue).

• Gather information to support the ex post assessment of the implemented projects implemented under the partnership.

• Implement a cross-fertilisation platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues.

• Put in place Provide a governance model structures which on the one hand promotes openness, transparency and representativeness, and on the other hand ensures efficient management with minimal overheads.
• Cooperation with Third Countries to develop coherent approaches in the cybersecurity market: identification and measure of common events, meetings and concrete activities (projects, standards, mutual recognition etc.).

• Coordination of the partnership strategy implementation also combined with regional and national activities and funds in the specific sectors.

• Disseminate successful results within and between sectors and across value chains through effective linking of participants.

4.7 Added Value of actions at European Union Level

To date, Europe\(^{39}\) is the world’s largest single market, with transparent rules and regulations, 500 million consumers, and a secure legal investment framework. This unique positioning has not (yet) been translated in the cybersecurity domain. Across the EU28, different Member States have different cybersecurity strategies both at definition and at maturity. Procurement rules across the public and private sectors often do not require a specific level of cybersecurity thus leading to uneven levels of security, and the diversity across legal frameworks impedes the effective take-up of measures against hackers.

To assess the added value for a European level approach, we have first to recognize that all European countries have developed either national cybersecurity strategies or “cyber-wellness profiles”. These policies provide excellent bases to build upon at European level.

Yet, efficient exploitation of resources for a better market growth, requires a cross-border framework for pan-European cooperation. A country-tailored policy solution will not be able to take into account the cross-border nature of cybersecurity, and will not per-se favour international collaboration aimed at excellence in research and the provision of efficient solutions.

Moreover, the existence of a highly interdependent Digital Single Market suggests that non-European coordinated actions would produce ineffective outcomes, and possibly create further barriers to spur innovation in the continent.

These policies provide excellent bases to build upon at European level.

Yet, efficient exploitation of resources for a better market growth, requires a cross-border framework for pan-European cooperation. A country-tailored policy solution will not be able to take into account the cross-border nature of cybersecurity, and will not per-se favour international collaboration aimed at excellence in research and the provision of efficient solutions.

Moreover, the existence of a highly interdependent Digital Single Market suggests that non-European coordinated actions would produce ineffective outcomes, and possibly create further barriers to spur innovation in the continent.

Against this background, there is a strong added value in defining a long-term collaboration at European-level that will create economies of scale and increase the competitiveness at global level of European trusted solutions.

Against this background, there is a strong added value in defining a long-term collaboration at European-level that will create economies of scale and increase the competitiveness at global level of European trusted solutions.

Europe has always been very good in research, but rather weak in innovation, i.e. bringing research to the market. This reality is closely related to the fact that market success requires wider cooperative approaches and wider economical ecosystems while excellent research results can be obtained through isolated projects.

In order to fully exploit the opportunities that cybersecurity offers, a coordinated action at European level is needed and hence a European Cybersecurity cPPP is proposed.

In a coordinated European approach for cybersecurity, we should see the creation of the cPPP as a first step into a wider scenario, including the ambitious objectives of the Juncker’s Commission for growth and jobs, as well as the objectives of specific policies like the one for the Digital Single Market (DSM), its consistency with the objectives of the new European Security Agenda, the fight against cybercrime, the proposed “Industry 4.0” approach, the coming NIS Directive and Data Protection Directive, and the elements of the existing European Cybersecurity Strategy. These European policies are indicating priorities where Europe should invest to deliver growth and increase jobs. In this

\(^{39}\) http://ec.europa.eu/trade/policy/eu-position-in-world-trade/
context, cybersecurity is an essential enabling factor, protecting citizens, the society and the economy. An increased digital autonomy for sensitive applications, i.e. where Europe can verify and certify the trustworthiness of the full supply chain of solutions produced either in its MS or outside, can provide the appropriate level of trust for development of the Digital Single Market.

| 1. Austria | Austrian Cybersecurity Strategy (2013) / Cyber wellness profile Austria |
| 2. Belgium | Belgian Cybersecurity Strategy (2014) (Dutch) (available also in French) / Cyber wellness profile Belgium |
| 3. Bulgaria | Cyber wellness profile Bulgaria (Republic of) |
| 4. Croatia | Cyber wellness profile Croatia |
| 5. Cyprus | Cybersecurity Strategy of the Republic of Cyprus (2013) / Cyber wellness profile Cyprus |
| 6. Czech Republic | Cybersecurity Strategy of the Czech Republic for the Period from 2015 - 2020 / Cyber wellness profile Czech Republic |
| 7. Denmark | National strategy for cyber and information security / Cyber wellness profile Denmark |
| 9. Finland | Finland's Cybersecurity Strategy (2013) / Cyber wellness profile Finland |
| 10. France | Information systems defence and security, France's strategy (2011) / Cyber wellness profile France |
| 11. Germany | Cybersecurity Strategy for Germany (2011) / Cyber wellness profile Germany |
| 12. Greece | Cyber wellness profile Greece |
| 14. Ireland | Cyber wellness profile Ireland |
| 15. Italy | National strategic framework for cyberspace security (2013) / Cyber wellness profile Italy |
| 16. Latvia | Latvia's Cybersecurity Strategy (2014) / Cyber wellness profile Latvia |
| 17. Lithuania | Programme for the development of electronic information security (cybersecurity) for 2011-2019 (2011) / Cyber wellness profile Lithuania |
| 18. Luxembourg | National strategy on cybersecurity (2011) - in French / Cyber wellness profile Luxembourg |
| 19. Malta | Cyber wellness profile Malta |
| 20. Netherlands | The national cybersecurity strategy (2013) / Cyber wellness profile Netherlands |
| 22. Portugal | Cyber wellness profile Portugal |
| 23. Romania | Cybersecurity Strategy in Romania (2011) / Cyber wellness profile Romania |
| 25. Slovenia | Cyber wellness profile Slovenia |
| 27. Sweden | Strategy to improve Internet security in Sweden / Cyber wellness profile Sweden |

This global approach is only possible by moving from a national basis to ensure major players can cooperate across Europe to, for example, align standardisation strategies efficiently on a European level or to produce real impact on market take-up and harmonisation at European-level.

Indeed, activities in fields such as regulation, standards, certification and market take-up will benefit from a unified European initiative due to its global nature.
It should also be considered that counterparts in global competition are coming from other regions with huge domestic markets. In order to provide stakeholders from Europe a similar opportunity and ensure comparable impact, cooperation at European-level would provide a similar size of resources and strength as in other regions, fostering the growth of a European cybersecurity industry and trusted offer.

Europe needs to define actions that support faster deployment and adoption of the technology and business models in real cases. This should be preceded by good communication on the way this process should happen and the benefits/impact that companies could achieve.

In addition, real cases should involve application domains thus ensuring the smooth integration of trusted European solutions in the whole European ecosystem.

In addition to creating roadmaps on future research, pan-European roadmaps should be created that support companies (particularly SMEs) in the innovation process. Some of the roadmaps can be based on incremental technology deployments that help them to understand the needs associated to each organisation and business context.

Involvement of users from various sectors is essential as needs may vary and expertise may be complementary.

Actions for education are also required to increase European knowledge and give European society a real cybersecurity culture.

Europe needs to build further on its position in the global cybersecurity markets, and it is crucial to align and coordinate this highly multidisciplinary and fragmented field. Europe needs to strengthen its industrial leadership by promoting wide-scale cooperation and greater integration across the whole research and innovation value chain, from advanced research to technology take-up, pilot lines and demonstration actions. A Cybersecurity PPP is seen as the optimal vehicle for achieving this critical next step in the level of integration.

4.7.1 Rationale for a European approach

The European industry needs an investment effort that can only be supported at a European level. In the market segments of operating systems, computer and mobile phones manufacturing, routers, processors, components and other various software, Europe suffers from a technological dependence in information technology vis-à-vis the foreign providers.

An investment of this scale cannot reasonably be undertaken by one Member State alone. In cybersecurity, when “national products and services” exist, they often correspond to specific “national sovereign needs” and are not usually capable to compete on a global scale. Although Europe has some positive examples of cybersecurity industry (e.g. for end-point security sector) their number and size in other sectors remain limited on the global scale. Facing this well-established competition and market maturity in certain sectors, the counties participating in the cPPP with their industry do not have the capabilities necessary to build something up alone. The development of a strong European cybersecurity industry and an industrial base requires extensive investment capabilities and a joint effort of the European Member States and other national public administrations participating in the cPPP.

The European Digital Single Market strategy comes at the right time as Europe is in danger of falling behind in the international digital economy. Its main elements are the following:

- CREATING THE RIGHT CONDITIONS AND A LEVEL PLAYING FIELD FOR ADVANCED DIGITAL NETWORKS AND INNOVATIVE SERVICES (“The Digital Single Market must be built on reliable, trustworthy, high-speed, affordable networks and services that safeguard consumers’ fundamental rights to privacy and personal data protection while also encouraging innovation. This requires a strong, competitive and dynamic telecoms sector to carry out the necessary investments, to exploit innovations such as Cloud computing, Big Data tools or the Internet of Things.”40)

  - Reinforcing trust and security in digital services and in the handling of personal data

- MAXIMISING THE GROWTH POTENTIAL OF THE DIGITAL ECONOMY

---

40 Text from the “Recommendations on Cybersecurity for Europe” of the Cybersecurity Advisory Group to Commissioner Oettinger; January 2016
Building a data economy: Big data, cloud services and the Internet of Things are central to the European competitiveness. Data is often considered as a catalyst for economic growth, innovation and digitisation across all economic sectors.

Boosting competitiveness through interoperability and standardisation: In the digital economy, interoperability means ensuring effective communication between digital components like devices, networks or data repositories. It also means connecting better along the supply chain or between industry and services sectors. It means connections that are more efficient across borders, between communities and between public services and authorities.

An inclusive e-society: in which citizens and businesses have the necessary skills and can benefit from interconnected and multi-lingual e-services, from e-government, e-justice, e-health, e-energy or e-transport.

As mentioned in the DSM strategy, one of the first objectives is to create a level playing field for European players with regard to cooperation, consolidation, regulation and market power.

In agreement with the NIS Directive and with the objective to promote a cybersecure European Single Digital Market all players of the Information and Communication Technologies value chain, operating or not from a European Member State, should adhere to equal requirements concerning data protection and cybersecurity.

This is to ensure that European citizens and businesses would have access to products and services with at least a basic adequate security level, independently of the provider.

It is important that all market operators of the Digital Economy share the responsibility for a secure cyber space. It has to be ensured that all players involved are committed to secure digital products, software and services. This includes Network Operators as well as hardware and software Manufacturers and Internet-based services. Only if the entire value chain is made secure the risk of attacks can be mitigated. Additionally, this would allow for a fair sharing of responsibilities and financial burden.

4.8  Added value of implementation via a contractual PPP

Europe created a joint strategy in 2013. The cPPP moves this strategy into implementation, by an effective and focused pooling of resources. It also moves this strategy forward towards a maturity model supported by KPI that monitor the quality and effectiveness of this implementation with the full involvement of the different players, industry, public institutions and academia.

Europe must set up an ecosystem that nurtures innovation supported by cybersecurity. This entails activities in terms of research & development, innovation, standardisation interfacing, definition of European policies and regulations. All this requires joint efforts and commitment by many stakeholders, including public and private sectors at European level.

The challenges facing the European cybersecurity sector are not limited to supply-side weaknesses that could be addressed through piecemeal support for R&D (and innovation) activities. The proposed cybersecurity cPPP would provide for a coordinated and long-term approach that, supported through accompanying policy actions implemented as part of a broader cybersecurity industrial policy, could strengthen European cybersecurity sector by strengthening research and innovation capabilities while simultaneously improving the functioning of cybersecurity markets in Europe.

Currently, the European cybersecurity sector is characterised by fragmentation both in terms of the supply-side (industry) and demand-side (users/customers), while markets themselves are fragmented by the absence of common European approaches and regulatory framework. While the primary strategic and operational objectives of the proposed cPPP are targeted at support for research, development and innovation activities (e.g. establishing a more coherent, efficient and effective long-term framework for R&D&I, including transition to the market), a key benefit of the proposed cPPP is to offer an opportunity to bring together multiple categories of actors as part of a ‘shared project’. Importantly, these actors not only include the cybersecurity industry (and the extended value chain supporting research and innovation activities) and user groups from different application domains but, also,
representatives from the public sector (i.e. MS administrations). In this respect, the engagement of a broad range of ‘stakeholders’ in the cPPP – and in the membership of the ECSO Association – should support achievement of the objectives and prospects for long-term sustainability (i.e. beyond the 2020 financing timeframe). This broad based approach may be particularly necessary if the cPPP is to support efforts to address wider issues of the cybersecurity market (e.g. legislation, regulation, business development, societal concerns, etc.).

To summarize, the main elements that are pushing for a cPPP include:

- The European Cyber Security Industry is at present active predominantly at national level rather than at pan-European or even global level. A cPPP would give the industry a pan-European presence.
- The industry is fragmented, made up of many small companies with little power and reach beyond their specific local geographies. Traditional EC instruments have had limited success with addressing fragmentation. A cPPP could engage in activities that include an even spread of companies by size and country.
- Up to now there have been no European wide requirements and regulations that would create demand and act as a magnet for companies to step up and provide pan-European solutions. A cPPP would be better placed than traditional instruments to take advantage, for instance of the new NIS Directive.
- A cPPP could ensure a longer-term partnership and cooperation beyond the time limits of Horizon2020.
- The Association itself would be better able to address non-research and innovation based aspects of a European cybersecurity industrial policy.

The present EC approach, based solely on existing instruments (e.g. H2020) would fail to effectively and efficiently address the present and future challenges. An example of such an argument is that, despite the fact that 334 M€ EU between 2007 and 2014 have been made available through the FP7 and H2020 frameworks, funds that have given EU support to academic research and industry to test new waters and develop solutions to better protect users, they have not sufficiently stimulated the competitiveness and innovation capacities of the digital security and privacy industry in Europe.

Indeed, even though some spin-offs and start ups have been created and the scientific excellence in Europe in cybersecurity and privacy has been demonstrated, the participation of innovative SMEs has been relatively limited.

Another example is the limited potential of disjoint initiatives to bridge the gap and to minimize the time taken between production of research results, innovation and commercialization.

The Research and Innovation Strategy contained in the cPPP Proposal sets out a number of non-technical aspects and supporting actions that go beyond the type of collaborative research efforts that may normally be supported through Horizon2020 (or similar national level R&I support) or by industry acting alone. These actions address the wider context of the environment of research and innovation that are important, e.g.:

- Education, training and skills development;
- Sector development and consolidation (cybersecurity ecosystems, clusters, value chain definition, SME support, …)
- Fast-track innovation support
- Standardisation, regulation and certification;
- Awareness raising / societal aspects

Common approaches and the coordination of these actions across the multiple technical priority areas and implementation mechanisms envisaged under the cPPP Proposal should a priori enable exploitation of opportunities for synergies and increased overall effectiveness and efficiency.

The proposed Cybersecurity PPP will:

- foster close alignment of industrial and public (regional, national, and European) strategies;
- pool academic, industrial and public resources to provide sufficient know-how and the investment that will be essential for achieving major progress towards this joint strategy.
Specifically value-adding benefits expected from the ECS cPPP are as follows:

- **Commitment to implement the European and National Cybersecurity Strategies:** Strategies that reinforce Europe and countries in the landscape of cybersecurity in terms of both technology supply and technology adoption. Research, development, and innovation all will play a crucial role. The cPPP commitment will be in terms of:
  - Support provided by a specific association (ECSO) to achieve the general and specific objectives described in this proposal.
  - Resources needed to accomplish such objectives.
  - Cooperation between different research projects in order to address a holistic system perspective, e.g. enable cooperation for interfaces definition.
  - Opportunities for creating coherence and complementarities with the diverse landscape of Member States and of other national public administrations participating in the cPPP funding policies in the field.

- **Long-Term Strategic and operational framework:** The cPPP will help in:
  - Capitalizing on research, development and innovation activities developed in previous framework work programmes in the domains of ICT security, ensuring that the most promising results can be enhanced, further developed and widely disseminated whilst taking into account that cybersecurity requires increased technological capacity, new tools and new skills.
  - Identifying and establishing links to research, development and innovation activities in Member States and in other national public administrations participating in the cPPP, including collaborative programmes, research institutes, and other public and private entities.
  - Maximizing the use of innovation instruments in the EC, as well as synergies with ongoing and future initiatives of relevance for the goals.
  - Secure commitment of industry and the European Commission, including funding and investments, to meet critical societal and industrial policy objectives.
  - Identifying and establishing ways to leverage additional funds, including links to public programmes in Member States and in other national public administrations participating in the cPPP as well as other public and private sources.
  - Long-term continuity of activities in order to achieve the defined long-term goals and targets.

- **Application Sector involvement:** Multiple parties took part in the discussions which have helped formalise the ECS cPPP initiative. These results and parties will be leveraged from and actively engaged through the Association Board to ensure that the cPPP results are viable, used and can reach sector expectations.

- **Representative approach:** A single industrial partner could never achieve the ambitious objectives like the ones proposed by this cPPP. An industrial alliance of industrial players would not be the answer since other stakeholders are needed such as European-level Public Sector, users in many different application domains, representatives of SME associations, RTOs, etc. The cPPP will ensure a balanced and fair representation of the different stakeholder, facilitating value chains and relationships among them.

- **Impact on the market:** This cPPP aims at creating a compelling portfolio of technologies that require a European approach not only because of the technical complexity, but because of the need to address the problems of legislation, regulation, business, economic and societal adoption and many other open issues that are due to the lack of a single European market.

- **Openness:** A cPPP provides an excellent framework to involve key stakeholders and make sure that new ones can enter. Openness will be applied not only at the level of membership, but will also be a main driver for technology development and delivery.

- **Accessibility and sustainability:** A single project cannot address long-term aspects such as sustainability of many of the relevant outcomes coming from European companies. The long term commitment of stakeholders that endorse this strategy will ensure that both of them are seriously tackled both at the organisational and project level.
- **Clear guidance:** How to evolve and how to contribute to aspects that may have already been identified. This will happen thanks to a Strategic Research & Innovation Agenda that will be the reference for the cPPP. This plan will be open, continuously updated regularly and monitored in order to assess both the progress on the objectives and the overall success of the cPPP.

- **Efficient management:** Leaner and faster organisation and governance of new projects under the cPPP umbrella, obtaining the benefits from a formalisation of the partnership (less time to set up, reduced costs, less legal and administrative burdens), when the necessary legal framework for cooperation across projects is put in place by the cPPP structure.

- **Development of national Cybersecurity organisations:** The cPPP will foster the creation of sectoral cybersecurity organisations at local and national level to improve coordination, up to the creation of national cybersecurity PPP that could better interact with the European cPPP.

- **Focussing funding for R&I and deployment:** The strategy developed in the cPPP would drive focussed use of resources for R&I but also would provide harmonisation of operational requirements from users / operators and procurement bodies, thus improving market growth.

The ECS cPPP will be realised using a set of different instruments in order to enable both a shift of focus and change of activities throughout the lifetime of the initiative. From this will follow developments towards technology maturity, emerging standardisation, and regulation to ensure future market adoption and take up of results.

A well designed cPPP will provide a more stable environment towards 2020 with respect to research topics and budget allocation in order to implement an agreed research Work Programme based on a publicly accepted SRIA.

Finally, a roadmap based cPPP allows to plan early in the process the technology validation and exploitation activities which are needed to realise the innovation objectives targeted by both public and private entities.

### 4.9 Actors behind this proposal

This proposal has been developed over several months identified by cybersecurity industry, research organisations and academia, governments and users, following an interdisciplinary approach representing both the supply side (technology and services providers) and the demand side (users of the technology in different sectors) as well as some policy / political guidelines provided by the public administration.

The formal kick off to the cPPP set up was given at the meeting organized by the EC on January 20th 2016, where representatives from Member States administrations and national associations gathered in Brussels and set the objectives and trace a common road for the setup of the cPPP to be signed by June 2016. Yet, the work for preparing to this cPPP has started well before.

The Commission was the first to recognize the unusual short time for setting up the cPPP as well as the complexity of the topic. That being said, the Commission highlighted at the 20th of January meeting that content support can be easily obtained by previous work done in the frame of FP7 (projects like CAPITAL, IPACSO, CYSPA, etc. - targeting the creation of an European cPPP alliance on cybersecurity), the work of the NIS Platform (in particular the WG3 with its Strategic and Research Agenda, supported by the activity of more than 200 experts), R&I agenda from specific countries, the contribution of the market analysis made in the 2015 in the mentioned EOS41 study for an European Cybersecurity Flagship as well as other market studies from consultancy firms.

An instrumental role has also been played by the Public Consultation on the public-private partnership on cybersecurity and possible accompanying measures42, opened by the E. Commission in December 2015.

It is important to notice that the demand side is largely characterised by industrial entities that respond to their customers’ requirements for secure systems and services. These entities use products and services of security technology providers as well as their own innovations and developments not only to meet baseline requirements, but also to distinguish their offers from the competition by means of leading-edge security and privacy qualities. Hence, when referring to European cybersecurity industry both security technology/service providers and providers

---

41 [www.eos-eu.com](https://www.eos-eu.com)

of secure systems and services are included. In fact, their interplay is seen as a catalyst for developing a particular European industrial strength on security and privacy.

To tackle one of the current weaknesses in the cybersecurity domain, i.e. the fragmentation of the domain and main applications and actors, many stakeholders from the public and private side have been involved during the planning phase. This has proven being beneficial and should be strengthen under the umbrella of implementing the vision of the cPPP.

Stakeholders who have participated in the pre-study and planning phase involve representatives of Member States (policy level, IT agencies level), SMEs, Large companies, Start-ups, high growth companies, clusters, associations, vital services providers, research and innovation organisation, academia, etc.

One of the challenges of this cPPP, is that the supporting Association is already a PPP, with strong participation from national public administrations.

Indeed, a peculiar characteristic of this cPPP is the presence and role of public administrations. The presence of public administrations (policy level, IT agencies level, representatives at the H2020 Programme Committees), is not only that of a “Mirror Group”, as they would have a larger role, contributing in the different policy aspects, underlying the sensitive issues and proposing how to deal with them, but also providing views on the SRIA from representatives at the Programme Committees.

The current proposal aims to involve not only those actors which are focussed and working on cybersecurity field but also those IT developers, not necessarily focussed on cybersecurity, but offering security products as part of their business and developments. In this respect, one important dimension of the cPPP is to extend collaboration across all application sectors of the economical society, ensuring that stakeholders become actors in increasing their own and the shared level of cybersecurity.

Today, at the eve of the incorporation of the ECSO Association, we have obtained the interest of many different stakeholders.

From the private side, we recognize interest from:

- Large Supply companies (products and services);
- SME (including start-ups and high growth companies) supply companies (products and services);
- SME users;
- Large users / operators – vital service providers (public or private);
- RTOs;
- Universities / Academia;
- Local, National or European sectoral Associations, Organisations, Clusters;
- Other (consultancies, investors etc.).

To setup this proposal for the cPPP we have contacted and shared / received information from more than 150 bodies in Europe. This announces a fast ramp up of the Association and of the future cPPP activities.
5 Research and Innovation Strategy

5.1 Introduction: Cybersecurity products and services

In this cPPP the industry perspective will be analysed and developed in order to contribute to the creation of the Digital Single Market:

- Stimulate the competitiveness and innovation capacities of the digital security and privacy industry in Europe.
- Ensure a sustained supply of innovative cybersecurity and ICT products and services along the full value chain in Europe.

We thus considers the main elements of the market and the security products and services and make those the cornerstone of our approach for the identification of the cybersecurity technical priorities as well as the main vertical sector of analysis as depicted by the NIS directive and consultation for cPPP.

We use the following classification for cybersecurity product and services (others could be used as well):

Cybersecurity Products & Services:

- Assurance, security and privacy by design
- Identity, access and trust management
  - Identity and access management
  - Trust management
- Data security
- Protecting the ICT Infrastructure and enabling secure execution:
  - Cyber threats management
  - Network security
  - System security
  - Cloud security
  - Trusted hardware/end point security/mobile security
- Cybersecurity services
  - Auditing, compliance and certification
  - Risk management
  - Cybersecurity operation
  - Security training

The “Products & Services” approach will be the cornerstone of our analysis for defining the technical priorities for the cPPP. In doing so we will consider the vertical sectors (as smart grids, e-health,...) and their needs vs security products. The main goal is to provide a set of cybersecurity capabilities technologies that can be used in different application domains with maximum efficiency and impact.

The first phase is set up these priorities. Also the maturity level of such products should be analysed in order to see if the European cybersecurity strength and weaknesses.

The vertical sectors will provide requirements and needs to the lower layers, by requiring proper technologies and processed to secure the development and operation. These products in turn will use security product and services. These are still in maturation and the research needs will be identified.
5.2 Mechanisms for SRIA implementation

The ECS SRIA will use a coordinated set of mechanisms to implement its research and innovation activities. In doing so, it will also be coherent with the H2020 framework although proposing also mechanisms to overcome some of its limitations.

These mechanisms are common also to other cPPPs (e.g. Big Data Value):

1) **Cyber Coordination Projects**: mainly devoted to coordination and support activities at several levels
2) **Cyber Pillars**: socio-technical ecosystems for innovation and experimentation
3) **Cyber Technical Projects**: mainly devoted to build the basic capabilities, often involving research and innovation actions
4) **Cyber Trustworthy Infrastructures** (“lighthouse projects”):
   - Large projects able to develop cyber infrastructures allowing a better protection of the European DSM, while promoting European innovative products and services across several application domains
5) **Cyber Pilots**: developed to pilot and experiment solutions in specific vertical domains

In principle other kind of instruments could be set up, especially when working at national regional level and by suing structural funding.

More detailed aspects of the envisaged R&I priorities are presented in the SRIA companion paper.

5.3 Technical Priorities

5.3.1 Identification and analysis of technical priority areas

Based on these considerations we have taken a solutions oriented approach when defining the technical priorities, focusing on those needs that have to be fulfilled to support citizens and organisations alike, reinforcing the “close to market” dimension of the cPPP.

This has led to focus on 5 key technical areas, that we then further split in technical priorities and research challenges.

We consider the following classification and grouping for the cybersecurity Products & Services:

- **Assurance / risk management and security / privacy by design**
- **Identity, access and trust management** (Identity and Access Management, Trust Management)
- **Data security**
- **Protecting the ICT Infrastructure** (Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security)
- **Security services** (Auditing, compliance and certification, risk Management, cybersecurity operation, security training services)

5.3.2 Assurance / risk management and security/privacy by design

5.3.2.1 Scope

The “quest for assurance” in cybersecurity is a long-standing issue with many facets and related aspects. It is commonly agreed that, in order to be effective security, privacy and trust considerations should be integrated from the very beginning in the design of systems and processes (i.e. security/privacy/trust by design). This entails a whole series of activities, including social and human aspects in the engineering process all the way to a certification that the developed systems and processes address the planned security/privacy/trust properties.
In addition to the aim of building a secure system, we often need to prove (through evidence) that the system is secure. This is also necessary when considering systems of systems, whose security depend not only on the individual security of subcomponents but also on the security of the integration of these subcomponents. The engineering process of the systems should thus take into account those security/privacy/trust/compliance requirements and should consider, in addition, costs and risks in the development process and in the system’s lifetime.

Indeed, cost and risk constitute two relevant factors in building and operating (security-sensitive) systems. This is a typical need of any risk management approach.

The cost of developing security countermeasure should be related to the value of assets to be protected (and often in the digital world these are less tangible). Therefore the issue in this respect is not only cost, but also how a value can be assigned to one or more assets, used by an organisation in its own economic sector of activity. On the other hand, risk is linked to the capability to predict the current strength of the system. Thus security and corresponding risk metrics are crucial (as other quantitative aspects of security).

This process of encouraging assurance techniques and processes can also be addressed by regulators. Indeed, the introduction of regulatory actions could ease and support the adoption of assurance techniques (delivering benefits to the overall security level of the infrastructures, systems and products).

Starting from these considerations, risk should be managed with respect to the assets to be protected, and investment in security should be aligned to the value of the assets. In this context, the residual risk could then be managed with other approaches beyond security countermeasures.

### 5.3.2.2 Expected outcome

- Integrated assurance frameworks (in a risk management approach) including the management of cost efficiency and risks, able to merge security and safety aspects
- End-to-end adaptive security engineering frameworks
- Adaptation to specific operating context and related risk exposure (and their evolution)
- Support of diverse deployment models (cloud, mobile, platform, platform services)
- Increasingly resilient systems
- User-friendliness, i.e. easy to comprehend and evaluate evidence
- Link to cyber-insurance policy elaboration and dynamic management

### 5.3.3 Identity, Access and Trust Management

#### 5.3.3.1 Scope

Despite being a well-established market in its own right, the Identity and Access Management (IAM) marketplace is still a dynamic and growing one. Notions of extended enterprises and more advanced B2B interactions based on Internet services become more commonplace, driven by e.g. cloud services, new hosting models and diversifying partners and relationships. Developments such as the Internet of Things (IoT) trigger diversity of form factors and capabilities of authentication tokens. Hence, current IAM approaches do not cater to the full range of needs created by the increasing mix of devices brought on by IoT, machine-machine and man-machine interactions and similar developments. Core challenges exist around cross-domain authentication, authorisation in new distributed contexts and the need to avoid monopoly situations and single points of failure, when users are authenticated and their authorisations are being checked. For end users to trust the digital society, they need to be able to not only understand but also manage the actual level of security delivered by different providers and control the degree of identification.

Indeed individuals need to be empowered to develop trust into digital services and/or apps for them to make informed decision. This calls for methodologies and tools to not only focus on Security and Privacy by design but also Trustworthiness by design. This calls also for proper lifecycles to be covered from development to management (monitoring) going through important steps such as certification, distribution and deployment.
It also calls for **innovation in managing the dynamic dimension of authentication**, when a user’s identity needs to be re-assessed after an initial approval.

### 5.3.3.2 Expected outcome

- Best practices in authentication are supported by usable technologies embedded seamlessly into applications, including management of different levels of authentication and dynamicity.
- Users and relying parties are provided with a range of authentication options that they can choose from to agree on a mutually acceptable way of authentication avoiding over-identification, delivering the degree of assurance and liability appropriate for the respective service.
- Citizens can enjoy the privileges of services needing strong authentication, focusing on those specific attributes that require this level of authentication.
- Certificates and signatures remain valid for at least a long as the corresponding documents and trust relations are commercially relevant and/or legally valid.
- Authentication operates in a distributed fashion without single points of failure on critical paths and considering small scale devices as used in the Internet of Things.
- Authentication operates in an interoperable fashion without overheads and additional security risks.
- Increased trust in the cyber world;
- Requirements for trusted security credential provisioning (e.g. trusted secure elements)
- More efficient on-line Business

### 5.3.4 Data security

#### 5.3.4.1 Scope

A major characteristic of current and future systems and applications is the ever-increasing amount of valuable data that needs to be properly managed, stored, and processed. Data can be produced by systems as a consequence, for example, of interconnected devices, machines and objects in the Internet of Things, and by individuals as a consequence, for example, of business, social and private life moving on-line, thus including data resulting from observations (e.g., profiling) and data intentionally provided (e.g., the prosumer role of individuals). As the value of data increases, opportunities based on their exploitation and the demand to access, distribute, share, and process them grows. Highly connected systems and emerging computing infrastructures (including cloud infrastructures) as well as efficient real-time processing of large amounts of data (including Big Data methods and applications) facilitate meeting these demands, leading to a new data-driven society and economy.

The collected data is often of a highly sensitive nature (e.g. medical data, consumer profiles, and location data) and need to be properly protected. With data being stored and processed in the cloud, and exchanged and shared between many previously unknown and unpredictable parties, this protection cannot stop at a single system’s border, but needs to be applied to data over its full lifecycle, independent of which system is processing the data, which access channels are used and what entity is controlling the data. Hence, a **system-centric view** on security and privacy, including, among others, secure devices and infrastructures (cf. sections below), needs to be complemented by a **data-centric view**, focusing on data lifecycle aspects.

Providing transparency on where data resides, who has access to it, and for which purposes it is being used, together with mechanisms that allow the data owner to control the usage of his/her data, have been identified by all areas of interest (AoSs) as essential aspects of a data-centric view and a prerequisite of a secure and privacy-preserving digital life. While research has already produced a number of relevant contributions (e.g., sticky policies, privacy policies, and techniques for protecting data at rest), many challenges remain open, including enforcement and usability. These challenges are not only of a technical nature: for example, lack of awareness of the value of data (and what data is actually produced when engaging in digital life) has been mentioned as an inhibitor of trust and growth of digital services.
5.3.4.2 Research challenges
A variety of challenges need to be addressed to take advantage from the availability of large amounts of data in a secure and privacy compliant way. These challenges should cover issues related to the protection of data as well as the use of data for security.

5.3.4.3 Expected outcome
- Secure and privacy aware data processing and storage
- Advanced mechanisms that protect effectively users’ privacy and guarantee the integrity and confidentiality of their sensitive data
- Efficient management and increased deployment of data-encrypted processing and storage solutions
- User friendly (i.e. also for non-expert users) transparency and control options incorporated as “standard features” across all storage solutions
- Increased and efficient uptake by users of the transparency and control options

5.3.5 Protecting the ICT Infrastructure

5.3.5.1 Scope
The increased interconnections created within the Internet as well as between the Internet and critical infrastructures have made our society vulnerable to attacks that spread across hundreds of thousands of computers, mobile devices or even intelligent connected objects at lightning speeds. This is one of the most challenging dimensions of cybersecurity, the speed and scope of cyber-attacks or incidents.

Furthermore, the ability to remotely compromise intelligence devices coupled with the potential value that can be created by stealing information or modifying operations through a device under attack has created a completely new environment for cyber-criminals.

Society, businesses and governments have become increasingly dependent on the correct and uninterrupted operation of networks, both at global and local levels. On the other hand, cyber criminals and terrorists are becoming increasingly skilled at compromising networks through sophisticated attacks. Therefore, all networks constitute, in one or more dimensions, a Critical Information Infrastructure – CII.

Unfortunately, contrary to the physical world where barriers can in some case limit negative impacts, cyber-space is effectively without frontiers at least across the democratic regions. In this context, cyber-space has to inherit from the physical world a concept of “barriers”, through a pro-active approach to protect critical information infrastructures. Strategic management of CII has to balance the benefits created through “ease of connection and remote control” versus the increased level of risks.

The protection of the infrastructure therefore requires a holistic approach pervasive across all the communication dimensions, including also the software and hardware involved in the network and connected to the network.

For instance, secure execution environments can be used by the software across solutions and services. These secure execution environments not only encompass the execution platforms and the operative systems, but also the mechanisms (e.g. security supporting services, control and intrusion prevention systems) that ensure a pre-defined level of security in the execution of all processes.

Another dimension is the hardware level, covering a broad range of fixed and mobile devices. Also important is the increasing use of IoT devices, and the set of pre-requisites to be fulfilled prior to trusting a connected device whether this device is used in the field of Critical infrastructure, Industry 4.0, Automotive (ADAS, V2V, V2X), Smart City, Smart Home, Building Automation, Healthcare, Wearables or any other connected system.

5.3.5.2 Expected outcome
- A larger base and range of data is available for a comprehensive and precise security analysis
- New threats are detected more rapidly through the increased collaboration and available information – solutions are deployed more rapidly, new security practices are routinely incorporated to the security assessment of system managers.
• Security control and intrusion prevention systems become more efficient and adapted to new and dynamic environments
• Network operations become more resilient
• Design guidelines and products implementing secure execution platforms, including secure boot, remote attestation, and secure virtualized environments
• Operating systems designed according to new security guidelines
• Security supporting services allow data protection and device protection
• Best practices for integration of secure components in a secure system with interoperability and management in distributed systems
• Secure virtualisation environments ensuring isolation for different architecture paradigms (e.g., virtual machines, containers, etc.)
• Trusted cloud operational environment based on dynamic root of trust
• Incorporation of mobile device owners in the overall security policy of a network (at technical and at collaborative levels)

5.3.6 Cybersecurity Services

5.3.6.1 Scope
This topic focuses on the processes (and their constituent elements) required to provide, manage and measure privacy and security, and the tools required to support them. The issues apply to formal and informal socio-technical organisations of all types and scales from individuals and families, through SMEs, to large businesses and governmental departments, multi-national corporations, nation states, Europe and the society at large.

Cybersecurity services can be delivered through a wide diversity of models, ranging from internal services (hosted within the customer organisation) to external (used from external hosted resources) and consultancy based approaches. The choice between these models is done based on a wide variety of reasons, from economic to sensitiveness of operations, from internal capability at technological level to ease of use and flexibility of external approaches.

For instance, large organisations (and ones for which security is a core business function) may elect to perform security processes using only internal resources, but increasingly, the complexity and wide coverage of the required skills and tools make outsourcing a more attractive option. For smaller organisations, affordability issues often make automated security-as-a-service (SaaS) offerings more attractive. Micro-businesses and individuals are likely to want fully holistic solutions.

But across all these dimensions, cybersecurity services increasingly have to address an end-to-end approach, and have to start from the values (and therefore assets) that are important to the business in which customers operate. How many man-hours will be lost if a process stops? If an asset stops operating? What will be the cost of reputation damage created if data is leaked to the outside world?

One increased complexity is the notion of responsibility –outsourcing some or all security functions does not absolve a customer organisation of its actual responsibility with respect to the outside world of customers, partners and society as a whole.
Cybersecurity services can be analysed through a ‘temple’ model, used to categorize security processes and the services used to deliver them. The pillars of the temple are the five core functions of the NIST cybersecurity framework:

- **Identify**: maintain a complete and accurate model of the organisation being protected and its business context;
- **Protect**: Develop, implement and operate the appropriate safeguards to ensure continued delivery of the organisation’s key services;
- **Detect**: Develop, implement and operate the appropriate activities to identify the occurrence of cybersecurity threats, attacks, breaches, etc.
- **Respond**: Develop, implement and operate the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover**: Develop, implement and operate the appropriate activities to restore any capabilities or services that were impaired due to a cybersecurity incident.

The temple pediment represents Governance, Risk and Compliance (GRC):

- **Governance**: the strategic management of security processes, including setting policies and defining a prioritised approach to risks;
- **Risk**: modelling, analysis, assessment, treatment, etc. of security risk;
- **Compliance (including certification)**: Measuring/assessing/auditing/certifying the extent to which internally and externally set security policies and standards are a) followed, and b) effective.

### 5.3.6.2 Expected Outcomes

- Definition of a cybersecurity strategy by each individual organisation, building on concrete and quantified prioritisation of assets most at risk linked to the business sector in which the organisation operates.
- Inclusion of cybersecurity policy as a strategic decision at executive / board level of organisations.
- Cyber-insurance policies becoming the norm across organisations, building on a common definition of “level of cyber-risks”, but an adaptation / personalisation to how this level is selected by an organisation based on its own operating context.
- European organisations and individuals have access to comprehensive security management solutions in line with their contexts, affordable, and evolvable to keep pace with escalating threats and innovations in technology and practice.

---

- European organisations and individuals provided with support and processes that help detect and respond to internal and external threats and failures, enable them to function under adverse conditions, and self-repair in order to resume normal operations as soon as possible.

- Creation of a dynamic and innovative European market in cybersecurity services, which will itself yield significant economic benefit, as well as serving the needs of European organisations.

5.4 Non-Technical Aspects and Supporting Actions

5.4.1 Education, training, and skills development

There is a need for re-thinking education at different levels. It is not a matter of standard recycling, but a real multidisciplinary, coordinated and coherent approach is needed. The customers of the education, training and skills development can be segmented as:

- General population – individuals that are not cybersecurity experts but users or ICT technologies and services.
- Students of all ages under an education curriculum. Targeting the education in primary and secondary schools as well as at university level.
- Experts - addressing the needs of continuous learning for professionals of different sectors that have high ICT dependency, in order to raise awareness and enhancing their skills.

In order to reach those segments, many tools need to be set up:

- At general population, ICTs have changed our lives as they have penetrated almost all domains and majority of the people are highly dependent of well-working ICT tools to conduct their daily business.
- At education level, there is a big awareness gap and lack of integrated training modules on cybersecurity related aspects on all school levels, starting from low awareness and skills of teachers themselves. The same is true for professional training on university level, including lack of cybersecurity modules in higher education training programs for vital service domains etc. Furthermore, there are only few existing cybersecurity higher education programs in Europe.
- At professional level, there is a lack of accessible tools for continuous awareness, training and skills development on cybersecurity aspects. Cybersecurity skills are more and more a prerequisite by employers in a multi-faceted approach (i.e. law, insurance, testing facilities from many ICT and non ICT sectors, critical infrastructures, etc.) and, at the moment, there are more jobs than qualified candidates, while the unemployment rate stays very high in some European countries. On the other hand, professional training programs are very fragmented and leaded by specific international companies that develop them for specific purposes or under request (usually also very costly).

It is clear that to reach these target segments, it is necessary to set up new training models (i.e., massive open online courses, etc.) and accessible tools to facilitate the access to knowledge and raise general awareness. Also efforts need to be made to enable career re-orientation to support entering the cybersecurity field in later stages of the career.

The benefits are obvious:

- Cybersecurity will produce new innovation paths and market niches such as cybersecurity insurance, cybersecurity risks and practices, security engineering, security management, and many more.
- Having a coordinated view will encourage Member States and the other countries participating in the cPPP to agree upon a baseline of cybersecurity indicators.
- In addition, there is a social aspect of cybersecurity as tool for awareness in human values (particularly among the youngest people) through, for instance, the user empowerment and control of personal data, the digital legal education (right to be forgotten, freedom of speech, anonymity versus trust and security, crowdsourcing versus legacy manufacturing etc.).

The common educational needs of the target segments identified above should have:
- Multi-disciplinary focus
- Responsiveness to changes in technology and societal environment
- End-to-end skill development
- Alignment of curricula and training with demand for skills
- Using appropriate methodologies for teaching cybersecurity at all levels, from awareness to focused expertise

Among others, one of the goals to be developed within the frame of the cPPP would be to set up a cyber College/Academia (or network of academia and colleges) with the goal to:

- Collaborate in preparing training materials and modules for professional training as well as training on lower educational levels.
- Generate a consensus on a core of European higher education curricula for cybersecurity studies at university level (both traditional and virtual education) as well as propose a plan for integrating cybersecurity studies modules to professional education of vital service providers and public servants. For that purpose, synergies with DG-Education programmes and funds have to be found. At the moment, there is a fairly sparse collection of courses and competences but not a unified approach.
- Coordinate a network of PhD studies on cybersecurity, deeply connected with the industry, i.e., under the format of industrial PhDs already existing in the H2020 Excellence Science Pillar.
- To promote creativity and innovation in young students and young researchers by proposing challenges, prizes, cyber-campus activities, etc., in order to connect them with the needs of the citizens and of the industry.

Finally, the scope of education, training and skills development can provide an opportunity for a close collaboration with other bodies (i.e., NATO, especially NATO CCDCOE and other decentralised European agencies).

5.4.2 Fostering innovation in cybersecurity

Innovation models have evolved from insular, linear, and reactive models of innovation towards the more contemporary models that are fluid and adaptable processes that aim to raise development efficiency and speed to market through inter-organisational cooperation and strategic alliances. The Cybersecurity Innovation value chain is enacted by an open ecosystem of small and large enterprises, individual inventors, research institutes and universities. Large enterprises are experimenting with a variety of schemes to stimulate and benefit from entrepreneurial activities outside their organisations. Similarly, national and European research programmes are trying out new instruments designed to encourage participation by small companies and to grow this sector of the market. Information gathering and analysis is still in progress, but it appears that while the general philosophy of Open Innovation is shared, there is considerable variation in how it is interpreted and applied, and a consensus on best practice has yet to emerge.

5.4.2.1 Develop a cybersecurity ecosystem

The breadth of cybersecurity and privacy challenges within wider technology, policy, and economic perspectives is vast in scope. In aiming to build systems with as few security flaws as possible, strong demands are placed on many stakeholder types, how best to introduce the right economic incentives that fairly balance those costs across the various actors in the security value chain is critical. In tandem, many cybersecurity clusters and accelerators have been created in Europe in recent years and we have several years of practical experience with organizing international as well as national cyber strategy.

There are many ways to develop the cybersecurity ecosystem further in order to create value for many other stakeholders including researchers, experimenters, SMEs, policy makers, universities and students etc. Innovation clustering initiatives are viewed as a key abstraction for creating the appropriate ecosystem, however these are often characterised and constrained by their regional nature, a European-wide initiative is recommended.

- Collaborating and competing
- Geographically dispersed across Europe but linked to other global initiatives

European Cybersecurity cPPP – ECS cPPP – Industry Proposal 63
- Specialized in a special field, linked by common technologies and skills
- Of a critical mass (this refers to fact that a cluster should include actors, which together have a certain weight in their sector in order to be able to build momentum, i.e. to be able to establish self-supporting processes.)
- Either institutionalised (having a proper cluster management) or non-institutionalised.

While clusters are usually created and thought of in terms of driving competitiveness and growth, particularly with regards to innovation, their definition may also be focussed on other primary objectives, such as providing a legal framework or similar umbrella to support funding or marketing initiatives, or in some cases to provide a supporting reference model for statistical measurement. The notion of clusters it is often used interchangeably with other terms such as innovation or technology “hubs”, “districts”, “milieu” etc. While some academic literature has suggested nuanced differences when comparing such terms, consensus on similarities and differences has been difficult to establish.

5.4.2.2 Key Cluster Characteristics.

Clusters of specific firms within a specialist industrial or technological domain are viewed as an increasingly important source of economic development across the advanced industrial economies, and a central focus of technology policy. By composition, there are generally accepted to be four cluster types:

1. Geographical cluster
2. Sectoral clusters (businesses operating together from within the same commercial sector)
3. Horizontal cluster (interconnections between businesses at a sharing of resources level)
4. Vertical cluster (i.e. a supply chain cluster).

Researchers have also attempted to decompose the structural topology and characteristics of clusters, noting several approaches such as:

1. “Hub and spoke” approach that is typically led by a few dominant anchor firms, usually large firms
2. “Satellite” approaches whereby organisations co-locate branch facilities of a similar nature in near proximity to one another - R&D divisions are often clustered in such a manner in a location away from corporate headquarters to achieve such benefits for example
3. State-centred clusters are another approach, led and dominated by the presence of one or a few large public or non-profit entities, such as universities, RTOs, or military/national security institutes (the latter particularly evident for PACs).

Broadly, it is agreed that the initial formation of the most successful clusters has resulted from accidental or serendipitous events, and is often driven initially by key anchor individuals with a vested interest in harnessing local networks in a given area, more so than top-down policy drivers. However, it is agreed that once a cluster reaches a certain point of scale, policy intervention can achieve significant impact and is indeed necessary for the cluster to be sustainable [ref IPACSO]. Despite this, within the cybersecurity spectrum some key emerging ecosystem initiatives on a global level are strongly premised on a top-down policy approach, the emerging shift of cybersecurity emphasis in Israel from Tel Aviv and Haifa towards Be’er Sheva being a strong case in point.

5.4.2.3 Key Characteristics of High-Performing cybersecurity Ecosystems

A broad range of complementary ingredients are necessary in order for innovation environment settings to flourish:

1. Sustained proximity to cybersecurity challenges
2. Provision of sustained talent flow
3. Strong ecosystem planning and oversight
4. Multi-faceted support from academia and research institutes
5. Appropriate funding supports
5.4.2.4 Funding of cybersecurity innovation

In a cybersecurity context more explicit funding supporting cybersecurity-based start-ups in Europe are emerging. For example, in June 2014 London-based C5 Capital became the first focused cybersecurity investment fund in Europe, providing a $125m fund for cybersecurity start-ups. So far two investments have been made, an $8m investment in monitoring provider Balabit, as well as investment in Qinetiq spinout Metrasens\(^{44}\). Managers of the fund now believe that European ICT and cybersecurity companies are now at an increased competitive advantage in Europe as a result of recent NSA surveillance scandals in the US, as such firms are not subjected to the same levels of data collection as their US counterparts. Traditionally, European cybersecurity companies have sought expansion funding to expand into US markets by default, but other markets such as the Middle East and Asia are now also seen as attractive alternatives\(^{45}\). Local European vendors will also always benefit from understanding the local needs of the region, often giving them a competitive advantage over US and other non-European vendors over others, but there is now increased demand for Europeans to provide alternative services to protect citizens and their embodied data in their own markets.

5.4.3 Define the cybersecurity value chain

Definition of “Cybersecurity” commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

Cybersecurity value chain challenges are shared between all pure players. Pure players are those who either have a cybersecurity product or a cybersecurity business unit. Other ICT players who are competing in other sectors, however their ICT solutions should be secure, are competing in other different sectors than cybersecurity, so their challenges are usually different.

European pure players in cybersecurity share:

- A common strategic market segment (cybersecurity),
- Same type of customers,
- Same trends,
- Same strategic challenges to overcome in the future

European companies which are competing globally, could benefit from a Digital Single Market, not only reducing market barriers inside European market but also it can be a tremendous opportunity to facilitate joint offering, mergers and acquisitions for having a more competitive offer from Europe as well as more competitive pure players and innovation chain.

As a first step, it is recommended to create and maintain an interactive catalogue of European Cybersecurity pure players as well as European clusters in cybersecurity to facilitate easy access to European products and services by any customer but also networking between all different actors inside the value chain to facilitate competitive advantage initiatives through joint offering, mergers or acquisitions.

It is also recommended to make a periodic (at least one per year) European cybersecurity market analysis in order to monitor revenue and growth (CAGR) indicators for European industries. Market analysis also allows the identification of different type of customers and their principal concerns while buying cybersecurity products. Individuals, governments (local, regional, national), SMEs, large enterprises, CIP operators, Defence, Home affairs are usually cybersecurity customers. Sophisticated demand concept is introduced as a catalyst for European cybersecurity industry by sharing ideas and opportunities as market challenges. For example finance, energy, CERTs, could be considered sophisticated demand in the way they probably know if a solution is available for a current or potential need. A good connection and intervention of sophisticated demand inside the innovation chain, could benefit the entire ecosystem ranging from researchers to pure players.

\(^{44}\) http://www.c5capital.com/
\(^{45}\) http://www.scmagazineuk.com/vc-funding-for-european-cybersecurity-firms/article/356360/2/
Market segments today range from ICS (industrial control systems) and CIP to monitoring and intelligence.

Common challenges for European pure players in cybersecurity might be:

- Market knowledge
- Sharing intelligence
- Local/regional/national market development
- International market (DSM and beyond)

Activities at European level along above axis could benefit the entire European value chain competitiveness.

The market is fragmented with at national and international level, with big players moving to lead different segments and product types (ranging from basic to corporate, or even industrial).

Key factors for CISOs are interoperability with legacy infrastructure and usability of each solution.

Public procurement, instruments definition to boost local procurement, incubators, accelerators, investors and venture capital dissemination as well as the promotion of cybersecurity talent are key differences from global leaders like US and Israel.

The definition and support by this cPPP of collective actions, either direct or indirect projects, could benefit the positioning and competitiveness of European Value Chain.

The value chain of pure players in cybersecurity arena includes:

- Manufacturers (SW, HW and mixed)
- Channel (wholesale and distributors)
- Services (integrators, consulting, managed security service providers (MSSP), value added resellers (VAR) and specialized services providers.

End users or customers represent the last mille of the value chain ranging from sophisticated demand to individuals.

Governments, clusters, forums and other IT related associations play a major role in the cybersecurity value chain.

In addition, there are also research and innovation providers, training providers, funding or venture capital events for entrepreneurship and start-ups initiatives.

The cybersecurity industry may keep a balanced representation of each type of entities along the whole value chain.

Today, manufacturers, MSSP and specialized service providers represent most of the industry representation today.

A differentiator of the cybersecurity industry is that we see far deeper integration in value chains of companies than traditionally the case. Delivering spare parts for an automobile producer does not require utterly deep integration into business procedures and operations of that producer. However, implementation of an early warning and threat detection system that scans all of the producer’s communication traffic in order to identify anomalies is a rather deep integration into the company inner workings.

The cybersecurity market is deeply influenced from various themes driven by technical, human, societal, organisational, economic, legal, and regulatory concerns among others; these factors combine to create marketplace and innovation ecosystem with complex value chain relationships.

Value chain positioning in the cybersecurity domain impacts on innovation focus and capacities; much of the innovation in the domain can be characterised as incremental (e.g. integrating components of technology from suppliers, tech plug-ins for a platform or providing a service wrap around technology delivery), as opposed to radical new developments that forces businesses to re-organize or leading to the emergence of wholly new markets.

A supply chain connects inputs to outputs by representing different stages of production. Supply chain analysis offers insights into the production of cybersecurity and privacy-enhancing goods and services. It allows the description of vertical relationships that exist between market players and their integration at different levels of the production process. Interrelations in the production of cybersecurity products and services are becoming more important the more functions are outsourced to partner firms.
Note that in today’s digital markets, it is not sufficient to speak about vertical relationships, as is done here for exposition reasons, networks of suppliers and buyers characterize these markets. Through increased integration, cybersecurity risks are shared between ever more partners in the supply network.

The supply chain analysis facilitates also a better understanding of the incentive structures inherent in vertical relations, because the firms’ contracts state rules on:

- The allocation of value added (and revenues extracted) in the production process between the different actors in the supply chain; and
- The allocation of risks and liabilities related to the production and provision of the security goods and services.

Firms may vertically integrate in order to internalize mark-ups or to offer a broader product portfolio. At this stage, there are a number of open questions. For example, it is an open question whether in cybersecurity markets, firms also vertically integrate hardware, software and services in order to obtain full control over the security of their supply chain. It is also not clear, if greater disintegration increases cyber-risks (i.e. through linkage attacks) and therefore negatively affects the resilience of ICT systems.46

While many still see the supply chain as a physical entity, digital services and product provision allows companies to deeply integrate into each other’s supply chains. One example is the outsourcing of real-time surveillance of networks to IT-companies. Another are e-forensics and e-discovery, where the contracted consultant scans vast amounts of diverse internal and sensitive documents (PDFs, e-mails, Word documents) and therefore obtains deep insights into a firm’s business dealings and secrecies. As stated above, in order to deliver secure cybersecurity products and services, the supply chain needs to be secure. Some interview partners put forth that in Europe there is an over-reliance on products developed outside of Europe.

The management of secure supply chains is a critical question not only for firms active in the cybersecurity business, but also for critical infrastructure industries. In the former, however, industry stakeholders often describe cybersecurity as part of their company’s DNA: In order to develop secure products, product development and production must be based upon secure processes and inputs.47 And the same must hold for the idea development stage. Some companies therefore establish an extra monitoring department that ensures whether security products have been developed securely. In the ICT business and the ICT security business, secure supply chain management includes software, hardware, business procedures and overall system architecture. Vulnerable software aside, hardware is also exploitable (e.g. by containing manipulated microchips). Further, hardware and software interact and both depends on each other.

The management of cyber-secure supply chains is also important in critical infrastructure organisations including banking and finance, water and utilities, and the health sector. These are – as end-users of products and services – at the final stage of the chain that needs to be secure in order to allow a secure operation of critical infrastructure.

Synonymous with ICT markets in general, cybersecurity firm-level innovation challenges transcend infrastructural, market, knowledge, cost and regulatory/legal domains. Typically, cybersecurity innovators’ competencies and investments are predominantly directed in the early phases of the innovation lifecycle (ideation through to concept development); whereas significant scope and requirements occur in the latter stages (test and implementation). Accordingly, the cybersecurity stakeholders surveyed identified a broad scope for innovation supports across the entire innovation value chain and ecosystem (i.e. strategy, business intelligence, ideation, portfolio management, resource management development, and launch).

Resonant of the ‘crossing the chasm’ debate, there are strong levels disconnect between ICT security researchers technology innovation and accompanying business development/diffusion innovation skills and acumen. While the imperative of underpinning innovation development activities with sound commercial business cases is recognised, competency and proficiency in this area is severely deficient.

47 The same holds for services.
Highly commoditised mass-market PACs product segments, with low levels of differentiation at the commercial level, and differentiation that is difficult to validate at the technical level. This makes it harder for PACs end-users to select and evaluate products, and for PACs innovators to differentiate themselves in the marketplace.

Very high market barriers to entry in established supply-side market segments, namely those serving (1) Larger Enterprise, (2) Government, and (3) Military/Defence.

Difficulty in creating ROI arguments and compelling value propositions around cybersecurity products, especially as next generation PACs products become more complex and expensive. This is being offset to some extent by growth in demand for Managed Security Services (MSS) and similar forms of outsourced security solutions.

Extending research into the behavioural aspects of legitimate stakeholders and malicious actors within the cybersecurity environment could further our understanding of underground markets and the threat landscape.

5.4.4 Boosting SMEs

Europe is 95% SME market, in the cyber domain SMEs are even more dominant. Therefore, SMEs should be the backbone of the European economy by developing R&D that enhances global competitiveness and plays a relevant role in raising the level of cybersecurity solutions for market demand. Yet recent statistics show that the number of European SMEs innovating in-house or collaborating with other companies on innovation or market-oriented projects is still too small. They often lack organisational resources, capacities, and knowledge.

SMEs need practical, hands-on support to overcome this challenge, particularly as new value chains develop that cut across transversal industrial sectors demanding cybersecurity products.

Essential barriers that avoid penetration of SME’s into European cybersecurity market has been classified in the following categories:

a. Difficulty accessing to European cybersecurity market consumers

Scalability is a challenge for SMEs that usually initiates their activities in their own country market, finding serious obstacles for internationalisation. The European cybersecurity market is taken by a reduced number of global brands, mainly non-European-based companies.

So European SME’s are usually forced to compete in a hostile environment and export efforts become too challenging, as big ICT security players protect their niches from newer and outer menaces and competitors benefiting from their strong market presence and adjusting of costs to enhance competitiveness. Smaller companies are confined in local markets and still dependent on public procurement in their home country.

b. Difficulty accessing finance for innovation

Shortage of the SME’s own financial resources is a seemingly perennial problem, but one that has certainly been exacerbated by the recent global financial crisis and current economic slowdown. Innovation is costly, and companies face investment choices regarding scarce resources. Innovation is often in competition with other business functions for this investment.

c. Lack of innovation and market-oriented management skills in SME’s

Market processes need to be managed from the generation of innovative ideas to the generation of profits with new products/services. Moreover, an increasingly complex innovation system combining ‘open innovation’ approaches with closed ones requires more sophisticated management skills.

d. Weaknesses in networking and cooperation with clusters, research communities and external partners

Successful innovation is highly dependent on the identification, cultivation and maintenance of good linkages between the different components of the global value-chain, and as ‘open innovation’ becomes more embedded in SME business strategies.
5.4.5 Bottom-up track for Cybersecurity Innovation

The European Union is determined to strengthen the cybersecurity industry to transform new ideas into commercially attractive products, processes and services while taking the necessary action to define a framework build on minimum requirements to security and privacy.

A specific funding mechanism is crucial for the competitiveness of European cybersecurity industry to fuel trusted innovations. The “Bottom-up Track for Cybersecurity Innovation” aims at reducing the time from idea to market, stimulate private sector investment and to take best-in-class-innovations on a fast track to outpace international competition. For cybersecurity and privacy innovations industry can propose any R&I topic related to any sector. This track aims at complementing the pre-defined pillars as well as set priority R&I topics. This gives maximum flexibility to push emerging and disruptive ideas of any kind forward, which is a necessity in increasingly challenging changing IoT world. It supports quick deployment and market take-up of innovations while reducing the vulnerability risks.

Scope: The Bottom-up Track supports projects related to any topic, sector or challenge undertaking innovation from the demonstration stage through to market uptake, including stages such as piloting, test-beds, systems validation in real world/working conditions, validation of business models, pre-normative research, and standard-setting. It targets relatively mature new technologies, concepts, processes and business models that need a last development step to reach the market and achieve wider deployment. To this end, if a proposal involves technological innovation, the consortium must declare that the technology or the technologies concerned are at least at Technology Readiness Level (TRL) 6, where appropriate.

Impact: Fast development, commercial take-up and/or wide deployment of sustainable trustworthy innovative solutions (products, processes, services, business models etc.) in enabling and industrial technologies and/or for tackling societal challenges. Increased industry participation, including SMEs, and more industry first-time applicants to Horizon 2020.

5.4.6 Standardisation, regulation and certification

5.4.6.1 Standardisation

As a common enabler for cybersecurity activities the standardisation process should evolve into a coherent, proactive, transparent, inclusive (open to all stakeholders) process.

As an example, the near future of Smart Infrastructures may need processes and resources more adaptive, decentralized, transparently collaborative and efficiently controlled. The more pervasive usage of ICT to comply with such requisites the more interoperable and hyper-connected it must be.

Due to the dynamic nature of cybersecurity and its threats, new products and services may need to be deployed continuously at the same time they should co-exist with other legacy systems still under depreciation, so interoperability is a major challenge. An equal level playing field for security and privacy in the EU and its 28 Member States and the other countries participating in the cPPP is key for creating trust in the Cybersecurity market.

The exponential explosion and availability of new ICT solution based on products and services as well as the diversity of components, applications and services, created, integrated and deployed from anywhere in the world, may need an extra effort of standardisation if we want any end-user to trust cross-boundary interoperable and privacy guaranteed communications as an example. First, better political and regulatory support is needed for a cross-border effective approach, and secondly, an industrial transparency of hardware and software components and functionalities used may happen. It should guarantee an appropriate balance between harmonisation through standardisation and innovation for standards. Regulations shall give guidance to standardisation by

- Establishing minimum requirements for security, privacy and trustworthiness,
- Ensuring high degree of interoperability and openness to innovation.

Following this guidance and in order to prevent too divergent practical implementations, these standards could develop respective profiles which offer practical implementation guidelines regarding specific technologies. Besides, the European Standardisation body should receive the mandate to elaborate new security and privacy standards earliest possible, e.g. not waiting until the ICT rolling plan is validated by the Multi-stake holder platform (MSP).
Cybersecurity must be considered as industry-transversal impacting many markets. As such, it needs to take into consideration the different markets where cybersecurity is critical. Moreover, the introduction of smart and connected objects is creating new and increasingly more security considerations on new markets. It is important to assess if the standardisation and certification schemes in place are effective toward those new problematic. The European standardisation bodies shall be commissioned to conduct a full assessment if and in which form standardisation and ICT related standards shall be updated.

There is a business opportunity for the European Industry to be the blueprint in privacy and security-by design to end users with crypto standardisation, its interoperability and usability is still being a challenge currently hindering a widespread adoption. Pre-standards can drive a faster adoption of R&I results by the industry. But at the same time policy makers shall enable a more effective policy creating an equal level playing field for security and privacy. Instead of plugging holes and fighting hazards (hacks, leaks, spying) regulation shall define minimum requirements as guidance and give trust to end users and planning certainty for industry.

5.4.6.2 Regulation

Standards may play an important role in the elaboration of legislation and regulations dealing with technical matters, such is the case of cybersecurity. In this an area the European legislation has at least four main horizontal instruments in force or close to be adopted (NIS, GDPR, eDAS, CIP) that need to be transposed and implemented at national level, and may require the adoption of more detailed secondary legislation at European level (i.e. implementing or delegated acts). Additionally cybersecurity aspects are more and more frequently considered in specific sectorial legislations, which may also need to rely on standards to define technical requirements.

A well-established tradition of cooperation between the European institutions and the ESOs (in particular via standardisation mandates) allows timely availability of the standards needed in legislation, and facilitates the contribution of the technical expertise from NSOs to the legislative process. Furthermore, Member States and the other countries participating in the cPPP may be easily involved in the standardisation process through its representation in NSOs. For all these reasons European Standards shall be taken as the default option for any technical requirement to be included in legislation or in its implementation.

This is particularly important in case of mandatory features of technical characteristics that may be imposed as “essential requirements” for specific products or systems. The New Legislative Framework (NLF) together with the CE marking system, which guarantees compliance with the relevant European Standards, has proved to be an efficient mechanism for the definition and supervision of those requirements while promoting the internal market in many areas, including highly sensitive areas\(^{48}\). It should be then the reference for the adoption of any mandatory technical requirement and its conformity assessment in the areas of cybersecurity.

Finally, technical specification and minimum security requirements also play an important role in public and private procurement processes procurement processes, which on the other hand may be used as a driver for the adoption or promotion of specific facilities or technologies. Special attention should be paid to the influence of the technical specifications for cybersecurity requirements in public and private procurement processes, which should be based as much as possible in European Standards, while fully respecting the relevant European legislation on public procurement (in particular Directive 2014/24/UE).

5.4.6.3 European Cybersecurity quality/trust label

There is a recognized need for a European Certification for cybersecurity products and corresponding Trust Labels. As suggested in topic 110 of the EP resolution of March 12th 2014). A European trust label for cybersecurity products, services, and mutual certification, respecting European values / sovereignty and empowering the national CERT (complement to national trust labels) shall be created to help identify trusted European products and services: it could use existing labelling procedures such as the CE Mark, Ecodesign or Energy Label. Support of lightweight labels such as “IT security made in Germany”, “France Cybersecurity” can be raised in addition as needed.

The creation and operation of European Cybersecurity Labels plus a transparent certification mechanism shall follow a defined set of criteria – based on generic, technology neutral and sector agnostic minimum requirements which should be – as far as possible – be testable and measurable throughout the entire product lifecycle. This would benefit label holders as a seal of guarantee of security as well as privacy in products or services, and can help

\(^{48}\) E.g. civil explosives, lifts or measurement instruments, and will be soon applied in pyrotechnic articles medical devices, gas appliances or personal protective equipment, among other areas
corporates and consumers to identify secure providers. Labels shall be built on best practices and internationally recognised existing certifications. The benefit of this European label resides in its European-wide recognition and acceptance, thus helping to fight the defragmentation of the European market, and creating competitive advantages with the creation of stronger market positions for trustworthy companies. Besides, a label will define the basis for a European equal level playing field and international products will have to follow the defined quality and trust level to stay competitive.

Different levels for the label can be devised, corresponding to increasing levels of security and privacy in the products and services (e.g. from G to A+++). Citizens, customers or companies of these products shall not be obliged in any way by law or regulation to buy higher labelled products. But with a defined level of basic security and privacy, they will choose better quality over time as transparency as well as awareness help them to make better buying decisions. Where labels have been used, compliance to the label requirements must be monitored and regularly checked. The set of requirements, methodology and process for the certification of trusted solutions, ought to be defined at the European level, coordinated by an European-level agency like ENISA in agreement with national security agencies of Member States and of the other countries participating in the cPPP (CERT), while enforcement can be delegated to national agencies in charge of cybersecurity practices. The set of requirements will be a single one for the whole of Europe (baseline) but the implementation will be under the responsibility of the national CERT. The National CERT can decide to sub-contract the Label award to some non-profit association.

The set of requirements, methodology and process for the certification of trusted solutions should be generic, technology neutral and sector agnostic and should focus on the entire lifecycle of ICT products rather than on test snapshots at a certain point in time of development. This implies that the verification of requirements should be possible throughout the entire lifecycle of the ICT product and linked to contractual requirements towards the supplier in order to enforce continuous compliance. By linking those minimum requirements to national and EU-wide legislation (NIS), it can develop a strong market pressure towards ICT providers to provide more secure and trustworthy solutions and services.

Some critical infrastructures at the national level might require some specific local criteria. In this case, additional local criteria will come on top of the baseline criteria. Compliance validation shall be conducted in the same manner by any national agency, and shall be recognised European-wide. The setting up and operation of this label mechanism will imply costs, so resources must be allocated to put this mechanism in place. The requirements for the basic level of label shall be defined at European-level. Higher levels shall be in the realm of sectoral stakeholders (Automotive, Health, Energy, etc.) in accordance with their respective regulatory authorities.

5.4.6.3.1 New certification processes

The current European certification process for security products is a worldwide reference and it is used in most of the countries in world that want to have a resistant product against potential attacks. It is even reference by the major payment brands for their security certification.

The new European certification process shall be based on this long-term experience and we should extend it to following the new cybersecurity eco-system.

Common Criteria evaluation scheme and European SOGIS MRA shall be leveraged and extended. A sector approach – energy, automotive, health, …- should be developed further together with the active participation of private stakeholders: the deployment of a security certification scheme supported by advanced Technical Communities (aTCs) can be considered. SOGIS MRA members and private stakeholders - suppliers and evaluation labs – will work jointly in advanced Technical Communities to run per-sector security certification schemes.

5.4.7 Societal aspects

As pointed out in the NIS Platform WG3 SRA, the development and implementation of raising awareness campaigns on cybersecurity for society at large, including companies (large and especially SMEs) and citizens, is of major importance, as ICT and its applications are changing so rapidly, alongside with their subsequent risks. While it is currently unclear who is best placed to take responsibility for these activities and would have the resources needed, national initiatives exist. For instance, in Portugal, public and private organisations have joined forces in the recently
announced prevention seminars targeted to businesses and residents. While this focus is often focused more on the concept of safer communities as a whole, the joint model is highly relevant to the cybersecurity domain as a whole.

Therefore, cPPP members could spearhead, along with the support of ENISA and relevant Member States and other countries participating in the cPPP actors, and H2020 projects expertise, and undertake a new paradigm shift towards raising awareness campaigns in relation to cybersecurity to a wider variety of public and private stakeholders.

The cPPP could act as a catalyst in this awareness raising activity as they could be responsible for centrally collecting information that could be used from various sources, from projects, Member States, other countries participating in the cPPP, trans-European bodies (ENISA) and they would be well placed to assist in the planning and implementing of raising awareness activities, if given proper resources.

The benefit of having the cPPP carrying out a central role in this activity would be their close proximity and awareness to the stakeholders that would gain maximum benefit, if given the right information within a reasonable time frame to attain maximum benefit.

5.5 Estimated budget

Given the current time frame we analyse the budget for 2017-2020 also considering that most of the topics have been also fixed already in the appropriate committees for 2016 (and mostly 2017).

We tried to balance among the different instruments, including the ratio between research and innovation activities, providing slightly more relevance to the latter.

It is estimated that for an entire programme of 4 years, and where projects will of course continue to run several years beyond, an investment of approximately €850M (with an hypothesis of €450M from the European Commission – note that following H2020 reimbursement rule, the EC contribution of €450M is roughly balanced by a contribution from project partners of about €400M) would be required to be allocated between 2017 and 2020. Given the current trend and the significant role of innovation in the cPPP Cyber, a tentative budget sharing has been developed:

- 40% of the budget will be allocated to research and innovation or related activities,
- 51% in Cyber Infrastructures (integration and demonstration) to bring innovation close to market
- 6% to projects developing the ecosystem
- 3% to coordination and support activities.

The estimated budget initially depicted by the cPPP SRIA WG is presented below. It is currently given in a coarse grain format.

The rationale for the following simulation of budget distribution is based upon the following elements.

The budget distribution over the 4 years (EC contribution + contribution from project partners) is considering in 2017 the amount presently envisaged in the ongoing call for proposal (ending August 2016). Also the distribution of the budget allocated in 2017 among the different priorities is following (as much as possible) the existing work programme. The budget in the following 3 years is more or less stable, for an average annual overall amount of roughly €250M.

Looking at the budget distribution in the different actions, the 6% budget (i.e. about € 50M over 4 years) for the development of the ecosystem, is roughly constant over the years, with a slight increase after 2017, for a possible better support to testing tools and education activities.

The distribution of 3% in coordination and support actions (i.e. almost € 30M over 4 years) is constant over the years.

The two main areas where the budget is distributed are the R&I actions (i.e. the technical projects based on technical priorities) with 40% (i.e. € 340M budget) and the Cyber Infrastructure actions (i.e. products / services for different applications) with 51% (i.e. € 433M budget).

While research activities will increase and peak in the middle of the programme, the innovation actions of novel applications and technologies (the “cyber infrastructure”) will start with an offset. Indeed, after the relatively limited value for R&I activities in 2017, the budget will more than double to provide strong support to new technologies and services.

The distribution of the €340M among the different topics (according to the provided product / services segmentation) has been divided in the 5 main areas:

- Assurance, security and privacy by design: 12% of the R&I actions budget
- Identity, access and trust management: 11% of the R&I actions budget
- Data security: 19% of the R&I actions budget
- Protecting the ICT Infrastructure and enabling secure execution: 44% of the R&I actions budget
- Cybersecurity services: 14% of the R&I actions budget

The budget for “Assurance, security and privacy by design” could look relatively high from an industry / economy point of view, but is considering the priorities imposed by the “societal security” approach.

The budget for “cybersecurity services” could look relatively low, when considering the high expected growth of the service sector. Likely this value, initially estimated by the SRIA technical experts, will be updated in the future when better leveraging upon marketing / industrial experts.

The budget for “Protecting the ICT Infrastructure and enabling secure execution” could look quite high (also 50% of the overall R&I actions), but we estimate that this is the core area where there will be strategic market evolutions in the future, and where European solutions will be needed, for instance of threat identification and management, for overall system security including IoT, 5G and other mobile devices, for cloud security etc. The D priority in Cyber Infrastructures (Secure Networks) is actually gathering several high priority elements. For this reason, its budget is considerably higher than the other priorities.

The budget for “Cyber Infrastructure” of €433M is divided in three areas:

- Integration Projects (for validation of existing technologies): 52% of the “cyber infrastructure” budget
- Demonstration / pilot projects (solutions implemented in different applications) : 38% of the “cyber infrastructure” budget
- Bottom up track on innovation (a new instrument to reduce the time from idea to market, stimulate private sector investment and to take best-in-class-innovations on a fast track to outpace international competition) : 10% of the “cyber infrastructure” budget

The budget for “Demonstration / pilot projects” is more or less equally spread across the different main vertical applications, with some priority given to those applications where Europe is leader.

The budget for the “bottom up track on innovation” is quite limited, as considered for the moment as a “tentative approach”.

The budget for the integration projects is quite important and is divided into the main areas for transversal validation of innovative technologies and services. Particular emphasis is given to the area of secure networks and ICT, as considered fundamental and strategic for Europe and the possibility to develop solutions in sensitive / strategic areas where an increased Digital Autonomy is needed.
### CYBER PILLARS

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>TOTAL</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustworthy Innovation Ecosystem</td>
<td>10</td>
<td>13</td>
<td>14</td>
<td>14</td>
<td>51</td>
<td>6.0%</td>
</tr>
<tr>
<td>Technical Experimentation Ecosystem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>36</td>
<td></td>
</tr>
</tbody>
</table>

### RESEARCH & INNOVATION ACTIONS (technical projects based on technical priorities)

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>TOTAL</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustworthy Innovation Ecosystem</td>
<td>44</td>
<td>107</td>
<td>98</td>
<td>90</td>
<td>339</td>
<td>39.9%</td>
</tr>
<tr>
<td>Technical Experimentation Ecosystem</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 3.1.1 Priority “Fostering assurance and security and privacy by design”
- 3.1.2 Priority “Identity and Access Management”
- 3.1.3 Priority “Trust Management”
- 3.1.4 Priority “Data security”
- 3.1.5 Priority “Cyber Threats Management”
- 3.1.6 Priority “Network Security”
- 3.1.7 Priority “System Security”
- 3.1.8 Priority “Cloud Security”
- 3.1.9 Priority “Trusted hardware/ end point security/mobile security”

### CYBER INFRASTRUCTURE (products/services used in different applications)

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>TOTAL</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Projects (validation of existing technology solutions)</td>
<td>20</td>
<td>63</td>
<td>71</td>
<td>70</td>
<td>224</td>
<td>50.9%</td>
</tr>
<tr>
<td>A) digital citizenships (including identity management)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B) risk management for managing SOC, increasing cyber risk preparedness plans for NIS etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C) information sharing and analytics for CERTs and ISACs (includes possibly trusted SIEM, cyber intelligence)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D) secure Networks and ICT (secure and trusted Routers, secure and trusted Network IDS, secure integration, Open source OS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Demonstration / Pilot Projects (solutions in different applications)

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>TOTAL</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy, including smart grids</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart &amp; Secure Cities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Services / eGovernment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industrial Critical Systems / Industry 4.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bottom up track on Innovation</td>
<td>0</td>
<td>13</td>
<td>14</td>
<td>17</td>
<td>44</td>
<td></td>
</tr>
</tbody>
</table>

### COORDINATION (Stakeholder cooperation for Roadmapping Dissemination & Communication; KPI monitoring activities; MS cooperation; International Relationship; EU observatory; Governance, ...)

<table>
<thead>
<tr>
<th></th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>TOTAL</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>27</td>
<td>3.2%</td>
<td></td>
</tr>
</tbody>
</table>

| | 100 | 248 | 254 | 248 | 850 | 100.0% |
6 Expected Impact

6.1 Expected impact on strategic objectives

The expected impact of the cPPP should be recognised in developing the cybersecurity domain from multiple points of view. Since the overall goals are rather wide, cybersecurity being a transversal topic, a holistic approach is needed. Thus the effect will reveal itself in many ways and impact many stakeholders – cybersecurity products and service providers, users from the public and private sector, academia as a collaboration partner but also a growing ground for more specialist for the field, critical service providers, policy makers, but also wider society through awareness raising initiatives and security solutions for a broad-based use.

Following is a summary list of main impacts:

- **Stronger support for secure implementation of European Digital Single Market** will emerge *market increase growth and job in European market*. The implementation of the DSM will bring along even higher digital dependency and even more connectivity between different critical ICT solutions cross-borders. Thus, the security aspects in its implementation need a more systematic approach as the chain is as strong as its weakest link – all Member States and the other countries participating in the cPPP need to put efforts into strengthening their capabilities and collaboration under the umbrella of the cPPP. The cPPP will create a fertile ground for harmonising the capabilities. This collaboration will also create a cross-border spill-over effect for strong cybersecurity solutions and provide a format for regular debates about best ways to move forward. Needed technical solutions will be developed to support the secure implementation of Digital Single Market and Europe will ensure an increased digital autonomy – in particular for sensitive applications – by making sure that strategic components are either developed on a full European base or meet the necessary requirements set for trusted supply chain components.

It is also important to recognise that the expected impacts of the cPPP go beyond those directly related to the cybersecurity industry. In fact, the wider strategic objectives of the cPPP address the challenge of protecting growth in the European Digital Single Market from cyber threats and, at the same time, there is an associated potential positive impact of the availability of (innovative) trusted cybersecurity solutions on growth prospects of European companies in other key and strategically important sectors (e.g. health, energy, transport, communications, public services, etc.) that depend on cybersecurity solutions.

- **New technological solutions and services** will be developed and piloted to fill the existing market gaps, especially to support adapting to new emerging technological realities (IoT, cloud computing, etc.). Collaboration between different sectors and stakeholder groups will be enhanced to have a better understanding of the needs and existing solutions and competences and to identify the gaps that need to be filled.

- **Acceleration of the Europe’s innovation process and time to market**. In order to stay ahead, European innovative technology start-ups and companies will have the possibility to cooperate with the large European enterprises, public sector and research organisations to productise the existing core technologies and facilitate creating functionally and commercially successful use cases. Piloting and deployment programs in cooperation with public and private sectors adopting these emerging technologies in cybersecurity and data governance in large scale will be facilitated. Collaboration mechanisms will be brought to life to find synergies in developing new innovative solutions, especially for SMEs.

- **Mobilisation of public and private resources to provide contribution to the development of trusted European solutions and implementation of a European cybersecurity policy for the development of European cybersecurity industry**. The focus of investments should be targeted towards two directions:
  - Amplifying already existing strengths in cybersecurity industry, creating synergies and boosting the competitiveness of the cybersecurity industry and SMEs in particular;
Creating strong European-based offering to meet the needs of the emerging technological realities and cover strategically important areas.

This approach would facilitate the use of certified, trusted solutions in vital areas for European society (e.g. ICT infrastructure and public services) and in applications where Europe is a market leader (e.g. aeronautics, car manufacturing, finance services and in general all the areas impacted by the envisaged Industry 4.0 / smart manufacturing approach). Areas of higher competence in Europe like Identification and Access Management (for instance security of smart cards) as well as Data Security (e.g. encryption) should be continuously improved to maintain leadership, while competitiveness should be increased in strategic components for Network Security Systems and Management of Security Services.

- **An integrated training and exercises ecosystem** will be built to support experience exchange, skills development, awareness raising, profiling, product testing and much more. The existing ecosystem components will be federated and the environments will be opened for many more stakeholders than they are today – e.g. wider use by universities, SMEs, critical service providers, policy makers etc.

### 6.2 Description of Industry commitment

The cybersecurity cPPP will define, structure, and organize the research and innovation actions needed to boost the European based cybersecurity offering, to achieve the expected societal, economical and industrial impact foreseen in current proposal.

The cybersecurity stakeholders will establish a non-for-profit Association (ASBL) located in Brussels. It will act as the legal representative of the core cybersecurity industry and research stakeholders in the cybersecurity partnership contractual arrangements according to Article 19 in “Regulation of the European Parliament and of the Council, establishing Horizon 2020 - The Framework Program for Research and Innovation (2014-2020)”. See Section 4 on Governance for further details.

The non-for-profit Association’s Statutes and Bylaws have been prepared and are currently in final negotiation between the legal departments of the Association’s members and will have at the time of evaluation entered into the administrative process to receive the Royal Decree for establishment. One of the major tasks of the industry Association is to regularly update the SRIA and maintain a set of research and innovation objectives that keep pace with the speed of technology and application advancements particularly prevailing in the cybersecurity domain.

The SRIA is based on the broad consent of Stakeholders. In fact, user requirements and demands were collected during the preparation phase of the SRIA and these requirements are integrated into the cybersecurity Strategic Research and Innovation Agenda. Feedback and public consultation responses were used to refine and finalize the initial SRIA.

After the consent from the Commission, the cybersecurity SRIA will be implemented following the guiding principles of inclusiveness, transparency and representativeness and the open and competitive call procedure for Horizon 2020.

The actors behind this proposal will strongly engage in participating in the projects as described in the proposal. They will aim to take a leading role in implementing the SRIA with the project instruments available. The industry behind this proposal represents a significant part of the cybersecurity cPPP participants. It is clear though, based on other industry lead cPPPs, that the total number of industry participants will be significantly larger than the initial actors behind the proposal.

The commitment for project activities running in the context of the cPPP is targeted to add leverage factor of 3 in addition to the contributions done under Horizon 2020 instruments.

Strong focus is on delivering new and innovative cybersecurity solutions as results of the projects. This goal will only become a reality if solutions and services meet the requirements of users (government agencies, businesses and citizens). Thus strong emphasis will be on setting up the consortiums with balanced membership including users as piloting partners to validate the deliverables of the projects.
A focus of the cybersecurity cPPP will also be to assure that sufficient ecosystems are developed to support achieving the goals of the proposal. Ecosystems will support raising awareness (thus generating the need), advancing skills, providing a range for trainings and exercise, growing competent resources, enabling testing for innovative solutions, risk profiling of organisation etc. Members of the Association will also commit to collaborating on creating training modules and study materials to integrate cybersecurity education on all levels and cross-domains.

Large companies and ICT SMEs will be offering cybersecurity services and secure ICT solutions to European and global end-users and organisations. Exploitation is the ultimate goal of the research and innovation and supporting activities of the cybersecurity cPPP. Substantial demand has been identified and the market size is growing. The cybersecurity cPPP will support industry taking the risk to invest on the scale that is necessary to offer competitive solutions that will be taken up by the market.

The ECSO Board of Directors and the cPPP Partnership Board will monitor the progress and impact of the activities implementing the program. The initial set of KPIs will be monitored and with the help of key stakeholders regularly reviewed and, if necessary, revised to maximize the outcome of the cPPP’s research and innovation activities.

Overview of how industry investment is leveraged outside the program (described in chapter “Ability to Leverage Additional Investments”) will be monitored by the Association and presented at the Partnership Board. It is envisaged that the cybersecurity cPPP projects will be catalysing further industry research and innovation activities through market orientation developments.

6.3 Ability to Leverage Additional Investments

The economic and industrial relevance of the scope of the cybersecurity cPPP will further facilitate R&D investments of funding actors in addition to and beyond the engagement of the public side in this partnership. In other words, EC investments within the partnership will leverage and stimulate further private investments.

The amount in collaborative research programs of the European Union is significant and has increased steadily from program to program. In the timeframe 2016-2020, which should (partly) correspond to the running period of the cybersecurity cPPP, the budget amount concerning ICT will increase every year, from EUR 1.0 Billion in 2016 to €1.3 Billion in 2020. While the European funding amount in research programs is increasing, the total private sector directly or indirectly leveraged investment related to the research areas is significantly higher. Much of it is triggered by collaborative research, which paves the way for the development of common specifications, shared views on solutions and consensus building towards future adoptions. Consequently, a strong leverage effect from the public investment by the European Commission in research in the cybersecurity cPPP needs to be coupled with private investment in R&D for systems and in the scope of the ECS cPPP.

Once again, this cPPP is different from other from another point of view: the expected public (non EC) contribution to the leverage factor. Indeed, in initial discussions with national and regional public administrations, they have on one hand declared their strong intention to participate in the cPPP and ECSO, having an important management role, but also to contribute to the leverage factor. Examples can be given at national level, when national initiatives, linked to R&I, envisaging budgets in sectors of relevance to the SRIA priorities could well be correlated to the ECY KPIs and the leverage factor. Also at regional level, we received expression of interest from local public bodies that would not only participate in the cPPP but also have declared the will to flag specific budgets (e.g. European regional / structural funds) dedicated to cybersecurity (e.g. for education and training, for supporting local research, but also for innovation in the cyber protection of vital infrastructures and services).

The link between the SRIA priorities with its R&I priorities which are the target of the ECS cPPP and the policy support activities which are one of the main targets of the ECSO Association is essential to get the commitment of the private sector and reach a satisfying leverage factor as envisaged in the cPPP H2020 rules.

Different sources of investments will be sought in the context of the cybersecurity cPPP not just because they are needed as previously explained, but also because a much wider plethora of stakeholders should be formally involved in this endeavour. Such additional sources can be categorized into:
• **Independent Industrial Research and Innovation:** R&I investments in cybersecurity technology and application is already part of the strategy of many global and European ICT companies including large and small size actors behind this proposal such as for example Airbus, ATOS, BT, CEA, Engineering, Ericsson, Finmeccanica, Guardtime, Infineon, NXP, Secunet, Telefonica, Thales, etc.

• **Increasing number of contributors from different sectors:** The cybersecurity cPPP implementation will likely involve at least 150 organisations already in 2016, and to grow at the rate larger than 30% in the first years. The experience from other PPPs like FI PPP shows that between 150 and 200 organisations are participating in the research activities having started from a smaller initial core of participants. Here the expectations and the participation seem to be much higher. Indeed, there is a significant Industrial participation in the cPPP which is much higher than the average of the rest of the Horizon 2020 programs. Participation of research organisations is still an indispensable element for the collaboration. The ambition of the Association is to involve many users of the created new technologies as verifiers of the necessity of the planned actions and to be piloting partners for new innovative solutions. The partnership of different stakeholders will further spur activities in technology and user companies to build R&I and take-up actions on top of it. Having users as driving partners involved, also building consortiums that involve a balanced number of solution providers and users (compared to academia) will support combining other investments with the investments of the Horizon 2020 instruments. Using Horizon 2020 funding to support go to market solutions that have proven a viable potential is the main key for finding potential for combining different sources for investments as this provides a way for potential users to mitigate financial risks. Boosting areas where the willingness of contributing to the R&D and driving from the users’ side is already high, has the best potential to achieve multiplication effect.

• **Structural Funds:** The number one of the thematic objectives of the European Structural and Investment Funds for the financial period 2014 – 2020 is to strengthen research, technological development and innovation, including enhancing research infrastructures and capacities or via "smart specialisation”. Smart specialisation especially targets innovation activities on regional level and aims to make more efficient use of European Structural Investment Funds and to increase synergies between different European, national and regional policies, as well as public and private investments. The Association in collaboration with the Member States and the other countries participating in the cPPP will focus special attention in finding ways to collaborate and combine these resources with the Horizon 2020 efforts. As ICT and cybersecurity has been defined as one of the key areas for smart specialisation in many Member States and as a key area in general in other countries participating in the cPPP, the fertile ground for funding amplification has already been created.

• **EIT ICT Labs KIC:** The KIC’s objectives are on education, research and innovation leveraging R&D achievements. In this context the aim is to leverage on the KIC to develop skills and competences on the basis of the cybersecurity cPPP developments. A MOU with EIT ICT Labs could be established to support training and education activities on new cybersecurity technologies.

• **National (research) Funding:** Several research programs in Member States and in other countries participating in the cPPP have been aligned to address cybersecurity. Examples of this realignment can be seen in Estonia where cybersecurity domain is one of the key investment areas for upcoming years in fields of education, boosting economy, supporting SMEs and start-ups etc. The cPPP is set out to collaborate with national initiatives to create synergies and avoid redundancies as much as possible. First steps are taken, inviting the representatives of those initiatives to collaborate in the Association that will coordinate the implementation of the cybersecurity cPPP. The cPPP will identify and establish ways to leverage other public and private resources continuously throughout its duration.

• **Previous Research Results and other cPPPs:** The cybersecurity cPPP will build its activities also on previous and on-going research performed within Europe (including those from existing related PPPs such as FI-PPP, 5G, Big Data Value, IoT, Cloud, etc.) and national programs as well as initial concepts from research and industry research independent from public research.

• **Incubators and Venture Capitalists:** More and more private organisations are providing private funds through dedicated incubators like VC Frost Venture Partners, Data Elite, SeedCloud or the fund launched by Nugg.ad in Germany. Startup Europe can also be a key enabler to support this development. Efforts European Cybersecurity cPPP – ECS cPPP – Industry Proposal
will be made by the Association to invite venture capital coordinators to collaborate in the Association to find synergies and amplify the effect of the funding for both sides.

A tentative simulation of the expected contribution from these funds and the allocation to the different stakeholders is given in Annex 1.

6.3.1 The leverage factor for industrial investments

Looking at the Article 25 of H2020 – Paragraph 3 we see that the leverage factor in a cPPP clearly relates to R&I.

For the H2020 definition of R&I (Art 2 of H2020): 'research and innovation activities' mean the whole spectrum of activities of research, technological development, demonstration and innovation, including the promotion of cooperation with third countries and international organisations, the dissemination and optimisation of results and the stimulation of high quality training and mobility of researchers in the Union.

There is no unique definition of how wide is the perimeter of R&I to be considered for the Leverage Factor in cPPP investments. We give here the position of the cPPP Photonics (under the condition that the exploitation takes place within Europe):

- R&I,
- Pilots & demonstrators,
- production - tangible assets, operational spending and human resources
- education and training
- investments in intangible assets, such as licensing and patent acquisition

The “Leverage factor” is defined as the financial ratio between two figures: the estimated (“private”) investments of related activities vs. the financial EC contribution to the PPP. In reality, there is no direct or unique relation between the EC contribution and most of these (“private”) investments.

The denominator of the ratio equals the financial EC contribution to the projects that are taken into consideration for the estimation of the leverage factor.

The numerator of the ratio is the estimation of the entire private or public (non EC) R&I investments that are related to the thematic and technological scope of the ECS PPP. These are investments done by supplier companies, public or private users / operators, technology or knowledge suppliers regardless of whether they participate in ECS projects or not. These investments are both related to the integration of the innovative manufacturing technologies and approaches in the products of the technology suppliers or the integration of the innovative technologies in European factories.

There are a number of challenges with respect to the interpretation of the sum of estimated R&I investment mobilised in the PPP projects and mobilised in other R&I activities related to the PPP:

- What investments should be taken into account?
  Investments that are related to bringing the project results into the market or full industrial application, could cover a period of at least 5 years after the project’ duration. The estimations should consider this envisages investments as well.

- How to identify the “R&I Investment mobilised in the PPP projects and mobilised in other R&I activities related to the PPP”?

Identifying the amount of the investments that are directly related to the developments done in an ECS project is not a trivial exercise. Considering that these investments are still necessary during a period exceeding 5 to 10 years after the project duration, identifying the amounts is challenging and resource-intensive.

These innovations are very much related to the scope and the outcome of ECS projects. The investments do not only cover the costs associated to acquiring or leasing the innovative manufacturing equipment, they also involve the internal and external cost (e.g. consultancy) associated to production engineering and ramping up the new systems. Furthermore, the ‘time gap’ between the formal project duration and the investments, the traceability of the relation to the PPP projects and the willingness to share the information are no trivial challenges.
A less obvious component of the ‘private or public (non EC) investments’ are those made by research
organisations, starting with the investment required for covering overhead costs that are not covered by the EC
funding.

- It is expected that those Members having participated at the creation discussion for the creation of
  the cPPP and in particular those that wants to have a driving role in the Association will engage on a
  higher contribution to the leverage factor.
- In the membership forms for ECSO we will request new members to declare how they will
  contribute to the success of the cPPP (at least wrt 5 KPIs) and how they will contribute directly or
  indirectly to the leverage factor.
- A similar suggestion could be made also to be considered by evaluators when scrutinizing the H2020
  proposals before attribution of the impact note.

As introduced previously, the ECS cPPP, differently from other cPPP of the E. Commission, the contribution to the
leverage factor coming from the private sector can also be complemented by public sector investments from
national or regional administrations investing in major or local programmes dedicated to cybersecurity (e.g.
education, innovation of cybersecurity for critical infrastructure, national R&I etc.).

In a broad sense the ‘leverage’ of a cPPP is more than a number calculated as the ratio between investments and
European funding. Possible dimensions of leverage are:

- **At private company level**: investment made by private companies (including, but not limited to,
  companies that participated in ECS projects), this includes:
  - Investments in spin-offs and start-ups created as a result of ECS PPP project follow up.
  - Investments associated to bringing the technologies into the commercial technology portfolio.
  - Investments associated to the innovation of their production line to become or remain
    competitive in the cybersecurity domain. These investments are not limited to companies
    participating in ECS projects, while some of their suppliers may have been involved in ECS projects
    or were more directly associated to the uptake of the project results.
  - Research and innovations contracts between companies and research organisations resulting
    from contacts and collaboration.
- **At RTO/University level**: increase in expertise and in the generation of additional contract research.
- **At national/regional level**: private-private or public-private initiatives at national/regional level the
  creation of which was stimulated by the ECS PPP and the ECS roadmap.
- **In general**: through community building and increased sharing of information, the ECS PPP increases
  efficiency by avoiding the redundant repetition of efforts (‘reinventing the wheel’) both on the supply
  side as well as on the user side of innovative manufacturing solutions. Considering the dynamics that the
  ECS PPP generates, it contributes to the faster and more efficient implementation of research and
  innovation activities that are happening in parallel or ‘downstream’ of the ECS PPP.

However, in general the notion of a ‘leverage factor’ of the ECS PPP implicitly assumes that some activities would
not have taken place without the existence of the PPP. However, it is extremely difficult to clearly identify which
initiatives or investments would not have taken place without the PPP. Similarly, it would be equally difficult to
identify what the volume of ‘related’ public and private investments would have been without the PPP.

In summary, the organisations participating in the cybersecurity cPPP will:

- **Build on Results** of European Framework Research programs, Horizon 2020 projects, EIT KIC ICT Labs, and
  National RTD projects and programs.
- **Bring in and Leverage Company Results** and standardisation activities in order to exploit results in global
  standards.
• **Use Developed Experimental Systems** for widening the scope for early adoptions and further developments towards large industrial systems.

• **Leverage on EIT KIC ICT Labs** to develop skills and competences.

• **Target Funds in Eligible Regions** for early adoptions and involvement of users both stakeholders and end users

A tentative simulation of the possible sources of funding for the ECS cPPP and an indicative average distribution across the different kind of members is presented in Annex 1.

6.4 Monitoring: KPIs

The European Cybersecurity cPPP has three main strategic objectives:

• The protection from cyber threats of the growth of the European Digital Single Market

• The creation of a strong European-based offering and an equal level playing field to meet the needs of the emerging digital market with trustworthy and privacy aware solutions

• The growth and the presence of European cybersecurity industry in the global market.

To reach these objectives, the Cybersecurity cPPP should leverage complementary work:

• The coordination of R&I in the frame of H2020 characterized by a cross-sectoral, technology-neutral, interoperable, and holistic approach

• The development of industrial policy activities to support the growth of the cybersecurity and ICT industry in Europe and broadly deploy innovative solutions and services for the most economically important and growing end markets as well as for security sensitive applications

To achieve maximum leverage for impact all proposed cPPP activities will:

• be designed and deployed to be technology-neutral, interoperable and transparent;

• combine security and privacy improvements – not only partially but with positive, measurable impact for the system solution all along the value chain;

• elaborate and indicate a reasonable level of security and give a workable guideline for supportive policy activities such as certification and labelling;

• provide evidence how the approach enhances trust and acceptance by citizens, consumers and businesses.

To better follow these objectives and the activities of these work streams, we introduce hereafter Key Performance Indicators (KPIs).

They are defined for all stakeholders engaged in the cPPP from industry, SMEs, associations, research organisation, to Member States, other countries participating in the cPPP and the European Commission. The KPIs are used to give guidance to any planned contribution or proposal and they can be used as evaluation criteria to select the best initiatives spurring Europe to become leader in creating and using secure and privacy respecting solutions.

Starting from the approach of the NIS-P WG3, the SRIA has defined a number of technical and non-technical priorities in a bottom up approach considering the inputs of experts from different sectors and using existing material produced from several communities (including the NIS WG3 SRIA as planned). These priorities will be regularly reviewed by the cPPP members to better adapt to the evolution of needs.

Moving to the cPPP industry driven context, these priorities have been analysed in a top down view, in order to provide a consistent and sustainable strategy for the protection of the DSM and the increase of European digital autonomy to secure sensitive applications.

The proposed KPIs structure therefore reflects the way in which an industry driven cPPP will be implemented.
KPIs are not always suggesting quantitative objectives, but looking for identification of the evolution of certain parameters (the “indicators”) which could show, year by year, the evolution of the market and of the cyber / ICT security ecosystem.

The KPIs are divided into 3 main categories:

- Industrial Competitiveness;
- Socio-Economic Security;
- Implementation and operational aspects of the cPPP.

Certain KPIs are directly related to funding and activities foreseen in the cPPP and, as such, they can be more easily measured. Yet, they have a real impact on the main cPPP objectives only when H2020 funded projects are showing results. Thus, it could take a few years before planes actions will start to generate significant value and some of the objectives mentioned for the following KPIs could be reached only at the end of the initial cPPP period (i.e. 2020).

Other KPIs, in the first years of the cPPP, are closer to present market values and will only progressively be affected by the industrial policy actions envisaged in the cPPP approach. These KPIs have an indirect impact to the cPPP but are important to provide the status and evolution of the market, to better track progress in the implementation of the cPPP and the uptake of the innovations created through the R&I work stream.

The KPIs here presented are considering the main topics that will allow tracking the objectives of the cPPP.

**Industrial Competitiveness**

- KPI 1: MARKET DEVELOPMENT
- KPI 2: FROM INNOVATION TO MARKET: STANDARDS, TESTING, CERTIFICATION AND TRUST LABELS
- KPI 3: USERS AND APPLICATIONS
- KPI 4: PRODUCTS and SERVICES SUPPLY CHAIN
- KPI 5: SMEs

**Socio-Economic Security**

- KPI 6: EMPLOYMENT
- KPI 7: ECOSYSTEM: EDUCATION, TRAINING, EXERCISES
- KPI 8: PRIVACY & SECURITY BY DESIGN
- KPI 9: DATA AND INFORMATION EXCHANGE & RISK MANAGEMENT
- KPI 10: IMPLEMENTATION OF LEGISLATIONS

**Implementation and operational aspects of the cPPP**

- KPI 11: INVESTMENTS / LEVERAGE
- KPI 12: cPPP IMPLEMENTATION MONITORING
- KPI 13: COORDINATION WITH EUROPEAN and THIRD COUNTRIES
- KPI 14: DISSEMINATION & AWARENESS
- KPI 15: TECHNICAL

European Cybersecurity cPPP – ECS cPPP – Industry Proposal
Industrial Competitiveness

KPI 1: MARKET DEVELOPMENT
Description: Evolution of cybersecurity revenues in the European and global market, including positioning and market share of the European industry
Baseline and data collection: The 2015 European market is of the order of 25% of the world market for products and services, with an average growth of 6% over the different sectors. This should be compared with results of a yearly market study, also identifying the number of European companies offering cybersecurity solutions and their market share, possibly in their different product lines.

KPI 2: FROM INNOVATION TO MARKET: STANDARDS, TESTING, CERTIFICATION AND TRUST LABELS
Description: Contribution to standards, use of testing, validation, certification infrastructures as well as European trust labelling procedures, best practices and pilots for innovative elements of the supply chain
Baseline and data collection: Data to be obtained from the Cybersecurity cPPP Projects funded under H2020, provided by the European Commission, other EC or private market studies as well as national validation, certification and standardisation bodies.

KPI 3: USERS AND APPLICATIONS
Description: Increased use of cybersecurity solutions in the different markets/applications, implementing Europe-wide strategic projects for specific deployments of existing or near-to-market technologies that demonstrate the potential impact of cybersecurity products across sectors.
Baseline and data collection: A yearly study, with the support of users, operators active in the cPPP would identify the present values and the evolution in % of use of certified and/or labelled cybersecurity solutions in the different application sectors (energy, transport, finance, eHealth, eGovernment, Industry – including manufacturing, 4.0 – ICT, mobile, IoT, Cloud, Big Data etc.) in Europe. Connection with national administrations will be needed to get data on call for tenders requesting use of trusted solutions.

KPI 4: PRODUCTS and SERVICES SUPPLY CHAIN
Description: development of the European cybersecurity industry and of the European cybersecurity capacities.
Baseline and data collection: Estimation of present participation and funding of the private supply sector in H2020 cyber related projects is about 37-40%. Data to be obtained from the Cybersecurity cPPP projects funded under H2020, provided by the European Commission, as well as by regular market study supported by H2020 actions.

KPI 5: SMEs
Description: Support the creation and development of start-ups having products and services that effectively reach the market.
Baseline and data collection: Estimation of SMEs participation and funding in FP7 and H2020 in this sector is of the order of 14 – 17%. Data to be obtained from the ECS cPPP projects funded under H2020, provided by the European Commission, as well as by regular market study supported by H2020 actions.

Socio-Economic Security

KPI 6: EMPLOYMENT
European Cybersecurity cPPP – ECS cPPP – Industry Proposal
**Description:** Develop employment in cybersecurity sectors (supply and users / operators)

**Baseline and data collection:** Initial study to be conducted with the support of cPPP members and regularly updated.

**KPI 7: ECOSYSTEM: EDUCATION, TRAINING, EXERCISES**

**Description:** Development of cybersecurity education and training for citizens and professionals to enhance the awareness of threats and needed skills for safe use of IT tools.

**Baseline and data collection:** Data collected from cyber range operators / service providers, Universities and other organisations providing cybersecurity training programmes on annual basis starting from 2017, regularly updated. Study to be conducted with the support of cPPP members.

**KPI 8: PRIVACY & SECURITY BY DESIGN**

**Description:** Development and implementation of European approaches for cybersecurity, trust and privacy by design.

**Baseline and data collection:** Study to be conducted with the support of cPPP members in the first year of operation and regularly updated.

**KPI 9: DATA AND INFORMATION EXCHANGE & RISK MANAGEMENT**

**Description:** Facilitate process for information sharing between national administrations, CERTs and Users to increase monitoring and advising on threats; better understanding risk management and metrics.

**Baseline and data collection:** Study to be conducted with the support of cPPP members in the first year of operation and regularly updated considering the whole European market.

**KPI 10: IMPLEMENTATION OF LEGISLATIONS**

**Description:** Implementation of the NIS Directive and market driving Regulations / Guidelines

**Baseline and data collection:** Input to be obtained from the Cybersecurity cPPP projects funded under H2020, provided by the European Commission, as well as by regular market study supported by H2020 or other activities at national level.

**Implementation and operational aspects of the cPPP**

**KPI 11: INVESTMENTS / LEVERAGE**

**Description:** Investments (R&I, capability, competence and capacity building) in the cybersecurity sector defined by the ECS cPPP objectives and strategy.

**Baseline and data collection:**
Data provided by studies to be conducted with the support of cPPP members and H2020 funds, regularly updated. Market study on development of venture capital and financing of high level innovation and IT security in Europe, their challenges and their expectations.

**KPI 12: cPPP IMPLEMENTATION MONITORING**

**Description:** Efficiency, openness and transparency of the cybersecurity cPPP implementation process.

**Baseline and data collection:**
Input by cPPP participant, data analyses to be provided by the European Commission on an annual basis.

KPI 13: COORDINATION WITH EUROPEAN and THIRD COUNTRIES

Description: Coordination of the cPPP implementation with EU Member States, Regions, other countries participating in the cPPP and Third Countries.

Not all technologies exist or will be developed in European countries. Integration of trusted non-European products and services shall follow the security and privacy (by design) requirements, certification or labelling schemes as defined in Europe (Lex loci solutionis) for an European trusted supply chain and procedures.

Baseline and data collection: Data to be obtained from the ECSO members, the projects funded under H2020 as well as by the European Commission, Member States, other countries participating in the cPPP and Third Countries involved.

KPI 14: DISSEMINATION & AWARENESS

Description: Dissemination and Awareness rising making the cybersecurity cPPP action and results visible in Europe and globally, to a broad range of public and private stakeholders.

Baseline and data collection: Data to be obtained from the ECSO members, the projects funded under H2020 as well as by the European Commission. The cPPP Secretariat and specific H2020 projects will disseminate the information in close coordination.

In the following, a link between these KPIs and the objectives of the cPPP mentioned in § 4.6 of this Industry Proposal.

<table>
<thead>
<tr>
<th>Strategic Objectives</th>
<th>ASSOCIATED KPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To foster cybersecurity market development, job and wealth creation in Europe through a long term investment commitment by cybersecurity industry, research and technology organisations (RTOs), academia, the European Commission, Member States' public administrations participating in the partnership as well as cybersecurity solution users;</td>
<td>11</td>
</tr>
<tr>
<td>• To support the use of innovative trusted solutions and services for major societal and economic challenges in Europe, e.g. in different essential services providers, particularly in areas where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);</td>
<td>3</td>
</tr>
<tr>
<td>• To accelerate Europe’s innovation process and time to market by addressing the full innovation and value chain of cybersecurity in different application sectors;</td>
<td>4</td>
</tr>
<tr>
<td>• To foster the development of European cybersecurity industry by creating a Europe-wide technology and application base, building up competence and competitive European cybersecurity companies, including SMEs, facilitating the acceleration of business ecosystems and appropriate business models with a particular focus on SMEs, start-ups and high growth companies;</td>
<td>4 &amp; 5</td>
</tr>
<tr>
<td>• To mobilise and leverage public and private resources to provide contributions to the development and implementation of European cybersecurity policies, regulations and standards (e.g. contributions to European policies; support to implementing legislation like NIS Directive, eIDAS regulation; contributing to creation and updating of ETSI/CEN/CENELEC standards).</td>
<td>2 &amp; 10</td>
</tr>
<tr>
<td>• To increase the awareness and demonstrate the value of cybersecurity solutions for businesses (including decision makers) and the public sector to accelerate the take-up, but also to improve the cybersecurity awareness among citizens and skills development of experts.</td>
<td>14</td>
</tr>
</tbody>
</table>
**SPECIFIC OBJECTIVES of the cPPP:**

### OBJECTIVES FOR IMPROVED COMPETITIVENESS

- **Support the evolution of cybersecurity revenues in the European and global market, including positioning and market share of the European industry:** aiming at maintaining the European cybersecurity market share at least at 25% of the global market and attaining a yearly growth of the European market at least of 8% by 2020;

- **Develop solutions leading towards the use of cybersecurity technologies in the fields of different vital infrastructure and service providers, in particular where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);**

- **Support activities for increased industrial competitiveness of Europe through the development and implementation of cybersecurity industrial measures (e.g. standardisation, use of testing, validation, certification infrastructures as well as trust labelling procedures, best practices and pilots for innovative elements of the supply chain, link to regulations).** The development of certification activities in cybersecurity will consider Regulation 765/2008 and Decision 768/2008 and certification provisions included in the General Data Protection Regulation 2016/679;

- **Stimulate existing and new alliances and the ecosystems along and across the value chain that reinforce competitive capabilities of European cybersecurity industry in existing market segments or help address new market segments;**

- **Support the development and link of clusters as a mechanism at local level and beyond (Regional / National) to develop the market and support SMEs and start-ups;**

- **Support the emergence of start-ups with products / services that effectively reach the market;**

- **Foster the creation of financial / investment instruments to support industry and innovation in IT and cybersecurity, helping to bring innovative solutions to full maturity as well as stabilize / develop SMEs: e.g. entrepreneurial (private fund) and venture capital (bank / financial entities) investments funds, cybersecurity bonds (corporate bonds) etc.;**

- **Support innovation in companies with high growth potential to achieve next level in business developments and cross-border solution delivery.**

### INNOVATION OBJECTIVES

- **Support the widest and best market uptake of innovative cybersecurity technologies and services for professional and private use by accelerating the wide diffusion of cybersecurity technologies in many industry sectors and the emergence of new business opportunities;**

- **Make the innovation process more inclusive, sustainable and effective through the direct involvement of players along and across the full value chain, including those communities, like “white hackers” and “open source”, that could bring disruptive views and breakthrough innovation;**

- **Facilitate networking between different actors (suppliers, users, R&D centres, public actors etc.) to find synergies and decrease the effects of fragmentation in the cybersecurity field;**

- **Support the creation of European-wide ecosystem for networking, training, testing and experience exchange through a network of integrated technical exercises environments, also to validate technologies from a technical and business perspective;**

- **Contribute to activities for pre-standardisation and / or standardisation to support development and use of products and services that meet the requirements set out in relevant legislation;**
- Support the development of a trusted European cybersecurity supply chain where relevant, for higher technological independence at National / European level, by creating a catalogue of trusted products and companies, and by increasing the visibility of SMEs, promoting the European cybersecurity offerings and allowing informed procurement.

- Support increased use of trusted European certified or labelled solutions introduced in the different markets / applications.

- Plan funding for disruptive innovation through accelerators and / or SME associations or clusters to improve funding opportunities for small players (start-ups, SMEs, high-growth companies).

### SOCIETAL OBJECTIVES

- Maintain and develop employment in cybersecurity sectors (supply and users / operators) in the European Union

- Develop and implement European approaches for cybersecurity, trust and privacy by design:
  - Develop new personalised and enhanced technologies, products and services adapted to consumers' and organisations' needs that will respect security and integrity of data and ensure the protection of personal data in a manner that is compliant with the new General Data Protection Regulation.
  - Foster trust in the data-driven economy, including through incentivizing the application of the principles of privacy and security by design as well as the cooperation with relevant authorities in case of data breaches and cyber incidents.
  - Support the implementation of eIDAS Regulation as well as the development and uptake of high-security authentication tools by citizens to protect their identity and assets in the cyber domain.
  - Address acceptance of new cybersecurity technologies by society and consumers by identifying potential barriers.

- Develop education, training and skills on cybersecurity products and safe use of IT tools in Member States for citizens individuals and professionals:
  - Support widespread know-how, education and skills in Europe through curricula to stimulate higher education.
  - Develop an ecosystem that supports the general awareness raising and basic-hygiene skills development in the cybersecurity field for citizens in Europe to help manage the risks that have come along with the ever-increasing digital dependencies of every-day actions of the citizens.
  - Foster the development of new cybersecurity training modules to be integrated into training programs in different educational levels to provide basic skills and awareness of cyber threats also in traditional educational training.
  - Support the increase of in-depth cybersecurity training and education opportunities for securing a skilled workforce for cybersecurity industry as well as provide cybersecurity experts for public sector organisations and critical infrastructure / essential service providers, in particular through the EIT Digital (European Institute of Innovation and Technology Knowledge and Innovation Community on Digital) action line on Privacy, Security & Trust.

### OPERATIONAL OBJECTIVES

- Establish an open, transparent and inclusive approach to determining and updating the SRIA.

- Bring innovative results to market via systematic use of the whole set of funding tools (at European and national level; public and private), showing the benefits and the link between European / National funds, European policies and market growth.

- Facilitate, together with the public side, that at least 20% of the participants of the calls to be funded are SMEs, start-ups or high growth companies (50+% increase in annual revenue).
- Gather information to support the ex post assessment of the implemented projects implemented under the partnership.
- Implement a cross-fertilisation platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues.
- Put in place a governance model structures which on the one hand promotes openness, transparency and representativeness, and on the other hand ensures efficient management with minimal overheads.
- Cooperation with Third Countries to develop coherent approaches in the cybersecurity market: identification and measure of common events, meetings and concrete activities (projects, standards, mutual recognition etc.).
- Coordination of the partnership strategy implementation also combined with regional and national activities and funds in the specific sectors.
- Disseminate successful results within and between sectors and across value chains through effective linking of participants.

<table>
<thead>
<tr>
<th>SPECIFIC COMMITMENTS BY THE ASSOCIATION</th>
<th>ASSOCIATED KPI</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Leverage the partnership investments through sector investments of 3 times the total estimated partnership budget;</td>
<td>11</td>
</tr>
<tr>
<td>· Establish an open, transparent and inclusive approach to determining and updating the SRIA</td>
<td>9 &amp; 12</td>
</tr>
<tr>
<td>· Increase the current level of investment in education, awareness and training across the supply chain and citizens;</td>
<td>7</td>
</tr>
<tr>
<td>· Facilitate, together with the public side, that at least 20% of the participants of the calls to be funded are SMEs, start-ups or high growth companies (50+% increase in annual revenue);</td>
<td>2</td>
</tr>
<tr>
<td>· Gather information to support the ex post assessment of the projects implemented under the partnership;</td>
<td>12</td>
</tr>
<tr>
<td>· Facilitate moving successful results into standards (for fast market uptake) and product enhancing services;</td>
<td>2</td>
</tr>
<tr>
<td>· Bring innovative results to market via systematic use of the whole set of funding tools (at European and national level; public and private), showing the benefits and the link between European / National funds, European policies and market growth;</td>
<td>11</td>
</tr>
<tr>
<td>· Implement a cross-fertilisation platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues;</td>
<td>12</td>
</tr>
<tr>
<td>· Ensure that the achieved results are fully compliant with relevant Union legislations;</td>
<td>10</td>
</tr>
<tr>
<td>· Leverage the EIT Digital KIC (Knowledge and Innovation Community selected by the European Institute of Innovation and Technology) Privacy, Security &amp; Trust action line to develop skills and competences in trust and security;</td>
<td>13</td>
</tr>
<tr>
<td>· Work with other PPPs to align goals and activities so as to ensure synergies;</td>
<td>13</td>
</tr>
<tr>
<td>· Disseminate successful results within and between sectors and across value chains through effective linking of participants;</td>
<td>14</td>
</tr>
</tbody>
</table>
- Actively involve all relevant sector players, in particular from the application areas, and put in place mechanism to secure their participation for the successful development of innovative new business models;  

- Put in place governance structures which on the one hand promote openness, transparency and representativeness, and on the other hand ensure efficient management with minimal overheads.

### Monitoring / Impact on Industrial Competitiveness and the Economy

- European cybersecurity market share at least 25% of the global market;  

- Yearly growth of the European cybersecurity market at least of 8% by 2020;  

- Increase of certified companies and products based on the existing European Common Criteria or SOG-IS certification schemes, and other possible future European ICT security certification frameworks, in particular those compliant with the provisions of Regulation 765/2008 and Decision 768/2008, to bridge the gap between Innovation and Market;  

- Monitor the take-up of research and innovation output coming from the partnership in the development of novel cybersecurity products and services;  

- Increase participation to at least 15% of users in partnership projects by 2020;  

- Implementation of at least 4 large scale projects funded by H2020 for critical infrastructure protection;  

- At least 80% of funding to projects that have a technical solution or service as a final outcome;  

- Increase SMEs and high growth companies (year-over-year growth over 50%) participation and funding in H2020 projects above the H2020 target of 20%;

### Monitoring / Socio-Economic Impacts

- Growth of the cybersecurity related employment, expected target 10% growth per year;  

- Development of cybersecurity companies, increasing job creation, keeping competences and capacities in Europe, while respecting Union law;  

- Development of cybersecurity education and training for citizens and professionals to enhance the awareness of threats and needed skills for safe use of IT tools;  

- Large scale international exercises using European based exercise ecosystem;

### Monitoring / Operational Aspects

- Monitor progress of the partnership implementation and of its R&I strategy: Number of R&I projects funded; Time to contract; Statistics of response to calls; Consistency of approved projects against partnership strategy and KPIs;  

- Monitor progress against the multi-annual research and innovation roadmap: Number of systems and technologies developed in the relevant sector in partnership projects;  

- Coordination of the partnership strategy implementation also combined with regional and national activities and funds in the specific sectors;
· Cooperation with Third Countries to develop coherent approaches in the cybersecurity market: identification and measure of common events, meetings and concrete activities (projects, standards, mutual recognition etc.);

· Dissemination of information and tangible examples on a quarterly basis about how cybersecurity and privacy respecting solutions contribute to trusted daily lives of individuals in the European Union and the economic operators by using various communication channels like social media, web, video, articles and publications, press releases, success stories, etc;

· Awareness and information actions for promoting the PPP activities to a broad range of stakeholders: events with European and National Institutions, targeted newsletters, social media, etc;

· Organisation, contribution and support to the Annual Cybersecurity partnership conference, starting in 2017, of Info-Days and Brokerage events.

MORE DETAILED POTENTIAL INDICATORS POSSIBLY LINKED TO THE ACTIVITY OF THE ECSO ASSOCIATION

In building up the industry proposal, we have considered the cPPP as an instrument for achieving higher objectives, for market and industry development, well beyond existing PPPs approaches set up in cooperation with the European Commission.

Based upon the industrial vision developed in the mentioned “cybersecurity flagship” study made by EOS, such objectives are the elements of a full-fledge cyber security European industrial policy, taking into account the urgent need to reinforce Europe’s digital autonomy in an environment where: (1) US companies are clearly favoured by the size of their domestic markets, the level of federal investment and the dynamics of venture funding, and (2) specific considerations must apply due to sovereignty constraints. We have therefore considered other objectives and a more detailed view of KPIs that can be pursued by the Association, in parallel and in support to the cPPP activities.

We think it is important to have in mind these more detailed indicators, built upon the main KPIs of the cPPP when developing the European market and industry. These indicators should serve as guideline for the activity of the Association, also considering that it will be through these indicators (and their implicit objectives) as well as the potential development of an effective European cybersecurity industrial policy that the cPPP will effectively reach the envisaged leverage factor.

We are of the opinion that a cPPP not supported by an adequate cybersecurity industrial policy, including a clever governance and approach in the way research priorities will be chosen, might end up in a slight improvement of “H2020 activities as usual”, with will have little chances of success and a limited industry adhesion.

Industrial Competitiveness

**KPI 1: MARKET DEVELOPMENT**

**Description:** Evolution of cybersecurity revenues in the European and global market, including positioning and market share of the European industry

**Objectives:**

a) European cybersecurity market share at least 25% of the global market by 2020.

b) Yearly growth of the European cybersecurity market a least of 8% by 2020.

c) Improved positioning (qualitative figure) of European companies in main reference studies and ratings (e.g. Gartner, European ratings, etc.).
KPI 2: FROM INNOVATION TO MARKET: STANDARDS, TESTING, CERTIFICATION AND TRUST LABELS

Description: Contribution to standards, use of testing, validation, certification infrastructures as well as European trust labelling procedures, best practices and pilots for innovative elements of the supply chain

Objectives:

a) Number of activities leading to standardisation (at project level), contribution to new standards, stemming from cPPP projects (interoperability standards and compliance regulations stemming from cPPP projects, to allow secure and seamless integration of solutions and services from multiple sources, European and non-European; open standards, open-source software and if possible hardware, stemming from cPPP projects, for making the whole supply chain from processor design to application layer more transparent, reviewable, trusted and secure; directly usable for public and private procurement processes in order to create a direct market pressure towards ICT suppliers to create secure and trustworthy solutions).

b) Number of patent applications (at project level) and awarded patents stemming from cPPP projects.

c) Increase of certified companies and products based on the European Common Criteria or SOG-IS certification schemes to bridge the gap between Innovation and Market, improving the market penetration potential of European cybersecurity solutions.

d) Establishment of a European trust and privacy certification compliance framework and label, considering security and privacy requirements along the value chain, with mutual recognition of quality across European countries, supported by European / National certified and independent validation platforms, and European ratings, also in the light of and increase the European Digital Autonomy for sensitive ICT and cybersecurity solutions.

e) Study of a possible European model of an institute supporting European standardisation, certification and definition of guidelines adapted to the European market (as in the NIST in the US).

f) Number of hardware and software solutions developed and validated by cPPP projects for trusted supply chains.

KPI 3: USERS AND APPLICATIONS

Description: Increased use of cybersecurity solutions in the different markets / applications, implementing Europe-wide strategic projects for specific deployments of existing or near-to-market technologies that demonstrate the potential impact of cybersecurity products across sectors.

Objectives:

a) Yearly evolution of the number of certified or trusted labelled solutions introduced in the different sectors in Europe (this depends on the degree of maturity and awareness of the different sectors).

b) At least 15% of participants of ECS cPPP projects funded by H2020 instruments must be users.

c) Implementation of at least 4 large scale projects funded by H2020 for critical infrastructure protection.

d) Number of yearly calls for tender at European and national level demanding priority procurement of European or National trusted solutions, or specific European suppliers, for sensitive applications.

KPI 4: PRODUCTS and SERVICES SUPPLY CHAIN

Description: development of the European cybersecurity industry and of the European cybersecurity capacities.

Objectives:

a) Identification of European industries in the different European countries, including SMEs, with particular emphasis on Eastern Europe.
b) Identification of the offer for products and services of European industries, mentioning if they are certified / labelled or not.

c) Analysis of European market needs with respect to existing competence to identify strategic, critical technologies with respect to main national or European security sensitive issues and critical IT assets needing developments to improve the trusted level of the supply chain and increase the European Digital Autonomy for sensitive ICT and cybersecurity solutions.

d) Increase cybersecurity private industry (supply sector and demand) participation and funding in H2020 cybersecurity related calls to at least 50%.

e) Dedicate at least 80% of funding to projects that have a technical solution or service as a final outcome.

f) Dedicate at least 20% of funding to projects that create an integrated European offer across sectors (e.g. anti-viruses / malwares; data protection; risk assessment; monitoring etc.).

g) Monitor the take-up of research and innovation output coming from the cPPP in the development of novel cybersecurity products and services. Number of Products and Services from cPPP projects effectively introduced in the market.

KPI 5: SMEs

**Description:** support the creation and development of start-ups having products and services that effectively reach the market.

**Objectives:**

a) Increase SMEs and high growth companies (year-over-year growth over 50%) participation and funding in H2020 projects above the H2020 target of 20%. All large scale investment projects have to have SMEs and/or high growth companies in the consortium.

b) Development of a network of European SMEs (including start-ups, incubators and accelerators) associations and clusters to share best practices and tools (e.g. web platforms for products’ awareness) and to support local / national cybersecurity SMEs to be aware of European initiatives.

c) Creation of a European cybersecurity accelerator and SMEs’ funding vehicle (with European funds) to fund 1% of new start-ups every year (with respect to the existing number of cybersecurity SMEs in Europe).

d) Explore the possibility of a European Cybersecurity Small Business Act to facilitate procurements oriented towards SMEs.

e) Yearly increase of European SMEs reaching the market with innovative solutions.

f) Estimation of the increase in turnover and employees in SMEs participating in the ECS cPPP projects.

g) Number of project results taken-up for higher TRLs using additional investments. Tentatively, each technology research project with TRL higher than 5, should transfer to commercialisation at least one innovation in the two years following the end of the project.

**Socio-Economic Security**

KPI 6: EMPLOYMENT

**Description:** Develop employment in cybersecurity sectors (supply and users / operators)

**Objectives:**

a) Evaluation of number of people directly employed in cybersecurity (supply and users / operators): target 10% growth per year and impact on employment increase in emerging markets (trust and acceptance will boost market uptake).
b) Identification and evaluation of skill gaps (actual market needs) of workers, graduates and scientists including comparisons with other European and main non-European countries.

c) Number of new types of high-skilled jobs and new curricula developed in cPPP projects.

KPI 7: ECOSYSTEM: EDUCATION, TRAINING, EXERCISES

**Description:** Development of cybersecurity education and training for citizens and professionals to enhance the awareness of threats and needed skills for safe use of IT tools.

**Objectives:**

a) Creation of a European Cybersecurity Academy or a network of national cybersecurity “academies” providing multi-disciplinary curricula and training recognized at European level. Training programs for SME’s, policy makers, cybersecurity specialists, associations, service providers, graduate students etc. using cyber range platforms. Tentative target: minimum 70 training sessions with at least 50 participants on each session using cyber ranges platforms. At least 20% annual increase in the number of training participants.

b) Creating a federated cross-border ecosystem for exercises, trainings and awareness raising as well as products testing. Tentative target: at least 5 countries participating in the cPPP collaborating, “technical federation” created between at least 3 “ranges”. At least 10 countries participating in the cPPP collaborating, at least 7 “ranges” federated by 2020.

c) Large scale international exercises using European based exercise ecosystem. Tentative target: minimum 20 large scale training sessions (at least 200 specialists per training session) with participants from at least 10 different countries.

d) Development of new training programs / training modules for cybersecurity educational programs, occupational trainings etc. including adding cybersecurity training modules to vital service providers’ formal education. Tentative target: at least 20 new training programs / training modules to be developed to enhance formal education and occupational training of cybersecurity specialists, and specialist of fields that have high dependency of ICT.

e) Creation of a European primary school level cybersecurity education programme, for instance in collaboration with National Safer Internet Centres that have been working on the primary school level for more than 10 years.

f) Evaluation of number of certification programmes for professionals and companies dealing with cybersecurity. At least 5% annual increase of the number of certified professionals and organisations.

g) Creation of a network of accredited cybersecurity experts and an online reference for independent cyber-experts for professionals and citizens.

h) Creation of a European cybersecurity centralised cyber threat intelligence facility (or set of connected facilities) to provide information to users and suppliers in an efficient and convenient way, e.g. using mobile and app technologies, and drive new services and solutions development.

KPI 8: PRIVACY & SECURITY BY DESIGN

**Description:** Development and implementation of European approaches for cybersecurity, trust and privacy by design.

**Objectives:**

a) Increase the use of security and privacy-by-design enhancing technology in European and national public procurement, and contribute to the development of a prototype for a European catalogue of ICT standards for public procurement.
b) Increase and quantify certification or labelling of product and services providing security and privacy by design (reflecting the standards and certification efforts from KPI 2).

KPI 9: DATA AND INFORMATION EXCHANGE & RISK MANAGEMENT

**Description:** Facilitate process for information sharing between national administrations, CERTs and Users to increase monitoring and advising on threats; better understanding risk management and metrics.

**Objectives:**

a) Creation and effective development and use in Europe of ISACs (Information Security and Analysis Center) in the form of a common European-level ISAC. Evaluation of effective participation of public administrations and private sector companies in sector-specific ISACs.

b) Creation, alignment and deployment of metrics for vulnerabilities, threats, incidents, mitigation functions and their financial implications defining the robustness of the solutions against attacks.

c) Measure the increase of application of Risk Management methods and standards in the European market, as well as use of the European agreed metrics to evaluate the threats compliance to cybersecurity risk management procedures of companies and public sector organisations.

d) Quantify evolution in use of cyber-insurances or management business models in Europe, leveraging upon cybersecurity Risk Management, possibly using European certified products, for an increased uptake of cybersecurity insurance policies by the private sector.

KPI 10: IMPLEMENTATION OF LEGISLATIONS

**Description:** Implementation of the NIS Directive and market driving Regulations / Guidelines

**Objectives:**

a) Quantify recommendations and measures supported by ECS cPPP projects for the implementation of the NIS Directive at national level.

b) Quantify recommendations and measures supported by ECS cPPP projects for the creation and implementation of other European Regulations and legislations (e.g. eIDAS, PSD2, minimum security and privacy requirements for IoT, labelling, etc.).

Implementation and operational aspects of the cPPP

KPI 11: INVESTMENTS / LEVERAGE

**Description:** Investments (R&I, capability, competence and capacity building) in the cybersecurity sector defined by the ECS cPPP objectives and strategy.

**Objectives:**

a) Leverage the ECS cPPP (R&I) investments through investments of 3 times the Cybersecurity cPPP total estimated budget (including R&I investment from “non EC” sources). Estimation of the total amount of the “non EC” investment mobilised in cPPP projects and estimation of the “non EC” investment mobilised in other R&I activities related to the ECS cPPP objectives (leverage factor).

b) Estimation of H2020 funds linked to other European / national programmes and procurement funds in cybersecurity contributing to the leverage factor for a strategic end to end approach.

c) Creation and development of new models of financial / investment instruments to support industry and innovation in IT and cybersecurity in Europe adapted to the current economic environment; set up of and participation in European or national investments funds for cyber / ICT security product and service
development: entrepreneurial (private fund) and venture capital (bank / financial entities) investments funds, cybersecurity bonds (corporate bonds) etc.

d) Creation of financial incentives and favourable fiscal conditions for the cybersecurity industry to ensure the business development, especially in strategic areas for Europe and to make sure strategic cybersecurity assets and companies remain in Europe.

e) Organise annual presentations of new innovative cybersecurity ideas and products stemming from cPPP cooperation between industry, RTOs, University and users, as well as innovative cybersecurity start-ups to potential investors.

KPI 12: cPPP IMPLEMENTATION MONITORING

Description: Efficiency, openness and transparency of the cybersecurity cPPP implementation process.

Objectives:

a) Put in place governance structures which on the one hand promote openness, transparency and representativeness, and on the other hand ensure efficient management with minimal overheads.

b) Implement a cross-fertilisation platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues;

c) Provide suggestions and monitor progress of the cPPP implementation and of its R&I strategy: Number of R&I projects funded; Time to contract; Statistics of response to calls; Consistency of approved projects against ECS cPPP strategy and KPIs;

d) Progress against SRIA roadmap: number of systems and technologies developed in the relevant sector in cPPP projects;

e) Annual outlook on lessons learnt.

KPI 13: COORDINATION WITH EUROPEAN and THIRD COUNTRIES

Description: Coordination of the cPPP implementation with EU Member States, Regions, other countries participating in the cPPP and Third Countries.

Objectives:

a) Leverage the EIT Digital KIC (Knowledge and Innovation Community selected by the European Institute of Innovation and Technology) Privacy, Security & Trust action line to develop skills and competences in trust and security;

b) Work with other PPPs to align goals and activities so as to ensure synergies;

c) cPPP strategy implementation coordinated and combined with regional and national activities and funds in the specific sectors (e.g. number of projects related to the cPPP strategy implemented with the support of national technology platforms and innovation clusters etc.);

d) Foster the creation of national PPPs and local or national cybersecurity association or clusters to better coordinate cybersecurity activities at regional level and market growth;

e) Cooperation with Third Countries to harmonise approaches in the cybersecurity market, also supported by cPPP projects: identification and measure of common events, meetings and concrete activities (projects, standards, mutual recognition etc.).

KPI 14: DISSEMINATION & AWARENESS

Description: Dissemination and Awareness rising making the cybersecurity cPPP action and results visible in Europe and globally, to a broad range of public and private stakeholders.
Objectives:

a) Regular information and tangible examples about how cybersecurity and privacy respecting solutions stemming from cPPP activities can contribute to trusted daily lives of European citizens and the economic sector by using various communication channels like social media, web, video, articles and publications, press releases, success stories, etc.

b) Awareness and information actions for promoting the cybersecurity cPPP and ECSO activities to a broad range of stakeholders: events with European Institutions and representatives from participating countries, targeted newsletters, social media, etc. At least quarterly events, media outlets etc. to raise awareness of cybersecurity.

c) Organisation, contribution and support to the Annual Cybersecurity cPPP conference, of Info-Days and Brokerage events.

6.5 Proposed methodology for monitoring the commitments

The ECS Partnership Board comprising of the European Commission and the Association will release a monitoring report with measurements to be published at European level.

All the KPIs and economic and market data described in the previous section will be monitored for industrial competitiveness and socio-economic impact on a quantitative or qualitative point of view.

We would remind that the proposed KPIs are meant to be the road signs for the ECS Roadmap. The Direct KPIs are those directly influenced by the cPPP and the foreseen funding. We expect that those KPIs are closely monitored.

A baseline, agreed with stakeholders and the European Commission, will be established for all relevant indicators. A regular update cycle will be agreed up-front and a monitoring tool for internal and external use by the community will be established by a respective support action.

In addition, the risks identified will also be assessed, classified and augmented as well as remedial advice and suggests for actions to be taken by the cPPP community. An initial list of risks and possible remedies is given at the end of this chapter.

Monitoring will be useful for several governance bodies including the ECSO Board, the Strategy Committee, the cPPP Partnership Board, and the different ECSO Working Groups.

ECSO members would provide overall figures, summarising their own company’s investments in the business area, without exposing commercial confidential information. The ECS cPPP commitment is based on the aggregate performance of the cybersecurity partners, not on an individual basis.

Data supplied by ECSO members would be supplemented by the results of the accompanying macro-economic study on the impact of the PPP and possible contribution from non ECSO members, particularly if involved in H2020 projects. This study should be ongoing throughout Horizon 2020 and would cover such aspects as job creation, training and skills development, dissemination, impact on societal challenges and development of SMEs. Participating stakeholders would be required to cooperate with the study and provide, in confidence, relevant information - where necessary, in the form of estimates) to the organisation conducting the study. Only informed estimates, rather than auditable quantitative information, will be requested to stakeholders (the cPPP has not the same rules of a European Joint Undertaking).

Organising an inquiry on a yearly basis among all ECS projects may be useful, but will most probably not reflect the leverage factor as defined in the previous sections. An inquiry addressing the members that participate in ECS may be bringing valid input. However, such an inquiry needs to be carefully prepared. A clear understanding and guidance needs to be developed in order to collect useful information.

In assessing the leverage of the cPPP it is assumed that the majority of private / public (non EC) investment will be back-loaded and that as a result the visibility of the impact of ECS would be difficult to discern in the early years of operation. This is due to a number of factors:
a) The time that it takes for public R&I investment to impact on private R&I spend varies with the immediacy of relevance to the market. In some cases it will be simply the length of the project where take-up is immediate, in others where the result is at a lower TRL level it may take from 5-10 years to impact.

b) There is a difficulty of making direct measurements of investment in cybersecurity R&I across all stakeholders in all impacted markets because it is impossible to track the path of innovation except in very particular cases.

c) Private side R&I investments often carry a high level of commercial confidentiality.

One task of an envisaged CSA dedicated to cPPP monitoring, to be made in cooperation with the Association, will also be to establish a “push” service for indicators of interest and relevance.

Strategic and the technological orientated KPIs monitoring results would be delivered twice per year, possibly in occasion of specific ECS Partnership Board and ECSO Board sessions.

Data will then be made public and available to the wider public after being reviewed by the ECS Partnership Board and ECSO Board. Particularly data from industry has to be treated according to its sensitivity.

Data gathering will most probably need to be performed by an independent trusted party due to the confidentiality of the data. Appropriate resources will be planned into the budget of an envisaged CSA.

The monitoring of the complementary R&D investments, direct and indirect in relation to the overall R&D investments, the multiplication effects and the leverage of other national and European funds will be a major task for the cPPP governance. Indeed, the Association with the help of other stakeholders and independent statistics (such as the European Innovation Score Board) or studies will report on the investment figures. Independent trusted research organisations (ideally related to market research), which are collecting such data from industry players on a confidential basis and are aggregating this data in anonymous forms for monitoring and reporting purposes will be invited to take part in this exercise. Potential partners for such an activity could be the Institute for Prospective Technological Studies (IPTS), a Joint Research Centre of the EC, or Eurostat.

Data sources for monitoring beyond the industry (non EC) commitments will include all involved entities and stakeholders, OECD, Eurostat, World Bank, Commission Sources, studies and reports to measure the ECS cPPP implementation and its impact.

6.6 Risks

The option of not doing anything on the European level in cybersecurity field is not a reasonable one as explained in the above chapters. Due to the increasing ICT dependency, changes in the cyber threat landscape and considering the goals of implementing Digital Single Market, immediate coordinated actions are needed.

However, in terms of the cPPP initiative itself, there are risks involved in achieving the goals set in the current industry proposal document. The main risks foreseen in the preparatory phase are highlighted below. These, and others revealed during the implementation phase, need to be fully determined and augmented overtime and monitored by the ECS cPPP Partnership Board, the ECSO Board and other relevant entities.

The following list of risks is based upon the list of KPIs previously exposed.

<table>
<thead>
<tr>
<th>Risks</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MARKET DEVELOPMENT / BUSINESS</td>
<td></td>
</tr>
<tr>
<td>European market and European supplier growth lower than expected</td>
<td>• Increase private investments (e.g. venture capital) in the sector. Select European suppliers for procurement of sensitive solutions.</td>
</tr>
<tr>
<td>Low rating of European companies</td>
<td>• Develop European ratings for an independent and fair view of European solutions.</td>
</tr>
</tbody>
</table>
### STANDARDS, TESTING, CERTIFICATION AND TRUST LABELLING

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of commitment from national administrations to develop European certification and labels</td>
<td>• Give example in a growing number of voluntary European countries to create a momentum.</td>
</tr>
<tr>
<td>Slow procedures to develop European standards</td>
<td>• Pressure from the economic sector on national and European standardisation bodies.</td>
</tr>
</tbody>
</table>

### USERS AND APPLICATIONS

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low participation of users in H2020 calls</td>
<td>• Increase dissemination and credibility of results to drag in users and operators.</td>
</tr>
<tr>
<td>Limited implementation of large scale projects</td>
<td>• Discussions with Programme Committees to present supporting arguments and get their support.</td>
</tr>
</tbody>
</table>

### PRODUCTS and SERVICES SUPPLY CHAIN / TECHNOLOGY

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Not enough new technological solutions will be created (not enough investment into go to market activities) | • Collaboration with the Commission in defining the funding instrument rules in a way that makes sure that the emphasis in majority of the funding calls is on delivering technical solutions to actual users or delivering pilots of technical solutions.  
• Regular reviews of funding decisions and results delivered to make sure that enough viable technical solutions will be delivered. In case needed, adjustments of rules will be negotiated with the commission.  
• Association Members will commit to making sure that consortiums have a reasonable balance of different stakeholders including large companies, SMEs, and users of the solutions. |
| Not sufficient participation of the cybersecurity sector companies                          | • Provide support to private sector in EC administrative procedures and credibility in the H2020 process and results. |
| Not enough projects tackling technology issues                                             | • Provide strategic vision and KPIs objectives to the H2020 evaluators to understand the targets before judgement. |

### SMEs

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMEs and start-ups will not use the funding as they are unable to handle the administrative burden of the collaboration and funding-related reporting</td>
<td>• Funding instruments for SMEs associations and accelerators will be introduced to enable better access to funding for SMEs and start-ups lowering their administrative burden by delegating it to the “middlemen”.</td>
</tr>
<tr>
<td>Not enough SMEs reaching the market with innovative solutions</td>
<td>• Provide more visibility to SMEs and their products, via a web Platform but also with a dedicated funding for economic support.</td>
</tr>
</tbody>
</table>

### EMPLOYMENT

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Difficulties in employing sufficient number of people in cybersecurity field to support the growth targets of the sector | • The Association and possibly other CSA funded by H2020, will support studies to clarify the efforts done. Studies will be conducted regularly and study results introduced to the board of directors for decision making.  
• Compiling an action plan to ensure resource pool growth. |

### ECOSYSTEM: EDUCATION, TRAINING, EXERCISES / SKILLS

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity skills are taught, but are unusable for the cybersecurity industry and other sectors for being too</td>
<td>• Within the collaboration framework under the Association the idea of businesses contributing to</td>
</tr>
<tr>
<td>Academic</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Creating high-quality study materials will regularly be promoted.</td>
<td></td>
</tr>
<tr>
<td>- Ecosystem will be built to support conducting hands-on practical trainings on a university level.</td>
<td></td>
</tr>
<tr>
<td>- The facts itself that members of the Association include academia, businesses, users, government etc. will organically have an effect of increasing the collaboration between the parties, opening doors for experts from businesses to become lecturers or guest lecturers in the universities etc.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Only students studying in ICT fields will get cybersecurity training, leaving other relevant stakeholders “in the dark” about basic awareness and skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Efforts will be made to include cybersecurity training modules to education on all levels, as well as other than ICT students (public administration, law, vital service providers’ fields etc.). Best practices will be shared.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The skills and awareness of general public will not change, there is a lack of tools to raise the awareness and skills for the public</th>
</tr>
</thead>
<tbody>
<tr>
<td>The parties involved in the collaboration will commit to making efforts to help raising the awareness of general public (by means of contributing to creating training modules, publishing articles, organising events etc.).</td>
</tr>
<tr>
<td>Training platforms will be introduced to raise the awareness of general public.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PRIVACY &amp; SECURITY BY DESIGN / SOCIETAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMEs are only included as recipients of Large Industry and Research activity and not sufficiently included in setting up and contributing to the project deliveries</td>
</tr>
<tr>
<td>The ECSO Board of Directors will follow and supervise the setting up of Working Groups and Task Forces, making sure that SMEs representation as contributors is adequate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The citizens will not benefit from the collaboration, the focus is on delivering results that are targeted to solve issues of businesses, government etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The benefits for the citizens are mostly indirect — e.g. providing solutions that help to support protecting personal data benefit the citizens.</td>
</tr>
<tr>
<td>The parties involved in the collaboration will commit to making efforts to help raising the awareness of general public (by means of contributing to creating training modules, publishing articles, organising events etc.).</td>
</tr>
<tr>
<td>Training and awareness raising activities will have a direct impact on citizens enabling them to protect their personal data and making sure they have the skills and knowledge to use IT tools in a safe manner.</td>
</tr>
<tr>
<td>Training platforms will be introduced to raise the awareness of general public.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMPLEMENTATION OF LEGISLATIONS - DATA / INFORMATION EXCHANGE &amp; RISK MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragmentation of the market does not change, making it difficult to achieve actual cross-borders delivery and thus impeding fulfilment of the export goals and harvesting the benefits of DSM</td>
</tr>
<tr>
<td>Work more closely with national administrations (regulatory bodies) and operators to mature their understanding for a common approach and increased information sharing, followed by a harmonized procurement of European trusted solutions. The cPPP Association structure can facilitate this dialogue.</td>
</tr>
<tr>
<td>Regular meetings of working groups and boards will organically lead into higher cross-border collaboration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Missing common agreement on metrics for risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing mutually agreed metrics for risk management as well as concrete scenarios cases (e.g. using insurance business models) and demonstrate the applicability and...</td>
</tr>
<tr>
<td>Issue</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Slow implementation of directive (NIS) and regulations</td>
</tr>
<tr>
<td><strong>INVESTMENTS; cPPP MONITORING; COORDINATION WITH EUROPEAN and THIRD COUNTRIES; DISSEMINATION &amp; AWARENESS</strong></td>
</tr>
<tr>
<td>The Partnership Board does not reflect all relevant stakeholders of the Cybersecurity community especially those that are difficult to represent - SMEs, etc.</td>
</tr>
<tr>
<td>The impact promised in this document is not achieved</td>
</tr>
<tr>
<td>The resources suggested from public bodies are limited or decrease leading to less investment in the cybersecurity sector</td>
</tr>
<tr>
<td>Difficulty to analyse investments for the leverage factor</td>
</tr>
</tbody>
</table>
7 Governance

7.1 Overview of the governance model

7.1.1 Overview

The proposed governance approach is dependent on the negotiated cPPP Contractual Agreement and the finalisation of the various agreements. The ECS cPPP proposers are committed to achieve the ECS impact in Europe through the establishment of an operational organisational structure which facilitates internal and external cooperation with the following facets:

- Openness
- Transparency
- Cooperation
- Inclusion
- Efficiency
- Neutrality
- Fair access
- Cross domain representation
- Cross stakeholder representation:
  - Industry – Large
  - Industry – SME
  - Research & Universities
  - User & Operators (public and private)
  - National public administrations (including regulators),
  - Regions (local economic interest)
  - Other (financial bodies, consultants, etc.)

This structure will be supported by an open membership organisation the “European Cybersecurity Organisation” Association (“ECSO” or the “Association”). It will be the formal legal counterpart of the European Commission to sign the cPPP contract.

The governance of the cPPP must be open and as much agile as possible in a demanding environment in which technology will evolve and sectors will change or converge and create new requirements. Conversely it is also critical that the partnership is sufficiently stable so as to run over several years to ensure that the cPPP objectives can be implemented, augmented, monitored and ultimately the KPIs delivered upon. As such it is anticipated the partnership should run for at least a decade although the scope and implementation priorities will need to be regularly adapted and new value propositions developed.

7.1.2 Structure

To consider the many requirements (and constraints) imposed by the public and private stakeholders of this cPPP as well as the complex and evolving cybersecurity environment we had to develop a structure which at the time is satisfies all these requirements and remains manageable.

The key organisational elements of the cPPPs overall structure relating to implementation and monitoring are implemented in the ECSO Association.
The management body of the Association is the Board of Directors, elected by the Annual General Assembly according to specific rules described in the ECSO Bylaws. The ECSO Board of Directors is steering the cybersecurity industrial policy issues and managing ECSO.

The ECSO Board is supported by the Coordination / Strategy Committee who is coordinating the activities of the different Working Groups and Task Forces.

The Working Groups and Task Forces are composed by the ECSO members and are tackling priority issues, as defined by the ECSO Board of Directors.

In particular, the Scientific & Technology Committee, as part of the Coordination & Strategy Committee, will coordinate the Working Group activities linked to the SRIA. The process for the definition of R&I priorities is described in § 7.2.

The General Assembly is also appointing the ECSO representatives at the Partnership Board, following the H2020 criteria for member participation. The Partnership Board is in charge of the dialogue between ECSO and the E. Commission for the R&I priorities defined by the cPPP and of the monitoring of the cPPP activities.

A body specific to this cPPP is the National Public Authority representatives Committee (NAPAC). Instead of traditional “mirror groups”, in ECSO we will create the NAPAC to allow Public Administrations to have their own space of dialogue with own rules, while remaining in close contact and participating to the ECSO activities, including the Board of Directors.

The aim of the NAPAC is to:

(a) Participate in the discussions and activities of the ECSO Working Groups and Task Forces to bring a governmental perspective and operational needs from the public administrations;

(b) Support the definition and implementation of the ECSO Strategic Research and Innovation Agenda and of the ECSO Multiannual Roadmap into the R&I Work Programme;

(c) Exchange best practice and promote cybersecurity and national / regional research programmes.

The European Cybersecurity “Council”, is an external (virtual body - not belonging to European Institutions or ECSO) that will meet annually to provide high level advice on the activity of the ECS cPPP and European cybersecurity in general. It would be composed by very high level political and economic decision makers at national and European level. It would meet in occasion of the major annual cPPP conference. It would be
The chosen structure could appear of challenging management. Yet, leveraging upon the experience from EOS or other European organisations, like ERTICO - active in the ITS (Intelligent Transport Systems) domain and gathering public / ministries and private members - we trust that the ECSO is manageable with a good decision-making capacity whilst guaranteeing transparency and openness to the widest possible relevant constituency. It also allows a mechanism for organisations to traverse membership types or and either be selected or proposed by the wider community to fulfill and role in the Board. This will also ensure that decisions reflecting the wider interests can be rapidly taken and action lines can be completed without every stakeholder having to explicitly give their decision and so create an agile process.

The directly involved actors are:

- **European Commission (EC)** is the executive arm of the European Union and implements the legislations such as the H2020 Research and Innovation framework. It broadly represents the ‘Public’ European part of the cPPP. As such it ultimately refines and adopts the H2020 Work Programme content (based on the recommendations of ECSO) and decides the implementation of the R&I through the European Cybersecurity cPPP – ECS cPPP – Industry Proposal.
project activities. The European Commission is the only entity (in this governance structure) that has the contractual relationships with implementation parties and decides on final Work Programme content, implementation, timing, evaluation and review criteria. However, in the context of the ECS cPPP it is fundamental that there is a strong / intensive dialogue between the ECSO and the EC.

- **European Cybersecurity Association (ECSO):** This is the formal representation of the ECS stakeholder community open to all stakeholders being a legal entity in “H2020 countries”. It will provide initial and updated SRIAs, KPIs to measure the progress of the cPPP and a community networking and collaboration function. The association will operate in an open way and will base its work on the expertise and competence of its members. It will draw on existing and new liaisons to maximise capacity to engage with user groups, other PPPs, standards bodies etc. The ECSO role is clearly defined both through its governance and is looking also at the different “support activities” to the cPPP.

- **ECSO Members:** These are the full expanse of all organisations interested in ECS. They will have a European presence, typically in Research or providing / using cybersecurity solutions and/or services, and should be legal entities. ECSO Members will represent differing organisational types (Large and SME industry, Universities, Research institutes, User etc.), nature (Private and Public sector), sectors (Energy, Health, Transport, Finance, etc.).

- **Partnership Board:** The Partnership Board (PB) is the formal communication channel between the European Commission and the ECSO Association to discuss the Horizon 2020 Cybersecurity cPPP Work Program, the implementation of the overall R&I program related topics and the monitoring of the cPPP commitments (KPIs). It allows for open dialogue between the members to reach the objectives foreseen by the contractual arrangement between the European Commission and ECSO. It provides oversight such as monitoring, advising, community support etc. The Partnership Board is composed by representative from the European Commission and ECSO Members. The Partnership Board members from ECSO are composed of 20 representatives (plus 10 substitutes) from any Legal Entity eligible in H2020 and Members of the Association, with exclusion of (non users) representatives from Public Administrations. The representations will include both large and SME Industry, representatives from public administrations, RTOs and universities as well as other stakeholders.

- **ECSO Board:** The Board of Directors shall establish strategic guidelines, financial objectives and any other directives for the internal management of the Association.

### 7.2 R&I priorities definition process

It is important to note the process, described also in the ECSO Bylaws, for the definition and finalisation of the SRIA before its presentation before the Programme Committees and the Commission.

- **Input:** Raw thematic proposals from the different working groups

- **Consolidated Input:** Structured thematic proposals prepared by the Coordination & Strategy Committee to be discussed by the ECS cPPP Partnership Board

- **Amended Consolidated Input:** Consolidated Input by the ECS cPPP Partnership Board discussed and amended/commented by the views of the national representatives of the PC configuration Secure Societies and ICT-LEIT (max 2 Reps. per country)

- **Final Input:** Amended Consolidated Input cross-checked and possibly amended/commented by the ECS cPPP Partnership Board and implemented into the Work Programme draft by the European Commission for discussion and final decision by the competent Programme Committee configurations.
7.3 Agreements linked to the ECS cPPP or ECSO

The ECS implementation represents the H2020 programme implementation in terms of Research, Innovation and Coordination to deliver the work set out in the Work Programme derived from the ECS SRIA. However, implementation actions in other areas may also be pertinent. Coordination action(s) will be proposed by ECSO and/or its members which will facilitate the light programme-level coordination of projects through community organisation and technical steering boards as well as CSAs for cross-cutting activities such as addressing legal, policy and regulation. Such CSAs will also host the steering/technical committees, stakeholder platform, stimulate dialogue and coordination and promote pilot projects.

To ensure cooperation, allocation of responsibilities between the various bodies, allow efficient working, and to manage interdependencies and complementarities, the following ECS cPPP Agreements are necessary:

- **European Grant Agreements**: Per-project agreement between project coordinators, other project beneficiaries and the European Commission for the implementation of the entire cPPP projects in context of Horizon2020.
- **Consortium Agreements**: Project agreement between project beneficiaries describing the internal relations between them
- **ECS Collaboration MOU**: Programme agreement between project beneficiaries, being a light cross-project agreement for all projects in the ECS implementation describing the relationship between them including IPR sharing arrangements
- **ECSO-EOS MOU**: To be agreed by the ECSO Board of Directors, between ECSO and EOS identifying the expectations and responsibilities between the two parties, allowing EOS to provide the Secretariat of ECSO under agreed conditions. Note that despite this agreement, EOS members will still need to sign individual membership agreements with ECSO.
This section deals with the two major aspects:

- Background IPR including data ownership protection
- Results of the research and innovation activities within the cPPP

The ECS cPPP is foreseen as a large scale research and innovation exercise to strengthen industry competitiveness and promote innovation. The cPPP will comprise a large number of different projects including research and innovation projects, innovation only projects, demonstration projects, incubator activities and a number of supporting actions e.g. on dissemination. A large number of organisations from various sectors and domains (public, private) and in a large variety of sizes including SMEs will participate in the research and innovation activities as providers and beneficiaries in many roles.

The outcomes of projects will range over: technical concepts, architectures, application, demonstration of artefacts, brokered value chain participants, reports on business models, reports on market development and framework conditions. The different business models for open source and proprietary software have to be taken into account since various combinations of licensing are commonly used in industry and the public sector.

This requires an information, dissemination, and IPR approach that is adequate for this specific cPPP having many different outcomes and results. The approach will need to rely on a common contractual and legislative foundation and need to be adaptable to the opportunities and restrictions of the various projects. This will facilitate the achievement of a major objective of the ECS cPPP which is to use its results to foster large-scale innovation and through a mix of activities and clear agreements.

Sharing information with the community will be governed by the Commission Guidelines that require a strategy for knowledge management and protection needs. The guidelines also include the need to provide open access (free on-line access, such as the ‘green’ or ‘gold’ model) to peer-reviewed scientific publications which might result from the activities. The principle is to share the achieved results to the maximum and at the same time protect the rights of the inventing party. Besides the individual projects within the cPPP, the CSA project(s) on horizontal issues that address joint dissemination will provide a platform for the interested community. The sharing of information within a cPPP project will be governed by the individual consortium agreements of the respective projects.

A major element for the success of the cPPP will be the information sharing between the various projects that implement the cPPP research agenda. Thus a central role will be played by the proposed ECS Collaboration MOU that includes a section on the information sharing between projects. Similar to sharing information with the community, the main principle for information sharing within this inner circle will be to respect intellectual rights of the owners while supporting the undertaking to progress efficient towards its goals.

Dissemination of results is particularly directed to the wider community of suppliers and users and to industrial and academic research. Besides the dissemination of individual projects the CSA on cross cutting issues will be dealing with the dissemination and furthermore the demonstration projects will contain a specific activity to communicate the success and impact of its implementation. Joint dissemination events will be organised and a variety of channels will be used to promote the achieved results and concepts with the major objective of adoption in global standards (de facto or more likely de jure).

Attention will also be given in this context to the proper usage of the ECS cPPP brand(s). The ECSO website has been reserved www.ecs-org.eu.

In conjunction with this the brand ‘logo’ is currently under development as an identity for all parts of the cPPP.

Handling of IPR is a main element of the Grant Agreement that each individual project concludes with the European Commission and of the consortium agreements established between the project partners. As described in the beginning of this section, the cPPP projects will develop a variety of technology, solutions, interface

---

specifications, etc. where the ownership conditions of the existing legal framework in Horizon 2020 will be adopted. The ownership definitions have been developed through several Framework Programmes and the set of rules are widely accepted and applied.

**Standardisation:** In areas where standardisation is highly relevant, the IPR of contributions to standards has to be secured, because this will have a significant impact on future exploitation. Particular attention has to be given to the approval process for parties to contribute to standards within projects.

**Access rights:**

- **Access rights for use** will be determined following “The Rules for Participation for Horizon 2020”\(^{51}\) as further detailed in Annex II to the Grant Agreement and as supplemented in the project specific Consortium Agreement. This provides binding rules for Ownership and Access Rights for the implementation of research and use (economic exploitation) for results and background. The partners in a project will supplement the provisions of the Grant Agreement in a Consortium Agreement. To achieve the goal of broad usage of the Results, the terms in the Consortium Agreement will be defined with an eye of being able to provide, even promote, broad uptake and long term use.

- **The cPPP proposes that all the project partners in the ECS implementation adopt a common model consortium agreement that a task force within the Association to ensure as many stakeholders as possible are involved. The expectation is that different options for access to results will be elaborated including, but not limited to open models of royalty-free access rights for commercialisation/use as well as favourable licencing for proprietary results whichever fits best with the business models of the owner and requester.**

- **Whilst the suggested model Consortium Agreement tries to implement a common understanding of IPR issues, the individual consortium agreements need to be flexible to allow for project specific agreements, that take into account the form of activity, the licence type of available background, be it open or proprietary, to not exclude individual exploitation and commercialisation of innovative cybersecurity generation technology or applications. The aim of the cPPP is to provide widespread access to the European community, and the Access Rights as defined in the Consortium Agreements will need to support this goal.**

- **Particularly SMEs have a high need to ensure that the outcomes and deliverables of the ECS cPPP are easily able to be used and that their ideas and solutions can be easily developed and protected since their resources are scarce for patenting etc. The legal helps desk and/or the legal clinic foreseen in the CSA for cross cutting topics will assist (particularly) SMEs to securely participate and develop their technology or application downstream to the market.**

The final structure and project correlations will depend on the European Commission’s decision on how to set up the cPPP through the Horizon 2020 and the following Work Programmes. Therefore the details of the IPR management will have to be elaborated following the Rules for Participation for Horizon 2020 and the concrete cPPP configuration is defined. The main guiding principle for generating impact by the ECS cPPP is the participation of all actors and players along the value chain and the reutilisation of results through agreements and principles. The IPR measures between the projects partners or between the projects within the cPPP may not be prescribed such that actors cannot participate due conflicts with their business models for later commercialisation.

### 7.5 Association Statues and Modus Operandi of the Association

#### 7.5.1 Objectives and Principles

ECSO is the formalised representation of the ECS stakeholder community. It will provide initial and updated SRIAs, KPIs to measure the progress of the cPPP and a community networking and collaboration function. The

---

\(^{51}\) Horizon2020 Rules for Participation for Horizon 2020,
association will be open to all stakeholders and will base its work on the expertise and competence of its members and drawing on existing and new liaisons to maximise capacity to deliver e.g. user groups, existing PPPs, standards bodies etc.

The primary objectives of ECSO are to support the implementation of the ECS cPPP for:

- The protection from cyber threats of the growth of the European Digital Single Market
- The creation of a strong European-based offering and an equal level playing field to meet the needs of the emerging digital market with trustworthy and privacy aware solutions
- The growth and the presence of European cybersecurity industry in the global market

ECSO will also stimulate the development and implementation of cybersecurity industrial policies activities (“supporting activities”) which would help to reach the three previously mentioned “primary objectives” leveraging upon the following actions:

- boosting European cybersecurity research, development, innovation;
- supporting definition and implementation of European Cybersecurity Policy actions;
- supporting use of European cybersecurity solutions for the development of a secure and trusted European Digital Single Market, by facilitating exchanges between European cybersecurity industries and the demand side.

To achieve these objectives the ECSO primary activities are:

- Collaborate with the European Commission to:
  - Establish a Public-Private Partnership
  - Develop and implement a SRIA and roadmap in the cybersecurity domain
- Develop strategic goals for ECS R&I and supporting their implementation
- Improve European industrial competitiveness through deployment and use of innovative ECS technologies, applications, services, and solutions
- Position ECS products and services as key enablers for solving Europe’s societal challenges
- Strengthen networking activities of the European cybersecurity community
- Promote European cybersecurity offerings and organisation
- Reach out to existing and new users and markets
- Contribute to policy development, education and technology transfer
- Support to the coordination of standardisation and certification strategies
- Recognising the ethical, legal and societal issues related to cybersecurity

In terms of specific ECSO outputs the following are the most notable:

- **Strategy**: Perform regular updates of sector and technology analysis to propose decisions about the strategy that should be taken by the cPPP, stakeholders and implementers. This strategy will be considered as prime input to the Work Programme of the European Commission in the cybersecurity domain since it will represent full and significant stakeholder interests. For example this could include an overall standardisation strategies for the various ECSO activities and results, to ensure harmonisation and interoperability principles related to various de jure and de facto standardisation bodies.
• **SRIA**: Produce a strategic plan from the strategy enshrined as a SRIA which is regularly updated with new opportunity and challenge areas. It will form a major input for the call for proposals in the ECS cPPP field. The Association will endorse the SRIA as part of the ECS Contractual agreement which will then be considered as prime input by the European Commission.

Out of this SRIA and its updates, the research actions, timing and overall plan will be produced and regularly updated. The evolution of the roadmap shall be a continuous interactive process, monitored by the Partnership Board. There should be flexibility in the lifetime of R&I Projects to respond and amend their work plans depending on the evolution of the roadmap.

• **Cybersecurity Industry Policy**: One of the main objectives of ECSO as support action to the ECS cPPP is the development and support to the implementation of a European Cybersecurity Industrial Policy. Elements of this policy would be: standardisation, certification, European trust label, etc. It is anticipated that several Working Groups of the Association will work on Cybersecurity Industrial Policy issues, providing support and advice on implementation of these activities.

• **Whitepapers**: Production of documents and other material which presents the ECSO community view on a subject and possibly offering options and recommendations for further actions

• **Roadmap Implementation Monitoring**: The Association will liaise with granted projects to evaluate to which extent these projects contribute to the ECS roadmap and what aspects of the roadmap need further commitment

• **Metric Reports**: Reports evaluating the achievements against the KPIs and monitoring industry commitments and leverage

To support these actions, ECSO will be established as a not-for-profit association (ASBL) under Belgian law of unlimited duration and based in Belgium. This is a flexible membership form of a legal entity which is often used in the context of European Commission programmes and cooperation.

The following categories shall be used to describe the types of organisation of Members of the Association:

(a) **Large companies** (directly represented): cybersecurity solutions / services providers;

(b) **National and European Organisation / Associations** (gathering among other, large companies, SMEs, RTOs, Sectoral organisations, public bodies) representing interests at national or European / International level.

(c) **SME** (as per E. Commission definition) solutions / services providers directly represented;

   Associations composed only by SME, Startups, Incubators, Accelerators.

(d) **Users / Operators** (where cybersecurity technology / solutions / services provision is not one their business activities): National public administrations or private companies (large or SMEs) directly represented.

(e) **Regional / Local** public administrations (with economic interests).

   Regional / Local Clusters of public / private Legal Entities with local economic / ecosystem development interests.

(f) **Public Administrations** at national level (national strategy / regulatory / policy issues, incl. R&I coordination).

(g) **Research Centers** (large and medium / small), Academies / Universities (directly represented, not via an associative body);

   Associations composed only by Research Centers, Academies or Universities.

(h) **Others** (financing bodies, insurances, consultants, etc.).
In addition general membership issues will reflect:

- **Leadership**: As an industry lead initiative where the leader of the Board and General Assembly should represent the Industry and where the overall ECSO must support the European Union strategies for Growth, Competitiveness whilst supporting societal value and demands.

- **Inclusivity**: Within the wider ECSO membership, in order to ensure inclusivity, the ECSO will put actions in place to ensure that where possible there is representative membership of the different organisational types (SMEs, Large, Users, RTOS, Academics, Public side), geographic balance, subsector interests as well as maintaining the ability to maximise liaison with other related parties.

- **Openness**: The organisation will operate in an open and transparent way to its members and the wider stakeholder community to facilitate the inclusivity and encourage a wide and trustful constituency.

- **Commitment & Liability**: The undertakings by the ECSO are global sector undertakings. Whilst individual Members and cPPP participants are expected to fully support the global sector commitments they do not incur any legal liability for them. The undertakings are further explained in the contractual agreement.

- **Public Support**: Beyond the strategic and resource support, as well as financial support of the members, it is expected that activities of the ECSO will be supported by one or more ECS cPPP CSA to facilitate the Work Programme and the wider public-partnership interests.

- **SMEs**: These will have a prominent role in ECSO in order to reflect the sector composition and also be represented in the ECSO Board and the ECS cPPP Partnership Board. This thus reflects European current SME strategies and the reality of the SME sector.

- **Membership Fees**: In the case the ECSO Secretariat is provided by EOS, the ECSO membership fees could be paid in kind (following decision of the ECSO Board) in that part of their EOS Members fees would contribute to fund the Secretariat (including overhead costs) as well as other organisational functions. In addition the non-EOS members will pay fees as decided by the Board of Directors to directly fund ECSO Secretariat and any other envisaged activity related to its objectives as agreed by the ECSO Board.

7.5.2 **Statues of the Association**

The text of the Statues of the ECSO Association is available on request. A companion document, the Bylaws (also available on request), specifies operational details of the Association, presenting in a deeper level of detail the composition of the Associations bodies as well as their power. The Bylaws are updated by the ECSO Board to allow more flexibility in the evolution of the rules of the Association, considering the fast evolution of the digital environment.

In the following, we present an itemisation of the most pertinent highlights of the Statutes structure and content noting that those items dealing with obvious or administrative matters, such as ‘Membership application’, are not commented upon.

**SECTION I: LEGAL STATUS/NAME/OFFICE/DURATION/OBJECTIVES/CONDUCT**

1. Legal Status, Name and Head Office
   - Name: European Cybersecurity Organisation (ECSO)
   - Location: Belgium
   - Form: non-profit Association (ASBL)
   - Jurisdiction: Belgian law

   European Cybersecurity cPPP – ECS cPPP – Industry Proposal
2. Duration
   - Indefinite period of time

3. Objectives and Activities
   - See previous sections of the Industry Proposal

4. Ethical Conduct

SECTION II: MEMBERSHIP

5. General provisions for membership
   - Legal presence in the EU, Associated Countries, or Candidate Countries
   - Classification of Members (presented in an earlier section of the Industry Proposal); details are given in the Bylaws
   - Membership rights and obligations

6. Application for Membership

7. Termination of Membership

8. Financial Contribution
   - Self-financed and independent organisation
   - Supported through Membership fees, grants, donations etc.
   - Membership fee and payment terms decided annually by the Board of Directors

SECTION III: ORGANISATION OF THE ASSOCIATION

9. Organisation Structure
   - General Assembly (GA)
   - Board of Directors (BOD)
   - Coordination & Strategy Committee (CSC), including the Scientific & Technical Committee (STC)
   - Financial Committee (FC)
   - National Public Authority representatives Committee (NAPAC)
   - Working Groups (WG) and Task Forces (TF)
   - Secretariat

10. General Assembly
    - Composed by all members
    - Observers and external experts can be invited
    - Meets at least once per year or on an extraordinary basis
    - Approves yearly activity reports and financial statements of the previous financial year
    - Appoints members of the BOD and PB (each category of members select their own representatives and present them to the GA for approval)
    - Amending statutes and dissolution of the association

11. Board of Directors
    - Operational management body to achieve objectives of the association
- Defines strategy, annual plans and actions
- Members are elected by General Assembly according to established criteria
- Ensures different member categories are fully represented
- Chaired by the Chairperson [of Board of Directors] (or vice chair)
- Sets up and dissolves WG and TF
- Drafts and approves Bylaws
- Appoints the Secretary-General and Secretariat
- Defines membership fees
- Proposing amendments to the Statutes of the Association to the GA
- Meetings maybe physical or virtual
- Adopted resolution binding on all members
- Minuted by the Secretary General and circulated to all Board members

12. Steering Committees
   - Coordination & Strategy Committee
     - Reviews and discuss Working Groups’ and ad hoc Task Forces’ suggestions and strategies,
     - Reviews and discuss overall main ECSO directions, policies and new activities related to European cybersecurity industrial policy
     - Reviews the suggestions from Working Groups’ and ad hoc Task Forces’ on the SRIA.
     - Prepares the elements to be proposed at the Board of Directors for approval.
   - Scientific & Technical Committee
     - Reviews the scientific and technical R&I challenges raised in the different Working Groups and / or Task Forces, collecting them and inking R&I issues to industrial policy and market development within the objectives of the cPPP.
   - Financial Committee:
     - Reviews the status of the accepted budget;
     - Discusses the budget of the following year;
     - Reviews the Association’s financial situation;
     - Reviews any other important financial and administrative issue linked to the Association’s activities.
   - National Public Authority representatives Committee
     - Governance rules for this Committee defined by its members (public sector)
     - Supports and discuss the activities of the private Members of ECSO at policy level and from a governmental perspective;
     - Proposes joint strategies, measures and activities at government and policy level.
     - Supports the definition and implementation of the ECSO Strategic Research and Innovation Agenda into the R&I Work Programme;
     - Exchanges best practices and promotes cybersecurity and national / regional research programmes.

13. Working Groups and Task Forces
- WGs and TFs established by BOD to consider matters of common interest
- BOD considers and approve mission statements and terms of references
- Works on operational definition of R&I priorities and cybersecurity industrial policy initiatives

14. ECSO Secretariat and ECSO Secretary General
- Executes day-to-day administration
- Operates under the authority of the Secretary-General

12. ECSO representatives at the Partnership Board
- ECSO (non-public) members are elected by the General Assembly at the Partnership Board to:
  - Discuss with the Commission the Cybersecurity cPPP Work Program,
  - Discuss the implementation of the overall R&I program related topics
  - Monitor the cPPP commitments (KPIs)
  - Prepare, in agreement with the Commission, any necessary updates of the Multi-annual Roadmap

15. European Cybersecurity Council
- High level advisory “virtual” body to provide the ECSO Board and the cPPP Partnership Board with guidelines and commitment for a longer term strategy.

SECTION IV: OTHER CLAUSES

16. Accounts Budget and Costs
17. Changes to Statutes
18. Dissolution
19. Group voting rules
20. Bylaws
- Board of Directors approves Bylaws
- Defines the size and seats for the BOD and the PB
- Regulates the operational activities of the Association
- In case of discrepancies between the Bylaws and Statutes, the latter shall prevail

21. Language
- Working language is UK English
- The French version of the Statutes is the official version

22. Applicable Law
- The Statutes of ECSO are governed by Belgian Law
ANNEX 1

8.1 Simulations of investments

As presented in the following table, we have made a tentative simulation of the possible sources of funding for the ECS cPPP, targeting a leverage factor of 3 with an initial input from the European Commission of €450M for H2020 projects. This simulation is purely indicative to have an initial view of possible engagements.

<table>
<thead>
<tr>
<th>2017-2020</th>
<th>Cybersecurity cPPP Budget M€</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INDICATIVE EXAMPLE</strong></td>
<td>EC</td>
</tr>
<tr>
<td>R&amp;I (H2020, ...), RIA, Pilots &amp; Demonstrators</td>
<td>450</td>
</tr>
<tr>
<td>CEF Digital⁵²</td>
<td>2</td>
</tr>
<tr>
<td>ESIF⁵³</td>
<td>0</td>
</tr>
<tr>
<td>EFSI⁵⁴</td>
<td>30</td>
</tr>
<tr>
<td>ISF⁵⁵</td>
<td>3</td>
</tr>
<tr>
<td>Other Investment funds (on innovative SMEs)</td>
<td>0</td>
</tr>
<tr>
<td>Other “own” Innovation funds</td>
<td>6</td>
</tr>
<tr>
<td>Education, training and exercises</td>
<td>2</td>
</tr>
<tr>
<td>Production or use of innovative solutions - tangible assets, operational spending and human resources</td>
<td>0</td>
</tr>
<tr>
<td>Investments in intangible assets: licensing, patent acquisition, ...</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>493</td>
</tr>
</tbody>
</table>

This first simulation is linked to another simulation we have made on the possible average amount of investments for the different kind of stakeholders contributing to the leverage factor.

A second simulation has been done to possibly answer to the many questions and doubts raised by the stakeholders engaging in the ECS cPPP. The goal of the simulation is to showcase, that breaking down the leverage factors to potential contributors, the average engagement of each stakeholder is reasonable.

In the second simulation, we have taken as hypothesis a contribution from the E. Commission to H2020 either of € 450M. The leverage factor is taken equal to 3. We have simulated the average contribution to the leverage factor from ECSO Members (up to 300 in the next 4 years) as well as a lower (20% of the total) contribution from other stakeholders not member of the Association (for which it would be more difficult to get quality figures; yet, considering that in FP7 the number of partners involved in ICT security projects was around 1000, we can expect a non negligible contribution from the “other” potential 700 contributors).

⁵³ ESIF – European Structural and Investment Funds http://ec.europa.eu/contracts_grants/funds_en.htm
⁵⁴ EFSI European Fund for Strategic Investments http://www.eib.org/efsi/?lang=en
A distinction has also been made between the contribution among of the different categories of stakeholders, between and their contribution to H2020 projects and to those for non H2020 R&I activities (yet linked to the leverage factor).

The simulation has been made over an average 4 year time span (the time to engage the H2020 projects). To compensate a possible “slow” start in engagement of certain members, we have also taken a compensating factor of 1.4 to increase the average needed contribution. In reality, as discussed before, the real time span to be considered is much longer, as we should consider the time to run the projects and calculate their impact on the market that can be seen 5 to 10 years after the end of a project.

<table>
<thead>
<tr>
<th>INDICATIVE SIMULATION</th>
<th>Average contribution - compensated - for each member over 4 years non H2020 R&amp;I</th>
<th>Average contribution - compensated - for each member over 4 years H2020 R&amp;I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Large companies</strong> (directly represented): cybersecurity solutions / services providers;</td>
<td>6.8</td>
<td>1.8</td>
</tr>
<tr>
<td><strong>National and European Organisation / Associations representing interests at national or European / international level.</strong></td>
<td>0.0</td>
<td>1.0</td>
</tr>
<tr>
<td><strong>SME (as per E. Commission definition) solutions / services providers directly represented:</strong> Associations composed only by SME, Startups, Incubators, Accelerators</td>
<td>2.1</td>
<td>1.3</td>
</tr>
<tr>
<td><strong>Users / Operators</strong> (where cybersecurity technology / solutions / services provision is not one their business activities): National public administrations or private companies (large or SMEs) directly represented</td>
<td>4.8</td>
<td>1.2</td>
</tr>
<tr>
<td><strong>Regional / Local public administrations</strong> (with economic interests);</td>
<td>6.0</td>
<td>0.0</td>
</tr>
<tr>
<td><strong>Regional / Local Clusters of public / private Legal Entities with local economic / ecosystem development interests</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Public Administrations at national level</strong> (national strategy / regulatory / policy issues, incl. R&amp;I coordination)</td>
<td>9.0</td>
<td>1.6</td>
</tr>
<tr>
<td><strong>Research Centers</strong> (large and medium / small), Academies / Universities (directly represented); Associations composed only by Research Centers, Academies or Universities</td>
<td>1.4</td>
<td>4.0</td>
</tr>
<tr>
<td><strong>Others</strong> (financing bodies, insurances, consultants, etc.)</td>
<td>16.0</td>
<td>1.8</td>
</tr>
</tbody>
</table>

In conclusions, we think that these figures can be reasonably reached by the different members of the association in a time span that can range from 4 – 5 up to 10 years (as discussed previously).