STRATEGIC RESEARCH AND INNOVATION AGENDA

WG6 I Strategic Research and Innovation Agenda

JUNE 2017

www.ecs-org.eu

ABOUT ECSO

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

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

Contact

For queries in relation to this document, please use wg6_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

This document integrates the contributions received from ECSO members to produce the Strategic Research and Innovation Agenda. Despite the authors' best efforts, no guarantee is given that the information in this document is complete and accurate. Readers of this document are encouraged to send any correction to the ECSO WG6 secretariat, please use wg6_secretariat@ecs-org.eu.

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

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

EXECUTIVE SUMMARY

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, Industry 4.0, communications and public services) must be supported by cybersecurity solutions that meet the needs of emerging digital markets.

Several challenges have been described in the cPPP European Cyber Security (ECS) industry proposal and initial cPPP Strategic Research Innovation Agenda (SRIA) v1.0. We can briefly summarize some of those here as follows:

- Market fragmentation;
- Innovation led by imported ICT products;
- Need to mitigate cyber security dependencies from external sources and achieve strategic supply chain in the field;
- Less funding to research and innovation available and often dispersed due to a lack of transnational approach;
- European industrial policies not yet properly addressing specific cybersecurity issues;
- Weak entrepreneurial culture and lack of venture capital;
- Human factor and skills shortage.

The ECS cPPP has its roots also in the convergence of the Secure Societies priorities of Horizon 2020 and the ICT Industrial and Technological Leadership; these two areas supported by different program committees of Member States (MS). This convergence has contributed to the definition of the main strategic objectives to be achieved by the ECS cPPP, which are:

- 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 Europe's cybersecurity industry in the global market.

The objective of the cPPP is to bridge the gap between capacity building and the deployment of trusted European cybersecurity solutions on European and international markets. Therefore, creating new business opportunities for Europe's industry while addressing the challenges faced by Europe and defending its stance on safeguarding the privacy of citizens. In particular, the approach of the cPPP ECS is overall to:

- Protect critical infrastructures and vertical sectors from cyber threats;
- Increase European digital autonomy;
- Provide security and trust of the whole supply chain;
- Invest in areas where Europe has a clear leadership or strategic needs;
- Leveraging upon the potential of SMEs;
- Increase competitiveness.

In this document, we describe the input of the European Cyber Security Organisation (ECSO) SRIA input to H2020 Work Programme 2018-2020 (WP2018-2020), as such, this document focuses on

activities of specific pertinence to H2020. So, its content should not be interpreted as the whole cPPP SRIA, since this would entail also policy activities and research and innovation funding possibly beyond H2020 (as national and regional).

In particular, since the projects in the WP2018-2020 would likely deliver their results between 2021-2023 (considering an average of three years of duration), the ECSO WG6, focusing on the research priorities, had to consider short to mid-term research goals as well as the evolution of the threats and technologies landscapes as well as of market conditions.

ECSO WG6 started from commonly agreed cPPP SRIA v1.0 and further refined it, also using several guidelines:

- Allow funding of applied research and innovation, by focussing resources on fields that could maximize European competitiveness in the cyber security market;
- Concentrate efforts on cyber security sectors strategic to Europe (and its digital sovereignty);
- Link the demand with the supply side of research in a top down approach: (i) identify the main requirements from the vertical application domains / users' needs, also useful to define large transversal infrastructures (applicable to several domains), (ii) leverage upon basic components, all in an improved ecosystem able to understand the challenges and (iii) use innovative solutions;
- Show the benefits of available cyber security technologies also from previous projects through main demonstrators and possibly based on European large cyber security transversal infrastructures;
- Foster continuous innovation also through further research for basic technologies and components as well as look forward for possibly disruptive technologies in order to keep medium/long term competitiveness for the products and services;
- Developed technologies should be applicable as much as possible to different vertical application domains, but should also be easily adapted to the specific needs of those verticals;
- “Reference Potential Customers" or "Targeted Users" when defining the research and innovation topics, we should clearly identify the reference customers/end users, in particular for demonstrators, and these stakeholders should be involved in the project proposal.

TABLE OF CONTENTS

1. INTRODUCTION

This document represents the inputs of the WG6 on the Strategic Research and Innovation Agenda (SRIA) of the European Cyber Security Organisation (ECSO) in order to suggest potential topics for calls of project proposals related to cyber security for the H2020 Work Programme 2018-2020 (WP18-20).

The structure of the document is as follows.

Section 2 describes the overall ECSO strategy for the consolidation and growth of the European cyber security market and industry.

Section 3 describes the kind of projects useful to achieve the goals of the cPPP and their relationships. Each kind of project and its possible call topics are detailed in the next sections. In particular, we describe the recommended topics for the H2020 calls in the format for the H2020 calls, i.e., *specific challenge, scope, expected impact, topic budget* and *time* planned for the call. In addition, we also inserted additional field to better motivate the choice of the suggested topics, including the market, the rationale for having this done at European level, the target users and other elements.

The following sections describe the kind of projects: Section 4 describes the cyber coordination projects, Section 5 describes the cyber ecosystem projects, Section 6 describes the pilot projects for vertical application sectors, projects, Section 7 describes the cyber transversal infrastructures and Section 8 describes the cyber technical projects. Section 9 summarises the overall tentative planned budget.

A market analysis is also provided in the appendix.

1.1 Main Instruments/Projects

ECSO WG6 identified the following four main kinds of projects for H2020, based on the previous work in the cPPP SRIA v1.0 and subsequent discussions/meetings of ECSO WG6 (involving more than 100 of members and experts) in the last three months:

- **Ecosystem:** socio-technical projects for the development of ecosystems favourable to better implement and use innovative solutions and protect applications.
- **Demonstration Projects**: demonstration of available solutions in specific vertical domains to provide national security, protect citizens and economic relevant EU market sectors, allowing economies of scale through engagement with users/demand side industries and bringing together a critical mass of innovation capacities. These projects should eventually deliver results with TRL[1] 6-9.

[1] Where a topic description refers to a TRL, the following definitions apply, unless otherwise specified:

TRL 1 – basic principles observed; TRL 2 – technology concept formulated; TRL 3 – experimental proof of concept; TRL 4 – technology validated in lab; TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies); TRL 6 – technology demonstrated in relevant environment

- **Transversal infrastructures**: projects able to integrate sector-neutral technological building blocks with maximum replication potential, to tackle transversal challenges (common to different application domains). These projects should eventually deliver results with TRL[1] 6-9.
- **Technological components**: mainly devoted to build those sector-neutral technological building blocks with maximum replication potential that can become market references at global level. These projects should eventually deliver results with TRL[1] 3-5.

It is however relevant to note that although we name those kinds of projects depending on the specific kind of output, the types of instruments of H2020 are mainly of three kinds, Coordination and Support Actions (CSA), Innovation Actions (IA) and Research and Innovation Actions (RIA).

Further detailing these concepts, we identified seven main priority themes for intervention as follows:

Ecosystem for Education, training, market growth and SME support (see Section 5)

- Cyber Range and simulation
- Education and training
- Certification and standardisation
- Dedicated support to SMEs

Demonstrations for the society, economy, industry and vital services (see Section 6)

- Industry 4.0
- Energy
- Smart Buildings & Smart Cities
- Transportation
- Healthcare
- E-services for public sector, finance, and telco

Collaborative intelligence to manage cyber threats and risks (see Section 7)

- **GRC**: Security Assessment and Risk Management
- **PROTECT**: High-assurance prevention and protection
- **DETECT**: Information Sharing, Security Analytics, and Cyber-threat Detection
- **RESPONSE and RECOVERY**: Cyber threat management: response and recovery

Remove trust barriers for data-driven applications and services (see Section 8.1)

- Data security and privacy
- ID and Distributed trust management (including DLT)
- User centric security and privacy

Maintain a secure and trusted infrastructure in the long-term (see Section 8.2)

(industrially relevant environment in the case of key enabling technologies); TRL 7 – system prototype demonstration in operational environment; TRL 8 – system complete and qualified; TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

- ICT infrastructure protection
- Quantum resistant crypto

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications (see Section 8.3)

- Trusted supply chain for resilient systems
- Security-and privacy by-design

From security components to security services (see Section 8.4)

- Advanced Security Services

The budget distribution and the sequence per topic as requested by the Commission is given in Section 9.

2. THE GLOBAL STRATEGY FOR R&I

Information and Communication Technologies has a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. The security of this infrastructure is central to economic growth, competitiveness, the correct functioning of democracy, and civil rights of the citizen. Yet, as it often happens, security is an afterthought and its market structure is still maturing, lagging significantly behind the ICT sector as a whole. This gives us the opportunity to build on the lessons acquired within the larger ICT hi tech market to improve the support to innovation and ease its transfer to the market and alignment to user needs.

At the moment, the European cybersecurity market represents about 24%, less than the contribution of Europe to Global GDP (i.e. about 26%) with an average yearly growth slightly larger, around 6%, when the world market is growing at about 8% year, so we must improve and do so fast.

In summary, we need to show our leadership in the area of cyber security; i.e. collect forces and provide solutions for the problems that are hindering the way toward a sustainable Digital Single Market. With cyber security as a transversal need across all economic sectors, one example of this leadership is to summon the actors from other PPPs and coordinate mutually interesting cyber security initiatives to enforce a common ground and ease the pervasiveness of cyber-secure approaches, solutions and processes.

2.1 Factors Affecting Growth

Before deciding what needs to be done, we must first understand and classify the underlying trends that affect growth and leadership in this field. Consider the following brief descriptions of these trends:

- Europe's share of the global economy is declining due to slower growth. Europe's average growth in the last years has been about half the rate of North America and Asia. European high-tech companies produce the majority of their revenue in domestic business.
- EU market is fragmented in practice, making growth difficult. Even if Europe's GDP accounts for 26% of the global GDP (Eurostat), it is not easy to tap into that potential for economies of scale, due to still prevalent cultural, language, legal, and regulatory differences. For an EU player, going abroad can be almost as complicated as it is for non-EU companies. This is true in most markets, but fragmentation is even higher in the cyber security sector, which is often intertwined with either national security issues or sensitive information within organisations.
- **Funding shortages and entrepreneurial support.** Europe's venture capital arena is small and fragmented, where it exists at all. Europe lacks a global high-tech stock market such as NASDAQ in the United States that supports growth and provides exit routes for investors. Even if certain parts of the EU have a thriving SME community (Northern Italy, Germany), they focus mainly on traditional sectors. Also considering the red tape involved in establishing a company, the risks of pursuing unproven technologies are less rewarded and encouraged, thereby hindering the creation and the uptake of innovations.

- Europe procurement policies focus too much on short-term savings without promoting customer-vendor partnerships needed for innovation. High government debt and the difficulty to couple austerity measures with structural reforms has induced a European procurement approach that seems single-mindedly focused on short-term cost reduction, asking suppliers to conform to commoditized specifications to obtain the lowest possible prices. We suggest that customer-vendor partnerships are needed to foster more innovation. In the United States and in parts of Asia, major buyers follow a deliberate strategy of supporting local high-tech firms with a view to long-term competitiveness. The U.S. government uses its vast procurement spending directly and indirectly to shape the U.S. high tech industry.
- **Less investment in R&D and little market success.** Europe invests almost one percentage point less of its GDP into R&D than the United States and 1.5 points less than Japan. Funding procedures are slow, especially at the national and local level, introducing intolerable latency between proposals and their realisation. The European research sector is often outstanding, but these innovations do not make it to market quickly enough. There is not enough collaborative projects where theory and innovation can meet, exchange views and ideas, and evolve in a joint fashion that can lead to commercial success. On the other hand, the R&D power of some non-EU players is massive, allowing them to take advantage of technological shifts.
- **Skills shortages.** Europe's universities are not producing enough scientific graduates (16% vs 29% in South Korea and 31% in China). In China alone, 700,000 engineers and computer scientists graduate each year vs. 500,000 in Europe). Europe's fragmented nature limits cross-country mobility. For instance, funding of PhDs in Cybersecurity across Europe can and should be increased urgently.
- **European companies favour execution over strategic vision.** Many high-tech companies have focused more on building operational capabilities than on pursuing long-term strategic planning. In fast-changing markets, this is a dangerous choice. For example, in the mobile telecommunication world, companies failed to recognise the importance of software and the smartphone, thereby not putting their strengths in the fast-growing applications market segment.

2.2 cPPP proposal

To support the growth the hi-tech sector and shore it up with cyber capabilities requires a cooperative approach between the main stakeholders involved:

- The European Union
- EU Member States and Public Administration
- Large Companies
- Small and Medium-Sized Enterprise
- Universities and Research Institutions
- Venture Capitalists and Financial Institutions

Some of the issues at stake in this area seem to have systemic causes — concerning the culture and structures in Europe. However, other issues are more susceptible to intervention — improving industrial policies, tackling the right challenges and incentives, redirecting regulation and reducing red tape, and funnelling investment to the right sectors.

Master plan with clearly defined cyber security focused areas. We must focus investments, based on informed and prioritised strategic choices, to ensure that resources are not spread too thinly. A strategic master plan for Europe that clearly defines the sectors and key areas in which it can and wants to achieve leadership will lead to more focused investments. Such a master plan requires EU institutions to work with national governments and the EU cyber tech sector, represented by major industry associations / key industry players as well as research and academia. Aligning most if not all public funds and actions with the plan will ensure it is executed with maximum force.

- Analysing the global competitive environment and the industrial strengths and cyber security technology leaders, we would encourage focusing on high-end, B2B and business-to-government (B2G) areas.
- We must focus on economic sectors in which Europe has a comparatively strong position, such as the defence, automotive, and process industries, mechanical engineering, utilities (including utility equipment vendors), telecom, and financial services.
- The master plan should focus on cyber subsectors that will specifically address the challenges of these industries and create a home market for European players. **These sectors include embedded systems (including semiconductors), intelligent networks (such as smart grids), cyber-physical systems, ICT-enabled secured smart automation (Industry 4.0 strategy), complex software systems, security systems, and big data and analytics solutions.**
- We must focus on the needs of these players and major EU buyers more than on technology to deliver solutions that give them competitive advantages. This could encourage large buyers to make investment and spending decisions based on a longer-term view that looks ahead and not only on prices in the present, in order to turn research and innovation into commercial success.

3. CYBER PROJECTS AND THEIR RELATIONSHIPS

Cybersecurity technologies are and have to be further deployed in several application domains. There is, therefore, a need to align these technologies to the needs of the application domains, and strongly link the demand side and supply side for such cyber technologies. In addition, cyber technologies have often to be adapted to the specific needs of each application domain. This adoption, experimented in the form of **pilot projects**, may entail the usage of large **trustworthy infrastructures** that will also contribute to create a digital autonomy in a field as strategic as cyber. In turn, these infrastructures may need further technical development of **basic components capabilities**.

Starting from these considerations, the main strategy of the ECSO in selecting the topics is based on how these will maximise the impact of the invested economic resources, by identifying the needs of the vertical sectors. There is also the need to create large infrastructures that **span several application domains** in order to avoid technological silos that could limit the interoperability of the systems. These large infrastructures may use existing components, or in the medium to long term require the development of technologies and knowledge for basic components, and this is achieved through research and innovation projects. This approach is exemplified in the following picture.

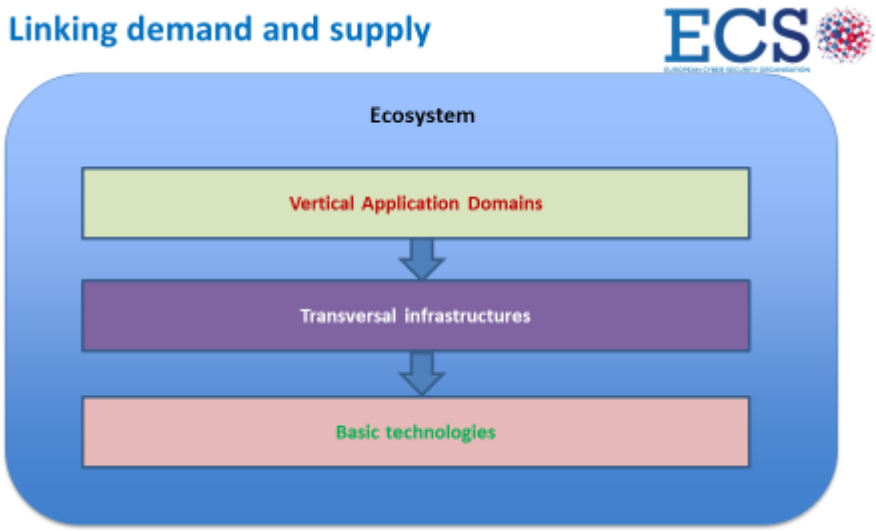

Figure 1 - ECSO approach in selecting the topics

Thus, in order to implement the research and innovation strategy and to align technical with cooperation and coordination aspects, five major types of mechanisms/projects are recommended:

- **Cyber Coordination (Coordination and Support Actions):** These projects will foster cooperation (also international) for the efficient sharing of information and coordination of activities.
- **Cyber Ecosystem**: Combination of organisational and technical elements – will allow challenges to be addressed in an interdisciplinary way and will serve as a hub for research, innovation, standardisation / certification, experimentation and transfer to market activities.

- **Cyber Pilots:** These projects, mainly innovation based, are devoted to piloting solutions in specific vertical domains. These pilots or demonstrator will possibly use the transversal cyber infrastructures and the capabilities developed in the technical projects to demonstrate how the developed innovations can satisfy specific requirements in key vertical sectors, garnering attention and the commitment of users and potential procurement bodies.
- **Cyber Infrastructures:** Large (lighthouse) projects that will help to develop large infrastructures in the cyberspace, mainly spanning across several domains with a goal to create a direct competitive advantage to industry and of strategic relevance for European countries. It includes large scale projects which could be funded through a number of different channels, including Horizon 2020 and structural funds. They are specifically designed to raise awareness of the Partnership and give it increased visibility. These large infrastructures need to have a sufficient budget (between 10 and 20 M€ of overall total budget) to provide significant results and impact.
- **Technical projects**: Small or medium scale technical projects, often R&I activities for developing new cyber security capabilities and components. We should ensure that these projects contribute to develop the technical competences and contribute to the KPIs of the cPPP. These projects would be based on clearly defined technical priorities.

3.1 Priority areas

Further detailing these concepts, we identified seven main priority themes for intervention as follows:

Ecosystem for Education, training, market growth and SME support

- Cyber Range and simulation
- Education and training
- Certification and standardisation
- Dedicated support to SMEs

Demonstrations for the society, economy, industry and vital services

- Industry 4.0
- Energy
- Smart Buildings & Smart Cities
- Transportation
- Healthcare
- E-services for public sector, finance, and telco

Collaborative intelligence to manage cyber threats and risks

- **GRC**: Security Assessment and Risk Management
- **PROTECT**: High-assurance prevention and protection
- **DETECT**: Information Sharing, Security Analytics, and Cyber-threat Detection
- **RESPONSE and RECOVERY**: Cyber threat management: response and recovery

Remove trust barriers for data-driven applications and services

- Data security and privacy
- ID and Distributed trust management (including DLT)
- User centric security and privacy

Maintain a secure and trusted infrastructure in the long-term

- ICT infrastructure protection
- Quantum resistant crypto

Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

- Trusted supply chain for resilient systems
- Security-by-design

From security components to security services

- Advanced Security Services

Those priorities are further refined in the next sections. We also considered a couple of coordination actions for international cooperation of ECSO with external bodies/organizations.

3.2 Interaction among instruments for implementation

The following image highlights the role of the different types of projects in the cPPP. In particular, technical projects are used to deliver the basic capabilities (building blocks), on top of which both large cyber infrastructures (cross domains) and domain specific pilots can be leveraged.

One of the main goals of the cPPP is the establishment of pilot solutions for cyber infrastructures. Such cyber infrastructures should address core aspects of ICT. The number and size of the pilot projects will also depend on the relevance of the sector for the cPPP members and on the need to avoid redundant efforts already made by other European initiatives.

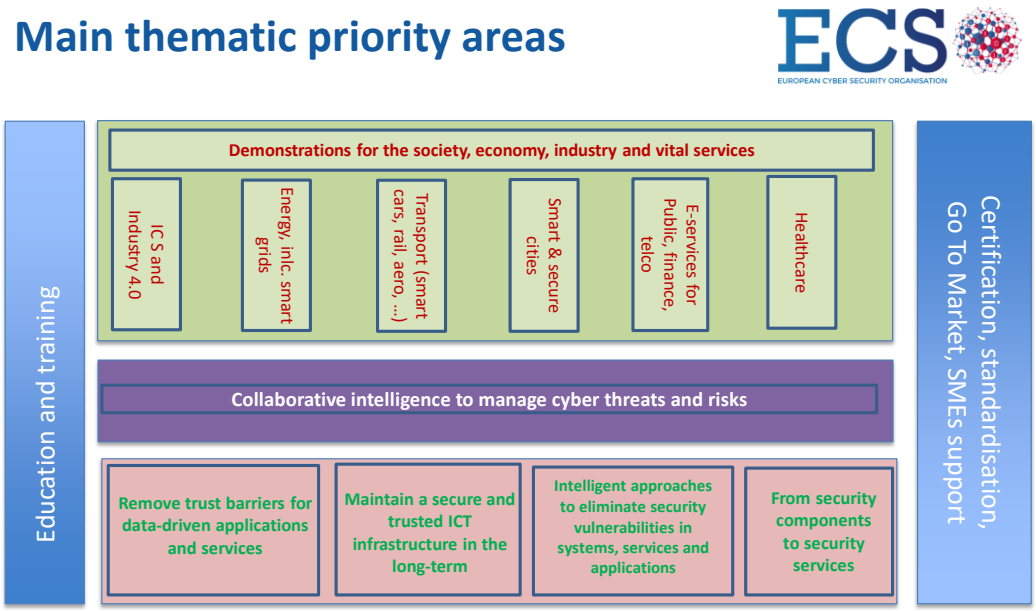

Figure 2 - Interaction among instruments (focus on infrastructures, technical projects and pilots).

4. CYBER COORDINATION PROJECTS

4.1 cPPP international cooperation

4.1.1 Specific challenge

The challenges to be addressed are:

- Developing and integrating cyber-security strategies at the EU, national, and regional levels.
- Promoting EU cyber-security and privacy research and innovation.

4.1.2 Scope

Proposals may cover one of the two strands identified below.

1) Coordinating cybersecurity actions within EU and in particular with other cPPPs

Security is a horizontal property of systems. Usually, security is conceived as an afterthought property, which might mean that the final services provided are not secure. On the other hand, it is a fact that other cPPPs consider security and privacy as a strong need, however their results on this regard must be necessarily aligned with the directions provided by the cPPP on Cybersecurity. The objectives to reach the scope are:

- Synchronise and align cybersecurity initiatives in Europe (including national and regional initiatives) to achieve a Security Digital Single Market to reduce the high risk of a “Digital Fragmented Market”.
- Analyse corresponding SRIAs for identification of alignments and divergences in Cybersecurity aspects and align them across PPPs with regards to cybersecurity.
- Look at further cPPPs harmonisation of actions during Cybersecurity cPPP life and beyond.
- Harmonization of cyber security actions during cPPP and beyond towards Digital Single Market within EU.
- Identify and engage relevant stakeholders in other PPPs, verticals, public sector, etc.

2) Cyber Coordination of international cooperation outside Europe

There is an increasing need to reduce the distance with the world-wide research communities dealing with cyber security and privacy issues. While there are currently several coordination actions, with US and Japan it would be useful to extend all the international activities to several other countries.

- Many activities worldwide on cyber-security, beyond US and Japan
- Identify relevant activities in other countries/regions
- Encourage and facilitate dialogue between EU and other worldwide stakeholders
- Promote EU cyber-security and privacy research and innovation activities

4.1.3 Expected impact

- For strand 1)
- Engage with a network of public and private cyber security stakeholders with supporting information sharing with regards to organisational, technical and economic aspects of cyber security, this should in particular include the role of coordination of cPPP with respect to others cPPPs.
- For strand 2)
- Establish international cooperation also outside the European borders in the field of cyber security

4.1.4 Budget / Time / Instrument

1ME (for strand 1), 1ME (for strand 2), 2018, CSA

5. CYBER ECO-SYSTEM

5.1 Overview and rationale – the need for an eco-system

Cyber-security is a challenge that pervades the entire society – and cyber-attacks can create chained reactions that can easily move from a purely IT environment to the physical world, creating havoc across cities, regions, infrastructures and operations.

This challenge has moved the actual topic from a purely technical one to a whole new dimension in which final users, whatever their level of expertise, have not only to be made aware of potential dangers but also trained to adapt their behaviour to the level of risks to which they are exposed, at work and at home.

Even when considering only the technical dimension, the *speed* at which cyber-attacks propagate and the *diversity* and multiplicity of mechanisms through which they propagate make them difficult to prevent and introduce a huge challenge. Addressing this challenge requires a *level* of collaboration between solutions, service providers and users that has never been experienced before.

It also requires an *organised approach* to speed up the move from innovation to solutions adopted by users, from the validation and certification point of view as well as from the adoption point of view, to create a level of awareness, interest, trust and confidence in the appropriateness, value and interaction of innovations with pre-existing environments.

Indeed, while the challenging speed at which the cyber-attacks evolves is increasingly being matched by a fast evolution of prevention and defence solutions developed by the ICT community, the actual adoption of these solutions has to be supported and managed, creating the need for a verification and certification approach in controlled environments.

Not all new solutions appearing on the market (e.g. usage of AIs) have been tested in different production environments (ranging from SMEs to Enterprises), nor is there a commonly agreed set of best practices and large-scale escalation performances' indicators.

Interestingly, the distance between research, attacks and innovation in ICT security is today at its historical minimum, because the driving forces and interests involved on all sides (cybercrime, cyberterrorism and ICT security) all head in the same direction. For example, both sides, enterprises and cybercriminals, carry out research for new tactics and techniques.

Cybercrime's economy is, already now, largely based on an ICT and human ecosystem of services and competences that is based on transitive trust, among cyber criminals that do not know each other. And, like any other ecosystem of this type (e.g., crime), it is vulnerable to sibling intrusions (e.g., police infiltration). The answer of cybercrime to this fundamental problem has been to increasingly become insular around more regulated, collaborative and small environments whose new members are carefully scrutinized. The ICT security has, over cybercrime, the advantage of being based on stronger and open trust chains, but is also weakened by a competitive approach

between its stakeholders and an overall lower willingness to collaborate. Therefore, the aim of having a **European wide eco-system** is to exploit the advantages, mitigate the competitive forces and create a real "co-opetitive" approach at EU level. The evolution on the one hand of ICT eco-systems, of collaborative technologies and mindsets (e.g., people are used to collaborative wikinomics approaches and to share on social media) and, on the other hand, the increasing speed of cybercrime and terrorism, offers the EU, for the first time, the opportunity to create a fully operational and effective approach to cater, together, to cyber-resilience needs.

Collaboration is the only way to succeed, on both sides of the barricades: cybercriminals, driven by pure profit logics, are facing today an unforeseen level of collaboration and commoditisation with the clear advantages of improving their competitiveness and return of investments[2]. A similar, elastic and rapid, level of collaboration is still not sufficiently present in the ICT Security community and between the providers and users.

In general, eco-systems are of two possible types:

- ICT eco-system: a network of integrated services that can interact with each other to offer the user a unique and seamless vision.
- Human eco-system: a community of people who interact, exchange information, combine, evolve in terms of knowledge, skills and contacts, to improve their lives and meet their own needs.

The evolution of the European cyber eco-system goes through the implementation of both eco-systems, a technological eco-system which is the baseline for supporting the human eco-system, where knowledge, skills and contacts are shared to improve the cyber resilience of the EU community.

Therefore, creating an operational eco-system is key to address the many issues that contribute to an overall increase in the level of cyber-security – and one of the challenges is to address **user needs** across **key strategic application sectors**, while reducing fragmentation across Europe and speeding up the creation of innovation, its uptake by users, and its transfer to the market.

To address the challenge, the approach is to create a continuum in terms of **constituency** – from users to solution providers and in terms of **mechanisms** – from need to innovation and market. The approach is to create a single integrated and inclusive eco-system that implements this continuum.

This continuum joins

- The **structured involvement of users**, allowing different sectors to express their specific needs that are then consolidated into an experiment open to many providers to join forces to combine their solutions in a single experiment
- **Specific support to SMEs** across Europe, across a range of measures ranging from networking, go-to-market and access to finance and links to different market actors,

[2] E.g., K. Thomas, "Framing Dependencies Introduced by Underground Commoditization," in *', Workshop on the Economics of Information Security (WEIS)*, Delft, Netherlands, University of Delft, 2015. [Online]. Available: http://www.inwyrd.com/blog/wp-content/uploads/2010/03/weis2015_blackmarket.pdf. Accessed: Nov. 29, 2016.

including investors and incubators, to increase their capacity to detect innovative players **earlier** in the development process

- The offering of **qualified profiles** thanks to the involvement of professionals in highly collaborative environments able to cover the whole value chain, from research to innovation and market, including attack strategies.
- The approach of a cyber range environment that enables the growth of cybersecurity industry and strengthens Europe's cybersecurity capacity by enabling four practical hands-on activities, that include training and certifying as well as experimenting and validating new approaches. The goal of these activities is to provide a facility that resembles real-life operational environments of attack and defence, for practicing, as many activities cannot be simulated in the real environments. Moving to the next level of details on each of these three activities:
    - *Training:* training professional work forces, either as a group of organisations (SMEs, sectoral association members) or as individual organisation against cyber-risks, including taking into account human factors in the spread of cyber-attacks. The training will also include the organisation of internships for students and young professionals.
    - *Certifying*: linked to the EU label under development. Certification is linked on the one hand to *compliance* of an individual solution to the EU label under development, but as importantly to "compatible with" other solutions, addressing the issue of solutions working together to deliver an (agreed / understood) level of protection against (identified / adequate) cyber risks (see also experimentation categories below).
    - *Experimenting*: testing how *combined solutions* can operate together to fully address a need defined for a user / a sector.
      The different steps include:
        1. Consolidate user needs into an experiment: this allows to take *very precise needs*, for a sector (transport, finance, health etc.), for a group of users.
        2. Detail the experiment to be run: requires an experiment coordinator, and collaboration with the users (creating the experiment from user needs).
        3. *Advertise* the experiment, opening up to all cyber providers (academic, industrial, public, private) to "subscribe to the experiment" by providing one or more solutions or innovations under development that can be combined.
        4. *Run* the experiment by combining the solutions put together by the organisations with users.
        5. Deliver the results of the test, leading to *certifying* a functionality, also understanding the limits of implementation.

      The experimentation functionality builds on the experience and best practices acquired during the ACDC pilot project that was funded under CIP-PSP programme, and run from 1st February 2013 to 31st July 2015. Its infrastructure has continued operations as a data sharing facility.
    - *Validating*: for a customer who has an existing environment and wants to ensure that a solution (or group of solutions) selected will deliver what the customer is looking for, that it will not create new vulnerabilities in the existing environment or that new vulnerabilities are considered.
    - *Creating competences:* support the creation and delivery of EU standard qualification profiles able to foster the EU cyber security market for SMEs and big Enterprises. The knowledge accumulated for the above key directions, can be used

to offer certified and up to date qualification profiles, to foster the professional competences through certified learning objectives.

The overall budget foreseen for the eco-system is summarised below and detailed in sections 5.2 to 5.5.

			2018	2019	2020	
Total			**15 M€**	**17 M€**	**10 M€**	**42 M€**
Cyber-ranges	Strand 1	Cyber-range across sectors		5 M€		5 M€
Cyber-ranges	Strand 2	Network of cyber-ranges			5 M€	5 M€
Education	Strand 1	Dynamics of education	4 M€			4 M€
Education	Strand 2	Integration of skills		3 M€		3 M€
Certification	Strand 1	EU trust label	2 M€			2 M€
Certification	Strand 2	Certification of cyber-security dynamicity			4 M€	4 M€
Certification		Certification "lite"	1 M€	1 M€	1 M€	3 M€
SMEs	Strand 1	Innovation for providers	6 M€	3 M€	2 M€	11 M€
SMEs	Strand 2	Innovation for users		2 M€	2 M€	4 M€

5.2 Cyber Range and simulation

5.2.1 Specific challenge

According to multiple converging sources[3], there is an increasingly pressing need for cyber-security professionals and experts. Emerging cyber-risks pose new challenges to society, and both public and private sectors need skilful cyber-security experts to take care of their services and infrastructures. In fact, it is well known that many employees of companies have specific training interests in cyber-security (e.g., security in industrial equipment, malware analytics, virtualization techniques, etc.). Establishing measurements and ranges to classify the capabilities of the professionals in cyber-security, as well as defining the degree of protection of the infrastructures against cyber-attacks, becomes fundamental. This will be not possible without simulation techniques that implement a wide number of complex scenarios and on-demand countermeasures. Simulation not only provides a clean solution to train professionals and to protect organizations while reducing costs in specific equipment, but also provides sustainable mechanisms according to the *Green* perspective of which Europe is echoed.

[3] http://www.informationweek.com/strategic-cio/security-and-risk-strategy/cyber-security-skills-shortage-leaves-companies-vulnerable/d/d-id/1326463 (Accessed: 22 August 2017).

https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf (Accessed: 22 August 2017).

The cyber-range and simulation concepts are of relevance to all stakeholders, regular users, professionals and experts. It is important to note that cyber-security experts need to continuously adapt their expertise to a constantly evolving attack landscape, a widening range of IT-impacted services, and changing regulations. The needs include, but are not limited to, analysts able to diagnose attacks and respond appropriately in real time, investigators able to extract information from increasingly voluminous and complex forensic data, and observers able to deal with threat intelligence and early warning.

Taking into account the fact that cyber-ranges are partially addressed during 2017 with the DS-07 call, the challenge focuses on extended capabilities of cyber-ranges:

- Focusing on extending the cyber range capabilities to incorporate **user domain specificities**, additionally to the ICT oriented cyber range approaches such as those covered already in the 2017 call. For instance, Cyber Range for SCADA, ICS, HVS models, mobile devices, health related devices and Internet of Things related devices etc. This will include development of the tools for mapping the real-life systems allowing the range system to automatically simulate an equivalent environment for testing and exercising, as well as cloning real life environments in order to provide realistic backgrounds for exercises and re-playing previous attacks.
- Development of integration / federation solutions for different simulation environments and enablement of secure sharing of simulation modules and artefacts to enable trainees to gain more versatile and relevant experience and facilitate knowledge sharing between European partners. It will also make it possible to involve range environments with very specific configurations that are difficult to recreate due to some domain specific components or to the sensitiveness of a domain environment (e.g. specific SCADA system ranges etc.).
- Development of tools to automate the preparation for large-scale simulation scenarios to ensure optimal use of human resources and efficient utilization of existing cyber range infrastructures.
- Development of tools for self-learning, adaptable and integrated red team capabilities within a simulation environment that are able to realistically replicate human behaviour and support development of new threat vectors.

Business impact of cyber-ranges:

- Fast and efficient deployment of on-demand security resources.
- Development of tools to enable comprehensive, efficient and error-free capture and preservation of simulation data that can later be used for research, analysis, developing new strategies, products, frameworks etc.
- Development of tools to enable replay, sophisticated automated analysis and visualization of historic data, e.g. automate analysis of situational awareness, risks and competences profiling, but also as input to new products development.
- Development of tools and technologies that allow the range system to be automatically verified and sanitised. The developed tools should provide the ability to encapsulate and isolate tests, data storage and networks to ensure secure and uncompromised range environment.
- Development of architectures and tools to enable the industry to test their products, services and solutions in an attack-defence environment, fostering and supporting industrial collaboration and enabling the development of higher quality products.

- Development of mechanisms to a) ease the translation from user needs to scenarios and experiments, and b) the deployment of combined solutions and services to cover all dimensions of an experiment
- Development of sustainable business models and related tools to enable scaling of the range environments to meet the needs of large spectrum of interest groups (critical infrastructure providers, universities, large companies, start-ups and SME-s etc.) to ensure the availability of such environments.

5.2.2 Current status

Cyber-ranges are also used to experiment novel technical tools and services within the exercise frameworks prior to their actual uptake in operational environments. Cyber range environments are not yet adequately supported by tools that capture the necessary data that can later be used for developing new strategies, products, frameworks etc.

Two projects already running and relevant to this topic have been identified:

COSSIM (A Novel, Comprehensible, Ultra-Fast, Security-Aware CPS Simulator) provides a simulator specifically designed for Cyber Physical Systems which is not designed to train people but to obtain fast and accurate results of these systems - http://www.cossim.org.

FORTISSIMO and FORTISSIMO 2 (https://www.fortissimo-project.eu/origins/fortissimo-2-project, EU project, H2020). The Fortissimo project “provides one-stop, pay-per-use, on-demand access to advanced simulation and modelling resources including software, hardware and expertise”. However, it is not build under the cyber-security perspective needed to the preparation of cyber-security professionals and the definition of cyber-ranges.

5.2.3 What market

The existing simulation infrastructures are often government funded and operated, as well as defence focused; however to reach the objective of higher competitiveness of European cybersecurity industry as well as more secure digital society in Europe in general, the systems also need to cater to the needs of start-ups, universities, SMEs and large companies, critical infrastructure providers, etc. and extend their applicability to foster services that a) target single providers and speed up the applicability of innovations, b) allow different providers to join forces to address a well-defined user needs by combining their offerings and c) ease the expression of user needs and speed up their transformation into exercisable experiments.

5.2.4 Why Europe

Cyber-attackers have no boundaries. One single cyber-attack can be catastrophic for society and economy in different parts of the globe (e.g., given the impact of the attack by itself or due to cascade effects). To establish a common understanding for describing the preparation of professionals and organisations in order to fight against cyber-threats under a common umbrella that embraces the different profiles and understandings on the entire European union should be a priority.

The European Union provides an ideal opportunity for creating a world leading ecosystem for simulation and cyber range platforms – EU Member States have very different cyber-security experience, and consequently, vast and diverse – if currently also dispersed – actionable knowledge base on the subject matter. While the NIS directive and its network of CERTs / CSIRTs is establishing a level of collaboration at prevention / reaction level, the importance of developing cyber-range capabilities across Member States represents an effort that directly complements the network by a) increasing the range of validated solutions that can be used at prevention / reaction level, b) speeding up the alignment of solutions to user needs by easing the collaboration between users and providers.

Harnessing this distributed knowledge base, combined with a common rules for digital society, data protection and business environment, makes it possible to create an efficient ecosystem that can become a benchmark in the world, enabling European workforce to receive more versatile training experience, European companies to create products and services with higher level of security more relevant to the real world and European infrastructure vendors to prepare against more varied set of threats. Also, given its unique distributed, yet unified characteristics, the created simulation, training and cyber range ecosystem has a high export potential outside of Europe.

5.2.5 Scope

Strand 1: piloting of networked cyber-ranges

- Develop highly customisable simulators for security professionals, practitioners and Member States public organisations to improve their ability to react to attacks, including the definition of a replicable cyber-range model.
- Develop a shared approach to express and transform user needs into actual experiments.
- Define tools to support the generation of current and future simulation scenarios, including the capabilities to clone, virtualize, animate and scale complex cyber-physical environments.
- Develop holistic simulation platforms capable of enabling different modes of operation including cyber-attack but also cyber-defence and cyber-war scenarios, with various levels of difficulty.
- Validate the cyber-range model across 4 different sectors.
- Validate the cyber-range model with involvement of SMEs.

Strand 2: extension of the cyber-ranges network

- Extend the cyber-range model (strand 1) to increase deployment across all EU Member States.
- Create the operational link to the CERTs / CSIRTs network across Europe.
- Integrate with the go-to-market SME support mechanisms.

5.2.6 Targeted Users

- Educational institutions for initial training of professionals and continuous/executive education (lifelong learning).
- Professionals wishing to update and improve their skills.
- Certification agencies.

- Private and public organisations, SMEs and large organisations interested in validating new solutions applicable to their environment / understanding the impact of an attack on similar stakeholders / training their workforce.

5.2.7 Expected Impact

- Generally improved resilience of the ICT infrastructure.
- Professionals better prepared to detect, block and mitigate emerging cyberattacks.
- Users more involved into expressing actual needs.
- Reduce time and costs in infrastructures for training users.
- EU countries better prepared to face malware campaigns and take down malicious infrastructures.
- Organised collaboration between a network of cyber-ranges and Europe-wide initiatives such as the CERTs/CSIRTs network of the NIS directive currently under deployment.

5.2.8 Budget / Time / Instrument / TRL

Strand 1: 5 M€ / 2019 / IA / involvement of SMEs is required / TRL 6-7

Strand 2: 5 M€ / 2020 / IA / involvement of SMEs is required / TRL 5-6

5.3 Education and training

5.3.1 Specific challenge

According to various reports, there is an urgent need for highly valuable cybersecurity professionals and this need will dramatically increase in the near future with the advent of a hyper-connected society. Moreover, security experts need to be in a constant learning process since this is an exceptionally complex and fast-evolving field, which is transversal to any imaginable computer environment. Precisely, one of the main challenges in security training is the growing scope of Security; it is very complex to understand the effect of the same attack in different operating systems, networks and devices. Besides, it is very costly (in terms of resources and time) to combine different devices in the same environment for training. Every advance in network infrastructures, computing devices or software platforms brings about new security threats and exploits.

The security training must go beyond the effect of the attack, it must be capable of training users with different profiles (e.g., from non-technical users to administrators) in order to (i) understand the effects of the attack, (ii) be able for applying countermeasures and (iii) to decide when these can be applied. Furthermore, new tools and models prepared to evolve dynamically based on the user's knowledge and behaviour should be defined. These models will adapt to the security awareness level of the end-user, and also be able to "teach" and "learn" from the end-user, receiving new feedback with each user interaction towards the training system. The adaptability and learning ability of humans and machines will go through a transitional phase during which the machine's role will decrease as the user's awareness and knowledge increases. These aspects

can help to define a common understanding to evaluate the degree of knowledge on security of professionals and other end- users.

Furthermore, the modern society is crossed by novel driving forces. The concept of "immersed humans" is characterizing the current society transformations, where the physical and the virtual life seamlessly merge, thanks to mobile and ubiquitous terminals into blended lifestyles[4]. The workplace too is changing, as employees can complete a task in any possible place, leading to an inevitable blending between private and professional lives. Also, the advent of online social networks has been heavily affecting people-sharing habits. These paramount changes are influencing the evolution of cybercrime[5], but from the defenders' point of view, they are also affecting the education and training methods, which needs a shift of their paradigms to increase their effectiveness.

At the same time, EU since few years is standardizing its education frameworks (e.g., e-CF is now a formal standard (EN) of the European standardization organization CEN: EN 16234, but also the European e-Competence Framework[6] is relevant), with the final aim to fully and efficiently integrate also the ICT Security workers and employers in the European e-Skills market. Unfortunately, there offering of certified tracks in ICT Security is still lagging.

The **European Qualification Framework** is going in this direction, fostering social dialogue to find common sectorial agreements and job matching approaches between workers and enterprises and, establishing governance mechanisms based on continuous improvement and quality labels. Security is still not completely included in these European frameworks because also of the profound and highly dynamic changes in the society and cybercrime, that are impacting the qualification profiles of ICT security professionals.

Moreover, defining realistic cyber-criminal profiles is mandatory for the education and training of the users in cybersecurity. Indeed, this should be a priority in any security training system because the boundary of the training will be limited by the boundary of the adversary. In the current paradigm, not only stenography applied to messaging but also virtual relationships between individuals, virtual identifiers, effect to news in forums and other human factors can be analysed to extract valuable information about individuals, public information that is fundamental to build tools and methodologies to determine and understand the profile of new criminals. Despite the clear disadvantages and problems of cybercrime, there are clear weapons that we are not using: while traditional criminology understands the criminal act only after the crime and requires human resources to do that, new methodologies can help to understand the cybercriminal before the cybercrime, automatically. Reaching this understanding is fundamental for education and training in security and cyber-security, but also to prevent future security risks.

[4] For example refer to the EIT ICT Labs (2014) *BLENDED LIFE IN A CONNECTED WORLD. Strategic Innovation Agenda*. Available at: https://www.eitdigital.eu/fileadmin/files/2014/docs/EIT-ICT-Labs_SIA_Q4_public_RevA.pdf (Accessed: 30 November 2016).

[5] AA. VV, *Combatting Cybercrime and Cyberterrorism Challenges, Trends and Priorities* (Advanced Sciences and Technologies for Security Applications), B. Akhgar and B. Brewster, Eds., 1st ed. Springer, 2016. [Online]. Available: http://link.springer.com/book/10.1007/978-3-319-38930-1

[6] European e-Competence Framework, http://www.ecompetences.eu/

Summarizing, the ICT Security has three concurring needs:

1. Standardize the qualification profiles within the EU standard frameworks;
2. Increase the dynamics of the education and awareness methods, to match the same rate of evolution of the cybercrime;
3. Integrate awareness into an eco-system of humans, competences, services and solutions, that is able to rapidly adapt to the evolutions of cybercrime or even surpass them.

5.3.2 Current status

Current security training methodologies are focused on specific contexts with concrete objectives and profiles (e.g., malware analysis on specific operative systems or devices). Most of the solutions are based on virtual environments pre-configured to respond to particular inputs or stimulus. However, new methodologies more dynamic and adaptive are needed in order to train users of different profile in heterogeneous environments, also considering the impact of the human factors in the final systems. Furthermore, recent analysis demonstrate that cybercriminals have their own communities and societies built in the web and that these can be analysed by human experts in the field. This analysis can be much more efficient if new technologies are applied. To do that, the perfect symbiosis between experts in the field and security computer engineers is more than a need. Unfortunately, despite the efforts of the European community, there is still no common language or framework which allows this understanding that would enable the developing of tools and the definition of common methodologies for the automatic processing. Main related projects are the following ones:

- TARGET (Training Augmented Reality Generalised Environment Toolkit) is an ongoing project aiming to develop a gaming platform for training Security Agents in critical situations. This platform is focused on immersing trainees in scenarios using augmented reality.
- CYBERROAD (Development of the CYBER crime and CYBER terrorism research ROADmap), FP7-SECURITY. “This project will identify current and future issues in the fight against Cybercrime and cyber terrorism in order to draw a roadmap for cyber security research.” The project defines different topics that can help as input of requirements to build cybercriminal profiles.
- COuRAGE (Cybercrime and cyberterrOrism (E)Uropean Research AGEnda), FP7-SECURITY. “consortium will deliver a measured, comprehensive, relevant research agenda for Cyber Crime and Cyber Terrorism (CC/CT) guided by the knowledge and experience of the highly experienced and exceptionally qualified consortium”. The results of this project can help in the definition of the requirements to understand the cybercriminal behaviour.
- e-CF COUNCIL[7]. The e-CF COUNCIL will build a stable network of reference stakeholders in the ICT sector to foster ICT professionalism at European and International level. They will be employer and professional associations, social partners, companies, Small-Medium sized Enterprises (SMEs), public authorities, training institutions, certification bodies. The main purposes: 1) Developing a common reference scheme for joint qualifications and

[7] E-CF Council ERASMUS+ project, Project Reference: 562364-EPP-1-2015-1-IT-EPPKA2-SSA, see http://ec.europa.eu/programmes/erasmus-plus/projects/eplus-project-details-page/?nodeRef=workspace://SpacesStore/55278f7e-6e07-4db8-b8cd-bc2d0460b98e (Accessed: 22 August 2017).

assessment, 2) Fostering social dialogue to find common sectorial agreements and job matching approaches between workers and enterprises benefitting from the shared tools settled; 3) Establishing governance mechanisms based on continuous improvement and quality label

5.3.3 What market

There is a lack of suitable training and testing environments available for the commercial sector to satisfy their needs for cybersecurity training and product testing. For example, there are very few open ranges to involve more participants to the exercises, trainings, testing, experimenting etc., and the existing ones (rootme, google gruyere, etc.) focus on their specific needs. Groundwork to prepare for one large scale training typically involves a lot of manual work that needs to be automated for efficiency and range availability, as well as increasing the speed and capability of dynamic adaptation of cyber-ranges to cyber-attacks; as a result, this type of training, while extremely useful, is usually not accessible to industry. There is also a lack of offering of closed black box ranges for parties that need a closed environment to conduct trainings (e.g. vital service providers that want to exercise domain specific or secret / sensitive scenarios). There is a lack of cooperation between different existing environments. Integrating / federation solutions and enabling secure sharing of exercise libraries would enable trainees to get more versatile experiences and knowledge. It would also enable to involve ranges that have very specific configurations that are difficult to recreate due to some domain specific components (e.g. specific SCADA system ranges etc.).

Thus, the potential of training remains largely under exploited, in terms of catering to the actual needs of target trainees but also as a source for new commercial offerings. Analytics of environments require more automation to enable better analysis, e.g. automate analysis of situational awareness, risks and competences profiling etc. The serious games environments are also environments that can provide input to new products development. Cyber ranges / serious games environments are rarely used in educational programs to build practical, hands-on competences of students.

5.3.4 Why Europe

Security is growing in complexity given the great technological advances in Europe. This can be a problem if the users (e.g., citizens, administrators, etc.) are unable to understand this complexity and therefore cannot use the security tools to protect themselves and their organisations against the local and remote threats. Moreover, unlike traditional crime, cybercrime is not restricted to a location. The opportunities for crime are higher because the access to resources and infrastructures is greater than ever before. Therefore, one single cyber-attack can be catastrophic for society and economy in different parts of the globe (e.g., given the impact of the attack by itself or due to cascade effects). Training professionals to fight against cyber-threats under a common umbrella that embraces the different profiles and understandings on the entire European Union should be a priority. In addition, the definition and analysis of criminal profiles cannot be dependent of a single country; it should be led by the EU to have a rich profile of use cases and inputs to help to understand the complex casuistry of crime, seen from the different social aspects and legal frameworks coexisting in the EU.

EU already invested a lot of efforts creating and standardizing the European Qualification Framework that covers a lot of professional competences, among which there are the ICT Security Manager and the ICT Security Specialist. The aim is to continue in this direction implementing innovative and dynamic qualification tracks, able to match the dynamicity of cybercrime. This is achieved through effective collaboration among different actors and leveraging the advantages of a EU-wide eco-system specialized in ICT-security.

5.3.5 Scope

Strand 1: increase the dynamics of the education and awareness methods, to match the same rate of evolution of the cybercrime; that is new methods of awareness/training and integrate with the European Qualification Framework offering more qualification tracks to fully and efficiently integrate ICT Security workers and employers in the European e-Skills market

- Define training tools to support different devices, technologies and services in order to allow the generation of current and future simulation scenarios.
- Develop training platforms that enable different modes of operation including cyber-attack but also cyber-defence and cyber-war scenarios, with various levels of complexity.
- Provide databases with vulnerable systems for training, services and attack vectors in order to facilitate the creation of intelligent agents capable of finding new vulnerabilities and/or defending from attacks.
- Define behavioural patterns (predictive analysis based on user's behaviour) for adaptive security training.
- Define user-friendly mechanisms for the mutual feedback (user and adaptive tools).
- Design and promote autonomous system actions based on the user's level of knowledge.
- Provide specific training for malware detection and analysis, focusing on advanced persistent threats and decomposing the analysis in levels of difficulty. Cybersecurity professionals should be trained in such a way that they can achieve objectives in compromised environments where malware is established.

Strand 2: integrate awareness into the eco-system of humans, competences, services and solutions, that is able to rapidly adapt to the evolutions of cybercrime or even surpass them

- Include smart education (teaching) using threat scenarios as to ameliorate the end-users' cyber awareness and progressively allow him/her to acquire more control of the system.
- Help to understand cybercriminal behaviour using automatic tools.
- Promote the European cooperation to understand human factors in cybersecurity.
- Build a live repository of cybercriminal profiles.
- Integrate with the European Qualification Framework to fully and efficiently integrate also the ICT Security workers and employers in the European e-Skills market.

5.3.6 Targeted Users

Targeted users include governments, companies (including SMEs) and universities interested in training security experts at different levels and in different scenarios. Also, Law Enforcement Agencies (LEA) will have an interest in the definition of cyber-criminal profiles which can be improved through the progressive use of the training system by different users.

5.3.7 Expected impact

- Professionals better prepared to emergent cyberattacks.
- Improved resilience of infrastructures to attacks.
- Reduce time and costs in infrastructures for training users.
- EU countries better prepared to face malware campaigns.
- Discourage cybercriminal behaviour, and reduction of its impact.
- Help to understand and to limit cybercriminal relationships.
- Improve the EU e-skills market I ICT security.

5.3.8 Budget / Time / Instrument / TRL

Strand 1: 4 M€, 2018, IA / involvement of SMEs is required / TRL 5-6

Strand 2: 3 M€, 2019, IA/ involvement of SMEs is required / TRL 5-6

5.4 Certification and standardisation

5.4.1 Specific challenge

It is essential to promote the development of basic knowledge on information security for users so as to raise awareness related to the risks posed by the use of products of unknown origin. It is then crucial to have mechanisms that certify the origin and the performance of these products.

Having this statement as a premise, the following challenges are foreseen, with a view to make the European market on cybersecurity competitive:

- To define a European Certification for cybersecurity products and services and corresponding Trust Labels, as suggested in topic 110 of the EP resolution of March 12th 2014. The challenge is to define a *unified criterion* for certification of cybersecurity products and services.
- To go a step beyond international standards and address specific technical and human requirements coming from the industrial experience in the certification, ensuring that the certification is meaningful across domains and relevant to user needs.
- To support economic growth by making a distinction between the organisations that develop solutions and services that have undergone the process to acquire the seal or label over other corporations not following the aforementioned security practices.
- To address the increasing concern of citizens about how service providers protect their data, what do they use it for and whether it is disseminated, by incorporating a Data Privacy Compliance Label that help users identify which companies respect their privacy.
- To address the essentially dynamic nature of cybersecurity to define a certification scheme that takes into account changes of the environment, including human aspects or rise of new vulnerabilities.

5.4.2 Current status

There are currently no existing certification schemes that produce a European certification label for security services. There exist, however, technology specific certifications such as, for instance, for the application domain of cloud computing, with the Cloud Security Alliance that offers their OCF (Open Certification Framework)- STAR registry. This is the most widely used and accepted cloud-relevant certification and attestation scheme, recently also used as a reference in an EC DG- DIGIT tender to procure cloud service for EU Institution (including the EU Parliament).

ISO provides several security certification schemes to assess the level of security assurance in ICT systems. In particular, the family of ISO27000 are the family of standards that help users maintain their assets secure. ISO27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). Other well-known standards include SSAE 16, ISAE 3402, SOC1-2-3, PCI-DSS. Unfortunately, they are not certifiable standards (they are code of practices), and therefore are not compulsory for an organization to achieve them. ISO provides these tools as a code of best practices but it does not provide certification.

Some previously funded EC projects have tried to address the problem of certification although none of them considered the development of a European trusted label. In the following we name some of these EU initiatives:

- AMASS- (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) is a H2020-ECSEL funded project that will create and consolidate the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets including automotive, railway, aerospace, space, energy.
- ASSERT4SOA (FP7 funded project) produced a security certification process for Service-Oriented Architectures to provide run-time security assessment.
- CUMULUS – Certification Infrastructure for Multi-Layer Cloud Services -(FP7 funded project) framework provided a way for service users, service providers and cloud suppliers to work together with certification authorities in order to ensure security certificate validity but only in the ever-changing cloud environment.
- A4Cloud- Accountability for the Cloud and other FI services (FP7 funded project) provided a set of tools and mechanisms to help assess the trustworthiness of cloud providers concerning how they dealt with PII of users. Even if it did not intend to deliver a certification mechanism this project went a step forward as it considered how the providers could be trusted.
- SPECS (Secure Provisioning of Cloud Services based on SLA Agreement) (FP7 funded project). This project offered a framework for assessing security properties in the cloud based on SLA.

5.4.3 What market

Cybersecurity overall market size was estimated at 75 B$ in 2015 and expected to reach 170 B$ by 2020[8]. With an expected growth compound rate of close to 10% from 2015 to 2020, this is a major contribution to the Digital Single Market. This growth will also strongly be reflected with the increase of the market size of Internet of Things, intelligent cars and the overall role of IT across all domains of our lives.

Therefore, it is of paramount importance that before users select software and services with a clear knowledge and guarantee of the effectiveness of their selection– that is, when and where the product works, how and where it breaks, and how often it works or breaks. It is for this reason that having a way of certifying these services and products will position users on a level playing field where certifications are recognized globally within Europe, as it will provide increased credibility for the user organization when working with vendors and contractors. It is equally important for providers to be able to position their offering in a defined context, to ease also the deployment of joint solutions from different origins, as this reflects the reality of many deployed solutions within operational environments.

Certification is therefore of importance to the users, but also the provider of solutions and services.

5.4.4 Why Europe

Europe is moving towards the Digital Single Market paradigm, however there are still some aspects in which Member States do not have a unified position making thus the European market less competitive. This is the case for the certification of security products and services.

There is not any label, seal or certification scheme that is standard for European security services and products. So far, Europe makes application domain certifications in an ad-hoc manner. It is then crucial for the economic growth of the European cybersecurity community to go to the market with quality products that are certified using a unified criterion. This will reduce the risk of a “fragmented” Digital Single Market.

5.4.5 Scope

Strand 1:

- To develop mechanisms that ease the process of certification at the level of services.
    - These mechanisms will include the creation of a *European Data Privacy Label* to give companies with privacy-respecting practices a competitive advantage over other companies that make profit from personally sensitive data. This will be possible by defining a methodology and a set of practices that guide the internal data management processes of the corporation. This will help to detect potential

[8] Forbes. Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020. Available at: http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#541a2c582191 (Accessed: 22 August 2017).

sources of data privacy leaks and measure their impact. Also, best practices should be mapped to tools and mechanisms that may help to provide privacy assurances to a certain degree.

- To design solutions by defining and exercising metrics that should be related to a set of threat models.
    - Quantitative and qualitative metrics for companies to be able to determine how fair they are from achieving the next level of certification. Moreover, the European Data Privacy Label must be user-friendly so that users can easily identify how their data will be stored and processed without the need of a deep technical knowledge. Certified monitoring mechanisms should also be in place to automatically detect whether the internal processes of the company comply with the privacy practices.
- Such metrics should take into account a set of basic requirements for the development based on technological or human aspects such as where/how the services and solutions are deployed, as well as the context (application domain) in which they are deployed.
- This system of 'metrics of reference' is to be provided to and tested with users to reach a pre-defined level of certification in terms of exposure to vulnerabilities and threats. It will also allow users to measure where they stand with respect to others operating in the same application domain.

Strand 2:

- To address the evolution of the level of certification with respect to the **dynamicity of the deployed environment**, also addressing the human factor of this environment. This challenge takes into account how to evolve the meaning of certification when faced with the constant evolution of vulnerabilities in terms of changes in the environment, processes, devices and people.

5.4.6 Targeted Users

The main beneficiaries are providers and users, the standardisation bodies and the organisations who deliver the label in practice. Of particular importance is to ensure that the needs of SMEs are taken into account.

5.4.7 Expected impact

- The use of certification schemes will have indirect effects on society as a whole through increased employment in the sector and as a consequence the associated tax returns for Member States and for the whole EU.
- Dynamicity of the certification schemes will translate into continuous surveillance of the policy, legal, and trustworthiness needs of users.
- Increase business case and the economic value as services become more reliable.
- Creation of the appropriate conditions for more commercial applications and services to integrate the use of the European label.
- Validation platforms able to handle the specificities of various jurisdictional or national systems to provide easy assessments.

5.4.8 Budget / Time / Instrument / TRL

- **Strand 1**: 4 M€, 2018, IA, TRL7 / involvement of SMES either directly or through associations is required
- **Strand 2**: 3 M€, 2019, RIA, TRL6 / involvement of SMES either directly or through associations is required

(also see the Certification Lite "strand 2" scheme under the SMEs section)

5.5 Dedicated support to SMEs

5.5.1 Overview and rationale

In the eco-system as envisaged within this document, SMEs are important actors at two different levels:

- as solution providers, SMEs are one of the innovation drivers, and their contribution to the creation of employment in Europe has been recognised, with SMEs responsible for more than two thirds of total employment in the private sectors[9].
- as users across very different sectors, SMEs are increasingly exposed to cyber-attacks[10], but do not invest sufficiently in improving their level of cyber-security, for reasons ranging from lack of awareness that they can be / are targeted by attacks to the complexity of selecting those measures that are appropriate to their activities and related costs. Given their key economic role, this is a dimension in which dedicated support has to be provided.

The support to SMEs is therefore designed towards SMEs as users and as providers, and addresses the following dimensions:

- easing access to user requirements, from both public and private users.
- facilitate the validation and testing of innovations in user environments.
- creating specific "go-to-market" support for innovations, and easing the certification process for SMEs.
- increasing the knowledge sharing across SMEs and between SMEs and larger providers.

5.5.2 Fast Track and Full Access to Innovation (provider SMEs)

5.5.2.1 Specific challenge

As creators of innovative solutions, provider SMEs need to be supported to access information and resources to better align their innovation to needs and ease their validation. The support should

[9] Eusrostat. Structural business statistics overview. Available at http://ec.europa.eu/eurostat/statistics-explained/index.php/Structural_business_statistics_overview (Accessed: 22 August 2017).

[10] The Guardian. Huge rise in hack attacks as cyber-criminals target small businesses. Available at https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses (Accessed: 22 August 2017).

include easing the piloting and field-testing to foster a collaboration between SMEs, large providers and users and ease the delivery of *joint* competences.

In parallel, the user SMEs need to be supported in democratizing access to tools and solutions of varied sophistication level for SMEs to make them also benefit from innovations and solutions that are currently reserved, due to cost as well as use of internal expertise, to larger organisations.

The specific challenge therefore addresses the full value-chain for both provider and user SMEs, through the use of the H2020 “Fast Track to Innovation” instrument on the one hand, and the SME instrument on the other hand.

5.5.2.2 Scope

Strand 1: pilot to incorporate SMEs into cyber-ranges as solution providers and ease their access to user environments

- Run experiments in user or simulated environments based on well-defined user needs.
- Support provider SMEs in creating joint experiments with large organisations and public / private sector users within a cyber-range or network of cyber-ranges.
- Available to single SMEs (through the SME instrument), or consortia of organisations (SMEs, large organisations) through the Fast Track to Innovation instrument.

Strand 2: increase the level of cyber resilience of user SMEs

- Develop a specific community methodology in collaboration with user SMEs to express their needs and evolve them into scenarios.
- Support SMEs in joining experiments in the context of a cyber-range or network of cyber-ranges.

5.5.2.3 Expected impact

- SMEs are able to utilise and apply research results widely.
- SMEs are made aware of the cyber-attacks to which they are vulnerable (in their own sector).
- Accelerating development cycle from the research to market.
- Accelerating joint developments and speed up uptake of innovations.

5.5.2.4 Budget / Time / Instrument / TRL

Strand 1:

- 2018, 6 M€, SME instrument (phase 2)
- 2019, 3 M€, FTI instrument
- 2020, 2 M€, FTI instrument

Strand 2:

- 2019, 2 M€, IA, TRL 6
- 2020, 2 M€, IA, TRL 6

5.5.3 Certification Schema for SMEs

5.5.3.1 Specific challenge

Creating a Certification scheme for SMEs ("cybersecurity LITE"), promoting a system of "light" requirements to receive a label or basic certification for software / hardware / solution / system. The seal of excellence will have to be designed in a way that is aligned with the main strategic objectives of the industry-led cPPP. Initiatives such as UK based Cyber Essentials are one example, but the goal is to enable a *much more precise and comprehensive* certification whilst at the same time creating a *progressive approach* to certification that eases and speeds up the process. The challenge resides in ensuring the right balance between a lighter certification scheme, supporting a progressive evolution to the full certification based on *user* needs, and creating a dynamic approach that also supports joint deployment (collaboration across providers, SMEs and large organisations included).

5.5.3.2 Scope

- Research cyber-security standards required by users.
- Define a set of mandatory security checks and development activities.
- Define evolutionary concepts for a certification schema, from a lighter to a full version

5.5.3.3 Expected impact

- SMEs are able to get light-weight certification for their products from trusted and well-known body, which facilitates growth
- SMEs are able to adapt their certification to the actual environment / user context in which their solutions are deployed

5.5.3.4 Budget / Time / Instrument / TRL

- 2018, 1 M€, IA, TRL 6
- 2019, 1 M€, SME instrument (phase 2)
- 2020, 1 M€, SME instrument (phase 2)

6. CYBER PILOTS

6.1 Overview and rationale

Each of these vertical sectors (also named application domains) demand specific aspects concerning cyber security. These needs will be analysed and included in research projects for products, services, and capabilities that, in turn, need new research and innovations.

In this context, the objectives of the pilot projects are:

- Achievement of security objectives (and efficiency) with regard to identified specific needs.
- Interoperability.
- Scalability.
- Usability/applicability.
- Long term perspective.
- Cost efficiency.
- Cross-domain applicability.

Expected impact and users:

- The pilot projects should highlight the importance of the role of the human factor in cyber security.
- The pilot projects could serve as input for security certification criteria.

Several criteria have been identified to define the priorities for the application domains:

- Market relevance.
- Needs for innovation.
- Impact severity of security threats on society.
- Importance of regulation.
- Evolving sectors.
- Maturity level (regarding cyber security).
- Long-term technology: e.g. industrial legacy systems which have to operate securely and tackle threats without relying on modern solutions.
- Impact of security failures and market traction.

According to these criteria, the identified application domains/vertical sectors have been selected and their relevance represented by the budget allocated.

6.2 Demonstrations for the society, economy, industry and vital services

6.2.1 Industry 4.0

6.2.1.1 Specific challenge

The European Industry is facing a number of competing challenges which need to be addressed with cyber-security concerns in mind. The rising global competition forces traditional industries to go connected, with the aim of reaching higher competitiveness, flexibility and productivity levels. In parallel, a number of new actors dive into a new industry age, enabled by innovative manufacturing methods & tools like additive manufacturing or collaborative robotics. This trend is fostered by technological, societal and economical transformations such as:

- Technology push: the rapid progress in digital intelligence, smart sensing, advanced system modelling and machine learning technology, enabling enhanced autonomy & efficiency of robotics, increased flexibility of manufacturing infrastructures and human-machine collaboration.
- Demand pull: the increasing demand for product customization, on-demand production, improved product life-cycle management and adaptation to circular economy model drive manufacturing infrastructures into a more connected, more intelligent and more collaborative mode.

Indeed, most traditional Industrial Control System (ICS) manufacturers have already gone digital, and adopted technologies coming from ICT world, drastically reducing acquisition, operation and maintenance cost, requiring regular updates, performing more complex tasks with a greater level of autonomy. Innovative industries have to remain competitive in this novel context, where enhanced customization, shorter production time, lower fabrication costs and improved product life-cycle management are required.

However, among other considerations, the fear of increased exposure to cyber-threats is one of the reasons why many countries in Europe are lagging behind in this competition. Indeed, legacy Industrial Control Systems (ICS) were designed to operate in a segregated way, with no or limited interaction with the outside world (supply chain, customers…). This has been known as the principle of security by isolation only. While this principle has for long been known to be a pure illusion, it becomes absolutely disastrous in this evolving context:

- **Maturity:** ICS security rarely got attention comparable to IT security. The ICS component domain generally has a low maturity level both in the supplier side and in the procurement side - many deployed systems even have no security whatsoever. 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. In fact, data gathered from commercial companies and national CERTS show a massively increased number of targeted attacks in this domain.
- **Exposure:** the digitization of the manufacturing sector, and the realization of the Industry 4.0 vision, will create an increasingly complex and heterogeneous environment. Here,

legacy systems will coexist for a time with novel, more intelligent protocols; various enabler technologies (Industrial Internet of Things, Cloud/Fog Computing) will be deployed, leading to increased interdependency. As a result, the attack surface will increase. Due to the growing distribution of intelligence in the lower layers of ICS, what was once known as an attack surface may soon become an attack fractal.

- **Complexity**: it is well known that software services of this level of complexity are difficult to execute, and therefore execute those in a way that results in a secure system. Digitizing an already complex control system is therefore something that requires a high level of skill in planning and execution – which may not always be available. Manufacturing processes are also more diverse and specific than information processes. Consequently, knowing the customer specific business and manufacturing process is required to effectively ensure the security of his infrastructure.
- **Safety**: In order to implement the necessary security infrastructures, it is essential to consider the specific needs and requirements of industrial settings, such as the stricter real-time requirements, the lifecycle of industrial plants, the importance of availability and fault tolerance, and the integration of safety mechanisms – such as reverting to a manual backup plan and safely shut systems down manually. Precisely, safety and security often conflict – a firewall or encryption on a communication layer add security, but also add an additional point of failure from a safety perspective.
- **Flexibility**: ICS components usually have a very long lifetime, often with vulnerable protocols and sometimes remaining in the field for decades. Thus, any security concept needs to be prepared to integrate legacy systems and architectures, and new systems need to be ready for requirements for an extensive period, without resulting in excessive pricing. Besides, as security will evolve over time, the protection of these industrial systems should be as modular, flexible, and extensible as possible.
- **Sustainability**: an additional problem from this long lifetime is the availability of the suppliers; few suppliers are willing to commit to provide maintenance and security patches for such a long time, and there is a high probability that some suppliers or their subcontractors may be outlived by their devices (e.g. Windows XP-based devices). Consequently, a number of ICS systems have been hit by attacks that usually target IT infrastructures, such as classical botnets (i.e., attack programs that turn outdated systems into spam-bots).
- **Constraints**: Due to their nature, various components in ICS systems are constrained in a number of ways, such as available memory, computation power, or user interfaces. Moreover, many ICS components have little hardware (such as execute-bits) or operating system support for security. To further complicate matters, constrained memory forces programmers to cut corners, omitting additional checks and error handling routines. This restricts the number of available security controls, increases the amount of vulnerabilities, and further complicates future-proofness.
- **Privacy**: at the same time customization (one-off items (lot size 1 in mass production) and very small quantities of products) raises privacy issues: especially individualised body-related consumer products (e.g. shoes, glasses, hearing aids) need sensitive (sometimes health-related) data to fit individually. Some of the data used for individualisation, e.g. personal photos to be printed on clothes or shoes tell a lot about preferences and circumstances of living. In terms of the number of potential receivers of the sensitive information especially long and complex value chains spanning several organisations and countries raise the challenge.

- **Confidentiality**: beyond customer privacy, we also have to consider the confidentiality of the different business processes, design models and manufacturing processes, as cooperative and autonomous manufacturing infrastructures might leak business intelligence (e.g. configuration, orders). In fact, the interconnection of industries, their equipment, machinery, and operators via wired or wireless communication links may expose the behaviour of internal processes and secrets to competitors via the analysis of the communications even though confidentiality mechanisms are in place. Moreover, long and complex value chains spanning several organisations and countries raise these challenges.

For these many reasons, Industry 4.0 is expected to provide solutions to conciliate security and competitiveness for European manufacturing industries. Projects addressing this topic should propose, design, validate and demonstrate technological and organizational solutions enabling enhanced digitalization & modernization of existing and new industries in Europe in a secure way. This secure digitalization should follow a holistic approach, considering the integration of security mechanisms and frameworks within all the elements and actors that participate in this industrial ecosystem. This integration should be facilitated, if possible, by the specification of specific standards and best practices, which will allow industries to choose measurable security solutions that satisfy their needs. In fact, the applicability of existing industrial security standards and guidelines (e.g. VDI/VDE 2182, NIST 800-82, IEC 62443) to this context should be considered.

6.2.1.2 Current status

Risk landscape: according to the key findings from the Information Security Survey 2016 by PwC11 for the Industrial products sector:

- Security compromises of IoT technologies, like operational systems and embedded devices, are reported as more than doubled in 2015.
- Most of organisations either have an IoT security strategy in place or are currently implementing a strategy.
- Half of the companies are using Big Data analytics to model for and identify cybersecurity threats.
- A majority of the organisations uses cloud-based services like real-time monitoring and analytics, identity and access management, and advanced authentication.
- Most industrial product companies have evaluated the increased risk of incorporating trade secrets in 3D printing digital files, as this is one of the most interesting technologies to introduce for manufacturing products.
- Risk-based cybersecurity frameworks such as the NIST Cybersecurity Framework or ISO 27001 have been adopted by many companies to help in their overall security practices.

However, information security budgets in 2015 were decreased after a significant increment in spending the year before.

Existing reference architectures: existing reference architectures, such as the Reference Architecture Model Industrie 4.0 (RAMI4.0) and the Industrial Internet Reference Architecture (IIRA), describe some of the security principles (security by design, holistic security) and security

[11] PwC. Turnaround and transformation in cybersecurity. Key Findings from the Global State of Information Security Survey 2016.

components (usage monitoring and anomaly/intrusion detection/reaction, identity (human/device) management, secure communication, data ownership) that should be integrated in this connected industrial ecosystem. However, these reference architectures do not describe how these components could be developed.

Existing security mechanisms: There are numerous security mechanisms that have been developed for the paradigms that make up the Industry 4.0, such as the (Industrial) Internet of Things, Cyber-physical systems, Cloud Computing, Big Data, and others. However, there are very few studies that analyse how these security elements and components could be integrated in an industrial setting. Moreover, many of these security solutions do not consider the specific needs (e.g. fault-tolerance and availability, maintain real-time processes, long lifecycle of industrial plants) of Industrial 4.0 scenarios.

Existing cyber-defence capabilities: cyber-defence concepts and capabilities have been initially tailored to IT security by analogy with pre-existing military doctrines for mobile warfare. Attempts to adapt these techniques to SCADA/ICS environments have been led by several security vendors targeting this particular market. Protocol-based detection techniques have been applied to secure SCADA layers which traditionally convey very predictable traffic. Anomaly-based detection is required to effectively detect attacks at lower levels (sensor/actuator). The need for joint investigation & response capabilities between safety and security professionals remains unaddressed as well as effective solutions to deal with insider threats.

Emerging cyber-resilience capabilities: traditional cyber-defence approach fails to fulfil the challenge set by advanced manufacturing systems in terms of availability level. Indeed, traditional countermeasures used to secure IT environments often lead to reduced availability, temporary unsafe state or process latency. Alternative approaches emerge to propose more adapted self-healing, auto-reconfiguration and self-adapting mechanisms, aiming to keep ICS in fail-save & fail-secure mode throughout the response phase. Yet very few of these techniques have been demonstrated in realistic environments and none yet on live real scale operational systems.

Previous and ongoing EC projects related to “Industry 4.0” sector are listed in the following table:

CockpitCI	Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
CP-SETIS	Towards Cyber-Physical Systems Engineering Tools Interoperability Standardisation
CRISALIS	CRitical Infrastructure Security AnaLysIS
CyberWiz	Cyber-Security Visualization and CAD-Tool for the Vulnerability Assessment of Critical Infrastructures
EURO-MILS	EURO-MILS:\nSecure European Virtualisation for Trustworthy Applications in Critical Domains
MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs
SECCRIT	SEcure Cloud computing for CRitical infrastructure IT
SERENITI	Cyber Security and Resilience of Networked Critical Infrastructures

SERSCIS	Semantically Enhanced Resilient and Secure Critical Infrastructure Services
TCLOUDS	Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure
TACIT	Threat Assessment framework for Critical Infrastructures proTection
CYPRES	CYPRES the ICS and SCADA security companion
DEIS	Dependability Engineering Innovation for CPS - DEIS
DISRUPT	Decentralised architectures for optimised operations via virtualised processes and manufacturing ecosystem collaboration
WATERGUARD	Safeguarding Water Distribution Systems from Contamination Threatsusing the SmartTap Platform
X2Rail-1	Start-up activities for Advanced Signalling and Automation Systems
TWISNet	Trustworthy Wireless Industrial Sensor neTworks

6.2.1.3 What market

The market potential for Security of Industry 4.0 is a future market which can be best predicted based on trend analysis of the following existing markets:

- ICS Security market
- Manufacturing analytics market
- Critical infrastructure protection market

These existing markets have diverging growth speed and transformation pace. Cybersecurity of future factory could stand somewhere between these existing markets.

ICS Security Market:

According to MarketsandMarkets survey on "Industrial Control Systems (ICS) Security Market by IT Solution, by IT Service (Risk Management Services, Design, Integration and Consulting, Managed Services, and Audit and Reporting), by Vertical & by Region - Global Forecast to 2021", the Industrial Control Systems (ICS) security market size is estimated to grow from USD 9.00 Billion in 2016 to USD 12.60 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 7.0%.

North America is expected to have the largest market share and would dominate the ICS security market from 2016 to 2021, due to the presence of a large number of ICS security vendors. Various companies such as IBM, CSC, Cisco, McAfee, Lockheed Martin, and Palo Alto Networks among others are operating in the market space. MEA offers potential growth opportunities for the ICS security market to grow, as countries in MEA are investing heavily to increase the development of DDOS, IDS/IPS, antivirus/malware, firewall, SCADA encryption, DAM, and other security solutions.

Manufacturing analytics market:

According to MarketsandMarkets study on "Manufacturing Analytics Market by Type (Solution & Services), Applications (Asset Management, Inventory Management, Emergency Management, Supply Chain Planning, Sales & Marketing Management, & Others), Industry Vertical, Regions -

Global Forecast to 2021", is estimated to grow from USD 3.14 Billion in 2016 to USD 8.45 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 21.9%.

The major forces driving the manufacturing analytics market are the adoption of advanced data-management strategies across varied manufacturing applications, increasing need for process optimization, emergence of Industrial Internet of Things (IIoT), increased business agility and scalability, and self-service access to centrally managed data. The manufacturing analytics market is growing rapidly because of the transformation from traditional BI techniques to advanced analytics techniques and massive surge of structured and unstructured manufacturing data.

North America is expected to hold the largest share of the manufacturing analytics market in 2016 due to the technological advancements and early adoption of analytics in the region. The market in APAC is expected to grow at the highest CAGR between 2016 and 2021. The primary driving forces for this growth are increasing technological adoption and huge opportunities across manufacturing industry in APAC countries, especially India, China, and Japan.

6.2.1.4 Why Europe

The above market surveys clearly show that Europe is lagging behind as a demand market as well as a supply market in both in cybersecurity of ICS and manufacturing analytics:

- **ICS competitive landscape: t**he major vendors in the ICS security market include: ABB Group (Switzerland), Honeywell International (U.S.), IBM Corporation (U.S.), Cisco Systems (U.S.), Lockheed Martin (U.S.).
- **Manufacturing analytics competitive landscape**: some of the Prominent Key Players in the Manufacturing Analytics Market are: SAS Institute (U.S.), Tableau Software (U.S.), Tibco Software (U.S.), Oracle Corporation (U.S.), IBM Corporation (U.S.), Computer Science Corporation (U.S.), Dell Statsoft (U.S.), SAP SE (Germany), Zensar Technologies Ltd.(India), 1010Data(U.S.), Alteryx (U.S.).

At the same time Europe has a reputation to lose in both safety and privacy protection as well as in reliable high-quality manufacturing. This reputation is the justification for manufacturing in Europe despite of relatively high (e.g. compared with China) labour costs.

In order to challenge the dominant US vendors and secure European supply chain for trusted ICS, a strong R&D effort is required. Cybersecurity should be promoted as an enabler for digitalization of European Industry. Indeed, it appears that one of the main roadblocks to adoption of advanced manufacturing methods and tools by European actors is the fear of new threats targeting these more intelligent and more interconnected industrial systems.

The secure digitalization and modernization of ICS services, plus the secure integration of novel Industry 4.0 services (e.g. “digital twins”, empowered “digital workers”, collaborative/autonomous agents, cloud-based manufacturing) will optimize existing manufacturing processes and enable new ones, which in turn will improve the competitiveness of European industry. In fact, a rapid survey on the global manufacturing landscape shows that the success of a national industry is deeply correlated with its ability to adopt advanced manufacturing tools and methods. For example, South Korea, Japan and Germany rank first 3 in numbers of robots per employee.

6.2.1.5 Scope

Projects addressing this topic should target one or both of the following strands:

Strand 1: Secure and privacy-considerate transition of an existing industry

- Projects addressing this strand should involve at least 2 industrial facilities from 2 different countries and focus on security upgrades and sustained security monitoring for existing industries involved in a modernization/digitalization program
- Industry 4.0 requires a significant evolution on current industry including more interconnected systems, intelligence products, cyber-physical systems, IIoT (Industrial Internet of Things), cloud solutions and Big Data. However, the transition to digitalization requires migration which is the highest constraint considering the high availability these systems require. Procedures must be identified to make this transfer without operational impact. Personal data associated with products (e.g. individualised consumer products) and with business processes must be protected even in long and complex value chains spanning several organisations.
- New approaches to Governance, Risk & Compliance Management that encompass both OT&IT; tools allowing security assessment of Industrial automation equipment (guidelines, techniques, etc.) when delivered by manufacturers;
- Standardisation of protocols, interfaces and applications when remote connection from third party is needed when dealing with enabler technologies such as the IIoT; replacement or supervision of insecure industrial protocols (Modbus TCP, OPC,...) should be enforced.
- Adapted protection / detection & remediation capabilities will be developed to enhance the security level of enabler technologies (e.g. Industrial Wireless Sensors Networks) without compromising the conformance to power, process, speed and autonomy and availability requirements.
- Solutions to secure connection points between IT and OT, as well as tools allowing supervision and event correlation of both domains;
- Tools and techniques enabling to continuously monitor the security & safety level of the industrial asset throughout the transformation program should be delivered, as well as means for collaborative response of security and safety professionals to a set of incident scenarios
- Appropriate security policies (including organizational and technological techniques) to ensure protection of sensitive/confidential data, as well as personal data (privacy), that consider the increasing cooperative functioning of highly interconnected industries.

Strand 2: Securing an advanced manufacturing lab

- Projects addressing this strand should involve at least 2 manufacturing labs from 2 different countries and focus on security by design for industries involved in the set-up of a new manufacturing lab/facility;
- Risk assessment on new industry models must reveal the highest risk assets, determine all necessary security controls to secure communication network (access control, authorization, VPN, IDS, FW, network segmentation, etc) and provide strategic plans to mitigate risks.
- Potential impact of new manufacturing methods and tools like additive manufacturing or lot-size 1 on the level of vigilance of humans and potential breach of security measures should be assessed

- Besides traditional risks related with enhanced automation, those related with the involvement of collaborative manufacturing systems (e.g. robots) should be identified, and their possible impacts (including on human safety) should be assessed
- Adapted specifications and countermeasures to avoid, reduce or mitigate the above risks should be proposed
- Enforcement of policy and procedures across the entire supply chain in new digital industry models.
- Recommendations for adapted regulations to cover concerns about data ownership, responsibility, traceability and privacy will be delivered

6.2.1.6 Targeted Users

In the context of Industry 4.0, we have to provide protection to all its elements (manufacturing devices, software elements/agents, human operators, supervisory networks, etc.) at all levels (real-time management, operation management, tactical management, strategic management) at any point of its lifecycle (inception, planning, building, production, dismantling). Therefore, our target is the whole European (and worldwide) manufacturing ecosystem: from suppliers to manufacturers to distributors, including technology providers. Examples of targeted users are proposed in the following industry verticals which are expected to ally strong security requirements and a need for enhanced productivity: fertilizer manufacturing, food processing, chemistry, oil refinery, manufactured goods, automotive, aeronautics, defence & space…

6.2.1.7 Expected impact

The projects should demonstrate their effective impact on the following:

- Technological impact: the project should boost the leadership of European actors in ICS security, security of advanced manufacturing systems, convergence of safety, security, and privacy tools and techniques
- Societal impact: the project should demonstrate the ability of outcoming developments to reach protection of European values, societal acceptance and effective adoption
- Economic impact: the project should propose new business models aiming to support a positive impact of industry modernization on employment, reduction of drudgery, re-industrialization of European countries.

6.2.1.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

ICS security needs addressed in “Industry 4.0” may be found similarly in Energy, Smart Buildings & Smart Cities, Transportation and Healthcare domains. Some of the developments may be re-applicable, taking into account the specific requirements of these verticals like:

- for Energy: incidents causing imbalance or disruption of energy networks are likely to trigger dramatic cascading effects on energy-dependent infrastructures like industrial plants
- for Smart Buildings & Smart Cities: the need to exploit cross-domain sensing & analytics
- for Transportation: the challenge to embed secure ICS in constrained environments
- for Healthcare: to properly assess the risk and impact on human health & safety

The conciliation of security and productivity can be seen as a specific requirement from “Industry4.0” versus the other verticals.

6.2.1.9 Budget / Time/ Instrument / TRL

15 ME, 2018, 10 ME 2019, IA, initial TRL: 4-5 and final: 6-8

6.2.2 Energy

6.2.2.1 Specific challenge

Energy infrastructures and electric systems in particular, are “meta critical” infrastructures as the functioning of society relies completely on energy. The ultimate goal of these infrastructures is to provide an uninterrupted supply of energy. Therefore, it is crucial for energy operators to ensure the safety and security of the whole interconnected energy chain, from generation to supply. Over the last decade, electricity infrastructures have undergone profound changes, characterized by the transition from a system where generation, based on fossil fuel, adapts to user consumption, to a system which has to manage different kinds of users connected to it – generators, consumers and those that do both. This transformation goes along with the massive digitalization of the whole infrastructure in order to optimize and to remotely supervise and monitor an increasingly complex infrastructure. Moreover, to cope with the global growth of energy demands and climate change, there is an increasing need for efficient and optimized use of energy. To save energy, demand-response services are proposed to users in order to optimize their consumption, for example by reducing or shifting their electricity usage during peak periods. These services rely on interconnected smart devices, such as sensors and actuators, widely deployed in households to measure energy use and reduce energy equipment consumption to prevent overload. It is predicted that these smart devices, or Internet of Things, will total several billion in the coming years. The benefits of this transformation are envisioned to be a more economical, sustainable and reliable supply of energy.

In the meantime, energy infrastructures are increasingly exposed to cyber threats. The attack surface is increasing due to the massive use of ICT (Information and Communication Technologies) and of new data interfaces such as new and connection-oriented meters, collectors, and other smart devices which offer new points of entry to attackers. In addition, energy systems present targets with potentially high impacts for attackers, e.g. major supply disruption or acquiring sensitive information. Cyber-attacks can also be motivated by the increasing amount of private sensitive customer data available to service providers, utilities, and third party partners.

In this profoundly changing context, while business continuity becomes challenging due to fluctuations of renewable based generation and to consumption optimization through demand-response actions, energy infrastructures have to cope additionally with cybersecurity threats with potential disastrous impacts on society (e.g. blackouts). Beyond the need to design security solutions enhancing resilience, integrity and availability, cybersecurity challenges for energy systems could be structured around three main domains with regard to their specific constraints and needs:

Smart Grids are the digitalization of electricity infrastructure and the transition from a closed, centralized, analogue infrastructure to an open, largely decentralized, digital infrastructure. This new scheme is based on a highly interconnected ICT infrastructure, allowing monitoring of the

different components of the electric system. While smart grids take substantial advantage of this new ICT infrastructure, they become at the same time more vulnerable as they are now exposed to communication networks and computer application cyber-attacks which could cause serious damage to the electricity network, as well as impacting the integrity and confidentiality of customers' data.

The main security challenges specific to Smart grids are:

- High level of complexity and very high volume of interconnected components deployed at country/continent scale. There is a need for security solutions preventing cascading effects, especially when a large volume of components is compromised;
- Energy systems usually have a very long lifetime, sometimes remaining in the field for decades. Security solutions should take into account resource constrained legacy systems and should be extensible and evolving to integrate new components and new security requirements.
- Privacy concerns have arisen, such as the possibility of creating behavioural profiles of customers if their energy consumption is transmitted into the Smart Grid especially in small time intervals;
- Attack surface is increasing over time due to new data interfaces such as new and connection-oriented meters, collectors, and other smart devices (IoT technologies) which cause new entry points for attackers. Thus, all components of the Smart Grid, from smart meters to power plants, or relays, including software components, could be targets for cyber-attacks, as well as the SCADA systems used to monitor these software components. These components could be compromised either because they are exposed to the Internet, or because physical security can be bypassed. There is a need for new security approaches detecting and preventing threats with severe impacts (e.g. blackouts).
- A Smart Grid is a system where electricity is traded as a commodity on international marketplaces. Mechanisms of trading marketplaces should be resilient.
- The use of hardware protection techniques must be integrated with the software development processes that shape the Smart Grid;
- It is crucial to devise means to defend against denial-of-service attacks that do not disrupt the Smart Grid;
- The Smart Grid architecture and governance must be such that compromised components are detected and isolated in a way that minimizes the impact on the rest of the infrastructure.
- Disaster recovery techniques are required in case of major disruption.
- Safety components are of major importance in smart grids operation. Thus, it is necessary to identify and control interdependencies between safety and security.

Distributed Energy Resources (DER) are expected to occupy in the smart grid landscape an increasingly important part of the global energy generation through a large number of energy sources on various scales (solar panels, small wind turbines, energy storage, etc.), highly dispersed across the whole grid. DER represent therefore an important part of the whole electricity generation due to their massive integration in the grid. An attack targeting a large number of renewable energy sources (e.g. windfarm) could have a severe impact on the grid and thus on electricity supply.

The main security challenges specific to DER are:

- Highly distributed and resource constrained systems which implies the need for distributed security schemes operating with limited resources;
- Limited or not connected systems (due to their difficult to reach location), such as offshore wind farms, which implies the need for autonomous security solutions and secure remote supervision.
- DER infrastructures encompass new components (e.g. power storage systems) crucial for the maintaining of the equilibrium of the whole grid, and operating through different models (e.g. Virtual Power Plants). More generally, they use technology which is still rapidly evolving and which needs rapidly evolving cybersecurity solutions.

Centralized electricity generation plants can have a significant long lifespan, and are now introducing the use of new ICT technologies. The combining of these two generations of technologies has to be considered while conceiving and developing security solutions. In particular, legacy systems have constrained resources and sometimes rely on old software that cannot always be changed. Moreover, as safety is a major requirement of these infrastructures, security solutions have on the one hand to mitigate security threats which can have an impact on safety, and on the other hand to manage potential interdependencies between security systems and safety systems. Finally, due to the use of new technologies such as IoT, privacy issues have to be addressed and solutions proposed.

The main security challenges of “centralized electricity generation” are:

- Energy systems usually have a very long lifetime, sometimes remaining in the field for decades. Security solutions should take into account resource constrained legacy systems together with new technologies (IoT, etc.). New security solutions should fit both generations of technologies and be extensible and evolving to integrate new components and new security requirements.
- Evolving threats should be detected and isolated as they could have disastrous impacts on generation plants;
- Safety components are of major importance in smart grids operation. Thus, it is necessary to identify and control interdependencies between safety and security.
- Privacy concerns have arisen due to the increasing use of industrial IoT technologies in power plants;
- Strong need of advanced physical access control schemes (distinguishing between the access rights of internal employees and of external personnel, e.g. for maintenance); Strong need for the early detection and isolation of compromised components and more generally of threats.

6.2.2.2 Current status

The analysis of past and ongoing EC projects shows that they either don’t or only partially cover the topics underlined in this document.

The SESAMO (SEcurity and SAfety MOdelling) [2013-2015] project confirmed the need to investigate and control interdependencies between safety and security through 8 industrial use cases. Nevertheless, the proposed solution with low TRL is inapplicable in operational contexts and this topic requires further work.

SEGRID (Security for smart Electricity GRIDs) [2014-2017] is based on a risk management approach for 5 specific use cases; SPARKS (Smart Grid Protection Against Cyber Attacks) [2014-2017] project focuses on big data, smart meter authentication, intrusion detection and control system aspects. SUCCESS (Securing Critical Energy Infrastructures) [2016-2018] focuses on the security of smart meters infrastructure. While these 3 projects deal with cybersecurity for smart grids and are not completed yet, they don't intend to cover the cascading effects of threats, control access problems, and the security of widely deployed IoT in the grid.

On the other hand, EC projects which have defined cybersecurity roadmaps supports the proposed topics. For example, among the identified prior topics by the CAMINO (Comprehensive Approach to cyber roadMap coordINation and development) [2014 - 2016] project are the development of new ways to counter new, robust botnets, the focus on detection and countering of malware, ransomware and botnets, investing in large-scale testing capabilities and the development of new paradigms for fighting against malware targeting mobile and small/micro devices (IoT).

The Research Agenda and Recommendations for Action for cyber-physical systems to ensure Europe's competitiveness proposed by the CyPhERS project (Cyber-Physical European Roadmap & Strategy) [2013-2014] recommends to "Harden Infrastructures". This recommendation is explained by the fact that cyber-physical systems make use of open information and communication technology – especially the global Internet – to coordinate the control of critical technical and organizational processes, including the electric grid with its switches and power stations as well as the marketplaces for energy trading, or telematic systems with their road-side installations as well as traffic control centers. Joint public and private investments are needed to assess and improve the security of both public and private information and communication technology to protect these critical infrastructures from cyber-attacks.

6.2.2.3 What market

The energy sector represents a major market at European and international levels:

According to EU Reference Scenario 2016[12], energy related investment expenditures on the supply side (power plans, power grids) should reach 500 billion euro, for the period 2016-2020, and more than 400 billion euro for the period 2046-2050. Investment expenditures in demand sectors (industry, tertiary and residential) is increasing and should be higher than 1 000 billion euro for the 2041-2045 period (and the following 5 years period).

At international level, according to the International Energy Agency[13], the world's energy needs continue to grow and the Agency 2016 main scenario expects a 30% rise in global energy demand to 2040. The World Energy Outlook 2016 states that a cumulative $44 trillion in investment is needed in global energy supply.

[12] European Commission publishes latest energy, transport and emission projections in EU Reference Scenario 2016. Available at https://ec.europa.eu/energy/en/news/reference-scenario-energy (Last access: 22 August 2017).

[13] International Energy Agency. World Energy Outlook 2016 sees broad transformations in the global energy landscape. Available at www.iea.org/newsroom/news/2016/november/world-energy-outlook-2016.html (Last access: 22 August 2017).

In a study published by ENISA in August 2016[14] assessing the cost of cybersecurity incidents affecting critical information infrastructures, the energy sector appears as one of the most impacted sectors having the highest incident costs.

Due to the increase of attacks on energy infrastructures, with potential serious damage, cybersecurity investments in this sector are expected to increase significantly[15]. The overall trend is confirmed by different reports. According to Energy and Resources Digest [16], Europe's cybersecurity market should see compound annual growth of 7.2% from 2014 to 2019, while marketsandmarkets[17] estimates that the cyber security market will grow from USD 122.45 Billion in 2016 to USD 202.36 Billion by 2021, at a Compound Annual Growth Rate (CAGR) of 10.6% during the forecast period.

6.2.2.4 Why Europe

- Securing Distributed Energy Resources is necessary for the development of renewable energy sources. Likewise, Europe has to face the massive proliferation of IoT technologies, especially when they are used in critical domains. In addition, promoting IoT based services for energy efficiency and development of DER would contribute to meeting European commitments to prevent climate change.
- The R&I topics contribute to the achievement of a more competitive, secure and sustainable energy system, an EU priority defined in the 2020 & 2030 Energy Strategy Frameworks.

6.2.2.5 Scope

Projects addressing this topic should target the following objectives.

- Control and management of cascading effects in smart grids to avoid major supply disruptions.
    - The proposals have to address control and management of cascading effects in smart grids to avoid major supply disruptions (e.g. blackouts). The proposals should provide tools to avoid a cascading effect when a large number of components are compromised, despite the high level of complexity and number of interconnected components deployed at a country/continent scale.
    - Security schemes specific to resource constrained components widely deployed as smart devices (IoT) are needed. The increasing use of smart devices (IoT technologies) which could reach several billion in the coming years, presents new entry points for attackers and is able to engender cascading effects due to their spread and interconnected nature;

[14] ENISA. The cost of incidents affecting CIIs. August 2016. Online https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

[15] Forbes. The Biggest Cybersecurity Threat: The Energy Sector. Available at http://www.forbes.com/sites/michaelkrancer/2015/11/04/the-biggest-cybersecurity-threat-the-energy-sector/#197a1c760ba6 (Last access: 22 August 2017).

[16] Energy & Resources Digest. Why 2016 Will Be the Year of Cybersecurity. Available at http://energyandresourcesdigest.com/invest-cybersecurity-2016-hack-cibr/ (Last access: 22 August 2017).

[17] MarketsAndMarkets. Cybersecurity Market by Solution. Available at http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

  - Security solutions should fit all generations of technologies, need to be evolving and have to handle new scalability challenges. The use of different generations of systems, e.g. legacy systems which have a very long lifetime and sometimes remain in the field for decades along with new technologies such as IoT, has to be considered during the security solution conception;
  - Identification and control of interdependencies between safety and security are of great importance in the energy context. Impacts of security breaches, as well as security solutions, on safety operation should be anticipated and avoided;
  - These needs are of particular relevance for **Smart grids, Smart home and Distributed Energy Resources (DER)** contexts which manage high volume of interconnected components (e.g. IoT) deployed at region/country/continent levels;
- Control and management of increased surface attacks over time in the context of the digitalization path of the energy system.
  - Identification of the wide variety of threats (sophisticated botnets, malware, APT, MITM, etc.) and analysis of their impact is required, as impacts of threats on energy infrastructures could be potentially very severe (human, ecological, economic, societal, etc.);
  - Need for early detection and isolation of threats;
  - Efficient solutions to DoS attacks, especially DDoS attacks, which could have severe impacts;
  - Response and notification tools (technical and organizational) to security alerts coming from Intrusion detection tools, as well as for disaster recovery techniques in case of incidents;
  - Security schemes for widely deployed resource constrained components, such as IoT devices, have to be developed while the increasing use of IoT technologies presents new entry points for attackers;
  - These needs are of particular relevance in all energy contexts: **Smart grids, Smart home, Distributed Energy Resources (DER) and Centralized Energy Generation** contexts where sophisticated threats could have very severe impacts.
- Advanced Access Control schemes (logical and physical) for strategic energy facilities.
  - Control access techniques managing multiple interveners/roles (e.g. internal employees and external personnel (e.g. for maintenance), as well as local and remote connections to systems;
  - Control access techniques should address privacy concerns and manage sensitive data due to the increase use of collectors, smart devices, etc.
  - These needs are of particular relevance in all energy contexts. **Smart grids, Smart home, and Distributed Energy Resources (DER)** increasingly rely on the use of smart devices such as sensors, collectors and actuators for their remote monitoring. An unauthorized access to these devices can lead to undesired behaviours which could have disastrous impacts on the whole electricity system. Moreover, each of these contexts can present specific additional requirements. For example, Remote control access solutions should handle limited connected DER systems regarding their localization. The need for Advanced Access Control schemes in **centralized Energy Generation utilities** is motivated by the involvement of multiple interveners in their operation (e.g. for maintenance purpose) which have to handle critical assets with limited actions.

6.2.2.6 Targeted Users

- Energy utilities (centralized and decentralized generation, distribution, supply) for a more economic, sustainable and reliable supply of energy;
- Energy service providers to ensure efficient use of energy;
- Individual consumers for optimized consumption.

6.2.2.7 Expected impact

- Technological impact: the project(s) should propose more efficient security tools and techniques more suited to energy infrastructures needs and constraints while respecting privacy and data protection needs;
- Societal impact: the project(s) should allow increased trust in security and safety of energy infrastructures and respect and protect European values;
- Economic impact: the project(s) should propose solutions with optimized costs for their effective use and aimed at supporting a positive impact of industry modernization on employment.

6.2.2.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Security issues which could be addressed through a similar approach than other verticals could be privacy, ICS and automation security issues, and security and safety interdependencies. In any case, energy context specifics, such as the complexity of energy architectures and their large scale, should be taken into account during the conception and development steps.

6.2.2.9 Budget / Time / Instrument / TRL

16 ME, 2018, IA, initial TRL: 4-5 and final TRL: 6-8

6.2.3 Smart Buildings & Smart Cities

6.2.3.1 Specific challenge

As more people move to urban areas, cities face ever more economic and environmental challenges, including resource constraints, economic restructuring, aging populations, and pressures on public finances. In their efforts to accommodate growing urban populations and the accompanying challenges, governments can use modern information and communication technologies to create “Smart Cities” and smart buildings that improve the quality and interactivity of urban services while reducing costs and ensuring sustainability.

For the last decades, visionary city administrations have started looking closely at ways to enhance quality of life for city dwellers. However, with today’s constrained resources, they face new and wide-ranging pressures[18]:

[18] Symantec. Transformational ‘smart cities’: cyber security and resilience – executive report.

- Population growth places increasing demands on new and existing services, sometimes to the detriment of quality.
- The prolonged economic crisis has progressively eroded investments in services for citizens.
- Central government has to comply with international carbon emission targets and cities play a major role in emission production.
- As energy requirements grow, pollution increases, supply needs to be managed efficiently and critical infrastructures need to be protected.
- Ageing urban infrastructure can be a ticking time bomb, especially in recessive economies.
- Public safety and security is becoming increasingly challenging.
- Citizens are becoming more demanding, particularly the younger population of so-called 'digital natives'.
- People are increasingly using unsecured Wi-Fi hotspots to access personal information (email, social network, Internet banking) and exposing themselves to various types of attacks.
- City governments are expected to address all of these challenges, on top of existing issues. This drives the need to create an ecosystem of ICT vendors, energy suppliers, building companies, health providers and education bodies; all engaged in providing state-of-the-art solutions in every field.

The increased complexity of city's systems, their interdependencies, globally connected social, economic and political sub systems have increased the vulnerability of a city's security.

The cyber threats get magnified as infinite supply of data becomes more integral to a wide array of operations. Like any other ICT system, the smart city technological and communication environment – the network infrastructure and the Internet of Things – is vulnerable 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.

The smart city aims to optimise quality of life by leveraging technology and integrating the different macro-functions. City governance should therefore ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy.

In the scenario of overlapping functions, among the different stakeholder involved, 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.

For example, Smart City applications have the ability to improve everything from traffic flow to emergency response to the operations of the buildings in which we live and work: lighting control systems, thermostats, sensors, and alarms – all connected to the IoT – can automatically adjust building settings according to real-time usage patterns, leading to energy savings, improved air quality, and an increase in overall efficiency.

In addition to saving energy, smart buildings improve the indoor experience for occupants: on a sunny day, windows automatically darken themselves, and when sensors detect an empty room, the heat automatically turns off. Buildings that employ these types of energy-saving technology

improve occupants' quality of life, workers' productivity, and students' chances for academic success.

The smart city experience involves systems and objects interconnected through various technologies, like local, wide and wireless networks. 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. "Someone" in the city has to 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.

A smart city is an urbanized area where multiple sectors cooperate to achieve sustainable outcomes through analysis of contextual real-time information shared among sector-specific information and operational technology systems:

- Smart grids and energy efficiency. It is estimated that cities are responsible for between 60% and 80% of the world's energy use. Optimising delivery and consumption is vital.
- Buildings, both residential and commercial, provide an important opportunity to optimise energy consumption and enhance the wellbeing of residents and workers. Intelligent buildings, particularly office environments, are able to leverage smart grid technologies to influence energy supply and consumption by controlling lighting, climate control and IT.
- Intelligent transportation. Keeping the city moving is critical. Transportation strategies have an impact on public safety, the environment, energy, rapid response services, the ability to do business, and critical deliveries.
- Connected healthcare. Healthcare delivery can benefit from a connected approach, with Electronic Patient Records available to all medical services. This will enable public health professionals and clinicians to collaboratively access information in a secure way, at any time, from anywhere and from any device. In many cases, telemedicine solutions, connected through broadband, wireless or satellite, can prove vital in situations where the infrastructure or specific contingencies do not allow for the physical presence of a specialist.
- Public safety and security. Above all, cities need to be safe. Public safety and security has become paramount for city administrations, whether protecting against crime, natural disasters, accidents or terrorism.
- Wireless communications and hotspots. Both large and small municipalities offer free wireless hotspots in addition to those provided by airports, hotels, and shops. As this trend is set to continue, given the popularity of the service, more and more citizens will be exposed to potential vulnerabilities.

Fundamental to the creation of smart cities is the generation, analysis and sharing of large quantities of data. Indeed, the *main aim of smart cities technologies is to make cities data-driven*; allowing city systems and services to be responsive and act upon data in real-time:

- Intelligence: the first and most important stage of security is surveillance and intelligence gathering. This calls for equipment such as CCTVs and Biometrics hardware and software to collect the essentials in its raw, unprocessed form. Secured network for transmission of data is important to ensure non- tempering of data.

- Analysing Data collected: Analytics help digest, decode and make sense of the terabytes of information and data collected, by providing secured storage, analysis and forensic tools. Change from byte-sized to bite-sized for effective prevention against threats or reaction to a calamity and provide situational awareness.
- Mobilising the Resources: There is human intervention in any security installation with physical security apparatus from perimeter protection to communication devices for personnel on the move. The effective mobilisation of people and equipment is crucial to the entire infrastructure of a steadfast and secured location.

The interconnectivity of people, devices and organizations in today's digital world, opens up new vulnerabilities — access points where the cyber criminals can get in. The multiplying effect of today's cybersecurity challenges presents an opaque universe of threats that often come from unexpected or unforeseen domains that induce an escalating effect.

Securing Smart Cities aims to solve the existing and future cybersecurity problems of smart cities through collaboration between companies, governments, media outlets, other not-for-profit initiatives and individuals across the world.

As they invest in smart technologies to improve services and save money, cities also need to step up security against cyber threats. Cities are incorporating new technologies at an increasingly rapid pace, becoming ever smarter. Newer technologies — along with faster and easier connectivity — allow cities to optimize resources, save money and provide better services to their citizens.

6.2.3.2 Current status

Most cities around the world are unprotected to cyber attacks, and the cities are really important, because they are the backbones of civilization and economy. In particular we can set up the following three hot topics:

- Physical Infrastructure refers to its stock of intelligent physical infrastructure such as the urban mobility system, high speed broadband infrastructure, the housing stock, the energy system, the water supply system, sewerage system, sanitation facilities, solid waste management system, drainage system, etc. which are integrated through use of technology. By extension, this integrates all the data generated by the infrastructure and its applications.
- Social Infrastructure relates to components that enable development of human and social capital, such as the education, healthcare, entertainment, etc. It also includes performance and creative arts, sports, the open spaces, children's parks and gardens.
- Economic Infrastructure pertains to developing proper infrastructure that generates employment opportunities and attract investments.

Starting from the three previous topics, cities currently face the following situation:

- Insecure Products & Insufficient Testing: one of the biggest concerns about smart buildings and smart cities is that the sensors in the equipment can be hacked and fed fake data, which could be used for all manner of mischief, like causing signal failures that shut down subways or allowing contaminants into the water supply.
- Huge, Complex Attack: the notion of "internal network" doesn't really translate to smart cities. The trend is, the smarter the city, the more computer systems, the higher integration level between the systems, and the more open the access to the data collected by all those systems.

- Lack of Oversight and Organization: "Who's responsible when a smart city crashes?". Some experts agree that in many cities there is still no clear cybersecurity leadership, and that cities need to establish *city-specific security operations centers*, not just for information sharing, but also for cross-function vulnerability assessment and incident response planning.

It is important to remember that cybersecurity is a city-wide issue and not just a technology risk. Since many opportunities for IoT will arise through technological integration and collaboration, which will continue to increase in complexity — this complexity breeds risk.

To effectively manage the risks in a Smart City, it is important to clearly define the limits of that ecosystem:

- Data Privacy and protection concerns: Privacy is considered as a basic human right and is protected by national laws in different ways. Privacy concerns include the acceptable practices with regards to accessing and disclosing personal and sensitive information about a person.
- Smart city technologies capture data relating to all forms of privacy and drastically expand the volume, range and granularity of the data being generated about people and places. Privacy can be threatened and breached by a number of practices which are normally treated as unacceptable, however are part of operations in a smart city eco system.
- Surveillance: Watching, tracking, listening to or recording a person's activities
- Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- Data leakage: lack of data protection policies can lead to leakage or improper access of sensitive information
- Extended usage: use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent
- Insecure Hardware: One of the major concerns about smart cities sensors in the equipment; buildings etc. are insecure and not tested thoroughly.
- Larger Attack surface: Smart city operations utilize complex, networked assembly of ICT infrastructure to manage various services. Any device that is connected to the network is vulnerable to being hacked; the number of potential entry points is multiplied in Smart Cities.
- Bandwidth consumption: Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there are possibilities of security lapses.
- Application risk: Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today.

Beyond the potential for human or computer error, smart cities will provide cyber threat actors with a large attack surface to target and potentially exploit and incorporate into broader campaigns:

- Cybercriminals - As we have described above, smart cities will be composed of thousands – if not millions – of interconnected devices. Such a structure is a boon to criminal actors

able to create or purchase and subsequently deploy self-propagating malware, variants of which have been known to proliferate across multiple connected networks.

- Cyber activists - As cyber activist groups grow increasingly capable and in some cases, more radical, smart cities will provide them with an attack surface enabling a broad range of attacks from those akin to nuisances such as defacements of a city's billboards, to the more extreme targeting of a smart city's energy grid with the aim of physical destruction.

The potential destructiveness of a cyber attack on smart cities is such that even the threat of compromise of the city's system is likely to be treated by governments and businesses as an existential one.

As the underlying network of smart cities will encompass most aspects of life within the city, if that network were to be compromised by an attacker, it would grant them unfettered access to a target individual or organisation. For instance, state-owned competitors could compromise a smart city's infrastructure to gather intelligence on a large number of rival private sector firms. This information could include movements of their executives within the city, private and commercial communications grabbed from the ubiquitous presence of 'free Wi-Fi hotspots' managed by the city, and many more. Moreover, organisations operating within the city are likely to have their networks overlap to some extent with the city's own network, or at the very least, have frequent data transfers from their networks to that of the city. This would enable highly advanced threat actors such as nation states to exploit weaknesses within a city's infrastructure to reach a target organisation and compromise the confidentiality of its network.

European Initiatives:

- OASC: the Open & Agile Smart Cities, global initiative based in Brussels, Belgium, with more than 89 cities from 19 countries in Europe, Latin America and Asia-Pacific. Closely aligned to specific objectives of the Digital Single Market[19], OASC is a unique, European based, environment that links to experimental initiatives and creates a global smart cities market by interconnecting national networks of cities on a global level. It also supports the creation of new opportunities for European market players beyond the European borders. OASC was created starting from the FIWARE environment.
- European Innovation Partnership on Smart Cities and Communities (EIP-SCC) brings together cities, industry and citizens to improve urban life through more sustainable integrated solutions. Launched in July 2012 (following an earlier more limited coverage), it covers Information and Communication Technologies (ICT), energy management and transport management to come up with innovative solutions to the major environmental, societal and health challenges facing European cities today.
- UDN – the Urban Development Network is made up of more than 500 cities/urban areas across the EU responsible for implementing integrated actions based on Sustainable Urban Development strategies financed by ERDF in the 2014-2020 period.
- URBACT - a European exchange and learning programme promoting sustainable urban development, which integrates economic, social and environmental dimensions. It enables

[19] Overview of the Open & Agile Smart Cities (OASC) initiative and its relation to the Digital Single Market (DSM) strategy. Available at http://www.oascities.org/wp-content/uploads/2016/02/DSM-OASC.pdf (Last access: 22 August 2017).

cities to work together to develop new, pragmatic and sustainable solutions to major urban challenges, reaffirming the key role they play in facing increasingly complex societal changes. So far 7 000 people from 500 cities, in 29 countries, have participated in the URBACT programme.

Previous and ongoing EC projects related to “Smart cities and smart building” sector are listed in the following table:

ALMANAC	Reliable Smart Secure Internet of Things for Smart Cities
ConnectProtect	A total cyber protection service to Small Businesses operating critical infrastructure and Residential customers (SME phase 1 project, i.e. business plan analysis phase)
Rerum	REliable, Resilient and secUre IoT for sMart city applications
SECRET	Security of Railways against Electromagnetic attacks
SMARTIE	Secure and smarter cities data management

6.2.3.3 What market

The global smart city technology market is growing. According to market research and consultancy firm Navigant Research, the sector’s revenues will reach $36.8bn (€34.8bn) in 2016. Despite the sector’s growing profitability, many cyber security experts are concerned that smart city technologies are being adopted faster than the technology needed to protect them.

Cities around the world — whether considered smart or not — face significant cyber security threats. These problems could have a direct impact on government, residents and the companies and organizations doing business there. Cyber security in cities is extremely important, but we have yet to fully realize the risk.

The global smart city market is expected to reach US$1.565 trillion in 2020, with one-half of smart cities from North America and Europe[20]. E-Services to citizens, such as e-Payments, e-Exchange, e-Sharing, etc., will empower citizens with real-time access to personal data and related services. Technology is expected to improve everything from traffic control and lighting to energy and water management

Although the exact form that smart cities will eventually take remains uncertain, organisations and city planners can take a number of precautions to ensure a smoother implementation process and, ultimately, more secure infrastructure[21]:

- Prioritise the security of critical assets: contemporary networks are already impossible to protect in their entirety, a problem which will apply equally to smart cities. Some components of the system will have to be made more secure than others. Public and private city providers

[20] Source: Frost and Sullivan. Available at https://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020 (Last access: 22 August 2017).

[21] EY. Cyber Security A necessary pillar of Smart Cities. 2016. Available at http://www.ey.com/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf (Last access: 22 August 2017).

will need to work together to identify the city's critical assets and oversee the institution of appropriate security measures.

- Behaviour based security: auditing millions of separate devices for signs of malware is simply not feasible. A more workable approach would be to evaluate the behaviour of smart city components and systems against an established baseline of normal functionality or network behaviour.
- Rapid component replacement: given the potential for component failure or attacks compromising these components, an automated replacement system will enhance the security of the whole system.
- Segment critical assets of private organisations from the city's network: paramount to the security of organisations in the smart city environment is the segmentation of their critical assets from the city's network.
- connectivity and digital networking followed by cyber/network security and a clear vision and objective for the future. Additional components identified as crucial by the respondents are resilience and vision of a city as a system of systems.
- reference architecture for data exchange in Smart Cities. Exchange is happening mainly among transport operators and/or transport-related operators as well as between transport operators and citizens. This integration leads to interdependencies that may bring cascade effect in case of an incident.
- Understanding and use of cyber security policy and critical assets are poor. The majority of respondents do not have a cyber security policy in place and do not use institutionalised and codified definitions for critical assets, either in business or societal critical terms. However, more mature organisations, tend to have a more formalised approach towards critical assets.
- Lack of transversal information sharing on threats and incidents. Threats appear to be multifaceted and directed against IT systems, data, infrastructure but also organisational structure (i.e., mismanagement) and the entire IPT infrastructures.
- Knowledge of cyber security: overall organisations in the city are not so willing to exchange information about cyber security, probably because of the reputational costs and other indirect losses related to cybercrime.
- Adoption of cyber security measures has been slow. Several cyber security measures and responses appear to be implemented by transport and SC operators following their level of maturity with some of the measures not fully deployed yet, which indicates that cyber security responses are rather new and on the making. The current lack of guidelines and good practices regarding cyber security limits the dissemination and acquisition of knowledge.

Imagine what could happen if one or more technology-reliant services stopped working. What would commuting look like with no working traffic control systems, street lights or public transportation? How would citizens respond to an inadequate supply of electricity or water, dark streets and no cameras? What if waste collection was interrupted during the summer?

Cities are currently wide open to cyber attacks, which presents a real and immediate danger. The more technology a city uses, the more vulnerable to cyber attacks it is, so the smartest cities face the highest risks. It's only a matter of time.

For cities, being prepared is key to preventing bigger problems and chaos. That means:

- Ensuring that the infrastructure is secure;
- Conducting a security audit of technologies before they are implemented; and
- Preparing an action plan in the case of a cyber attack.

When we combine the fact that the technology used by smart cities can be easily hacked with the knowledge that there are cyber security problems everywhere, smart cities risk becoming dumb cities.

Cities are incorporating new technologies at an increasingly rapid pace, becoming ever smarter. Newer technologies — along with faster and easier connectivity — allow cities to optimize resources, save money and provide better services to their citizens.

6.2.3.4 Why Europe

With over 500 million citizens, the European Commission recognised the importance of strengthening the urban dimension in the EU policymaking. This evolved from an initial CITIES forum in February 2014 to a European Urban Agenda, and the identification of 12 priorities of which one that include the Digital transition[22]. The overall, increasingly integrated approach to cities, is reflected through a number of collaborations – and accompanying this integration by a corresponding increase in the awareness, tools, solutions and services to deliver cyber-resilience is key to avoid major cyber-attacks impeding the uptake of new integrated approaches. Europe is currently at a unique turning point in terms of collaborative urban development – and the networks are in place that open the opportunity to weave into this collaboration the appropriate, joint and tested approaches to cyber-security.

6.2.3.5 Scope

Pilots in this domain should focus on the following key points:

- Simulation and detection of the additional security threats created through the inter-connection of smart systems (“systems of systems” within the Internet of Things, IoT). As an example, in an extended scenario, so-called smart building botnets or cyber physical botnets (CPS botnets) are thinkable and feasible, i.e. botnets consisting of a high number of CPS like buildings and utilize their sensors and actuators to perform malicious activities that are made feasible due to their interconnection.
- Delivering a cyber-security framework to ease the collaboration across all smart cities stakeholders, from urban planners to infrastructure operators, IT supervisors and providers across organisations. The collaboration should extend from highlighting cyber-security risks linked to evolving urban planning scenarios to supporting the procurement process of new solutions and services, and their management in terms of joint challenges related to cyber-security.
- Supporting and implementing a *common approach* to securing and managing the data from all the systems of a smart city / smart building – supporting both the citizen and the public authorities in creating transparent, efficient and accountable cyber-secure data handling processes

[22] http://urbanagendaforthe.eu/wp-content/uploads/2016/06/State_of_Play_Revised.pdf

6.2.3.6 Targeted Users

- Infrastructure operators (transport, ICT, utilities etc)
- Urban planners and architects
- Building maintenance teams
- Security officers
- Public authorities

6.2.3.7 Expected impact

The expected impact is to ease the continuous increasing level of integration by developing a complete cyber-security framework for smart cities, including smart buildings. The cyber-security framework, addressing all phases of the life cycle, from definition of needs to procurement and from procurement to deployment should ease

a) the *expression of needs* by individual stakeholders, part of the overall management of a smart city
b) the *integration of different needs* into smart city scenarios – and facilitate the creation of shared scenarios (elaborated by incorporating the needs of multiple actors) and the awareness of which vulnerabilities need to be adressed and how
c) the deployment and most of all transformation of cities legacy systems into a manageable smart city concept with the *agreed, prioritised and maintained* level of cyber-resilience
d) the management of the *dynamics* of cyber-security, taking into account the *multiplicity* and interconnexion of systems and humans

Overall, the expected impact is to support a human-centric management of a fully integrated concept of cyber-security across a smart city and its smart buildings.

6.2.3.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Smart Cities is a unique integration environment that builds on solutions from all other underlying verticals – transport, health, utilities, e-Government, ICT networks etc.

It is therefore on the one hand an application domain in its own right – with *urban planning* as the major development policy. And it is, on the other hand, a unique transversal domain in its capacity to integrate and demonstrate all other domains in a collaborative deployment model.

6.2.3.9 Budget / Time / Instrument / TRL

13 ME, 2019, IA, initial TRL: 4-5 and final TRL: 6-8

6.2.4 Transportation

The transportation cyber pilot covers all security aspects of transport systems (for people and freight) whose compromise (as a result of coordinated attacks) may have macroscopic effects at National and/or European level. For example, a single hacked traffic light in a small town would not significantly impact security at a European level. However, replicating this attack in a coordinated attempt to block the routes of emergency response teams (e.g., by causing smart cars to crash at

the intersections) may have a tremendous effect both at a National and European scale if this cyber-physical attack is accompanied by a large scale terrorist attack.

Specific transportation types exhibit specific challenges, which we exemplify in the following for autonomous, possibly cooperating, unmanned aerial vehicles, maritime units and smart cars and trucks and railway system.

6.2.4.1 Specific challenge

Smart Cars, Trucks and Road-Side Infrastructure as part of the automotive domain cover semi- and fully autonomous and cooperating ground vehicles for the transportation of goods and people and the infrastructure they use to coordinate traffic in dense urban situations. Unlike industrial robots or UAVs, smart cars operate in close proximity to humans and in environments that lack physical separation. Cybersecurity attacks targeting smart cars may therefore cause severe civil upset through life-threatening accidents but also through smart-car based or assisted terrorist attacks. Besides this societal impact, smart-car based cyberattacks pose a severe economic threat since trucks cover 75% of the European domestic good transport.

While the automotive industry is currently working in the 5GPPP to enhance Vehicle-to-Everything (V2X) communications, evolving from 802.11p to specialized LTE infrastructures, there is still much work to do when it comes to security protocols needed to support the use cases that arise in those environments. Trust is again the key word in this scenario: pedestrians, vehicles and the infrastructure need to be able to trust each other. They need to authenticate other parties and the data they provide to be able to use this data. And, in some cases, they must do that even without knowing each other and without disclosing their identities, to respect their privacy too.

Actually, the Vehicle will be another consumer smart device, but with a longer live expectancy than smartphones. This will require the ability to update the cryptographic algorithms and, in general, any part of its SW, to adapt to upcoming challenges (e.g. revocation of cryptographic material and certificates, revising protocols and blacklisting, upgrading and patching of SW, etc.). Other challenges are related with Identity Management (identification of entities and up-to-date certificates), Misbehaviour detection (tampering on-board sensors) and Privacy Protection.

The specific cybersecurity challenges of smart cars are:

- The tight coupling of safety, security and timeliness in the control tasks required for autonomous driving (with and without V2V and V2I cooperation);
- The absence of easily reachable fail-safe states. That is, smart cars cannot easily be stopped or autonomous driving functionality disabled without risking the lives of the car's passengers or of traffic participants in the car's proximity. Instead, the car must fail operational until a safe parking space is reached respectively until a human driver becomes aware of the situation and takes over control;
- The longevity of cars well beyond the lifetime of third party suppliers;
- The requirement to use some of the computational resources in harsh environments (e.g., in close proximity to the engine), where limited heat venting and physical stress limit how much of possibly latent available computational power can be activated and for how long; and
- Exposure of the vehicle and its infrastructure to physical attacks.

- Privacy is urgently to be protected due to the sensitivity of especially location and movement data

Like UAVs, smart cars have to balance the improved situational awareness that cooperation with other cars and infrastructure may provide and the security threats that this cooperation and the wireless V2I and V2V infrastructure implies.

Maritime Vessels (such as cargo or cruise ships to transport goods and people) **and their infrastructure** at land (ports) are at the heart of the global economy: 90% of the international trade of goods are transported overseas, within Europe approximately 60% of goods are carried by maritime transport, and 3 European ports accounted for around 10% of overall traffic volume. These maritime streams of goods and people have significant bottlenecks: for instance, a major proportion of the goods transported between Asia and Europe navigate through the Strait of Malacca, which is a narrow stretch of water between Indonesia and Malaysia. Thus, a cybersecurity attack in the maritime domain can trigger perturbations on the economy at a global scale. The maritime domain faces cybersecurity challenges that are similar to those affecting ICS based industries, as well as specific challenges stemming from its particular operating environment:

- A vessel is indeed a floating system of systems where ICS and standard IT networks are operated. For instance, the propulsion system, the navigation system, the energy generation system, the HVAC system of a vessel such as a cargo vessel all rely on ICS. The operation of a port relies also on ICS, for instance for the automatic loading and unloading of cargo vessels.
- For example, cargo tracking and cargo identification are increasingly subject to cyber security incidents resulting from cyber-attacks. The same applies for the automated systems handling the cargo in ports. Data theft, for criminal purposes, may also increase as a direct result of insufficient cyber security measures – or measures not sufficiently matching the complexity of the ICT environment involved.
- The increasing connectivity of smart systems is also a characteristic of the maritime domain that leads to additional security threats previously not foreseen, for instance during the design phase of the vessels. There is a challenge of cybersecurity by design that needs to be addressed in the maritime domain.
- The maritime domain has also to tackle specific cybersecurity challenges. The isolation of the vessels and its limited crew is a factor that needs to be taken into account. These specificities imply technical and training cybersecurity challenges.

The use of **Unmanned Aerial Vehicles** is becoming very popular; a trend supported by dropping prices and enhanced capabilities. This success calls for attention to accidental, malicious, or criminal misuses. On the other hand, UAVs may carry out surveillance and response missions for border security, homeland security, and critical infrastructure protection. Depending on environmental constraints, the nature of targets and threats, the use of UAVs to detect, intercept, and neutralize rogue drones may be a cost-effective countermeasure to this expanding threat. To protect wide-distributed infrastructures, such as energy, telecommunication, or water or transport networks over wide, unsupervised areas, Sentry UAVs (SUAVs) appear to be a cost-effective solution. They can form into swarms to get advantage over Rogue UAVs (RUAVs). Any accessible point to a Rogue UAV is by nature accessible to a Sentry UAV, not necessarily to manned vehicles or fixed units. RUAVs have the advantage of preventing the exposure of humans and overcoming the range limitations of fixed ground units. Cyber-interception appears to be a good alternative to physical neutralization in a context where roaming drones may not easily be characterized as

accidental, malicious, or criminal intruders. Thus, interest in cyber-weapons embedded in defensive UAVs is growing.

However, such solutions have to face a number of technical and operational challenges. SUAVs need to present superiority in stealth, robustness, autonomy, detection, interception, combat, recovery, and collaborative and cognitive capabilities to have an advantage over their fellow targets in a situation where the attacker has the advantage of initiative. The split of functions between ground and aerial segments supports the optimal mix of autonomy/properties of the drone system. Existing solutions implement a panel of detection and identification means, relying on Wi-Fi and GPRS/EDGE, 3G or 4G sniffing or acoustic sniffing based on software-defined radio (SDR). Data fusion from heterogeneous sensor sources may be performed to enhance the level of precision and trust in the detection. Sniffing over the wireless medium whenever a thread is detected helps infer whether the rogue device is guided from a nearby location or indeed mission–based. Determining the RUAV controlling station is key to enable legal actions against the attacker. Observation and tracking functions rely on movement prediction algorithms, which require significant computing power, but provide a useful advantage over the RUAV. Interception and neutralization may be performed through a wide set of electronic counter-measures (ECMs), like GNSS spoofing, digital wideband jamming, or MEMS disturbance, in a progressive escalation of severity.

Remaining limitations and areas for improvement include the ability to operate in swarm setups for improved effectiveness of detection and countermeasures and enhanced communication and collaboration between manned / unmanned, airborne / ground-based detection, investigation, interception and neutralization means. State-of-the-art experiments show a number of remaining obstacles to the adoption of SUAVs in operation, starting with high rates of false alarms, lacking precision in identifications, poor energy efficiency, and reduced operability in bad weather conditions. Electro-Magnetic Pulse (EMP) may cause severe collateral damages. A distant high power microwave interferer may be harmful for friendly devices if not properly deployed. Speed of neutralization, speed of ECM activation, response and switching, GNSS spoofing accuracy, MEMS disturbance-reaction time can be improved with targeted research and innovation efforts. A key challenge is also to optimize performance / consumption trade-off. Last, but not least, the application of machine training and learning capabilities to SUAVs is likely to significantly increase their operational performance to a level that would genuinely challenge traditional (manned/human) means.

Projects addressing this topic should propose innovative security frameworks to support the design of robust cost-effective SUAVs, tailored to surveillance missions towards RUAVs.

Railway as well as other transportation systems is considered as a safety critical application, i.e., it is a system whose failure may result in financial disaster, death or serious injury to people. A failure occurs where the application or system is no more able to guarantee its required function. Safety critical applications are not necessary controlled by computers, however, as application complexity grows up, computers are much more reliable than humans to perform safety tasks and therefore computer are replacing tasks done by humans in the past. This is why the majority of transportation systems are computer based, and therefore cyber-security plays an important role.

Nowadays the wired and wireless networks used by railways operators are usually heterogeneous, not protected well enough and they don't fulfil the usual cyber security requirements in term of sustainability, protection and attack detection. The railway infrastructure is highly distributed, thus

difficult to protect, and it has been built before having had to deal with threats and risks to sensitive data networks. Every country has its own infrastructure, its own networks and every operator has its own strategy regarding cyber security.

Some encryption protocols have already been standardized but their application is restricted to particular ETCS interfaces. These standardised protocols are based on the prerequisite distribution of symmetric keys to all communicating entities. The process of installation/update of these keys in trains or trackside devices requires the manual intervention of an operator on site, leading to high maintenance costs and hardly reducing the global security level of the system. The protection of other railway communication channels is not addressed by these protocols and is managed on a case-by-case basis.

The lack of standardisation is a major impediment for the development of cyber secure signalling system. This is even more critical due to the long life and development cycles of the signalling systems.

There are many devices and rooms which are not secured. The access protections to trains and shelters are usually mechanical (keys, padlock or even a common key for many devices…). The profile selection is usually very poor and when this feature is provided it is usually based on the user name.

The current solution is not sustainable in the long term due to:

- its high maintenance cost
- its lack of flexibility, upgradability and interoperability
- its weakness in term of protection and detection

Applied to the railways system, the main objective of the security system is to ensure high availability, authentication and integrity of the railways system by preventing attacks or errors. The railways system is a safety-related system and safety highly relates to security. Safety cannot be ensured in case of lack of security.

The cyber security addresses:

- the protection of data against unauthorized disclosure, modification, or destruction
- the protection of the computers against unauthorized use, modification, or denial of service
- the protection of the railway IT network against attacks and malicious acts
- the buildings, the infrastructure and the trains. Improving the security in the European railways also implies a more controlled and restricted physical access.

It is also important to reduce the infrastructure and maintenance costs of railways operators and improving compatibility and interoperability by standardizing the security system at European level. This will apply to all new ICT used in railway (e.g.: traffic management, interlocking, Urban signalling communication, …).

6.2.4.2 Current status

The CAR 2 CAR Communication Consortium proposed the use of PKI solutions. The PRESERVE project (Preparing Secure Vehicle-to-X Communication Systems.) elaborated on that idea and on top of that includes a pseudonym CA to help implement some privacy preserving principles. Still,

new innovative crypto schemes should be developed to overcome the limitation of traditional PKIs. The EVITA project (E-safety vehicle intrusion protected applications) focused on on-board networks security, covering protection against tampering and compromise of sensitive. Some related H2020 projects are the following:

- UMOBILE: UNIVERSAL, MOBILE-CENTRIC AND OPPORTUNISTIC COMMUNICATION ARCHITECTURE. Users can share information directly with other peers without relying on infrastructure or expensive connectivity services. Some ideas can be exported to the Connected car scenarios.
- ADASANDME: Adaptive ADAS to support incapacitated drivers Mitigate Effectively risks through tailor made HMI under automation. This project will develop robust detection/prediction algorithms for driver/rider state monitoring towards different driver states. Although they don't explicitly deal with drive authentication, the same data acquisition architecture could be used for this purpose.
- AutoMATE: Automation as accepted and trustful teamMate to enhance traffic safety and efficiency. They have a defined 7 enablers, one of them being "Sensor and Communication Platform". Again no mention about security.
- CarNet: Rapid Data Communication Network for Connected Cars. Rely on plastic optical fiber to implement in-car network. Assume security by using a closed channel.

The cybersecurity of the maritime sector has not yet been addressed in European project leading to pilots, although being an issue of great concern for the European Commission. The European Commission has met industrial players to be presented the challenges and the specificities relating this subject. The ENISA published one of the first reports on this subject in 2011, highlighting the large area of exposure of the maritime domain to cybersecurity risk and the specific challenges of cybersecurity in the maritime sector.

The railway infrastructure mostly relies on computer-based devices which are interconnected through wired or wireless networks, making the railway transport vulnerable to cyber-attacks. The railway infrastructure is highly distributed, thus difficult to protect, and it has been built before having had to deal with threats and risks to sensitive data networks. Above that, every country has its own infrastructure, its own networks and every operator has its own strategy regarding cyber security.

However, some encryption protocols have already been standardized but their application is restricted to particular ETCS interfaces: EVC-RBC wireless communications and RBC-RBC communication[23]. These standardised protocols are based on the prerequisite distribution of symmetric keys to all communicating entities. The process of installation/update of these keys in trains or trackside devices requires the manual intervention of an operator on site, leading to high maintenance costs and hardly reducing the global security level of the system. The protection of other railway communication channels is not addressed by these protocols and is managed on a case-by-case basis[24].

[23] Igor Lopez and Marina Aguado. Cyber Security Analysis of the European Train Control System. IEEE Communications Magazine, October 2015.

[24] European Commission. Shift2Rail Joint Undertaking Multi-Annual Action Plan, 2015.

Regarding security assessment, preliminary joint threat analyses have been performed by the ERTMS user group. Such initiative has not yet led to common approaches, requirements or policies for cyber secure railway signalling system; each operator having its own standard and policy. This lack of standardisation is a major impediment for the development of cyber secure signalling system. This is even more critical due to the long life and development cycles of the signalling systems.

Security in railways system has also been addressed by the PROTECTRAIL-project[25]. The objective of the PROTECTRAIL-project was to provide a viable integrated set of railway security solutions, by considering:

- The extent of the assets involved,
- The nature of the possible threats,
- The amount of technical requirements and operational constraints.

PROTECTRAIL developed mission oriented solutions vs. asset-specific threats and made them interoperable by designing a modular architectural framework where each solution can be "plugged" in and also provided the basis for a streamlined process of federation, integration and interoperability of the developed solutions.

The European project SECRET has also highlighted the vulnerability of the railways regarding the jamming of the signalling, localization and communication information[26]. This project has:

- Identified physical parameters which can be monitored to efficiently detect attacks on communication channels and on localization signal (i.e. GPS);
- Developed jamming detector sensor prototypes for communication channel and localization signal;
- Developed concept of resilient network architecture.

Given the lack of guidance to assist the implementation of cyber security measures suitable to public transport, the European project SECUR-ED defined a common reference for implementation of cyber-security by any public transport operator.

Previous and ongoing EC projects related to the "Transportation" sector are listed in the following table:

CYRail	Cybersecurity in the RAILway sector
EATS	ETCS Advanced Testing and Smart Train Positioning System
IT2RAIL	INFORMATION TECHNOLOGIES FOR SHIFT TO RAIL
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
CARONTE	Creating an Agenda for Research ON Transportation sEcuity
PROGRESS	Protection and Resilience Of Ground based infRastructures for European Space Systems

[25] PROTECTRAIL Project. The Railway Industry Partnership for Integrated Security of Rail Transport, FP7, 09/2010 to 06/2014, Ref: 242270.

[26] SECRET Project. SECurity of Railways against Electromagnetic aTtacks, FP7, 08/2012-11/2015, Ref: 285136.

SCOUT	Multitech SeCurity system for intercOnnected space control groUnd staTions

6.2.4.3 What market

Maritime transport is the most important mode for long distance transport of goods to or from the EU, in tonnage terms[27]. In addition to demonstrating the crucial importance of the maritime sector for the European economy, this fact illustrates that ports infrastructures through which these goods are transiting are one of the main markets for maritime cybersecurity (cybersecurity market of critical infrastructures). The other market is obviously the shipbuilders, Europe being the home of the world leaders in shipbuilding of complex ships (for instance cruise ships or offshore vessels for the oil & gas sector).

The next 20–30 years will see unprecedented demand for growth in transport. European railways have to deliver increased productivity to fulfil growth demands across all modes in freight and passenger services by 80% and 50% respectively by 2050[28].

The European railway network has been incrementally developed over many years and is, too often, a patchwork of components, sub-systems and localised improvements. Railway networks are in general non-optimised and susceptible to performance issues due to this legacy.

6.2.4.4 Why Europe

European Automotive industry is currently leading innovation worldwide.

European railway companies currently lead the world market. The digitalisation of the railways makes necessary for them to evolve considering all the potential threads that may exist. Traditionally, railways focused in safety to ensure the quality of the service, however nowadays the railway system should also take into account security not to decrease the quality of the service and continue with the market leadership.

European shipbuilding is the world leader in building complex ships. For instance, the industrial players capable of building the biggest cruise ships are found in Europe (mainly in France, Italy and Germany), and no other country outside Europe have industry able to build these kind of ships (even China, Japan and the USA have never managed to compete Europe on this market segment).

6.2.4.5 Scope

- Safety case analysis of transportation system transition from a likelihood of failure based consequence analysis to a situational analysis where safety must also be maintained while the system and analysis is under attack
- New standards and certifications are defined for the safety and security of the autonomous vehicle software stack

[27] Eurostat. Maritime ports freight and passenger statistics. Available at http://ec.europa.eu/eurostat/statistics-explained/index.php/Maritime_ports_freight_and_passenger_statistics (Last access: 22 August 2017).

[28] European Commission. Shift2Rail Joint Undertaking Multi-Annual Action Plan, 2015.

- New technologies and innovative mechanisms are researched and developed to enforce the former.
- Security architectures and mission equipment for SUAVs, tailored to anti-RUAV missions
- Detection, identification and interception techniques to prevent intrusion of RUAVs
- Technologies enabling adapted behaviour of SUAVs to operate in synergy with fellows (swarms) and complementary systems (patrol aircraft, ground systems…)
- Transition from human guided to more autonomous and cooperative vessels
- Maintain and improve navigation security & safety despite growing attack surfaces and increasing attack sophistication
- Mitigate extreme traffic situations through cooperation
- Privacy preserving authentication in V2X scenarios.

New mechanisms and protocols to support V2P, V2V and V2I authentication that do not impose a significant overhead and provide privacy safeguards and allow instant creation of trusted contexts among devices. Anonymous authentication should be enabled for situations where the identity of the communication party is not needed. Partial linkability should also be supported, allowing parties to be “tracked” only for the needed amount of time (e.g. while crossing an intersection) but no longer than that. Special attention should be paid to constrained (e.g. offline, low power, low resources, etc.) devices involved in the communication, such us road or on-board sensors, that might require of some assistance (e.g. proxies) when negotiating a trusted context with regular devices. Multimodal driver authentication, using wearable devices and biometric characteristics to prevent driver impersonation.

6.2.4.6 Targeted Users

European citizen will get better services when the connected car is a reality. European countries will reduce traffic accidents and improve traffic management. Car manufacturers will have access to new tools for securely communicate their cars and manage them remotely.

European citizen will also benefit from a better security of the maritime transport of goods, raw materials and fossil fuels. Indeed, the majority of non-European goods consumed by citizens are imported through maritime routes.

Definition of railway cyber security system will allow the use, in a secure way, also public or non-proprietary network for railway applications. A new application could not need a proprietary or specific telecommunication system; one can design a general-purpose network using standard components, or even reuse an existing network, with obvious cost benefits.

Protocol standardisation will allow the specification of different monitoring functions, cryptographic techniques and / or key lengths. Should a given technique become not reliable anymore, one only needs to choose a newer / better technique supported by the involved entities. No modifications to “application” logic is required, nor specific testing to that particular technique.

By defining standardised and secure interfaces, information exchange among different countries will be greatly simplified. This will allow a better integration of existing services at European level,

as well as the development of new applications. Passenger information system, for example, can greatly benefit from this integration[29].

6.2.4.7 Expected impact

- minimization of CO2 emission by enabling a secure, coordinated and automatic resolution of extreme traffic situations,
- increase of road safety, both by reducing the number of deaths caused by road incidents (accidental and intended) and by removing benign smart vehicles from the weapons arsenal of terrorists,
- secure Europe's domestic and international goods transportation as an enabler for the continuing growth of the economic sector, and increase of the mobility of people at large but also of individuals (including both the youngest and the eldest)
- Set standards for UAV sensing, communication and C2 capabilities.
- Promote the development of advanced compliant technology in Europe.
- Support densification of the legitimate UAVs fleet involved in security missions.
- Set standards for cyber-security of maritime traffic before international players subvert Europe's maritime traffic regulations.
- Promote the development of advanced compliant technology in Europe.
- Support traffic growth by adapted cyber-security measures and solutions.
- Standard and open mechanisms and protocols for authentication in V2X
- Promote the development of advanced compliant technology in Europe.

6.2.4.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Each transportation modality requires different solutions and have different needs depending of the particular scenarios but in general we can highlight the following needs:

- Lightweight cryptography for reliable and timely authentication of vehicles. Also relevant to Industry 4.0 where real-time system require efficient cryptographic solutions.
- Multimodal authentication schemes to identify and authenticate driver and other humans involved in transportation scenarios. Also relevant in Smart Cities were citizen need to interact with the city services and be recognized by their elements.
- Embedded cryptographic modules supporting security services, more relevant for constrained devices. Also relevant to Industry 4.0, energy, Smart Buildings & cities and Healthcare where constrained devices need to be involved in security protocols.
- Tamperproof communication protocols to avoid channel hijacking. Also relevant to Industry 4.0, energy, Smart Buildings & cities and Healthcare where hijacking of control channels might lead to a critical situation or catastrophe.

[29] European Commission. Shift2Rail Joint Undertaking Multi-Annual Action Plan, 2015.

- Privacy preserving authentication. Relevant to all verticals. The trade-off between authentication and privacy will always be there, but we need to work on solutions that respect user privacy as much as possible.

6.2.4.9 Budget / Time / Instrument / TRL

18 ME, 2019, IA, initial TRL: 4-5 and final TRL: 6-8

6.2.5 Healthcare

Security in healthcare systems, services and applications is positioned as a major concern due to the high privacy and confidentiality requirements of sensitive healthcare data. e-Health faces many security challenges, most of them common to any critical infrastructure. Major trends in the field of e-health with an impact on security include:

- The massive trend towards seamless system and data interconnection, mobile services, smart devices and data analytics has already started and will lead to revolutionary changes in health care and nursing.
- It will be necessary to move towards a 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 care and prevention. As this information is extremely sensitive, it will be necessary to enable mechanisms that preserve the privacy of the citizens and the confidentiality and integrity of their data.
- A long-term radical change of perspective happened in the health services in the last few years, it goes under the name of “Patient Ecosystem”. It consists in the evolution of the hospital place of care to a network of services for patients, provided in home environments, smart cities etc., through different channels and technologies.
- The development of Assisted Living systems is one of the evolutionary aspects that healthcare is facing to support the creation of such an ecosystem. “Moving to the Humans is the new wave”, referring both to the many technological developments, that have as common characteristic to “centralize” the user (wearable systems, natural interfaces, and emotional design for user-centred innovation, etc.), and, above all, the way in which the access to services is provided
- Organizations around the world are choosing to implement e-Health to ensure better clinical outcomes and improve the patient experience. Major drivers include:
    - Efficient and secure use of technology to save time and reduce costs.
    - Reducing administrative and medical errors.
    - Improving patient experience.
- The proliferation of new technologies in healthcare is exploding. Wearable devices to monitor a variety of physical conditions, new medical IP-enabled devices, increased data demands to support advanced decision making, among other technological advancements, represent new security challenges.
- Government agencies, health departments and provider organisations, either public or private, constitute the main actors of any healthcare system. The way they interact with each other and with the patient determine the degree of effectiveness of any healthcare policy.

6.2.5.1 Specific challenge

- eHealth service resiliency against cyberattacks, prevention against data-leakage and loss of patient data and identity theft.
- Systems availability and business continuity is the key component for providing seamless electronic healthcare services. Access to critical health information by authorized professionals as well as secure access control by end-users needs to be guaranteed in order to ensure the best healthcare services. Lack of system availability may affect significantly the eHealth service delivery and some of the critical aspects of e-Health systems. In order to guarantee an acceptable degree of healthcare service availability, the whole healthcare service needs to be provided not only with security mechanisms but with the means to automatically recover from a cyberattack in the shortest time possible.
- Data security and integrity is another important challenge, in particular related to data storage, network elements (e.g. an access router to a site hosting the e-Health application) for exchanging health data and Identity and Access Management Systems (IAM).
- Medical Research can largely benefit from access to a large set of data not only coming from clinical trials, but also from monitoring the actual health parameters of patients and correlating them with environmental characteristics, population data, location etc. Healthcare digitalisation can provide these data in unprecedented volume and quality, but it need to be assured that data privacy as well as data integrity is preserved and data subjects can control the usage of their data. Transparency of the usage of the data is a prerequisite.
- Hospitals became incrementally digitalized often with complex and still largely unsolved security problems, tied to the standards used, the lack of harmonization of services and problems with both roles in the hospitals and harmonizing laws among different countries (especially in Europe).
- Include security and privacy by design in the evolution of hospital services.
- Hospitals evolved from a place of care to a delocalized network of care services. The development of Assisted Living systems is, only one of the evolutionary aspects of the healthcare system. The long-term radical change of perspective goes under the name of “Patient Ecosystem”. This evolution started few years ago, but it is exponentially accelerating thanks to all the following factors: the recent evolutions of mobile services, the better penetration of information technology to the patients and the increased impact of mobile wellness solutions.

6.2.5.2 Current status

Some of the EU funded projects in the field of e-Health include:

Tabula Rasa	Protecting biometric recognition from external attacks
SPaCIos	Testing the Security of Internet services
CACE	A toolbox for cryptography software development
ABC4Trust	The Privacy-ABCs to gain trust in the digital world
SHiELD	European Security in Health Data Exchange
KONFIDO	Secure and Trusted Paradigm for Interoperable eHealth Services
EPSOS	Smart Open Services - Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription

DECIPHER	The DECIPHER Project (Distributed European Community Individual Patient Healthcare Electronic Record)

These projects are listed by the European Commission as relevant under e-Health even though not all of those are not specific to the particular domain.[30] The tools and technologies developed under these projects can be applied in the domain. Some of the tools and technologies could potentially also be applied and relevant in the other Cyber Pilots.

6.2.5.3 What market

It is currently a trend in Europe that the population is aging. In other words, the proportion of the elderly people in our countries is increasing, due both to fewer children as well as a longer life expectancy. According to the report *Redesigning Health in Europe for 2020*[31], nowadays the healthcare costs in Europe are increasing. These costs are a constantly growing component of public finances, rising to 9% of GDP and representing between 6% and 15% of spending in most EU Member States. Another important aspect of the Health Sector in EU is that about 40% of the population above the age of 15, i.e. over 100 million citizens, are reported to have a chronic disease. This proportion climbs to 66% of the population who have reached retirement age having at least 2 chronic conditions.

In this scenario the EU Member States are facing the situation where more than 70% of healthcare costs are spent on chronic diseases, and this figure is expected to rise in the following years. For this reason, EU Member States are trying to achieve an affordable, more efficient, less intrusive and more personalized care of the citizens. For achieving this vision, the application of Information and Communication Technologies and also the use of data could be of great help. In other words, the use of the concept known as eHealth will increase. This involves a broad group of activities that use electronic means to deliver health-related information, resources and services. These include supportive eHealth policy, legal and ethical frameworks, infrastructure development and developing the capacity of the health workforce through training.

The impact of using ICT Technologies will be reflected mainly in the following fields[32]:

- **Health Analytics and Big Data in Health**. Analytics is in this context the transformation of data for the purpose of providing insight and evidence for decision- and policy-making. The term big-data makes reference to a big amount of data, larger and more complex than traditional data processing can process. This requires the use of distributed systems and advanced methods of data analysis.
- **mHealth**. Use of Mobile Technologies to support health information and medical practices. The main active of mHealth is the potential to reach wide geographical areas and the use of portable forms. mHealt is incorporate into health care services such as health call centres

[30] European Commission. EU funded societal challenges projects | From Lab to market. Available at https://ec.europa.eu/digital-single-market/en/lab-market-what-happens-after-projects-end (Last access: 22 August 2017).

[31] eHealth Task Force. Redesigning Health in Europe for 2020. European Union 2012.

[32] World Health Organization Europe. From Innovation to Implementation. eHealth in the WHO European Region. 2016. Available at http://www.euro.who.int/en/ehealth

or emergency number services and also includes functions such as lifestyle and well-being apps, health promotion and wearable medical devices or sensors.

- **Telehealth**. Medical Services delivered from a distance that encompasses remote clinical diagnosis and monitoring. Telehealth also include a wide range of non-clinical functions encompassing prevention, promotion and curative elements of health. It also involves the use of electronics means or methods for health care, public health, administration and support, research and health education.
- **Electronic Health Records (EHRs)**. Electronic health records are real-time patient-centred records that provide immediate and secure information to authorized users. EHRs include typically a record of the patient's medical history, diagnoses, treatment, medications, allergies and immunizations, as well as radiology images and laboratory results. The fact that this information is in digital format makes easier to search, analyse and share.
- **eLearning in Health**. This topic refers to he use of electronic technology and media for training and education that could be used to improve the quality of education and also to increase the access to learning in geographically isolated locations or those locations with insufficient training facilities. This will contribute to increase the number of trained professionals with specialized or general skills.
- **Social Media in Health**. These online communication channels, which are informal and socially driven, can be used by health care providers to share health information and educate the public, discuss care policy and practice, promote healthy behaviors and increase awareness of the services. Patients can also make uses of Social Media to communicate with health care providers as well as with other patients.

These topics can be summarized in five main levers that will move the Health sector in the following years:

- **My data, my decisions**. Patients and institutions share their data with flexible consent mechanisms.
- **Liberate the data**. Health outcomes and performance data will be freely published with full transparency.
- **Revolutionise health**. Technology and information management drives the pace of change.
- **Connect up everything**. This will link the lifestyle data with health data by means of lots of new apps and tools.
- **Include everyone**. In other words, the contribution and benefits from eHealth for all.

From the cybersecurity point of view, all these trends should be carefully analysed. All of them are related to the use of Health and care information of patients: from monitoring signals, health status and patient's history and data in electronic format, ready for sharing. All this information should be considered confidential and sensible data. Therefore, high requirements and efforts to conveniently anonymize and protect should be made, when thinking specially in possible threats and the trends in cyber-attacks.

Cyber-attacks are constantly increasing. This kind of attacks focusses mainly on stealing financial information, billing information, and bank account numbers using stolen devices with un-encrypted data, phishing and spam mails. Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats (APT), zero day attacks, and advanced malware.

However, we are seeing the trend of an increasing number of cyber-attacks to Health sector. Lack of adequate IT spending by healthcare organizations and lack of awareness about cyber crime have exposed the vulnerabilities of healthcare organizations. The overall impact of cyber attacks on the hospitals and healthcare systems is estimated to be nearly six billion per year.

Furthermore, these organizations face internal threats due to factors such as the use of cloud services, unsecure networks, employee negligence, bring your own device (BYOD), lack of internal identification and security systems, stolen devices with un-encrypted files.[33]

6.2.5.4 Why Europe

Healthcare sector is defined as an operator of essential service in the European Union and falls under the stringent rules set out under the newly adopted Network and Information Security Directive.[34] Further, it is deemed as one of the critical infrastructures of many of the EU Member States therefore it is of utmost importance that these systems are secured. This is even more so in Member States who are already creating cross-border healthcare services. Cybersecurity solutions developed in Europe would ensure digital autonomy in this sector as it is critical to our society at large.

6.2.5.5 Scope

In order to broaden the scope as much as possible, this Cyber Pilot should focus on an existing e-Health service involving as many stakeholders as possible, including but not limited to end users (patients), healthcare service providers, doctors and other professionals. The integrity of healthcare data being distributed among these many actors is one of the key issues that should be thoroughly reviewed and tested within this pilot. The e-Health service should also involve different IP-enabled devices and mobile applications. The security of such technological elements is of paramount importance for the adequate provision of the healthcare service.

The overall security of the selected e-Health service will have to be analysed first, with a special focus on data integrity, privacy and interoperability. Where needed, additional security features and/or new technology elements will have to be introduced to increase the resilience of the global e-Health service. After that, the e-Health service will be put under attack to test its resilience and find out its weaknesses.

The human layer in healthcare must be properly considered and integrated with all the other security layers. This is especially important in Healthcare because it is one of the most targeted sector for social engineering enhanced attacks and because healthcare is one of the critical infrastructure which most relies on human competences and knowledge.

The pilot may include a scenario where patients are encouraged to share their health data for analytical tasks, including medical research, optimised health insurance schemes, etc. This scenario should allow sharing in a privacy preserving manner under the control of the data subject

[33] Predictions 2016: Cybersecurity Swings to Prevention. Forrester.

[34] Directive (EU) 2016/1148 of the European Parliament and the Council. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (Last access: 22 August 2017).

(e.g., by adequate anonymization or the exploitation of secure computing schemes for their analysis), while still preserving the utility of the data.

6.2.5.6 Targeted Users

As stated before the cyber pilot shall cover as many stakeholders as possible including:

- Patients: They shall be the final beneficiaries of the cyber pilot project by receiving trustworthy, reliable, safe and secure eHealth services with full confidence that their private personal information is being handled responsively and only for those purposes they have previously authorised.
- Healthcare Service Providers: Cybersecurity solutions better suited to the healthcare environment shall be provided to respond to the stringent requirement of the patient ecosystem and the increasing demand of more secure services.
- Doctors and other health professionals: They shall be capable of performing their activity efficiently with guaranteed availability of the required systems and information to execute their normal tasks but at the same time providing confidence in that sensitive information is fully reliable and handled securely.

Other stakeholders will also benefit from the cyber pilot such as the pharmaceuticals or research centres by having more controlled, reliable and faster access to relevant information to perform supply management or research activities among others while at the same time guaranteeing that personal information privacy is preserved at all times.

6.2.5.7 Expected impact

The conclusions obtained from the cyber pilot would provide valuable input information not only to secure e-Health services, but to improve their capability to automatically recover from cyberattacks, restoring the eHealth service level to its nominal status.

Possible outcome of the cyber pilot includes new secure design methodologies and new technological elements to enhance the current resilience level of eHealth services.

Increased resilience of a national critical infrastructure.

6.2.5.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

There is no doubt that ICT will be a relevant player within the next future in Health, predictive, preventive, personalise and participative medicine will be the main pillar of future medicine. In this context, nowadays technologies like telemedicine, home care systems, remote monitoring, mHealth, wearable, big and smart data are just some examples of technologies that will be relevant to assure the quality and sustainability of future health care models. In this environment, resilience of healthcare systems and the full patient ecosystem is a crucial need. It is a pillar in the generation of trust and confidence to the patients in the eHealth services. However, in the last years we have seen on the contrary and increase in attacks threatening and jeopardizing this availability due to the increasing interconnection of healthcare systems, the stronger reliance on IT to execute the basic healthcare activities and the growing interest of attackers in attacking health organizations

because they have proven to be an easy target prone to pay requested ransoms in order to be able to regain control of their attacked systems.

The cyber pilot will address this fundamental need by studying the resilience of all elements within the patient ecosystem in order to provide reliable and trustworthy services to society.

Another essential need is full confidence in the integrity of information being managed since false data can lead to invalid researches, incorrect diagnostics and ultimately even serious threats on the health of the patients. The need for confidence in the integrity of information is increasing mainly due to two current trends being experienced within the healthcare sector. On the one hand, the increasing amount of health information being gathered from patients sometimes even in a continuous manner. On the other hand, the growing number of medical devices which are network connected and poorly protected. These devices introduce a triple threat to the healthcare services. First, their lack of resilience due to the lack of adequate protections. Second, the serious threat to the health of the patients if information exchanged in and out the medical device is intentionally or unintentionally altered. Third, and last, due to their poor protection they introduce an entry point to the full health organization IT systems potentially compromising not only the availability of all systems as discussed before but also the integrity of information stored and exchanged.

The third and last essential need within the healthcare environment is the need of providing confidence to patients that their information is being handled responsibly. A responsible management of private patients' information involves several aspects. Patients are full owners of their personal health information. They have the rights to decide for which use such data is allowed, as well as who and when is allowed to use it. Privacy of this personal information is therefore crucial. Responsible management is also that the information is available when and where needed as long as this does not contradict the previous condition. Hence, secure health data exchange and access solutions have to be defined and available. On the other hand, data access and how to obtain relevant and valuable information from those data will be a key pillar for new advances like personalize medicine. Solutions that permit a simple, fast and accurate access to that information while at the same time preserving the first two clauses for responsible management would be a huge facilitator for the health research sector empowering its growth.

6.2.5.9 Budget / Time / Instrument / TRL

10ME, 2020, IA, initial TRL: 4-5 and final TRL: 6-8

6.2.6 E-services

6.2.6.1 E-government and Public Administration

6.2.6.1.1 Specific challenge

- Enhance the protection of real local and public administration systems
- Necessity to cut cost and become more cost-efficient.
- Citizens expect public services and data to become more open and trustworthy and this trust extends for years to come. Tools for data recovery in digital format are required.
- Mobile devices provide a ubiquitous entry point to services that need to be secured.
- Popularity of social media raises challenges that would usually be for the media and telecommunication industry. However, the political nature of e-government often leads to

intensive discussions in e-government-related fora. Then freedom of speech is especially important but also one needs to avoid that hate-speech and propaganda take the upper hand.

- Legacy systems in use.
- A trend to shift government services towards cloud-based infrastructure.
- Users have different security background (and many have none).
- Citizens are requesting more transparency in the administration of public resources and, as a result, governments, public agencies and even organisations are starting to offer their data for scrutiny. Besides promoting trust in public institutions, the principles of open Public Administrations can be useful to different stakeholders in order to make their services more attractive, user-friendly and effective, or to improve their decision-making processes. However, the release of potentially sensitive information involving citizens and organisations opens the door to enormous privacy risks due to insufficient or inefficient data sanitisation/obfuscation mechanisms before data release. There is an urgent need for privacy guarantees to the actual data owners of these data.
- Secure exchange of data across borders is becoming increasingly relevant to the goals of Digital Single market. Wider scale federated layers of e-government should be tested.

6.2.6.1.2 Current status

Some related EC projects are BigDecisions, SUNFISH, WITDOM, although none of them is explicitly aligned with the topic of open public administrations with privacy guarantees.

Other projects that could be related to the topics include:

ABC4Europe	The goal of ABC4Trust was to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC).
FutureID	identity management
STORK	Take your e-identity anywhere in Europe

6.2.6.1.3 What market

E-Government and Digital Public Administration can provide a number of benefits to both citizens and businesses, including improved data transparency and service availability, increased participation of citizenship in political affairs (e.g., e-voting), more convenient contact with administrations and access to Public Services, reduced administrative burden, and overall major economical savings to Governments.

Various reports forecast that the digitalization of Government and Public Services will bring about massive cost reductions. According to the Secure Identity Alliance and The Boston Consulting Group[35], eGovernment Services will help us save up to $50 billion per year by 2020 globally. Besides, the savings to the public purse, digital access to Public Administration can be very

[35] https://www.secureidentityalliance.org/index.php/news-events/news/155-egovernment-services-would-yield-up-to-50-bn-annual-savings-for-governments-globally-by-2020-while-increasing-convenience-trust-and-citizen-satisfaction

effective to save the money of taxpayers and businesses. Simply by adopting electronic billing and invoicing, Europeans could achieve up to 80% cost savings according to Richoh Europe[36]. The implantation of e-invoicing in Denmark has resulted in savings of €150 million a year to taxpayers, and €50 million to businesses.

The most immediate market to the aforementioned services and technologies is the European public sector, as there are multiple European- and national-level regulations that oblige public administrations to switch to digital solutions, in several areas (e.g., taxes, justice, banking, etc.), as described in the EU eGovernment Action Plan 2016-2020. This necessity opens up space for European industry to provide adequate solutions and services to numerous administrations, ranging from local to national (and even European) level.

6.2.6.1.4 Why Europe

After the financial crisis, European citizens are requesting their Governments, Public Administrations, Political parties, and also private companies (i.e., banks) to be transparent and open. Meanwhile, the U.S. Government already has a portal[37] where they offer open datasets and tools to the general public. Also, some initiatives exist across Europe, for example the Government of Spain[38] and the BBVA bank[39] are offering their own data through open APIs. This is in line with EU's open data policy, which is part of the Digital Agenda for Europe, and that sees open data as a driver for innovation, growth and transparent governance.

6.2.6.1.5 Scope

- Cyber protection of real systems used by public administration and citizens
- The main objective is to provide the Administrations with suitable tools and mechanisms to sanitise data repositories and to quantify potential privacy erosion, supporting this way a privacy-aware provision of open-access data. Data protection techniques – outsourced storage and processing can potentially increase the risk of exposing sensitive information to privacy & security breaches.
- Frameworks and technical solutions for cross-border data exchange between governments and private sector in the EU, including identity management frameworks.
- Privacy enhancing technologies and solutions:
- Anonymisation-pseudonimisation for data-intensive applications.
- Privacy techniques for machine learning applications, preserving utility for data analysis, privacy / utility trade-offs.
- Meta data privacy, including query privacy.
- Privacy metrics, economic value of data, combining data sources without breaking privacy regulations, differential privacy.

[36] BusinessWire. Ricoh Europe: Businesses could save up to 80 per cent through electronic billing and invoicing Available at http://www.businesswire.com/news/home/20150611005020/en/Ricoh-Europe-Businesses-save-80-cent-electronic (Last access: 22 August 2017).

[37] https://data.gov

[38] http://mapa.datos.gob.es/

[39] https://www.bbvaapimarket.com/

- Privacy-preserving technologies for data intensive applications, including operations over encrypted data, property-preserving encryption, secure multi-party computation, data exchange models and analyses.
- Data distribution, fog computing.
- Runtime assurance and transparency on the use of personal data. Enabling technologies for right to access, right to be forgotten, and right to data portability.
- Data Protection techniques and protection against data leakage.
- Personal data user empowerment, enabling right to access data,
- Cloud security and security service assurance.
- Mobile device protection.
- Threat management. High level protection even for:
    - Obsolete web applications
    - Different agencies with their own security requirements.
    - Increased attack surface, e.g., because of mobile devices, social media, smart TV, etc.
- Secure methods for eVoting
- Development of scalable technical solutions to enable data integrity preservation and real-time tampering detection in mission critical operational IT solutions, especially in the areas where there is no paper fall-back any longer. Solutions need to be scalable and domain-independent.

6.2.6.1.6 Targeted Users

Main beneficiaries are:

- Individual users, which will increase their trust towards public (and, in some cases, private) organizations.
- Public and private organizations, which will have access to tools that facilitate the provision of open-access data in a privacy-friendly way.

6.2.6.1.7 Expected impact

- Promote a culture of transparency in governments, companies, organizations and citizens, which in turn increases overall trust within the different actors in society.
- Leverage the usefulness of technology as a transparency-enhancing mechanism.
- Open Government
- User-friendly, reliable and effective services
- Increased trust in Governmental services
- Improve quality of decision-making
- Economic efficiency

6.2.6.1.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Privacy enhancing data handling tools and technologies that ensure confidentiality, integrity and availability is a common concern in all the verticals.

6.2.6.2 Finance and Insurance

6.2.6.2.1 Specific challenge

- The Financial sector can be considered as the backbone of the Economic development and competitiveness of a region. To foster European competitiveness the implementation of a Single Financial Market is a pre-requisite and many steps have already been undertaken toward the harmonisation of different national frameworks (eg. EMU, Target2/T2S, SSM). The regulation to create a Single Digital Market across EU, strengthening Europe's cyber resilience, and the regulation to foster the stability of the Single Financial Market highlight some common challenges and risks, to be tackled to reach a **Single European Digital Financial Market**.
- Operating in an open economy and with high level of interdependency does introduce a **high systemic risk** that covers the entire EU financial system. In such an integrated system, the high relevance of the **Cyber Security** in the financial field is crystal clear taking into account that:
    - Digital Banking is a prominent mean to do banking nowadays whether this happens with the advanced applications used in physical Bank premises (e.g. digital signature, biometric identification), or remotely through ATMs, home-banking or any other digital device;
    - European citizens daily life entails digital banking as final step in most purchasing activities;
    - Proliferation of digital devices represents the omni-channel challenge requiring efficient authentication and authorization means;
- New players are entering the financial competitive arena. They can actively be involved in the payments value chain, (e.g. as PISP under PSD2) and they use intensively the digital means. Mostly these new players are not regulated and are not necessarily used to adopt the strict banking processes and procedures toward risk mitigation.
- Cyber risk management is a top priority to the financial industry. The increasing number and frequency of sophisticated **cyber-attacks** to the banking sector highlights the need to develop a comprehensive cyber security framework to protect the integrated financial market and to combat **cyber fraud**.
- The financial system resilience needs to be enhanced. Even more taking into account the developments of innovative solutions based upon a collaborative integration such as DLT and blockchain. Each and every single financial institution should take all possible measures to identify, mitigate and protect itself from cyber risk. Nonetheless, in a highly integrated financial world all the components and connections need to be protected to **enhance** the **overall financial system resilience**. To reach an appropriate and consistent level of risk mitigation, it is important to foster awareness through the **data and information sharing**, even to the extent of sharing common infrastructures (such as CERTs, irrespective of the centralised or distributed architecture). Furthermore, the information sharing could be extended beyond the financial industry.
- The management of **cyber-secure supply chains** is also important in critical infrastructure organizations, even more in financial institutions, that are end-users of innovative products and technical solutions. In order to develop secure financial products and services, product development must be based upon secure components, processes and procedures. As a matter of example to cope with **EBA's Guidelines on the security of internet payments**,

the banks' **authentication and authorization** processes need to leverage innovative solutions to increase security for online payments.

- **Privacy, Data Protection, and Data Integrity**, represent major challenges in the digital banking era, these are key items across all the financial industry (both banking and insurance) and need to be protected.
    - Insurance and finance sectors operations often involve cross-border transfers. In addition, the financial institutions deploy different channels of interaction with their customers (mobile, point of sale, ATMs) which each use different identification techniques. Combining the cross-border and the multichannel interaction modes requires a high level of data management and data protection against cyber-security threats adopting a privacy preserving approach to cross border data transfer.
    - Under the PSD2 Directive (2366/2015) not regulated third party providers (TPPs) can cover partially the value chain of payment systems. The PSD2, with XS2A accounts provision, also introduces the obligation to provide them with access to information and therefore to sensible data, increasing the cyber risk on privacy, data protection and communication protocols.
- Insurances have traditionally priced risks based on risk factors, the challenge is to combine privacy preserving approach and risk evaluation. The shift towards more risk sensitive prices, driven by increased data availability, means that insurers will collect and analyse a larger amount of data, mainly personal and sensitive ones. The collection and management of data in a digital framework highlights several needs, among the others customers awareness, user friendliness, privacy and cyber-security assurance.
- The **Insurance sector** involvement is at least twofold:
    - on the one hand the insurance sector like any other industry is leveraging the digital innovation and cyber security products and services, as such it needs to manage the cyber security risks;
    - on the other there is a stream of innovative products and services that the insurance sector can put forward to provide across industries trusted means of transferring cyber security risk (Cyber-insurance), this entails a research and innovation stream to make cyber risk measurable.
- The **creation of a measuring system for "Cyber Risk Exposure"** to quantify, mitigate and manage the cyber risk can be considered one of the necessary target in order to create a common EU Cyber risk benchmark that can be used to compare enterprises' resilience to cyber risk across Europe. Since insurance prices are built upon loss frequency and costs, measurability is a must for a risk to be insurable. However, existing actuarial models cannot rely on historical data loss, since the quantity of historical data is scarce and its homogeneity is compromised by continuous technological innovations. The lack of reliable models to estimate the value of loss/stolen data also prevents the reliable evaluation of losses. Models for computation of correct premiums and coverage must be considered as a priority need.
- In many domains, when a major event occurs that imposes a heavy burden on an insurer, the re-insurance mechanism ensures that there is a geographical distribution across different insurances (e.g. in case of earthquake insurance) or through a re-insurance of high losses. Re-insurers for cyber risks do not yet exist at all, whereas the size of the potential risk requires this re-distribution across organisations and geographies. Thus, the promotion of a re-insurance structure for cyber-security represents a new challenge and a new opportunity. More accurate and standardised statistical models should help to address some of the needs for the re-insurance.

- Creating a clear set of Cyber Security definitions and measurements, could also enable the introduction of a framework for standardisation, labelling and certification.
    - Pricing the value of “Cyber Secure Environment”: to establish a risk profile, similarly to what has been developed for physical data center to create a “Data Centre Site Infrastructure Tier Standard”, it might be worth creating a references schema for evaluating “Cyber Secure” Environments (logical and physical).
    - Labelling “Cyber Secure Services”: if a reference measurement is created then it might be possible to create “Cyber Premium Services” that could leverage more sophisticated cyber security features and could be offered at a premium price.
- The **implementation of educational and training program** is the last, but not the least success factor in tackling Cyber Security issues. The human factor cannot be neglected for several reasons and at different levels. Beside the extreme case of fraudulent behaviours that entail cyber frauds, eventually by-passing all measures to cope with the Cyber-risk, it is of the utmost importance to have skilled resources with respect to Cyber Security issues.
    - Top Management and executives involvement, with an accurate understanding of the Cyber Risk consequences, can ease the adoption of new technologies and features that can reduce the cyber risk, accepting to undertake the associated additional costs. Furthermore, for any financial institutions’ employee, a minimum common degree of understanding of Cyber Risk could be considered as part of a mandatory training.
    - Even before employment, specific education programmes should be set up with the universities to avoid the lack of skilled IT personnel. Already today, a shortage of experts can be observed and growth of the market will be inhibited unless sufficient numbers of experts are trained in cybersecurity
    - Customers should also receive some communication and training around cyber security, to reduce the chance to be victim of cyber frauds, to develop awareness around the value of Cyber Security and to become active part of Cyber Risk mitigation.

6.2.6.2.2 Current status

The analysis of recent and ongoing EC calls and projects shows that they do not or partially cover the specific topics underlined in this document for Finance and Insurance sector.

The continuous evolution of Threats and IT risks makes Cyber security stand high, especially in the Finance and Insurance sector. There are some basic considerations for the continuous investments to protect the Finance sector versus the cyber risks:

- The high impact on all European citizens;
- The systemic risk associated;
- The ability to support the competitiveness and the growth of the entire European economy;
- The huge amount of sensible personal data managed through the Banking and Insurance sector.

In the past few years, there were no specific calls and project in Finance sector, but it is possible to identify some cross industries projects and calls that could address some financial needs identified in the document. Although none of them is fully consistent with the specific challenges identified in this document for the Finance and Insurance sector. Among the previous EC call, it is worth mentioning:

- C3ISP - Collaborative and Confidential Information Sharing and Analysis for Cyber Protection: ongoing project (from 2016-10-01 to 2019-09-30), H2020-EU.3.7 programme;
- WISER - Wide-Impact cyber SEcurity Risk framework: ongoing project (From 2015-06-01 to 2017-11-30), H2020-EU.3.7 programme;
- PROTASIS - Restoring Trust in the cyber space: a Systems Security Proposal: ongoing project (From 2016-05-01 to 2020-04-30), H2020-EU.1.3.3. programme;
- HINT - Holistic Approaches for Integrity of ICT-Systems: closed project (2015), FP7-ICT programme;
- PRECYSE - Prevention, protection and REaction to CYber attackS to critical infrastructures: closed project (2015), FP7-SECURITY programme;
- CAPER - Collaborative information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime: closed project (2014), FP7-SECURITY programme;
- IPaCSO - Innovation Framework for Privacy and Cyber Security Market Opportunities: closed project (2014), FP7-ICT programme.

6.2.6.2.3 What market

It is pretty difficult to have a precise indication of the market size. Indeed, it is a general understanding that there is a lack of market knowledge: standardized market definitions, statistical information, market monitoring and trend analysis.

The first challenge is to define what should be taken into account in the calculation of cyber security market, the second step should be to create harmonised accounting principles, and finally there is a need for accurate statistics. Indeed, in the market reports very often the market size refers to ICT costs and expenditures, in some cases the reference is done to the damages, in others there is a reference to the revenues.

When it goes about the solutions adopted to enhance the cyber security architecture the budget is often allocated to generic ICT expenditure and basic components useful in Cyber Security, are seen as general-purpose components of IT infrastructure.

Cyber security costs, could be distinguished among HW, SW, encryption tools, diagnostic tools, data feeds, network protection and so on, they could also be distinguished among Detection, Recovery, Containment, Investigation, Incident Management, similarly a distinction could be done taking into account Business disruption, Information Loss, Revenue Loss, Equipment Damages.

Moreover, while the cost of cyber crime impacts all industries, companies in energy & utilities, financial services and technology have experienced the highest annualized cost[40].

All the above, highlights that there is a clear need to define a framework to create and monitor an EU statistics related to Cyber Security altogether and by categories. Notwithstanding the challenge to put in place standard definition and measurement, to have an idea of the dimension of the phenomenon, it is worth reporting some findings of relevant researches:

[40] Ponemon. 2014 Global report on the cost of cyber crime. Available at http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime

- According to "Cybersecurity Market Report – Q3 2016" published by Cybersecurity Venture[41], globally the cybersecurity market by 2017 will be worth $170 billion.
- According to PwC "Insurance 2020 & beyond: reaping the dividends of cyber resilience"[42] paper, Cybercrime costs the global economy more than $400 billion a year.
- European Banks are major investors in IT infrastructure and services, pouring billions of euros every year into innovation, research and maintenance. Research among banks conducted by Celent in 2015 shows that European banks in 2018 expect to invest 62 billion in IT[43].
- The 2013 Ogone report on "Online & mobile payments: new opportunities & threats"[44] reported that European B2C e-Commerce market should reach €625 billion by the end of 2016, and mentions that online payment fraud remains the largest category of fraud – with 73% of payment fraud taking place over the internet. "Third report on card fraud - February 2014"[45], published by ECB shows that, in 2013, the total value of fraudulent card transactions, in SEPA area, amounted to $1.44 billion, and 66% of the total value (€958 million) results from so-called card-not-present (CNP) payments made via the internet, post or phone.

Besides all other figures, according to Forrester research[46] some 214 million people in Europe will use mobile banking services by 2018 and, according to EY "Global Commercial Banking Survey 2014"[47], customers see Security as the main concerns when using digital channels, and, they want from their bank, enhanced security.

- The insurance sector looks at cyber market from two different points of view: on one side insurance companies are subjected to expenditures and potential losses arising from cyber security threats (e.g. data breaches, stealing of sensitive data) similarly to other financial institutions. On the other hand, cyber risk represents for the insurance sector a revenue stream and a potentially huge opportunity. This peculiar situation has to tackle the same difficulties in sizing and quantifying the "cyber risk". In addition, statistical data on the financial impact of cyber-attacks are limited, making more complex the evaluation and pricing of cyber risk, in order to define adequate cyber-insurance contract. As a reference

[41] Cybersecurity Venture. Cybersecurity Market Report – Q3 2016: Available at http://cybersecurityventures.com/cybersecurity-market-report/

[42] PwC. Insurance 2020 & beyond: reaping the dividends of cyber resilience. Available at http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html

[43] EBF. The EBF blueprint for digital banking and policy change. Available at http://www.ebfdigitalbanking.eu/EBFDB_2.html

[44] Ogone. Online & mobile payments: new opportunities & threats. Available at http://www.ingenico.es/zee_uploads/all/all/gallery_gallery/3760/white-paper-online-and-mobile-payment-opportunitie.pdf

[45] ECB. Third report on card fraud. February 2014. Available at https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf

[46] Forrester Research. European Digital Banking Forecast, 2014 To 2018. Available at https://www.forrester.com/report/European+Digital+Banking+Forecast+2014+To+2018/-/E-RES115988

[47] EY. Global Commercial Banking Survey 2014. Available at http://www.ey.com/gl/en/industries/financial-services/banking---capital-markets/ey-global-commercial-banking-survey-2014

for the potential opportunity we can consider that according to PwC “Insurance 2020 & beyond: reaping the dividends of cyber resilience”[48] paper:

- Annual gross written premiums are set to increase from around $2.5 billion today to grow to $5 billion in annual premiums by 2018;
- Cyber insurance market could reach $7.5 billion by the end of the decade (2020).

The potential size of the generated cyber solutions in “Finance & Insurance” sector represents a huge opportunity to boost European economy, by overcoming the customer fear and enhancing their trust in digital means. As stated by the EC[49], the Digital Single Market could contribute Euro 415 billion per year to the European economy, with as many as 3.8 million new jobs, boosting growth, competition, investment and innovation. The cyber security can hinder or foster the development of such a Digital Single Market, paving the way to its growth and “bringing down barriers to unlock online opportunities”.

6.2.6.2.4 Why Europe

The Eurostat reports that in Europe there are 315.000.000 users that use internet every day, and the EBF highlights that 15% of European consumers bought online from other EU countries in 2014. These figures outline that there is a great opportunity for growth in Europe. Each single user accedes several marketplaces, applications and payment methods. Each single access needs cyber protection, with respect to both identity, data and privacy, and last but not least payments and account information. European citizens are particularly sensitive to cyber-security. The more people feel comfortable in leveraging the supply of digital marketplaces, the higher the trust on security features, the steadier will be the growth of the Digital Single Market.

On the supply side the introduction of new technologies, smartphones, tablets, and new security solutions make it easier and safer to leverage the opportunities of digital infrastructure combined with the trust offered by the banking industry. Digital banking is much more than home banking, is about making all the customer experience convenient, whether this is for e-commerce, or trading activities.

On the demand side, another very important consideration is the demographic evolution. At present and, even more, in the next future the demand-side will be led by generations of people that have higher education, are acquainted to use internet and English, have more and more digital devices, less borders. Millennials (Generation Y) and Digital Natives (Generation Z) are the born European citizens, their mind-set is different, the new generations have a fast and open approach to whatever offered on the market. In the next future the digital banking must be able to cope with the rapid evolution of the Digital Single Market. Studying, travelling, buying, working, trading is going to be done at least at European level, leveraging a border-less digital environment is part of daily life, therefore ensuring a safe digital banking environment is the basic requirement for the smooth growth of European economy.

[48] PwC. Insurance 2020 & beyond: reaping the dividends of cyber resilience. Available at http://www.pwc.com/gx/en/industries/financial-services/insurance/publications/insurance-2020-cyber.html

[49] EC priority Digital Single Market. Bringing down barriers to unlock online opportunities. Available at https://ec.europa.eu/priorities/digital-single-market_en

6.2.6.2.5 Scope

The implementation of Finance and Insurance cyber pilot projects should address all the specific challenges described above.

- Enhancing the resilience of the financial industry, also through Infosharing and cyber crisis simulation (war gaming)
- Reducing the systemic risk
- Fostering the understanding of cyber security and cyber risk
- Introducing Risk Measurement and risk evaluation models
- Leveraging innovative Authentication and authorization tools to foster the Digital Single Market
- Leveraging also the Cyber Trustworthy Infrastructures to stress test cyber resilience

6.2.6.2.6 Targeted Users

- Government and public administration
- Public institutions
- Private corporates
- Financial and Insurance companies
- Fintech
- European Citizens

6.2.6.2.7 Expected impact

- Increase the awareness around cyber-risks in the Financial industry
- Increase the resilience of the Financial Industry
- Increase the perception of “Single European Digital Financial Market” as Cyber Secure
- Leverage cutting edge innovative solutions to foster Data Protection, Data Integrity and Privacy
- Enlarge cyber-insurance market by easing the process of cyber insurance policy definition

6.2.6.2.8 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Several needs and solutions identified in Finance and Insurance industry are in common with other sectors.

Telecom operators, smart cities, health and e-government, do all face authentication and authorization issues, and can leverage the technical solutions that foster the data protection, data integrity and privacy. Similarly, they can all leverage cyber-safer networks and communication means.

All industries could benefit of the results of scientific research on definitions and measurement of cyber-risk, and of the implementation of a common statistical framework.

Both private and public entities can enhance the procedures to foster cooperation during crisis management, all sectors can benefit of infosharing protocols and an extended dialogue on how to cope with cyber–attacks. Every institution can experience the same benefit from prevention through education and training.

Awareness is a must for all European citizens, that will benefit of increased knowledge about the risks and the opportunities of a Single Digital Market.

6.2.6.3 Telecom, media, and content

Telecoms and digital media and content are financially important market sectors in which Europe has important players on the world stage. They are increasingly closely related:

- Telecoms and cable and satellite TV companies are offering 'quadruple play' packages bundling fixed-line and mobile telephony with internet access and broadcast/on-demand TV.
- Some telecoms operators (e.g. BT) are making their own content and distributing over their own TV channels.
- TV and other media companies are delivering content 'Over the Top' (OTT) via the Internet as well as over managed telecoms networks and satellite and terrestrial channels.
- Content is increasingly being consumed on mobile devices over cellular networks and wifi (public hotspots and private access).
- Even in the case of traditional terrestrial TV, telecoms networks are used to carry the content from the studio to the transmitter.

While the sectors are highly competitive an innovative, markets are mostly national. Reasons include national differences in regulatory and licensing regimes, the high investment required to build out new network infrastructure, and terms and conditions of media licensing.

The UK Centre for Protection of National Infrastructure (CPNI) includes Communications as one of thirteen infrastructure sectors[50] and it will be featured on similar lists of other EU member states and nations world-wide. Telecoms networks are a core component of the current and future digital infrastructure (see section on Transversal Infrastructures), and indeed most or all of the other areas of critical infrastructure depend on them. Consequently, ensuring their security and dependability is vital to the European and global economy.

The nature of the telecoms business is evolving rapidly. Most operators are moving away from dependence on low-margin connectivity products, and are moving 'up the stack', developing and selling network-based ICT services. This brings them into competition with large IT service providers and other players in adjacent sectors who are also converging on this area, as well as with agile start-ups with innovative OTT offerings.

Current situation in the telecoms sector can be summarized as follows:

- Increased usage of mobile devices
- Increased number of heterogeneous devices and different standards and protocols
- Increased requirement for reliability and security, since operation of entities depend too much on the Internet connection.
- Increased number of content and media generated.
- New legal requirements for traffic control (e.g., obligatory attack report)
- High competition
- Cross-border obstacles for collaborative protection.

[50] http://www.cpni.gov.uk/about/cni/

- Large number of available (and poorly managed) WiFi connections.

Data centre construction and transformation is boosted by the above trends. The development of smart uses generates a huge pressure on data storage. In the same time, our dependency towards a non-trusted supply chain for data storage and processing equipment rises up, causing shameful safety and security issues. Upon that, cloud services tend to replace private networks, relying on enhanced storage virtualization, load balancing and application sharing capabilities. In this context, security may no longer be ensured by physical segregation and perimeter protection. For proper management of security and privacy requirements, end-to-end data encryption is required.

Paradoxically lawful interception also needs to be enhanced, which may require appropriate improvements of traceability measures, data integrity, provenance, data forensics, including the ability to retrieve evidence over encrypted / protected storage, and mechanisms against misuse of the interception measures (including appropriate documentation).

6.2.6.3.1 Current status

Telecoms operators are amongst the more sophisticated types of company regarding cybersecurity, employing large numbers of professional staff to defend their networks and operations, and to sell this capability externally e.g. as managed security services to business and public-sector customers. Such numbers are needed because telcos are high profile, high value targets and the consequences of disrupting operations are highly visible and have widespread impact.

They are currently investing heavily in new technologies to allow the provision of new services and to reduce costs. These include:

- network virtualisation using Software Defined Network (SDN) and Network Function Virtualisation (NfV) approaches
- cloud and multi-cloud platforms
- Internet of Things and Smart ‘X’ platforms.
- 5G networking technologies

Previous and ongoing EC projects related to the Telecom sector are listed in the following table:

MUSES	Multiplatform Usable Endpoint Security
NEMESYS	Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem
A4CLOUD	Accountability For Cloud and Other Future Internet Services
5G-ENSURE	5G Enablers for Network and System Security and Resilience
ADWICE	Advanced Wireless Technologies for Clever Engineering
ANIKETOS	Secure and Trustworthy Composite Services
CYBERVOTE	An innovative cyber voting system for Internet terminals and mobile phones
D-MILS	Distributed MILS (Multiple Independent Levels of Security) for Dependable Information and Communication Infrastructures
FIRE	Facilitate Industry and Research in Europe
FI-WARE	FI-WARE: Future Internet Core Platform

LOBSTER	Large Scale Monitoring of Broadband Internet Infrastructure
MASSIF	MAnagement of Security information and events in Service InFrastructures
NESSoS	Network of Excellence on Engineering Secure Future Internet Software Services and Systems
SECURED	SECURity at the network EDge
SPaCIoS	Secure Provision and Consumption in the Internet of Services

6.2.6.3.2 What market

Internet Service Providers (ISPs) and large hosting companies are both rated in the High Likelihood for Attacks category by Radware[51]. Both can be either primary or secondary targets (i.e. targeted with the goal of impacting their customers). The other sectors in the High Likelihood category are Gaming, Government and Education.

According to the PWC Global State of Information Security Survey 2017[52]:

- The number of information security incidents detected by Entertainment, Media and Communications (EMC) respondents has steadily increased since 2014, reaching 7,674 this year-Total financial losses as a result of these incidents soared 81% in 2016.
- EMC businesses are attempting to keep up with evolving cybersecurity and privacy risks by steadily increasing their information security investments. This year, EMC companies boosted security budgets More than half (52%) of respondents say that digitization of their business is driving security spending.

6.2.6.3.3 Why Europe

Telecoms is one sector in which European companies are major players on the world stage.

Europe has a reputation to lose in both privacy protection as well as in reliable high-quality systems management. This reputation is the justification for hosting data and systems in Europe despite of relatively high labour costs.

Telecoms are a strong EU industry and leveraging Data to provide intelligent Digital Services while respecting data privacy in a way current internet players outside EU don't do will be key differentiator.

6.2.6.3.4 Scope

- Mobile security
- Run-time traffic, media and content monitoring, threat and illegal content detection and analysis.
- Timely reactions on detected threats and illegal content.

[51] Radware. Global Application & Network Security Report 2015-2016

[52] PwC. Industry findings: Entertainment, media and communications. Available at http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/entertainment-media-communications-industry.html (Last access: 22 August 2017).

- Cooperation in reducing security threats (like DDos) and illegal content (like child pornography or bomb-making videos).
- Interoperability of security
- Sharing experience and means for collaboration on security issues.
- Cross-border frameworks for collaboration.
- Physical and tamperproof protection
- Application & web-layer filtering solutions
- Identity and access management solutions adapted to virtual cloud environments
- Attack detection over encrypted traffic
- Data forensics over flash memories
- Advanced security monitoring for large data-center infrastructures
- Personal Information Management:
    - Tools to help companies protect personal information, while enabling at the same time usage of data to provide smarter digital services.
    - Analyze regulatory and internal policy impact
    - Provide visibility & control to the user

6.2.6.3.5 Targeted Users

- Security Operations staff and systems integrators in telecommunications companies, networked ICT service providers, and media and content companies;
- Providers of Managed Security Services and secure service platforms to the above, plus their supply chains.

6.2.6.3.6 Expected impact

- Reliable telecommunication services
- Economic efficiency
- Blocking attacks in the middle and at their initial point (e.g., spam sending).
- Less illegal content and media available on-line.
- Run-time control over the traffic.
- Cooperation of telecommunication providers on security issues.
- Higher protection for clients of telecommunication providers.

6.2.6.3.7 For the verticals: identify what are the specific needs / solutions and what are the needs / solutions in common with other verticals (re-applicability)

Some topics are common with the existing Public Services/eGoverment etc. subtopic:

- Data protection, privacy and data integrity and sharing tools and techniques
- Protection of real local and public administration systems
- Privacy metrics, economic value of data, combining data sources without breaking privacy regulations

6.2.6.4 Budget / Time / Instrument / TRL

16, 2019, IA, initial TRL: 4-5 and final TRL: 6-8

10, 2020, IA, initial TRL: 4-5 and final TRL: 6-8

7. CYBER TRANSVERSAL INFRASTRUCTURES

7.1 Overview and rationale for Collaborative Intelligence to Manage Cyber Threats and Risks

This section of the proposed work programme is concerned with providing the foundations for the operating system of the future digital Europe. As the operating system of an individual computer exposes computational, data and communication resources to applications via an API, so the future digital infrastructure will provide access to a variety of key services upon which applications, business processes, and the lives of individual citizens depend. This infrastructure is a complex entity composed of elements utilising diverse technologies and owned by different entities, including network operators, cloud service providers, national and local government agencies, end user companies and private individuals. Nevertheless, the interfaces it exposes must hide this complexity behind appropriate abstractions so that applications are not dependent on implementation details.

Because much of European business and society, including the verticals considered elsewhere in this programme, depend critically on the digital infrastructure, it must be highly resilient and trustworthy. This must be achieved despite an escalating cyber-threat that will find the digital infrastructure an enticing target, and perpetual technical innovation. Technical innovation is both a challenge and an opportunity for cybersecurity. On the side of challenges, new technologies combined in new ways, require security measures to be implemented in new ways, affect security-related assumptions made, and are also likely to possess new vulnerabilities. Furthermore, threat agents may be able to utilise the new technologies to enhance their tools and techniques. On the plus side, the same technologies may also be leveraged to enhance defences.

While it is not possible to foresee in detail the evolution of technologies utilised in the future infrastructure, there are a number of on-going trends we can expect to continue:

- Ever-more intimate and ubiquitous coupling of the physical and cyber-worlds via networked sensors and actuators embedded in the environment, worn and carried by people, and incorporated in vehicles and equipment;
- Virtualisation of computational, storage and networking resources, and even of people;
- Provision of capabilities ‘as a service’, allowing end-users to exchange capital for operational expenditure and out-source non-core activities;
- Higher bandwidth fixed and mobile access network technologies combined with greater processing capability at the edge;
- Application of Artificial Intelligence, Semantic Technology and Machine Learning techniques individually and in hybrid combinations;
- Aggregation of data and advances in the ability to analyse extremely large and heterogeneous collections of data to glean insight into a variety of phenomena;

- Various forms of distributed computing, opening possibilities for better performance, higher privacy, smarter resource consumption strategies, but also new risks;
- Cloudification of applications, ubiquitous web and cloud services for business and personal use;
- ...

These trends are not occurring in isolation but are colliding and coalescing into a chaotic mixture from which the future digital infrastructure must emerge. Our challenge is to both track and influence this process in order to ensure that the infrastructure that results is resilient to attack, accident and error, and also exposes to the developers and operators of applications the services they need to secure these applications and assure themselves of the trustworthiness of the infrastructure.

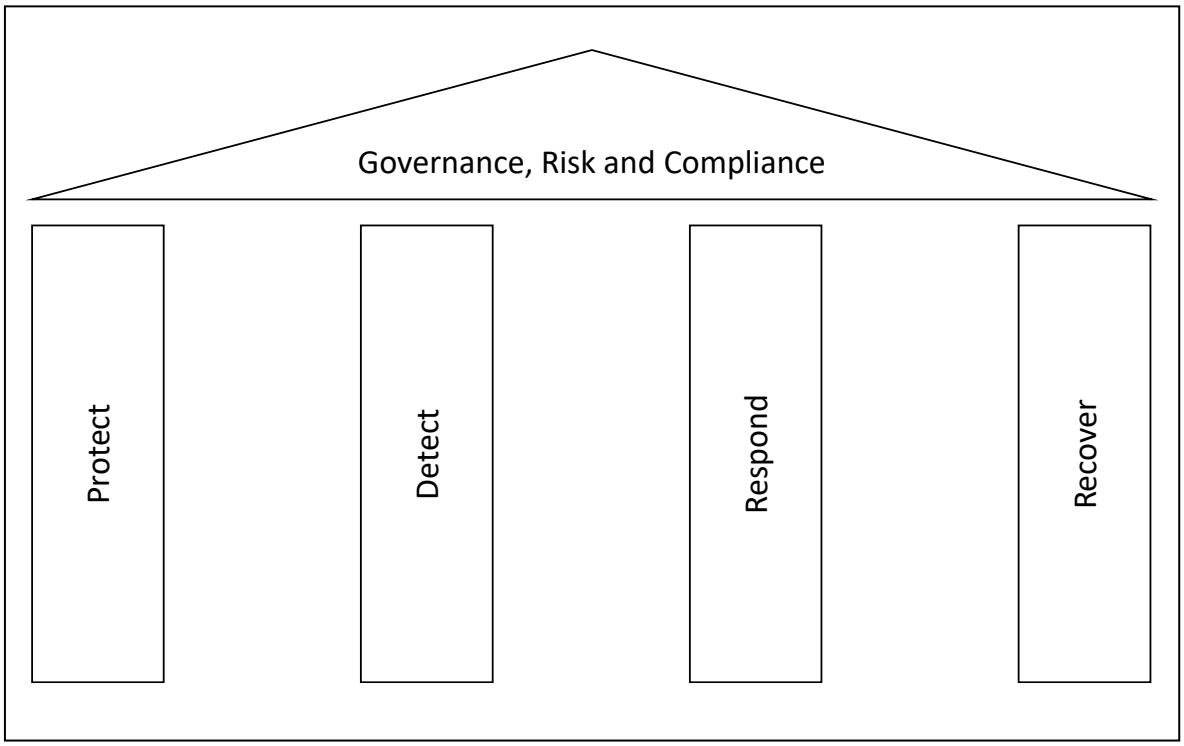

Figure 3 - The Temple of Security

There are two basic, complementary approaches to making a system more secure: the first is to harden the functional elements of the system in order to make them more resistant to attack and/or failure; the second is to incorporate additional security-specific components and processes into the system, which we may refer to as the security sub-system. The main functions of such a security sub-system are shown in**Error! Reference source not found.**:

- **Protect**: This aims to prevent attacks succeeding. It includes processes to achieve security by design, reducing attack surfaces through appropriate configuration of system elements and means of assisting the users in handling security-related tasks (e.g., credentials management tools), vulnerability scanning, penetration testing, patching, and also deployment and operation of protective/preventative controls such as firewalls, intrusion protection systems, etc.

- **Detect**: This observes the system under protection and its environment in order to anticipate, detect, diagnose and investigate retrospectively actual and potential attacks. It includes sensors and probes introduced into the system to gather observational data, and processes that analyse the information produced by these along with other sources such as miscellaneous log files and open source intelligence (including surface and deep/dark web, and virtual HUMINT – Human Intelligence – solutions) in order to provide actionable knowledge concerning the security situation of the system and its environment.
- **Respond**: This aims to take appropriate and timely action in response to detection of attacks or other suspicious activity, in order to disrupt them, mitigate their impact, investigate their origins, etc. Responses include the sharing of information with other organisations in order to prepare them for similar attacks and to co-ordinate actions. Digital forensics technologies and activities are a part of Response and also provide key contributions to Recovery operations planning.
- **Recover:** This aims to restore the system to normal operation following an attack. It may include measures to ensure that similar attacks will not be successful in future, or at least that they will have less impact.
- **Governance, Risk and Compliance (GRC):** This is concerned with overseeing and co-ordinating the above functions, making sure that the policies of the parent organisation are followed and legal obligations and commitments to various stakeholders are fulfilled, assessing overall risk exposure and ensuring that it is in line with the risk appetite of the parent organisation.

The above applies to individual elements of the digital infrastructure, the digital infrastructure as a whole, and to the applications and organisations that depend on the infrastructure. Consequently, all of the functions also need to incorporate aspects of co-operation and co-ordination, both laterally (e.g. between infrastructure service providers) and vertically (e.g. between infrastructure service providers and user organisations and national CERTs).

Organisations following current best practice will already be performing all of these functions. Similarly, security technology vendors and open source projects already have a variety of tools that support these activities. Despite this, there is still general agreement that the threat agents have the upper hand, and unless urgent action is taken, things can only get worse. Consequently, as well as adapting the implementation of these functions to new technologies, there is an urgent need for on-going enhancement of tools (both commercial and open source) and processes in order to improve effectiveness. Amongst other factors, attackers reconnoitre and probe defences until they find the single weakness they need, so defenders need to adopt an integrated, holistic view of security.

The following sections outline requirements for large scale integrated pilot projects in the areas depicted in the temple diagram:

- **GRC**: Security Assessment and Risk Management
- **PROTECT**: High-assurance prevention and protection
- **DETECT**: Information Sharing, Security Analytics, and Cyber-threat Detection
- **RESPONSE and RECOVERY**: Cyber threat management: response and recovery

Response and Recovery are addressed as a single topic as increasingly the two functions will be merged and interleaved.

The intention is that there will be one or two projects in each area, each of which results in a reference implementation of a proposed sub-platform framework, combining state-of-the-art commercial and open source tools with results of R&I projects by means of a flexible and adaptable architecture. Based on the size, quality, and complementarity of the proposals for a given topic, the evaluation committee may decide to fund a single project using all the budget, two smaller projects, or one smaller project with the remaining budget rolled over to a later call. Where two projects are funded, they should complement each other by taking alternative approaches or focusing on supporting requirements for different classes of application.

The frameworks and their reference implementations should be designed to interoperate, so that collectively they will form a platform that spans the complete security space, and satisfies the requirements of the domain-specific large scale demonstrator projects (see Section 6), with which they will need to be carefully co-ordinated. Because this approach requires active co-ordination across projects, it is proposed that a CSA be formed to provide overall management and collective decision-making.

7.2 GRC: Security Assessment and Risk Management

7.2.1 Specific challenge

Risk management is the process of identifying risks, assessing and responding to them. For this purpose, it is necessary to assess the likelihood that an incident can occur as well as its potential impact. This information can be used to define the acceptable level of risk a given organisation can tolerate and define mitigation plans. The aim is to enable risk management decisions, address threats and improve decisions by learning from previous experiences.

Security assessment and risk management must use an integrated approach taking into account people, processes and technology, as well as the interrelationships between physical and logical security, and between safety and cybersecurity. When managing risk in critical infrastructures or in cyber-physical systems, security, safety, resilience and reliability properties and requirements should be concurrently studied in an integrated manner, consolidated and reconciled. At the same time, security risk management must be aligned and interlinked with enterprise risk management.

Cost and risk constitute two relevant factors in building and operating (security-sensitive) systems. The *cost* of developing security countermeasures should be related to the value of the assets, services and data to be protected (which are often less tangible in the digital world). 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 ability to predict the current strength of the system. Thus, security metrics and corresponding risk metrics are crucial, along with required measurement methods (as are 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, services and data to be protected, and investment in security should be aligned with their value and the impact of their potential malfunctions. In this context, the residual risk could then be managed with other approaches beyond security countermeasures. Risk transfer to insurances or risk acceptance strategies may benefit from advanced decision support tools.

7.2.2 Current status

CockpitCI	Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures
RASEN	Compositional Risk Assessment and Security Testing of Networked Systems
PANOPTESEC	Dynamic Risk Approaches for Automated Cyber Defence
MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs
WISER	Wide-Impact cyber SEcurity Risk framework
CyberWiz	Cyber-Security Visualization and CAD-Tool for the Vulnerability Assessment of Critical Infrastructures
PROTECTIVE	Proactive Risk Management through Improved Cyber Situational Awareness
A4CLOUD	Accountability For Cloud and Other Future Internet Services
COCOCLOUD	Confidential and Compliant Clouds
ASSERT4SOA	Advanced Security Service cERTificate for SOA
CUMULUS	Certification infrastrUcture for MUlti-Layer cloUd Services
CYRAIL	Cybersecurity in the RAILway sector
D-MILS	Distributed MILS (Multiple Independent Levels of Security) for Dependable Information and Communication Infrastructures
EKSISTENZ	Harmonized framework allowing a sustainable and robust identity for European Citizens
ENABLE-S3	European Initiative to Enable Validation for Highly Automated Safe and Secure Systems
EURO-MILS	Secure European Virtualisation for Trustworthy Applications in Critical Domains
MUSES	Multiplatform Usable Endpoint Security
OPTET	OPerational Trustworthiness Enabling Technologies
POSECCO	Policy and Security Configuration Management
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in Research
SECCRIT	SEcure Cloud computing for CRitical infrastructure IT
SERECA	Secure Enclaves for REactive Cloud Applications
SPACIOS	Secure Provision and Consumption in the Internet of Services
SPECS	Secure Provisioning of Cloud Services based on SLA management
SSICLOPS	Scalable and Secure Infrastructures for Cloud Operations
TRESPASS	Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security
MUSA	MUlti-cloud Secure Applications
TACIT	Threat Assessment framework for Critical Infrastructures protection
EUCONCIP	European Cooperation Network on Critical Infrastructure Protection (Prevention, Preparedness and Consequence management of Terrorism and other Security-related Risks Programme). DG Home Affairs
CAMINO	Comprehensive approach to cyber roadmap coordination and development.
DARWIN	Expecting the unexpected and know how to respond

7.2.3 What market

Critical Infrastructure protection has been identified as a key market in earlier work and this is reflected in ongoing projects, and calls such as CIP-01-2016-2017. The need to extend security assessment and risk management to other verticals as digitalisation continues has become apparent in light of attacks utilising insufficiently protected connected consumer devices. Currently attacks generate mostly external costs, but regulative controls can be foreseen if the situation continues to deteriorate.

A competitive analysis of the UK cyber security sector[53] identifies risk management as the key catalyst for cyber security. It also notes that there are few software tools to support management, and that most organisations do not have capable internal teams.

General Data Protection Regulation (EU) 2016/679 includes “a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing” as one key measure for ensuring the level of security appropriate to the risk.

7.2.4 Why Europe

General Data Protection Regulation and NIS Directive will be unique driving forces in Europe in the upcoming years. Europe has taken practical approach and focused on risk management as the main tool to drive adequate protection of data. This gives European companies an environment where risk management solutions thrive naturally.

It could also be geo-strategically important to make sure that the tools come from European companies, so that entities don’t have to depend on political interests.

7.2.5 Scope

This challenge is closely related to the “Assurance/Risk Management and Security/Privacy by design” Cyber Technical Projects (sections 5.1.1 and 10.1.5.2 of the cPPP SRIA).

GRC infrastructure needs to provide an integrated security view (logical, physical, safety, resilience, juridical, organisational) holistically taking into account people, processes and technology in its analysis of potential threats and vulnerabilities, their impact and potential countermeasures in order to enable strategic oversight of the effectiveness of an organisation’s security processes. It synthesises a strategic picture using input from tactical/operation security systems and process (see Protect, Detect, and Respond and Recover), and provides an organisation’s senior management with means of assessing and improving its security posture.

No organisation is an island, and both intra- and extra-organisation dependencies need to be taken into account, not only statically, but also dynamically. Complex dynamic effects can lead to

[53] BIS/13/1231 Competitive analysis of the UK cyber security sector, A study by Pierre Audo in Consultants for the Department for Business, Innovation and Skills.

amplification and widespread propagation of the impact a security incident. For example, an interruption of electricity services due to a failure in the SCADA systems can have an impact on several industries and on society at large. Highly complex cyber systems which demand the real-time and cross-system assessment of vulnerabilities and threats require new risk management approaches, e.g. based on data analysis, including real-time analysis.

The solution also needs to facilitate inter-organisational co-operation and co-operation with supra-organisational institutions. This includes trusted sharing of information about threats, vulnerabilities and incidents, perhaps on an industry basis, to help the creation and co-ordination of preventive and corrective plans. Information sharing is mandated for operators of essential services by the directive on security of network and information systems (NIS Directive). Information sharing and co-operation also needs to take place at a tactical/operational level, and this is covered under the Detect heading.

Data based risk management approaches need to be part of the GRC solution, to achieve better preparedness through the analysis of data fed from multiple domains (infrastructure, process, operations, and observation) and multiple sources or even sectors to provide additional intelligence.

Proposed projects should incorporate state-of-the-art and beyond risk management technologies in large scale pilots involving heterogeneous cyber systems.

Projects should address:

- Risk-based situation awareness, assessment and decision support: What is the situation, and which actions should be taken? What is the human element in the risk?
    - Capability to build security metrics, linked with policies, to indicate the current security situation, and to balance alternative design approaches from the risk mitigation perspective.
    - Capability to visualise security risk as a whole, from the system-level monitoring to quantified risks, in order to support security risk management. This raises compositional security assurance challenges for complex systems
    - Strive for risk management in real-time.
    - Architecture for automatic, confidential, trusted threat, vulnerability and incident information sharing within industry cooperation groups and CSIRTs.
- Automated assessment, at design, implementation, and operation / run-time stages, including systems updates taking into account:
    - Penetration testing, security testing, model checking approaches
    - Assessment of human-related risks in combination with technology-related ones
    - Tools supporting compliance auditing
    - Adherence to applicable standards where possible
    - Link with incident response: providing context and evidence
- Cyber risk governance: safety vs security vs reliability analyses, impact analysis, insurance
    - Cyber risks as an integral part of overall organizational risks
    - The legal obligations and commitments factor in cyber risks governance
    - Compliance to regulations, customer demands, and internal policies
    - Translation mechanisms from high-level requirements to policies to configurations and settings

    - Analysis-based policies for risk acceptance levels, insurances and other ways of covering non-acceptable risks
    - Reconciling cost-efficiency with security and compliance
- Use of cyber ranges, simulation, and training:
    - Simulation of risks and evaluation of risk mitigation actions, methodologies and supporting tools
    - Widely distributable “entry-level” training material such as MOOCs, for regular users
    - Simulation-based training of users
- Certification of operators
    - Accountability and compliance, balance between transparency and privacy
    - Supporting certification of security properties for cloud and hybrid infrastructures
    - Links with ECSO WG1: standardization

7.2.6 Targeted Users

The results of this sub-programme will benefit:

- Those responsible for strategic management of cybersecurity, security risk exposure, and policy and regulatory compliance within organisations, supra-organisational bodies, etc.
- Managed-service providers offering GRC services to support the above
- European GRC technology vendors

7.2.7 Expected impact

- Security Assessment and Risk Management are closely related to the NIS Directive and their results will be helpful for the application of the Directive in the Member States.
- Data analysis based risk management should result in efficient risk management, with reduced cost and improved efficiency for organizations and governments alike (thereby benefiting the general population)
- Contribute to standardisation (WG1) an automated assessment framework for secure networks.
- Integrated holistic methodologies for combined information security, cybersecurity, safety, and reliability risk management will enable informed decisions on security-related investments at the corporate and national level.

7.2.8 Budget / Time / Instrument / TRL

1 project, 18 ME, 2018, TRL 7 or higher at the end of the project

7.3 PROTECT: High-assurance prevention and protection

7.3.1 Specific challenge

The prevention of and protection against attacks in modern ICT components, infrastructure, and systems remains a complex task. The complexity of heterogeneous collections of hardware and software components finds its roots in a diversity of individual development contexts and levels of maturity. It is compounded by growing means of networked interactions, and varied lifecycle schedules that generate highly dynamic behaviours in these systems. In addition, software components are not often designed with security in mind, as shown by recent attacks against connected devices.

This has led observers to identify the current state of software trustworthiness as a hindrance to the ongoing digital revolution. A highlighted in the Cybersecurity Strategy of the European Union:

“For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, […] almost a third of Europeans are not confident in their ability to use the internet for banking or purchases”

In order to tackle this challenge, there is a need for the design, implementation, and verification of high-assurance components, systems, and infrastructures. DARPA’s HAMCS program, for instance, has shown that high-assurance components fostered significant and measurable improvements in the security of critical systems. By showing high levels of assurance, this infrastructure will provide a technical foundation for building tomorrow’s secure ICT systems.

Furthermore, technologies used directly by the end-user (Digital Citizen) are a key security vulnerability, giving attackers access to endless potential victims, eroding trust from users in digital services and infrastructures. Attackers exploit misconfigured security settings, introduce vulnerable software into users´ systems (e.g. man-in-the-browser attacks), and exploit vulnerable software or poor security designs which in the end drive digital citizens to circumvent security measures. Solutions for these end-users require also high-assurance security that prevent tampering or make tampering clearly evident to the end-user, to expose a system as insecure whenever it indeed turns so, without hindering the user experience in their normal use of technologies.

7.3.2 Current status

SECCRIT	SEcure Cloud computing for CRitical infrastructure IT
PRACTICE	PRACTICE: Privacy-Preserving Computation in the Cloud
SWEPT	Securing Websites through malware dEtection and attack Prevention technologies
SAFURE	SAFety and secURity by design for interconnected mixed-critical cyber-physical systems
WITDOM	empoWering prIvacy and securiTy in non-trusteD envirOnMents
SUNFISH	SecUre iNFormation SHaring in federated heterogeneous private clouds
PRISMACLOUD	PRIvacy and Security MAintaining services in the CLOUD
SERECA	Secure Enclaves for REactive Cloud Applications

TAPPS	Trusted Apps for open CPS
SafeCloud	Secure and Resilient Cloud Architecture
REVEN-X1	REVEN-X1: Automatic Vulnerability Detection in Binary
ENABLE-S3	European Initiative to Enable Validation for Highly Automated Safe and Secure Systems
HDIV	HDIV: SELF-PROTECTED WEB APPLICATIONS
ProBOS	Protection Beyond Operating System - Development of the next generation cyber security solution
ABC4TRUST	Attribute-based Credentials for Trust
ARIES	reliAble euRopean Identity EcoSystem
ASPIRE	Advanced Software Protection: Integration, Research and Exploitation
CYBERVOTE	An innovative cyber voting system for Internet terminals and mobile phones
DOGANA	aDvanced sOcial enGineering And vulNerability Assesment Framework
FUTUREID	Shaping the future of electronic identity
HEAT	Homomorphic Encryption Applications and Technology
HECTOR	HARDWARE ENABLED CRYPTO AND RANDOMNESS
HINT	Holistic Approaches for Integrity of ICT-Systems
LIPVERIFY	Feasibility study on the development of LipVerify - a new viseme based user authentication service
PCAS	Personalised Centralized Authentication System
PQCRYPTO	Post-quantum cryptography for long-term security
PREEMPTIVE	PREVENTIVE METHODOLOGY AND TOOLS TO PROTECT UTILITIES
SAFECRIPTO	Secure Architectures of Future Emerging Cryptography
SCR	Disruptive Cybersecurity SaaS for SMEs and freelance developers
SECFUNET	Security for Future Networks
SECFUTUR	Design of Secure and energy-efficient embedded systems for Future internet applications
SECURED	SECURity at the network Edge
STANCE	A Source code analysis Toolbox for software security AssuraNCE
TABULA RASA	Trusted Biometrics under Spoofing Attacks
TREDISEC	Trust-aware, REliable and Distributed Information SEcurity in the Cloud
TRESCCA	TRustworthy Embedded systems for Secure Cloud Computing Applications
TAMPRES	TAMper Resistant Sensor node
DOGANA	aDvanced sOcial enGineering And vulNerability Assesment Framework

7.3.3 What market

The market for protected, high-assurance, infrastructure – regardless of the domain of application – is significant indeed. Business Insider estimates $655 billion will be spent on cybersecurity initiatives to protect PCs, mobile devices, and Internet of Things (IoT) devices between 2015 and 2020. This spending is broken down as follows: $386 billion spent on securing PCs; $172 billion spent on securing IoT devices; and $113 billion spent on securing mobile devices.

7.3.4 Why Europe

The innovation community around the prevention and protection of components, systems and infrastructure has strong European roots. A strong scientific and technical expertise has been built throughout the past programs, from FP6 and FP7 to H2020: European approaches, tools, and methods are recognized as high-efficiency worldwide, and in particular in NSF and DARPA

programs. Europe is thus in a unique position to capitalize on its strengths and drive the development of next generation of high-assurance systems.

From an impact point of view, Europe is also a strong choice both in terms of internal demand, and export opportunities. A report from TechSci Research indicates that North America and Europe are the leading cybersecurity revenue contributors. Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries.

7.3.5 Scope

Proposals should cover means to protect digital infrastructures and the applications that use them by preventing cyber-attacks on them being successful. An integrated, holistic approach should include minimisation of attack surfaces through appropriate configuration of system elements, trusted and verifiable computation systems and environments, secure runtime environments, as well as assurance, advanced verification tools and secure-by-design methods.

They should take into account the many technological (IoT; application, platform and computing and network virtualisation, service orientation, mobility, use of public, private and hybrid clouds, etc.) and business innovation trends that are converging to revolutionise the nature of digital infrastructure. Not only do these innovations change what needs to be protected, but also provide new means of implementing the protection.

Security, privacy and trust considerations should be involved from the very beginning in the design of digital infrastructure, systems and processes (i.e. security/privacy/trust by design). This could entail a whole series of activities, including social and human aspects in the engineering process until developed systems and processes address the planned security/privacy/trust properties. Proposals should also provide means to prove, through evidence, that the system is secure, specially taking into account systems of systems, whose security could depend on the security of subcomponents. The engineering process of the systems should thus take into account those security/privacy/trust/compliance requirements.

Trustworthiness also depends on a secure execution environment and systems. Proposals could cover such secure execution environments not only including the execution platforms themselves plus the operating systems, but also the mechanisms (e.g. security supporting services, control and intrusion prevention systems) that ensure an adequate level of security in the execution of all processes. Moreover, proposals should also approach this topic from a holistic point of view, where multiple execution environments interact with each other due to the delegation and distribution of tasks. If these execution environments cannot be secured, then major problems will arise. It should cover: Secure execution platforms, Operating Systems Security and Secure Integration. In this last aspect as multiple systems and paradigms will interact with each other in a distributed and dynamic environment, it is crucial to achieve a full secure integration of all of them., taking into account the integration/migration of legacy systems, whose components and protocols are not usually up to the security and privacy risks.

Proposal should also encourage the reuse of protected ground components, libraries and systems, as well as the implementation of ground security functions, like:

- Data protection, including encrypted computing technologies

- Cryptographic support, including resilient trust architectures, and the associated validation, certification, and revocation processes

Proposals could also take into account means of assisting the users in handling security-related tasks, providing users with usable information on the trustworthiness of systems and environments and including citizen science approaches to improve the quality of human sensors network for security.

7.3.6 Targeted Users

By preparing them better to resist advanced attacks and their consequences, protection capabilities will target all users of ICT and ICS infrastructure. The design of high-assurance components and infrastructure will be leveraged by:

- service and technology providers to provide additional complex functionalities without incurring the cost of designing and securing basic functionalities;
- systems integrators who can rely on protected components to establish and maintain system-wide security guarantees;
- certification authorities that will be able to use protected components and infrastructure as a “fast-track to certification”.

7.3.7 Expected impact

- Increase the trustworthiness of European ICT services and products and the competitiveness of the European industry.
- Increase trust in ICT and online services.
- Protect the European Fundamental Rights of Privacy and Data Protection.
- Establish and share a ground set of high-assurance components, libraries, and systems.
- Protect against emerging advanced threats.
- Contribute to guidelines and trusted perimeters as part of PPP WG1 – standardisation
- Integrate with results from PPP WG6 Topic: Assessment and Risk Analysis

7.3.8 Budget / Time / Instrument / TRL

1 project, 20 ME, 2018, TRL 7 or higher at the end of the project

7.4 DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection

7.4.1 Specific challenge

It is generally accepted today that protective and preventative controls make life more difficult for attackers, but cannot prevent them from breaching defences. Accordingly, organisations must act

on the assumption that attackers have penetrated their systems, and actively search for the evidence pointing to who, what, when, where and how.

Cyber threat intelligence is an advanced process that enables an organization to gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the specific threat landscape, its industry and markets. This intelligence can make a significant ability to anticipate breaches before they occur, and its ability to respond quickly, decisively and effectively to confirmed breaches. In this sense, it is important to obtain and exploit synergies between the following, apparently independent, scenarios of analysis:

1. Anticipation of nascent attacks by detection of suspicious precursor activities (ex-ante analysis) so as to enable pre-emptive action to be taken. This includes analysis of social media content on the web, and requires the ability to understand the behaviour of people (the intention and mood related to something or someone) intending to carry out cyber-attacks (behavioural algorithms);
2. Studying of best practices and retrospective analysis of incidents to extract lessons learned (ex-post analysis). Understanding how similar events has been managed in the past, and examining what has been successful and what has failed, will provide knowledge that may be used to enhance future operational actions.

SIEMs and SOCs are currently struggling with the challenge of integrating multiple sources of data, including a multitude of ICT and ICS systems on one side and diverse threat information data on the other side.

The intelligent integration and interconnection of this data is, however, crucial for successful threat detection; identification of APTs can be compared to the proverbial finding of a needle in the haystack and requires sophisticated correlation and analysis methods in order to distinguish real threats from false-positives. So, we need more intelligent and effective approaches for integrating and using the mass of data available. This includes, but is not limited to Big Data analysis methods for use both off-line and real-time.

It is essential to establish how information should be shared and which level of abstraction is effective. Information sharing and analytics interfaces allow the generated information to be used for taking or planning decisions and actions, collaborative threat intelligence and responses. Threat feeds, incident formats, reputation, and the confidentiality of the shared information should not be forgotten.

The analysis has to be done across different information sources both unstructured (textual content and multimedia) and structured ones. Unstructured sources include surface web, deep/dark web, and virtual HUMINT solutions involving access by avatar to data not directly accessible to the preceding techniques.

It must be noted that the English language and Roman alphabet are not used universally, and natural language analysis must take into account the many official and unofficial languages dialects and scripts, as well as typos and linguistic errors. Building an analysis platform that is able to operate in different languages is a significant challenge. Machine learning and in particular, Deep Learning technologies have allowed a rapid development of new language modules through “training by reading” of numerous texts. These techniques could be helpful in obtaining Cyber Security Intelligence from the Dark\Deep Web.

The sharing of security information requires necessary trust mechanisms among the entities involved in sharing their data. This research should explore the requirements for data sharing controls, trust mechanisms for data sharing, and other factors limiting the willingness to share such security data, in order for data sharing to become a reality. Establishing a common, normalised terminology and framework is important in facilitating sharing of information and reducing response and processing times, like MITRE standards (STIX,TAXI, …). Similar approaches and standardization programs in other sectors in Europe are: Swedish Initiative or Europol SIENA (under EIXM scenario) for the LEA environment, and the CISE Model for the Navy environment.

Intrusion Detection Systems (IDS) are appliances or software agents raising incidents upon detection of unauthorised programmes, protocols or activities on a supervised network or system. These incidents would generally be collected on Security Incident & Event Management (SIEM) systems for alarm correlation and filtering in an attempt to maximize detection rates and minimize false positives.

The limitations of existing intrusion detection systems are numerous. Traditional signature-based IDS would reach lower false-positive rates but typically fail to detect unknown (Zero-day) attacks, while anomaly-based detection techniques would likely generate more false-alarms but could provide higher detection rates. The IP packet is usually one of the elements in use for signature-based detection. Consequently, they can be falsified by any attacker using anonymity networks that typically provide fake IP addresses. IDS are generally unable to process encrypted packets. They fail to detect malicious encrypted payloads which tend to be more and more common. Network Intrusion Detection Systems will typically fail to detect insider-threats which would not need to pass through internet boundaries. Also the trend towards cloud-based infrastructures, mobility and IoT would limit the effectiveness of NIDS. HIDS may prove effective in those conditions but would have significant impact on the host in terms of processing power and energy consumption. Also given the prediction of exponential growth of data traffic in the future cyber-space, traditional NIDS will need to scale-up to big data, rising from an average of 1 to 10 Gbps of processing speed by 2020.

One area that is currently very active is User and Entity Behaviour Analytics (UEBA), which aims to detect anomalous behaviours and to find attackers, including insider threats. According to a 2015 Gartner study, “UEBA successfully detects malicious and abusive activity that otherwise goes unnoticed, and effectively consolidates and prioritizes security alerts sent from other systems… organizations need to develop or acquire statistical analysis and machine learning capabilities to incorporate into their security monitoring platforms or services. Rule-based detection technology alone is unable to keep pace with the increasingly complex demands of threat and breach detection.” Using Machine Learning Models, UEBA systems should ideally identify the entities (human and technological, inside and outside the organization) that are behaving suspiciously towards sensitive data, endpoints and applications.

Proposals in that subtopic would target the improvement of detection and analysis of cyber-threats at a system, network meta-system and process level based on a combination of existing and new techniques. Specific developments may target challenging environments like ICS/SCADA, mobility & cloud, IoT, virtualized networks or embedded systems where traditional IDS would meet with specific requirements that existing systems cannot yet match perfectly. The complementarity between end-point and network detection capabilities should be enhanced as well as that between deterministic and probabilistic approaches. Solutions for the above limitations should be proposed as well as countermeasures to the most successful evasion techniques like packets fragmentation,

avoiding defaults, coordinating low-bandwidth attacks, address spoofing or pattern changing. Scalability to big data should also be enabled.

7.4.2 Current status

LOBSTER	Large Scale Monitoring of Broadband Internet Infrastructure
NOAH	NoAH: a European Network of Affined Honeypots
VIS-SENSE	Visual Analytic Representation of Large Datasets for Enhancing Network Security
SAWSOC	Situation AWare Security Operations Center
SISSDEN	Secure Information Sharing Sensor Delivery event Network
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
SIEX	Semantic Information Exchange[54]
SWEPT	Securing websites through malware detection and attack prevention. Funded by CIP programme.
FORWARD	Managing Emerging Threats in ICT Infrastructures
DMASD4CA	Distributed Multi-way Analysis of Stream Data for Detection of Complex Attacks
CAPTOR	cAPTor captures Advanced System Threats
SHIELD	Securing against intruders and other threats through a NFV-enabled environment
CockpitCI	Anomaly detection. Included under GRC, but relevant here as well
ConnectProtect	A total cyber protection service to Small Businesses operating critical infrastructure and Residential customers (SIEM)
CRISALIS	CRitical Infrastructure Security AnaLysIS (vulnerability detection, IDS, attack analysis)
CYPRES	CYPRES the ICS and SCADA security companion (data analytics, IDS)
DiSIEM	Diversity Enhancements for SIEMs (SIEM, TI, visualization)
Eye-O-T	Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes (monitoring and analysis for IoT networks)
MALCODE	MALCODE: Malicious Code Detection using Emulation (malicious code detection based on emulation)
MASSIF	MAnagement of Security information and events in Service InFrastructures (SIEM)
NEMESYS	Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem (attack analysis, early warning)
PROTECTIVE	Proactive Risk Management through Improved Cyber Situational Awareness (situational awareness, security monitoring, TI sharing, alert prioritization)
SCISSOR	Security In trusted SCADA and smart-grids (security monitoring, SIEM, decision and analysis, human-machine layer)
SCOUT	Multitech SeCurity system for intercOnnected space control groUnd staTions (sensors and analysis for detecting attacks on SCGS's, restoration, reconfiguration)
SecTrap	Critical urban infrastructure and soft target cyber attack protection. Users and application Behavioural Analysis supported by artificial intelligence to preempt security cyber attacks.

[54] http://www.insiex.eu/

	(AI to detect and block abnormal program behaviour, based on Virtual Machine Behavioural Introspection)
ThreatMark	Advanced Fraud Detection System - Protecting digital transactions against cyber attacks (data analytics for detecting online and web fraud, malware, criminal and account takeover)
I-FIND	Information Finding In Non-structured Data (http://www.ifind-project.eu/)
SYPCIT	System for Prevention and Combat Identity Theft (http://www.sypcit.it/)

7.4.3 What market

According to Mandiant Consulting report[55], in 2015, the median time from penetration of a network by attackers to their discovery was 146 days. While this is an improvement on the 2014 figure of 205 days, it shows the magnitude problems faced by organisations currently. Despite the availability of numerous appliances, software components/applications, and services, it remains difficult for organisations to anticipate, detect, diagnose and investigate retrospectively actual and potential attacks.

The largest annual cost difference of cybercrime to companies pertain to detection activities[56].

7.4.4 Why Europe

There is no native European threat intelligence feed. Europe, in this respect, is fully dependant on non-European sources. In the interest of digital sovereignty, we should strive for establishing a native threat intelligence feed managed by an 'independent' European agency, and create mechanisms for distributing this information effectively among the stakeholders, especially operators of critical infrastructures as defined by the NIS Directive.

7.4.5 Scope

Proposed projects should aim to define, validate, demonstrate and exemplify an advanced, integrated cyber-threat detection and intelligence platform concept that could provide a pattern for products, managed security services and solutions throughout Europe and beyond. The platform should be able to integrate embodiments of various detective capabilities by means of a modular and flexible framework. This framework should in principle accept any component complying with the relevant API specification. Furthermore, instances of the platform should be able to interoperate, and in particular to co-operate by exchanging intelligence on threats they have encountered. Thus, European instances of the platform operated by public agencies, organisations and security service providers should collectively form a network helping to protect European society as well as improving the effectiveness of the of the individual platforms. The abstract platform should be capable of serving the needs of all industry sectors/application domains, but could admit the possibility of variants specialised to particular domains or organisation types. A

[55] M-Trends 2016, Mandiant Consulting, February 2016, https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

[56] Merrill Lynch Report, pg. 44, pg. 87, http://xxlsec.com/wp-content/uploads/2015/06/BankOfAmericaCyberReport.pdf

reference implementation of the platform should be delivered, that validates and demonstrates its ability to provide advanced performance by integrating the results of research projects with off-the-shelf open source and commercial components and services.

Capabilities in scope include the following:

- Creating a European Cyber Intelligence Network:
  - Advanced means for the detection of threats on the Internet:
  - Multi-lingual open source intelligence
  - Analysis of sources on the deep/dark web
  - Automated intelligence sharing and processing of received intelligence
  - Native European threat intelligence feed
  - Threat intelligence clearing house
  - Semantic information interchange standards
  - Creation of human-readable bulletins, alerts and dashboards
  - Advanced means for consolidation of alerts at an operational level
  - Protection of confidentiality
  - Uniform threat metrics and measurements to collect the information
- Advanced means of detecting system anomalies and integrity violations
  - User and Entity Behaviour Analytics
  - Analysis of the integrity of deployed applications
  - Detection of insider threats
  - Distributed detection
  - Ability to deal with ‘non-IT’ contexts and emerging technologies, such as Industrial Control Systems, IoT, Transportation (connected vehicles), virtualised and service-oriented systems, virtualised networks (SDN/NfV)
- Intelligent, ‘Big data’ security analytics
  - Deriving actionable insights from analysis of heterogeneous data from security appliances, log files, etc.
  - Application of machine learning techniques to heterogeneous security-related data
  - Application of graph-processing techniques on a large scale
  - Streaming security analytics
  - Distributed inline rate data analytics
  - Model-based security analytics informed by intelligence feeds
  - Accurate detection of APTs and stealthy attacks
  - Reduction of false positives and negatives through correlation of sources
  - Improved visualisation and man-machine interfaces for improved threat detection
  - Countering deception technology
  - Risk-based prioritisation of alerts
  - Time-bound security analytics, i.e. taking time constraints into account, delivering analysis in time for appropriate action to be taken
  - Collaborative security analytics taking into account confidentiality and privacy constraints on usage

7.4.6 Targeted Users

The results of this project will benefit:

- cybersecurity vendors, resulting in innovative and in-demand capabilities being embodied in new, interoperable products and services available on the market;
- managed-service providers, enabling them to integrate these products and services to provide security analytics and intelligence services to end-user organisations;
- ICT infrastructure providers enabling them to provide robust, resilient, reliable and trustworthy ICT services to end-user organisations;
- End-user organisations, enabling them to detect threats in a timely fashion.
- EU and national CERTs

7.4.7 Expected impact

Decrease in the number and impact of successful cyber-attacks as a result of high-quality, timely threat intelligence and early and accurate detection of attacks/breaches.

More effective and timely co-operation (organisation-organisation, organisation-CERT, CERT-CERT) resulting from the fast sharing of information and dissemination of threat information on a high level of quality (IOCs, MO, artefacts, ...). This topic is an enabler of the NIS Directive's implementation (information sharing and risk management are directly connected to the NIS Directive), as companies need to be able to identify incidents in a qualified way for them to be able to report these incidents in the first place

Availability to European organisations of comprehensive security analytics and threat intelligence technology and services that are appropriate for their circumstances, affordable, and able to evolve and keep pace with escalating threats and innovations in technology and practice.

A stronger and more competitive European security industry as a result of the standards/platform-based approach enabling creation of flexible best-of-breed solutions, challenging the vertically-integrated solutions of the currently-dominant vendors.

7.4.8 Budget / Time / Instrument / TRL

1 project, 20 ME, 2019, TRL 7 or higher at the end of the project

7.5 RESPONSE & RECOVERY: Cyber threat management: response and recovery

7.5.1 Specific challenge

The **Respond** security process is concerned with planning and executing, or whenever possible automatically executing, appropriate actions following the detection of a security event. Here, 'security event' covers a range of possibilities including:

- An imminent threat or the precursors to an attack;
- An attack in progress, involving a degree of penetration of the system being protected;
- An indication that the security of the system being protected has already been compromised.

The objective in this situation is normally a combination of:

- Gathering information about the attacker and his/her techniques that can be analysed and used later;
- Preventing the attack proceeding further;
- Limiting the impact of the attack.

The purpose of the **Recover** security process is to restore the system being protected to 'business as usual' status. This is not necessarily the *status quo ante*, as e.g. there is little value in restoring to the vulnerable state that enabled a compromise. Thus, the objective is normally a combination of:

- Discovering and repairing damage caused by the attackers;
- Modifying the system being protected in order to remove vulnerabilities;
- Modifying the security controls in operation to improve defence against this type of attack.

Digital Forensics and **Attack Attribution** are important associated activities that play key roles in improving security technologies, controls, and postures of attacked entities, and in legal investigation of cybercrime cases.

Challenges arise from multiple sources:

- The information on which to base decisions is often incomplete, uncertain or conflicting. In cases of partially or fully successful attacks, the attackers have good chances to modify or destroy such information.
- The defenders typically operate under time pressure, especially in the Respond process.
- It is not always easy to foresee the consequences of actions; there is a danger that a defensive or a recovery action may cause more disruption than the attack it is combatting.
- The speed at which attacks take place is accelerating, meaning more of the decision making and action needs to be automated, increasing the risk of mistakes
- There is a need for human defenders and automated controls to work in a harmonious and symbiotic partnership, as many attacks are very hard or impossible to stop or recover from without human expertise, in particular, due to the diversity of defended environments and attacker tactics and tools.
- At the same time, smaller organizations and individuals typically cannot afford expensive services of security experts, which again prompts for higher automation.
- Attacked users often lack knowledge in cybersecurity and experience in dealing with security incidents and may complicate response and recovery activities by their actions.
- High level decisions expressed in abstract terms need to be interpreted and elaborated in order to obtain low level instructions that are communicated to the ICT and Security infrastructure. A single high level decision may result in multiple instructions that need to execute in a co-ordinated fashion sent to different infrastructure elements implemented using diverse technologies.
- Attackers may modify their tactics depending on the response of defenders. Thus, the defensive responses need to be highly flexible and adaptive.
- While sharing information about attacks, their impact, security weaknesses exploited by attackers, successful and failed defensive and recovery actions, etc. is highly useful for other organizations and entities, such information is usually very sensitive and may not be

revealed, sometimes even partially. Also, diversity of security technologies and data formats may complicate information sharing.

- Log management practices are not mature. In addition, if cloud services are used for storing logs, the associated costs may demotivate organizations to keep complete logged information for a long time.
- The widespread use of SaaS / cloud-hosted applications prompts for special tools supporting remediation and impact assessment, and such tools are often missing. E.g., if attackers obtain access to an employee's Google account, they could share many confidential files from Google Drive, and there are no easy ways to discover all shared files.

7.5.2 Current status

PRECYSE	"Prevention, protection and REaction to CYber attackS to critical infrastructures"
ACDC	Advanced Cyber Defence Centre
PROTASIS	Restoring Trust in the cyber space: a Systems Security Proposal
PANOPTESEC	Dynamic Risk Approaches for Automated Cyber Defence
PROGRESS	Protection and Resilience Of Ground based infRastructures for European Space Systems
SCOUT	Multitech SeCurity system for intercOnnected space control groUnd staTions
SecTrap	Critical urban infrastructure and soft target cyber attack protection
SHIELD	Securing against intruders and other threats through a NFV-enabled environment
WISER	Wide-Impact cyber SEcurity Risk framework

One more example is SENDATE: SEcure Networking for a DATa center cloud in Europe, a large ongoing Celtic-Plus project, which has in the scope activities related to digital forensics.

We want to observe that none of the projects in the list above focused specifically on response and recovery mechanisms. In all the cases, those mechanisms were more or less essential parts of the comprehensive solutions and approaches, complementing the risk-based security management, protection, and detection functions. On the one hand, this shows that tightly connecting response and recovery with the other security functions is often a natural choice in research and innovation projects. On the other hand, this may indicate challenges related to building response and recovery functionality on the top of third-party detection and other technologies.

Given the relatively modest size of the above project list, it is fair to note the healthy assortment of the selected application domains. It includes such critical infrastructures as energy, transportation, telecommunication networks, Global Navigation Satellite Systems, and Space Control Ground Stations, as well as smaller organizations, which can employ protection technologies as services.

7.5.3 What market

Response and Recovery capabilities are required essentially for any entity targeted by cyberattacks, that is, most anyone possessing financial assets, IP assets, personal data, or sometimes just computational resources. Obvious examples are operators of critical

infrastructures, organizations in such domains as defence, law enforcement, and gaming and gambling, but also SME's and other smaller organizations with their specific constraints.

Response and Recovery are typical ingredients of managed security services, the global market size of which was USD 8.7 billion in 2015, and the forecasted compound annual growth rate of it is 12% to 15% until 2020. The increasing demand from SMBs is one of the key drivers for the growth of this market.

7.5.4 Why Europe

For European companies, compliance with the upcoming legislation, in particular, General Data Protection Regulation and NIS Directive, will help gain a competitive edge or at least avoid the legal consequences associated with noncompliance. Strategic importance of the availability of cybersecurity technologies and services from European providers is complemented by the fact that physical proximity to customers is often very helpful in delivering Response and Recovery services. In particular, although remote Incident Response activities are technically possible and certainly useful, the success of operations often depends on existing business relationships, understanding of subtle cultural aspects, etc.

Higher public awareness of cybersecurity incidents, expected to be brought by General Data Protection Regulation, will likely lead to an increased demand in defensive technologies and services from European organizations.

7.5.5 Scope

The challenges presented above are highly demanding. It is unrealistic to expect them to be solved completely in the time horizon of the Work Programme. In any case, the challenges will themselves escalate and evolve as time passes. The main objective is to validate and demonstrate an integrated security infrastructure supporting the Respond and Recover processes that are appropriate to the technical, business and threat environment that is prevalent in the year 2020. This infrastructure will consist of a reference implementation of a Respond and Recover platform integrated with state of the art tools and capabilities, including those arising from Horizon 2020 Cybersecurity and Privacy projects, but also commercial and open-source ones. Requirements will be driven in part by the analysis of the needs of application verticals and domains exemplified by Lighthouse Projects.

The Response and Recovery related items to address are:

- Combining automation with human expertise, in ways adapted to specific customer environments and requirements (e.g., various types of critical infrastructures and SME's). Capabilities to support human operators, such as IR professionals, in controlling Response and Recovery actions, including information visualization.
- Specification and support of appropriate interfaces and data formats for integration of platform components and interoperability between multiple instances of the platform operated by various entities. Link with WG1: Standardization.
- Risk- and cost- based models for Response and Recovery decisions to evaluate, prioritize, and select security countermeasures and remediation actions for complex cyberattacks;

metrics of the Return On Response Investment (RORI) type. Taking into account potential cascading effects.
- Integration and cooperation between modules implementing GRC, Protect, Detect and Response & Recovery functions. Link with WG1: Standardization.
- Utilization of and contribution to appropriate Threat Intelligence sources. Relevant information sharing within industry cooperation groups and CSIRTs. Link with WG1: Standardization.
- Response and Recovery aspects specific for such environments and emerging technologies as Industrial Control Systems, IoT, Transportation (including connected vehicles), virtualised and service-oriented systems and networks, cloud and hybrid ICT infrastructures, cloud hosted applications.
- Log management principles, tools, and practices. Utilization of logged information for Recovery activities and retrospective analysis, including forensics. Link with WG1: Standardization.
- Forensics and attack attribution for better protection against similar attacks in the future and for supporting possible investigations by Law Enforcement Agencies.
- Remote forensics capabilities for shortening incident response and recovery actions planning time. These also help avoid mistakes and accidental destruction of evidence by unprepared users.
- Measuring the platform and related Response and Recovery processes against red-team assessments.
- Guidance for the users and security personnel: security incident reporting, security incident taxonomy, symptom checklist, IR service activation checklist, etc. Link with WG1: Standardization.

7.5.6 Targeted Users

The results of this sub-programme will benefit:

- cybersecurity vendors, resulting in innovative and in-demand capabilities being embodied in new, interoperable products and services available on the market;
- managed security and incident response service providers, enabling them to integrate these products and services to provide integrated response and recovery services to end-user organisations;
- ICT infrastructure providers, enabling them to provide robust, resilient, reliable and trustworthy ICT services to end-user organisations;
- End-user organisations, enabling them to respond to threats in a timely fashion, minimise the impact of security incidents, and restore normal operation smoothly and rapidly in the wake of an attack.

7.5.7 Expected impact

In addition to the expected results of more general types, mentioned earlier in this document and relevant for activities in Response and Recovery, such as increased trust in ICT and online services, a number of more specific impact items can be listed:

According to the Ponemon 2015 Cost of Data Breach study, the average cost of a data breach for a company is $3.79 million. Better Response and Recovery technologies and services will help organizations significantly reduce the impact of breaches with various levels of success in penetrating the defences.

Novel and effective approaches and tools for Response and Recovery operations in cloud and hybrid infrastructures, which are rapidly growing in importance and popularity.

Proven and standardized (connecting also to PPP WG1 – Standardisation and certification) techniques and practices of security log management, incident reporting, cost-based Response and Recovery decision-making, and incident information sharing. These will also enable more effective and timely co-operation (organisation-organisation, organisation-CERT, CERT-CERT) in resolving incidents and higher preparedness of the users to dealing with incidents and their consequences.

In particular, the technological and operational enablers of co-operation in Response and Recovery will contribute to the development of the CSIRT Network, which is one of the key targets of the NIS Directive.

7.5.8 Budget / Time / Instrument / TRL

1 project, 20 ME, 2020, TRL 7 or higher at the end of the project

8. CYBER TECHNICAL PROJECTS

8.1 Remove trust barriers for data-driven applications and services

8.1.1 Data Security and privacy technologies

8.1.1.1 Specific challenge

- Machine Learning is starting to dominate data-intensive applications in all domains
- Value and sensitivity of data increases (“data as a currency”)
- Data-intensive applications are seen as a threat due to uncertainty of who has access to which data in which context (e.g. time, application situation)
- Operations on manipulated or biased data sets can lead to discriminating decision making (e.g. market manipulation), need to protect data as well as the algorithms operating on them.
- User data have been repeatedly abused/leaked

8.1.1.2 Current Status

Data Security and Privacy is a very wide field. It has been repeatedly funded by the European commission and has been explored by several researchers. There is hardly any current project in the area of security and privacy that does not involve data security and data protection in one way or another. What makes however this field unique is that data security and privacy is practically a moving target. The adversaries, the mechanisms and the motivations keep change, probably faster than what we can keep pace with.

8.1.1.3 What Market

We expect the market for data protection and privacy-preserving data processing to significantly grow in the future. Indeed, the recent data breaches have shown us that (i) they incur very high financial costs for the companies which suffer a breach and (ii) they undermine the trust of end users to such companies. We expect that companies will turn to solutions that ensure better data protection and better privacy for the end users.

8.1.1.4 Why Europe

Europe has traditionally been very conscious about protecting user privacy. In this aspect (i) it has developed the technical expertise to lead the area of data protection and (ii) it has developed the political will that can help push innovative solutions into the market.

8.1.1.5 Scope

- Data protection techniques – outsourced storage and processing can potentially increase the risk of exposing sensitive information to privacy & security breaches
- Anonymisation-pseudonimisation for data-intensive applications

- Privacy techniques for machine learning applications, preserving utility for data analysis, privacy / utility trade-offs.
- Meta data privacy, including query privacy
- Privacy metrics, economic value of data, combining data sources without breaking privacy regulations, differential privacy
- Privacy-preserving technologies for data intensive applications, including operations over encrypted data, property-preserving encryption, secure multi-party computation, data exchange models and analyses.
- Data distribution, fog computing
- Runtime assurance and transparency on the use of personal data User empowerment. Enabling technologies for right to access, right to be forgotten, and right to data portability

8.1.1.6 Expected impact

- Secure and privacy aware data processing and storage
- User friendly (i.e. also for non-expert users) transparency and control options incorporated as “standard features” across all storage solutions
- Balancing privacy needs and business demands
- Facilitate the implementation of the regulatory context, e.g., the GDPR

8.1.1.7 Budget / Time / Instrument / TRL

20 ME, 2020, RIA, TRL 5-6

8.1.2 Distributed Identity and Trust Management

8.1.2.1 Specific challenge

- Single trust roots may be single points of failure and may require distributed solutions
- Authentication and authorization approaches need to protect the identity and privacy of users much better than they currently do
- Existing authentication tokens and credentials frequently lead to over-identification, as they contain attributes that are not needed in the current authentication situation

8.1.2.2 Current status

Although a complete listing of all projects in the area of distributed identity and trust management is beyond this scope of this document, large-scale projects like STORK-based eIDAS-implementations using the PEPS model and projects closely aligned to these infrastructures focus on single trust roots per member state and on single interfaces between member states. Also, the credentials used in these cases are not designed to “stand on their own. These “credentials” are only references to “identity providers”, who then transfer the actual assurance information to the relying parties. Therefore a few “identity providers” and gateways between member states (often only one “identity provider” and gateway per member state) are used and are therefore informed about all transactions of the users (citizens, consumers) of the respective member states. Moreover, users cannot select attributes to be presented to relying parties without involving the “identity providers”, which consequently learn which attributes are relevant for users in which situations. This makes “identity providers” and gateways extremely attractive targets for every kind

of identity-related attacks. Effectively, such systems do not fulfil the privacy-by-design requirements of the eIDAs regulation.

FutureTrust demonstrates positive business cases for the reliance on electronic signatures, sealing services, and long-term authenticity of data and documents, all with a focus on accountability, transparency and usability.

LIGHTest creates a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions.

8.1.2.3 What market

Although it is difficult to predict the market size, the authentication/authorization market is estimated to be a multi-billion euro rapidly increasing market with a growth rate estimated at 22%

Similarly, the distributed trust management market is estimated to be in the area of several billion euros, with the Blockchain technology market to reach more than 2 billion euros by 2021.

8.1.2.4 Why Europe

Europe has successfully invested into distributed identity and trust management and enjoys a better reputation for decentralized and privacy-friendly services than several other areas. The need for distributed trust management combined with the need for privacy, puts Europe in a leading position in this area that, if properly engaged, it may lead to significant innovation in the market.

8.1.2.5 Scope

- Authentication of artefacts (code, (sensor) data, …),
- Flexible authentication and authorisation, dynamic integration of different schemes, compatibility assessment
- Interoperability and Scalability of authentication
- Distributed trust management solutions, e.g., ledgers, Block Chain, formalised characteristics of such solutions that allow the assessment of their feasibility in a specific context (Security assumptions)
- Distributed root of trust, dynamic root of trust
- Long-term aspects of solutions
- Machine-to-machine and machine-human authentication mechanisms for IoT components
- Partial identities (or identity diversification). Research is needed to build technologies that allow users to split their identities for different aspects of life

8.1.2.6 Targeted Users

All users will benefit. Customers and citizens will enjoy better protection from identity fraud. Relying parties will experience more users interested to be authenticated and authorized with the improved credentials systems, which reduces the need and cost of out-of-band-authentication. Identity service providers can make a service offering, which can be clearly distinguished from the competition of large (non-European) Internet portals and social networks offering simple authentication services that cause major privacy risks.

8.1.2.7 Expected impact

- Privacy-respecting identity management schemes
- Further steps towards interoperable, scalable identity management schemes
- Authentication operates in a distributed fashion without single points of failure on critical paths, with due consideration for the small-scale devices used in the Internet of Things
- Large adoption of distributed trust management frameworks
- 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.
- Citizens will enjoy the privileges of services needing strong authentication
- Increased trust in the cyber world
- Requirements for trusted security credential provisioning (e.g. trusted secure elements)
- More efficient on-line Business

8.1.2.8 Budget / Time / Instrument / TRL

15 ME, 2018, IA/RIA, TRL 5-6

8.1.3 User-centric Security and Privacy

8.1.3.1 Specific challenge

- People are considered the weakest link in the chain of defence: social engineering, phishing, poor choice of passwords, etc.
- Difficulties for individuals to assess the risk involved in digital activities
- Individual users lack the knowledge and don't have the right tools to understand the technology, i.e. to be able to assess and compare the security / privacy gains of different technologies and to be able configure their own security and privacy controls across applications
- Security should not become an obstacle potentially discriminating against certain people
- European companies need to protect their customers' personal information and respect the emerging data privacy regulation, while at the same time enabling their usage in smarter and more secure digital services and giving the right visibility and control to the user.

8.1.3.2 Current status

Providing user-centric solutions is very difficult. Nevertheless, there are already exist projects that deal with user-centric security solutions. Such projects include SUPERCLOUD, COURAGE, INSPECT2T, CASPER, etc.

8.1.3.3 What market

Identity protection and privacy are topics of general interest for different markets since they are transversal to several areas and can be used for digital services. Additionally, authentication is a key issue for guaranteeing security. The necessity of handling identity fragmentation is present for industry, telcos, banks, etc.

Moreover, the challenge of adapting authentication to the conditions of the environment or the critical level of the operation being performed by the user is a key issue for service providers situated in markets such as banks, retail and so on.

Besides the general interest of different markets in user-centric security and privacy, more specific cases can be mentioned. Examples of markets involved in these topics include E-Government, since they are interested in guaranteeing the privacy and security of citizen's data. In relation to that, the emerging data privacy regulations of the European Union open the challenge to handle and protect data of citizens that require different levels of privacy and security protections. Furthermore, associating virtual identities with the corresponding physical person is a major concern for E-Governments.

Additionally, the Telco, Media and content market is also interested in these topics given that they handle data from clients and users that could be used for digital services, but at the same time, they should provide adequate protection to their customers' personal information.

8.1.3.4 Why Europe

Protecting identity is a top priority for Europe, arguably more than other regions in the world. On the one hand, because identities and user data are a key business asset and, on the other hand, because user privacy is a main concern and sensitive data should be protected. Offering the technology to adequately handling and protecting identity would position Europe at the peak of innovation, besides guaranteeing citizens' rights and security – as e.g. codified in the GDPR or the Privacy-by-design provisions of the eIDAS regulation.

In fact, some of the new European laws related to this topic allow users to decide about the privacy level of their data. Therefore, it is very important to increase the awareness of individuals in relation to security and privacy in order to make these decisions correctly.

Sectors such as Industry and Telcos are key pillars of the European Economy and are increasingly interested in designing new digital services and processes that make possible to find a balance between exploiting data and user privacy.

8.1.3.5 Scope

- Risk management for individuals, families and private homes, but also small enterprises, that are basically run by individuals or whose ICT infrastructure depends very much on individuals.
- Non-technologist alerts, warnings, security configurations, anti-tracking technologies etc.
- Threat intelligence concerning the exploitation of human behaviour and human-system interaction characteristics
- User-friendly and inclusive security mechanisms, also considering people with disabilities (e.g. alternative multi-factor authentication)
- Understanding human reactions when dealing with tools, applications, incidents, warning, or alerts
- Understanding individual users' needs and proposing solutions for protecting their digital assets
- Producing easily consumable threat models and security reports
- Legal, social and economic contexts

- Multi-factor and adaptive authentication mechanisms that match the security requirements of each operation hiding the complexity to the end-users.
- Anti-tracking protection systems for more secure and privacy-conscious digital services.
- New technologies and tools to help users manage their various online identities and data e.g. identity discovery, disambiguation and management by the users themselves in cases of identity fragmentation, control personal information usage and exposure by third parties.

8.1.3.6 Targeted Users

Users that will benefit from this are twofold. On the one hand users who consume digital services, some of which don't have access to professional (e.g. corporate) ICT or ICT security support, and therefore need to organize security and privacy by themselves. And on the other hand, companies that provide such services, and are liable to European legislation.

8.1.3.7 Expected impact

- Increased awareness
- Fewer cases of identity theft
- Security and privacy as an implemented and not just claimed human right for everyone
- Best practices in authentication are supported by usable technologies embedded seamlessly into applications, including the management of different levels of authentication and dynamicity.
- New tools and technologies for both digital service providers and end users that enable user-centric security and privacy.

8.1.3.8 Budget / Time / Instrument / TRL

13, 2019, RIA, TRL 5-6

8.2 Maintain a secure and trusted ICT infrastructure in the long-term

8.2.1 ICT Infrastructure Protection

8.2.1.1 Specific challenge

The increased interconnections created within the Internet as well as between the Internet and the internal communication networks of 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 cyber security, considering the speed and scope of cyber-attacks or incidents. Furthermore, the ability to remotely compromise intelligent 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 and other cyber-attackers. Also, while many of these new devices may not be critical, some of them may have life-critical functionalities, and the integrity and availability of information flows may have an impact on our daily lives as citizens. On

the other hand, even non-critical devices pose a serious threat to the whole ecosystem if they are compromised.

In addition, the ICT infrastructure has become increasingly flexible, scalable and open. Virtualization of machines and data centers, followed by the ongoing virtualization of networks using SDN and NFV, is likely to provide users with flexibility and economy of scale. These same properties are already leveraged by attackers for hosting, command and control, and attack. New data analytics techniques will also be leveraged by attackers to find new vulnerabilities, and to better take advantage of the openness of the ICT infrastructure. It is worth noting that these very properties also make the ICT infrastructure increasingly complex to deploy and manage; this has a direct impact on our capability to deploy safe and secure ICT infrastructures, and to monitor their function to ensure that they remain safe and secure.

The following items are of particular interest in this challenge:

- The ability (i) to analyse the risk aspects of the evolving technology landscape, including migration to new and legacy ICT systems, (ii) to propose risk mitigation techniques to alleviate or prevent these risks, and (iii) to ensure that the desired level of protection is still available.
- The ability to deploy sophisticated patterns for ensuring that a deployed ICT system complies with a desired level of protection and risk management. This includes AI-powered algorithms to enable real time threat hunting that combines information coming from any security and network equipment, application log files, fixed and mobile endpoint malware solutions, user behaviour and external threat intelligence. Such algorithms, designed to be resilient to attacks designed to mislead the AI engine, should have (i) a low rate of false positives (ii) increased accuracy of advanced attacks detection, and (ii) sophisticated visualization tools for human intelligence analysts.
- The ability to deploy sophisticated trace, monitoring, and detection tools, particularly aiming at easing and supporting anomaly detection, in order to rapidly detect existing and new threats and to verify that the risk profile and the protection measures are still pertinent. This includes leveraging data analytics and visual analytics for situation awareness, technical compliance to business goals, regulatory compliance and business impact management.
- The ability to quickly and accurately react to threats, if possible with a strong degree of automation, in order to support operators with the simplest tasks and ensure that they devote their time to analysis and diagnosis in the context of highly complex layered and distributed systems, and the ability to provide business or mission impact. This includes the ability to automatically update and orchestrate security policies for focused incident response.
- The ability to take into account the extremely wide set of potential attack sources and victims, including cyber-physical environments and Internet of Things, and to provide solutions for securing and monitoring these attack sources, including strongly constrained environments.
- The ability to provide and consume threat intelligence information for more effective protection, detection, and mitigation of attacks, in the context of a rapidly changing threat and business landscape. Information about vulnerabilities is shared in specialized forums and software exploiting the vulnerabilities is sold in illegal markets using anonymized networks. This ecosystem underpins the growth of cyberattacks. Therefore, CERTs and similar organizations need to extract cyber intelligence from Dark Web, such as Darknet or Deepnet, to prevent cyberattacks. Due to the amount of information in these networks,

automated tools that fuse information from different sources, also leveraging on natural language processing capabilities are essential.
- The ability to provide more resilient environments, able through management, monitoring and mitigation to autonomously face threats and continue offering services.

8.2.1.2 Current status

There exist several projects on ICT infrastructure protection. Although a complete list is outside the scope of this work, a partial list is included below:

Projects focusing on services

- ANIKETOS (Secure and Trustworthy Composite Services) provides methods for analysing, solving, and sharing information on how new threats and vulnerabilities can be mitigated
- ASSERT4SOA (Advanced Security Service cERTificate for SOA) ASSERT4SOA produces novel techniques and tools – fully integrated within the SOA lifecycle – for expressing, assessing and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced, and running within complex and continuously evolving software ecosystems.
- DiSIEM (Diversity Enhancements for SIEMs) aims to enhance existing SIEM systems with diversity-related technology. More specifically, DiSIEM wants to (1) enhance the quality of events collected using a diverse set of sensors and novel anomaly detectors, (2) add support for collecting infrastructure-related information from open-source intelligence data available on diverse sources from the internet, (3) create new ways for visualising the information collected in the SIEM and provide high-level security metrics and models for improving security-related decision project, and (4) allow the use of multiple storage clouds for secure long-term archival of the raw events feed to the SIEM.
- HINT (Holistic Approaches for Integrity of ICT-Systems) addresses these new challenges by proposing the development of novel integrity technologies to guarantee that a system is a genuine, non-modified one including the hardware components.
- RASEN (Compositional Risk Assessment and Security Testing of Networked Systems), on the one hand developed support for systematic composition of security assessment results, allowing global security assessments to be derived from assessments of smaller parts of the system. On the other hand, RASEN developed support for systematically combining high-level security risk assessment with low-level security testing, such that risk assessment can be used to derive security test cases and security test results can be used to verify or updating the risk assessment.

Projects focusing cloud infrastructures, including all the computing, networking and data components.

- CocoCloud (Confidential and Compliant Clouds) aims at allowing the cloud users to securely and privately share their data in the cloud. This increases the trust of users in the cloud services and thus increase their widespread adoption with consequent benefits for the users and in general for digital economy.
- PRISMACLOUD (PRIvacy and Security MAintaining services in the CLOUD) yields a portfolio of novel security enabled cloud services, guaranteeing the required security for sensitive data in the cloud. A distributed multi-cloud data storage architecture shares data among several cloud providers and improves security and availability. Dynamically updating

shares by means of novel techniques avoids vendor lock-in, preserves data authenticity, facilitates long term privacy and promotes a dynamic cloud provider market.
- Tclouds (Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure) builds a resilient Future Internet platform.
- SuperCloud (USER-CENTRIC MANAGEMENT OF SECURITY AND DEPENDABILITY IN CLOUDS OF CLOUDS) proposes new security and dependability infrastructure management paradigms that are : 1) user-centric, for self-service clouds-of-clouds where customers define their own protection requirements and avoid lock-ins; and 2) self-managed, for self-protecting clouds-of-clouds that reduce administration complexity through automation.

Projects focusing on trusted networking infrastructures and virtualization, including:

- SHIELD (Securing against intruders and other threats through a NFV-enabled environment) proposes a universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks.
- SoftFIRE (Software Defined Networks and Network Function Virtualization Testbed within FIRE+) focuses on new technologies like SDN and NFV in order to create a reliable, secure, interoperable and programmable experimental network infrastructure within the FIRE+ initiative.
- SECURED (SECURity at the network Edge) proposes an innovative architecture to achieve protection from Internet threats by offloading execution of security applications into a programmable device at the edge of the network such as a home gateway or an enterprise router.

8.2.1.3 What market

According to the Working Group 3 of the NIS platform (deliverable “Business Cases and Innovation Paths”, May 2015) the cybersecurity market today faces five major challenges:

- Lack of market knowledge: There is a lack of publicly accessible market knowledge in the form of standardized market definitions, statistical information, market monitoring and trend analysis.
- Research into product transfer: Europe has many outstanding research outcomes, yet they often fail to reach the market.
- Awareness: Existing cybersecurity products do not always reach the customer
- Regulation: Each country has specific regulation and legislation toward data and privacy this impacts the pan-European service and product offering.
- Sensitivity for end-users: Citizens of Europe are particularly sensitive to cybersecurity. The impact the digital environment has on personal lives, accessibility and vulnerabilities is unique and thus the risk associated is difficult to measure and mitigate against.

According to Cybersecurity Ventures[57], the worldwide spending on cybersecurity products and services is expected to eclipse $1 trillion cumulatively for the five-year period from 2017 to 2021. In particular, they anticipate 12-15 percent year-over-year growth through 2021, by considering the cybersecurity market not only related to the core ICT infrastructure, e.g., servers, networking gear,

[57] http://cybersecurityventures.com/cybersecurity-market-report/

data centers, etc., but also to non-computer devices and non-IT centric platforms and environments — which covers entire sub-markets i.e. aviation security, automotive security, IoT security, and IIoT (Industrial Internet of Things) security, as well as the consumer side.

8.2.1.4 Why Europe

Every state has a need for asserting its sovereignty in the digital domain. With the increasing move of state-based services (identity, taxation, etc.) to ICT platforms, Europe must control the networks, systems and platforms that are hosting these services, and must be able to protect them from threats. Otherwise, the risk is high that citizens become reluctant to use these services, depriving nation states from the benefits brought by these technologies.

Furthermore, there are specific requirements of European citizens that are not well supported by other cultures. In particular, Europe has a strong focus on privacy, protecting the data of its citizens. It is extremely clear that privacy can only be supported if the entire architecture of ICT services is considered secure, safe and resilient to threats.

NFV and SDN enable the support of services for a wide portfolio of networks. In particular, 5G networks are using virtualization technologies to deal with security and scalability problems among others. Therefore, given the expected impact of the density of devices and users in the infrastructures in the next years, the virtualization of the resources in the infrastructures seems the more sustainable option. Intentional faults or attacks against these infrastructures will be more than probable and, therefore, providing native solutions to fight against cybercrime in these environments is a problem that definitively concerns Europe.

8.2.1.5 Scope

- Threat Management
    - Advanced threat analysis and intelligence, and attacker modelling (e.g., assumed ML capabilities)
    - Monitoring across all layers of complex systems, from the hardware and the network to the application
    - Threat intelligence management, including advanced threat detection and forecasting
    - Active probing, including honey tokens in applications
    - Protection against new types of malware
    - (Automated) remediation and mitigation
    - Visualisation and visual analytics, particularly for decision support
    - Extending security information and event management (SIEM) systems with predictive capabilities, big data analytics for security, association of detection and remediation/mitigation
    - Information sharing for protection, remediation, insurance claims and investigative purposes.
- Network security
    - New protocols for network management and applications
    - Security impacts of new network paradigms like NFV and SDN
    - Respecting privacy in the network protocols
    - Attribute-based encryption
    - Intrusion detection/tolerance

    - New trust models in the network infrastructures, including for critical infrastructures related to accounting, addressing, routing, naming and network management
- Protocol transition / migration to secure systems
    - Secure integration
    - Secure update “on the fly”
    - Handling of legacy systems
- Secure execution environment
    - Trustworthy hardware
    - Trustworthy containers / VMs / platforms / hypervisors
    - Hardware security, tamper protection, hybrid software-hardware security
- Device and System Security
    - Trustworthy consumer devices e.g. for protected use of the Internet (trustworthy surfing device)

8.2.1.6 Targeted Users

Expected users are:

- Citizens using government-provided services and ICT services provided by critical infrastructure operators
- Professionals, particularly SMEs with little capability to operate and maintain their own infrastructures.
- All individual users, that don’t have access to trustworthy infrastructures or professional (e.g. corporate) ICT or ICT security support, and therefore need to organize security and privacy by themselves

8.2.1.7 Expected impact

- Measurable higher security level of infrastructures
- Facilitating the broad availability and use of trusted devices
- Facilitating the easy uptake of security solutions and migration of legacy systems while securing investments
- Enabling competitive advantages for European infrastructure solutions, e.g. networks and public clouds
- Supporting the implementation of the NIS directive

8.2.1.8 Budget / Time / Instrument / TRL

13 ME, 2018 and 25 ME 2020, RIA, TRL 5-6

8.2.2 Quantum Resistant Crypto

8.2.2.1 Specific challenge

The development of quantum computers is still at an early stage, but a large-scale quantum computer able to break current standard asymmetric cryptographic algorithms in a matter of hours is expected to be available about 2025-2035. Quantum computers allow efficient computation of integer factorization and discrete logarithms. This leaves several currently widely deployed asymmetric cryptographic systems (“public key crypto”) vulnerable for attack. For symmetric

cryptography, the issue seems to be less critical but there is still a need to develop more solutions with keys of 256 bits and beyond.

Hence, secrets encrypted with present-day cryptographic techniques can be revealed with the use of large-scale quantum computers that may be constructed within the next ten to twenty years. This will have serious implications, in particular to medical data and data in classified systems related to national security. Classified information is normally declassified after 30 years, sometimes 50 years.

- The migration of current technology will be costly, time consuming and complex. There is an urgent need for a strategy to meet the challenges of quantum computing as a threat to current cryptographic systems.
- There is still a lack of standards for quantum-resistant cryptography, although ETSI is working in the area with NIST and NATO. NIST has called for proposals for new quantum-resistant standards, with a deadline in November 2017. There are also some initiatives inside the IETF (IPsec and TLS).
- National security authorities may have plans and solutions for countering the challenge of quantum computing but so far, they have not made those public; private enterprise has no clear strategy yet.

8.2.2.2 Current status

The following projects represent some of the most recent and ongoing projects related to this topic:

- PQCRYPTO: Post-quantum cryptography for long-term security (2015-2018). QCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things.
- SAFEcrypto: Secure Architectures of Future Emerging Cryptography (2015-2018) will provide a new generation of practical, robust and physically secure post-quantum cryptographic schemes based on the hardness of problems in lattices. In addition to public key agreement and digital signatures, schemes for identity based encryption (IBE) and attribute based encryption (ABE) will be developed.

8.2.2.3 What market

Currently there are close to 30 billion cryptographic devices, half of which use public key cryptography. A substantial part of this market is formed by secure ICs or SOCs, in which Europe has a leading position. One can expect that with the internet of things this will grow in the next decade to 100-200 billion devices. This presents a huge market for implementations in software and hardware as well as key management mechanisms. Cryptographic functionality is a core component for cybersecurity.

8.2.2.4 Why Europe

Europe has a unique expertise and an excellent research community in postquantum cryptography and is a worldwide leader in secure implementations of cryptographic algorithms in both hardware and software. In view of the strategic importance of cryptography, the development of these technologies is core to maintain European leadership in this area.

8.2.2.5 Scope

- Research into short-term alternatives for the migration to post-quantum cryptography, such as increased key lengths or other "drop-in" solutions
- Developing new quantum-safe crypto methods and algorithms for both asymmetric and symmetric cryptography.
- Research on the usability and efficiency of current and novel suggestions for methods for post-quantum cryptography including their integration in security protocols; as they offer present performance challenges, it is anticipated that the protocols need to be adapted to make optimal use of them.
- Transition from present-day crypto systems to quantum-resistant cryptography (or post-quantum cryptography)
- Developing evaluation criteria for quantum-resistant public key cryptographic standards and implementations.

8.2.2.6 Targeted Users

Beneficiaries are everyone using public key cryptography therefore ANYONE developing and using Internet services. The increasing deployment of encrypted protocols such as HTTPS, SNTP, secure DNS, secure SMTP and many more is a major step towards higher security on the Internet, both on infrastructure and application levels. They all depend on asymmetric cryptography. Making these protocols secure for the future protects the end users of these services, regardless whether they are private citizens, industry or public sector. Without migration plan for secure asymmetric cryptography, no Internet service will be secure in the long run.

8.2.2.7 Expected impact

- An industry well-prepared for the eventual appearance of quantum computers
- Maintaining the lasting confidentiality for classified information
- Reducing the relative "window" of unsafe cryptography as much as possible
- Standardisation towards quantum-resistant cryptography with forward secrecy
- Successful research in this field will hopefully also help government agencies in protecting sensitive/classified information, preserving national security

8.2.2.8 Budget / Time / Instrument / TRL

16, 2020, RIA, TRL 4-5

8.3 Intelligent approaches to eliminate security vulnerabilities in systems, services and applications

8.3.1 Trusted Supply Chain for Resilient Services

8.3.1.1 Specific challenge

- Increased use of 3rd party services, components, and open source material leads to complex and potentially untrustworthy and/or untrusted supply chains
- The open source approach has shown to not always lead to more secure solutions (cf. HeartBleed). Uusally only the top open source projects are properly scrutinized.
- Complex open source libraries only partially used
- No consumer control over development lifecycles, methods, or tools
- Lack of trust in the security qualities of the components used
- Cost effectiveness / Poor cost validation
- Advanced persistent threats

8.3.1.2 Current status

There are a number of EU-funded research projects that have worked or are working in solutions for Trustworthy Composite services and Trusted Supply Chains.

Project Acronym	Project title
ACTOR	ACcelerate Trust in digital life Organisation and Relations
AMASS	Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems
ANIKETOS	Secure and Trustworthy Composite Services
ASCEMA	ASCEMA: Content Aware Technology for IP Protection in Supply Chains
ASSERT4SOA	Advanced Security Service cERTificate for SOA
ATTPS	Achieving The Trust Paradigm Shift
PINCETTE	Validating Changes and Upgrades in Networked Software
SPaCIoS	Secure Provision and Consumption in the Internet of Services
STANCE	A Source code analysis Toolbox for software security AssuraNCE

When it comes to trust on consumed **Cloud Services** from third parties, there are a number of solutions developed to ensure not only the security and dependability aspects but also the data protection and privacy provisions of the Cloud Service Providers. The Data Protection, Security and Privacy in Cloud Cluster of EU-funded research projects launched by the European Commission's DG-CNECT in April 2015 was born with the aim to join forces towards increasing the impact of the clustered projects. Currently 25 projects participate in the cluster in a voluntary basis and they work in looking for synergies between the projects and analysing the technology trends and research gaps to help in the identification of future research roadmaps in Europe. Note

that it is planned that in the next months newly starting H2020 projects on Cloud security and privacy will join the cluster. More information can be found in the website of the Cluster here: https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

The current list of projects in the cluster is the following:

APPHUB, A4CLOUD, CLARUS, CLIPS, CLOUDWATCH, CLOUDWATCH2, COCO CLOUD, CREDENTIAL, ESCUDO-CLOUD, MUSA, OPERANDO, PAASWORD, PRISMACLOUD, SECCORD, SECURECLOUD, SERECA, SLALOM, SLA-READY, SPECS, STRATEGIC, SUNFISH, SWITCH, TREDISEC, TRESCCA, WITDOM

Many of these projects like SPECS, MUSA, SLALOM, SLA-READY advocate for the use of security and privacy-aware Cloud Service Level Agreements for the transparency and assurance of applied security controls in Cloud Service Providers, which increases trust in third parties' Cloud and Cloud-based services. The lack of models, mechanisms and tools for supporting dynamicity in SLAs and in compositions is one of the remaining challenges. In addition, evidence based Cloud certification is also a path just started to be explored.

Other previous projects on Cloud security and privacy are:

Project Acronym	Project title
CIRRUS	Certification, InteRnationalisation and standaRdization in cloUd Security
PRACTICE	Privacy-Preserving Computation in the Cloud
SafeCloud	Secure and Resilient Cloud Architecture
SECCRIT	SEcure Cloud computing for CRitical infrastructure IT
SSICLOPS	Scalable and Secure Infrastructures for Cloud Operations
TCLOUDS	Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure

8.3.1.3 What market

As described in ISO 25000 Portal[58], the ecosystem of software assurance and certification is composed in general by the following stakeholders:

- Organizations interested in quality evaluation, improvement and certification of their software products. Software development companies, entities that have outsourced the development of their software, or companies interested in the acquisition of a software product.
- Certification/audit body responsible for awarding software product quality certificates according to specific standards. Their role consists in auditing the organisation that develops the software product and issue a certificate specifying the quality level of the product.
- Accredited external software product quality evaluation laboratory that acts as an external entity capable of providing independent evaluation reports that the certification body can use as input to the certification process.

[58] http://iso25000.com/index.php/en/

- Third party expert consultants in software quality, that may take part previously to the certification process itself.
- Companies developing tools for software product monitoring and measurement.

8.3.1.4 Why Europe

With the advent of smart digital services in complex scenarios such as Internet of Things, Inter-cloud environments, Industry 4.0, etc. it is becoming clearer that a single company of the average size in Europe (i.e. SMEs) can hardly address the whole service supply chain by their own. Collaboration and open innovation are key for the success of our industries in the Digital Single Market. There is a clear need of joining forces and orchestrating systems and services of different nature and suppliers to create competitive added value. Achieving trust in the provisioned composite services involves ensuring and demonstrating resilience and security quality in all the supply chain pieces. This is particularly important for open source software created in open communities with blurred responsibility for its quality and security.

8.3.1.5 Scope

- Methods for developing resilient systems out of potentially insecure components
- Certification and security assurance methodologies:
    - Composition: defining security claims for composed systems and certifying the security contributions of components
    - Certification methods allowing harmonisation and mutual recognition based on evidence and not on trust
- Open source security: Identifying and assessing vulnerabilities, understanding the source code (incl. slicing, impact analysis, dependency analyses)
- Black-box security validation: model generation, automated testing, fuzzing, coverage
- Binary code security analysis: malware de-obfuscation, verification, relation to source code assessments
- Interplay between functional safety and security. Tackle degraded modes due to safety or security issues

8.3.1.6 Targeted Users

All users of third party software systems and services will benefit from solutions that enable trust in the overall product or service. As primary users of open source software, the SMEs will take the most benefit out of solutions addressing the validation and the transparency in specification of offered security controls in open source solutions.

8.3.1.7 Expected impact

- Increased trust along the supply chain
- Improved market opportunities for security component vendors
- Stimulating the market for solutions with demonstrated security qualities, e.g. certified systems (as opposed to certified components)
- Improved harmonisation of certifications

8.3.1.8 Budget / Time / Instrument / TRL

18 ME, 2020, RIA, TRL 5-6

8.3.2 Security and Privacy by Design

8.3.2.1 Specific challenge

- Software and hardware must be designed with privacy and security in mind from the beginning.
- Privacy and data protection features are ignored by traditional engineering approaches when implementing the desired functionality.
- Efficiency and automation – More sustainable spending on cyber security is needed to keep up with increasing cybercrime.
- Cost and risk considerations – providing adequate security and privacy in challenging environment.
- Eliminating vulnerabilities by specific technological solutions.
- Providing security and privacy measurements and guarantees.

8.3.2.2 Current status

The following projects represent some of the most recent and ongoing projects related to this topic:

- NESSoS (2010-2014). This Network of Excellence created a community on secure service engineering that overcome the fragmented research that have been developed until that moment. The roadmaps included in NESSoS proposed research in this line although it was not accomplished at that time and has not been done yet
- PRIPARE (2013-2015) considered only privacy-by-design but it did not accommodate it with the rest of the security or trust aspects of systems.
- SAFURE (SAFety and secURity by design for interconnected mixed-critical cyber-physical systems): 2015-2018. Not able to find any results from this project.
- One of the objectives of the NECS Marie Curie Training network on cyber security (2015-2019) is to develop trustworthy systems, although it will only pay attention to the inclusion of trust in not all the phases of the SDLC.
- CP-SETIS: Towards Cyber-Physical Systems Engineering Tools Interoperability Standardisation (2015-2017)
- DEIS: Dependability Engineering Innovation for CPS (2017-2019). The DEIS project will impact the CPS market by providing new engineering methods and tools reducing significantly development time and cost of ownership, while supporting integration and interoperability of dependability information over the product lifecycle and over the supply chain.
- HDIV: SELF-PROTECTED WEB APPLICATIONS (2015-2017). The project presents HDIV, a technology that follows a security by design approach, generating self-protected web applications.
- MODSEC: Model-based Design of Secure Cyber-Physical Systems (2013-2016). "The objective of MODESEC is to develop a design methodology that integrates security in the model-based design (MBD) process of cyber-physical systems (CPS).

- SHARCS: Secure Hardware-Software Architectures for Robust Computing Systems (2015-2017). A framework for designing, building and demonstrating secure-by-design applications and services,
- STANCE: A Source code analysis Toolbox for software security AssuraNCE (2012-2015). STANCE will define, implement and validate a set of program analysis tools capable of verifying the security of complex software systems made in C, C++ and Java.
- SWEPT proposes a security solution that incorporates different cost effective security mechanisms and tools for automatically mitigating web site attacks, maximizing the security posture of websites with a minimum intervention from web site owners and administrators.
- The main objective of the TENSOR project is to provide a powerful terrorism intelligence platform offering LEAs fast and reliable planning and prevention functionalities for the early detection of terrorist organised activities, radicalisation and recruitment.

8.3.2.3 What market

"Many companies are beginning to develop "secure-by-design" applications, starting with their most critical new applications. This best practice is already mandatory in certain industry especially those involved in embedded, industrial, technical and scientific software like defence, aerospace, energy, hi-tech and spreading to telecoms and finance."

Although it is difficult to estimate the size of security and privacy "by design" market, the global security testing market is already a multi-million euro market and is expected to grow from USD 3.31 billion in 2016 to USD 7.61 billion by 2021.

8.3.2.4 Why Europe

Europe enjoys a high reputation for Privacy and Security by Design. This reputation combined with the respective products leads to global sales opportunities. Moreover, Europe needs these services to secure its values and assets in the Internet age, as e.g. codified in the GDPR or the Privacy-by-design provisions of the eIDAS regulation.

Application, services and devices represent a key segment for Europe economy, accounting for their business volume, number of jobs created and growing trend. As such, its security represents a key asset and represents a key guarantee for the market actors and users.

Europe is already leading in technology production and manufacturing related to e.g. automotive, telecom, durables and energy. Software plays an increasingly larger role in these industries, and this software must be designed and developed to adhere to the European needs for security and privacy.

The overwhelming majority of European software developer organisations employ an agile development approach, and the discussion on whether agile development is "secure enough" is moot – instead we need to research activities, tools and mechanisms that can ensure that software developed in an agile manner has the appropriate level of software security.

8.3.2.5 Scope

- Methods and tools for developing privacy enhancing and secure software and hardware

  - Security and privacy requirements engineering, including attack and threat modelling, and risk analysis
  - Automated model-level security validation and testing (static and dynamic and their combination), exploiting the knowledge of architecture, code, and development environments (aka white box) and coverage.
  - Secure development lifecycles adopting current paradigms, e.g. agile development and DevOps.
  - Automated code-level security verification: test, runtime verification, static analyses, and their combinations. Focusing on scalable taint analysis, information-flow analysis, control-flow integrity, security policy, and protocol enforcement. Considering the relation to secure development lifecycles.
  - System-wide consistency: Connection between models, objectives, policies, and functional implementations.
  - Automated vulnerability discovery, analysis and prediction, based on large data sets (machine learning)
  - Metrics for secure and privacy-friendly development
  - Secure programming languages, HW design languages, development frameworks, secure compilation and execution
- Security and privacy architectures
  - Architectural principles providing isolation of security functions in implementations with reduced complexity
  - Isolation of sensitive information processing in hardware enforced devices. Reference architectures and their implementation guidelines, targeting cloud, IoT etc.
- Secure deployment
  - Reinforcement of complex systems
  - Container / VM security
  - Preventive security measures eliminating vulnerabilities, including runtime countermeasures

8.3.2.6 Targeted Users

The main beneficiaries for the use of these solutions are software developers and suppliers within vertical market segments, since they can incorporate privacy and security mechanisms without deep knowledge of these aspects. This will in turn benefit security consumers, who can more firmly trust the security-related capabilities of their software, and that their systems do not breach privacy requirements imposed by legislation. The final end-users will benefit from these improved, both because the software they use on their computers will be less prone to compromise and inappropriate exploitation of personal data, and because the myriad of IoT-devices that surround us will be better protected from malicious hacking.

8.3.2.7 Expected impact

- Measurable / demonstrable improved security and privacy levels and efficiency gain
- Market stimulus for secure / privacy-friendly by-design solutions
- Increased trust both by developers using the components and by end-users
- Better compliance with regulations and standards

8.3.2.8 Budget / Time / Instrument / TRL

18, 2018, RIA, TRL 5-6

8.4 From security components to security services

8.4.1 Security Services

8.4.1.1 Specific challenge

This topic focuses on the processes (and their constituent elements) required to provide, manage, measure, certify, restore, etc. privacy and security, and the tools required to support them. The target audience of such processes is 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 society at large. The cybersecurity services market is at the moment led by North American players, so acquiring a larger market share is both a significant challenge and a clear indicator of success for European security service providers.

- Smaller entities (including SMEs and individuals) need to have access to security services that allow them to exploit state-of-the-art security technology and maintain an adequate level of security relying on the expertise of service providers.
- Collaborative approach: by sharing data about security posture, threats, etc. stronger solutions can be offered to the individual entities. This information is available to MSSPs, CERTS, and large companies, but not readily available to SMEs and citizens. Sharing of threat intelligence and other relevant information is often complicated by privacy and confidentiality concerns.
- Constantly changing threat landscape, growing speed and volume of attacks, and cost-efficiency considerations make it necessary to increasingly automate key functions of cybersecurity services. A proper balance between human expertise and machine intelligence is required, however, to minimize the number of mistakes and provide timely reaction to attacks.
- It is often preferable for the customers, quality- and cost-wise, to acquire a comprehensive set of security services from the same provider, including relevant elements of GRC, protection, detection, response, forensic analysis, and recovery. This sets high requirements for the provider expertise, operational capabilities, and interoperability of the technologies and tools used.
- Continuing the previous item, standards for interfaces and data formats enabling effective interoperability between security tools and technologies are required and need to be supported by the vendors.
- Attackers are highly inventive and adaptive in pursuing their goals, which requires great flexibility and adaptiveness from cybersecurity service providers.
- Diversity of customer environments to defend, emerging technologies (such as autonomous vehicles and SDN), growing use of cloud and hybrid infrastructures complicate the task of security service providers and prompt them for risk-based approaches in managing customer security.

- Many end-users lack understanding of security threats, typical attacker goals, attack and defence tactics and tools, so they often do mistakes, fall victims of social engineering, accidentally remove important evidence, and weaken their security and security of their organizations in other ways.
- Cybersecurity services and their providers are clearly attractive attack targets, so a great care must be exercised by them not to become a security risk for their customers and partners.

8.4.1.2 Current status

While quite many projects developed tools and technologies that can be utilized in security services, the number of those, which had service aspects in the focus, is modest. Below we list some of the projects that set their main goal as producing a security service. It is interesting to observe that most of those projects belong with the “SME instrument phase 1” type.

ConnectProtect (A total cyber protection service to Small Businesses operating critical infrastructure and Residential customers), SME instrument phase 1 – The project planned to build a total cyber protection service for SMEs and residential customers. The core element is a reporting engine capable of correlating events/logs from multiple security products across multiple organisations and constantly updating each event in real-time to generate the relevant classification of potential threat. The report engine is able to generate a case for security personnel to deal with an incident in real-time and allowing the customer to view their security state via a dashboard.

PreserviX (Reshaping Digital Preservation), SME instrument phase 1. – The focus was on developing an innovative business model to bring to the market a technology for preserving valuable data for future use, protecting customers’ confidentiality and privacy, and to study the feasibility of the model as a "Managed Service".

SCR (Disruptive Cybersecurity SaaS for SMEs and freelance developers), SME instrument phase 1. – The goal is to provide vulnerability scanning of software assets as a service, focusing the efforts on the needs of developers active in the Internet of Things, where security is in its infancy.

Eye-O-T (Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes), SME instrument phase 1. – The project goal is to build a centralized diagnostic solution for the Smart Home Operators to monitor and analyse in real time a large number of IoT networks, distributed over many remote sites and running different local communication protocols. This reduces the Smart Home maintenance cost for operators and enables them to provide a service to Smart Home owners to minimise their house and privacy vulnerability to security breaches and malicious attacks.

SPECS (Secure Provisioning of Cloud Services based on SLA management), CP / FP7. – This project plans to integrate desired corporate security services (e.g., credential and access management) into Cloud services and explore approaches to develop and deploy security services that are "Cloud SLA-aware". SPECS will develop and implement an open source framework to offer Security-as-a-Service, by relying on the notion of security parameters specified in Service Level Agreements (SLA) and providing the techniques to systematically manage their lifecycle.

PROTECTIVE (Proactive Risk Management through Improved Cyber Situational Awareness), IA. – PROTECTIVE system is designed to provide solutions for public domain CSIRTs and SME’s

through improved security monitoring, increased sharing of threat intelligence between organisations within a community for CSIRT, and ranking of critical alerts based on the potential damage the attack can inflict on the threatened assets.

SISSDEN (Secure Information Sharing Sensor Delivery event Network), IA. – The goal is to provide no-cost victim notification and remediation via organizations such as National CERTs, ISPs, hosting providers and Law Enforcement Agencies such as EC3. This should especially benefit SMEs and citizens, which do not have the capability to resist threats alone. The service is based on multiple high-quality feeds of actionable security information that will be used for remediation purposes and for proactive tightening of computer defences.

The following project focused on market-related studies and perceptions for security technologies and services:

IPaCSO (Innovation Framework for Privacy and Cyber Security Market Opportunities), CSA. – The project plans to develop a structured knowledge and decision-support innovation framework for identifying, assessing and exploiting market opportunities in the privacy and cybersecurity technology space and assessing existing economic barriers to innovation. It plans to identify appropriate economic incentives needed to increase security product and service adoption. The proposed work focuses on key thematic areas within the PACs domain, for example, security concerns across different OSI layers, emerging mobile and telecoms security, security monitoring and incident response, emerging notions of privacy and identity, embedded security, and emerging managed security services models.

Securing other services was the key goal of the following projects:

ThreatMark (Advanced Fraud Detection System - Protecting digital transactions against cyber attacks), SME instrument phase 1. – The project vision is to secure the assets of people/companies by better protection of digital transaction systems against cyber-attacks and to dramatically improve the detection and protection capabilities of cyber-operators against threats, fraud, and incidents. The key features to deliver are complex preparedness, rapid detection, and faster response.

ANIKETOS (Secure and Trustworthy Composite Services), CP / FP7. – Aligns existing and develops new technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users. The plan includes methods for analysing, solving, and sharing information on how new threats and vulnerabilities can be mitigated. A platform for creating and maintaining secure and trusted composite services is the key project goal.

Finally, we will list several projects that focus on building service-enabling technologies:

SAWSOC (Situation AWare Security Operations Center), CP-FP / FP7. – Convergence of physical and logical security and technologies for running Security Operations Center (SOC) are in the plan, in particular, those for detection and diagnosis of attacks.

DOGANA (aDvanced sOcial enGineering And vulNerability Assesment Framework), IA. – A framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment", reducing the risk created by modern Social Engineering 2.0 attack techniques. Outcomes of the project are also expected to provide a solid basis to revise the insurance models for cyber-attacks related risks

AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems), ECSEL-RIA. – AMASS plans to combine techniques and tools to lower certification costs and establish holistic and reuse-oriented approach for architecture-driven assurance (fully compatible with standards), interoperability between assurance/certification and engineering activities along with third-party activities (external assessments, supplier assurance).

ASSERT4SOA (Advanced Security Service cERTificate for SOA), CP / FP7. – The project plans to develop techniques and tools – fully integrated within the SOA lifecycle – for expressing, assessing and certifying security properties for complex service-oriented applications.

8.4.1.3 What market

Essentially any entity, from individuals to large enterprises and governments, has a need of cybersecurity functions of certain types. While those needs naturally vary significantly and can be addressed with internal and external means, it is perhaps fair to claim that it is not feasible, or at least not cost-efficient, for the absolute majority of organizations and individuals to maintain an adequate level of security just by purchasing appropriate technologies and relying purely on internal operational capabilities. External security expertise and operational assistance are increasingly in high demand, which means the security services market has an excellent growth potential in the coming years, likely stronger than the security software market. According to Gartner, the security services market for enterprises was worth USD 49.6 billion in 2015, and it is expected to grow by 9.9 % annually in 2016-2019. (All expected growth rates are in constant US dollars.) Consulting and IT outsourcing are currently the largest categories of spending on information security, and until the end of 2020, the highest growth is expected to come from security testing, IT outsourcing and data loss prevention (DLP). Managed security services, the global market size of which was USD 8.7 billion in 2015, have the forecasted compound annual growth rate of 12% to 15% until 2020. The increasing demand from SMBs is one of the key drivers for the growth of this market. Managed detection and response (MDR) is emerging, with demand coming from organizations struggling to deploy, manage and use an effective combination of expertise and tools to detect threats, and then bring their environment back to a known good state. This is particularly true for targeted advanced threats and insider threats. With more MDR providers emerging targeting the midmarket, Gartner foresees these services being an additional driver for security spending for both large and smaller organizations. (http://www.gartner.com/newsroom/id/3404817)

8.4.1.4 Why Europe

For European residents and organizations, the availability of cybersecurity services from European providers is often of a high importance due to such matters as trust, requirements of laws and regulations, existing business relationships, subtle cultural aspects, etc. At the same time, given the current market trends mentioned in the previous section, success in the security services market will be a major contribution to the European economy development. To stay globally competitive, the European cybersecurity industry must aim at leading positions in delivering comprehensive services to end-customers and avoid the confines of the technology provider role. In fact, having successful European players in the global security services market will enable creation of cybersecurity ecosystems in Europe, also opening opportunities for innovative start-ups and competence development.

8.4.1.5 Scope

Projects should address technology-, process-, and business-related aspects of building and running cybersecurity services, including approaches to service quality assessment to support customers in their service and provider selection efforts. Analysis and validation of business models and service designs for individual services and viable combinations of those, depending on selected verticals and market segments, fall in the scope, in particular, for:

- Security analysis, consulting, and training
- Real-time risk assessment and management
- Security monitoring and attack detection
- Incident response, forensics, and recovery
- Threat Intelligence
- Certification and assurance
- Cyber insurance – defining coverage, brokering, offering, re-insurance

SLA models are important business ingredients of cybersecurity services, influenced by the choices of security tools and technologies, platforms for integrating those and delivering services to the customers, and expertise of the service provider's personnel.

Key issues to cover on the technical side are:

- Standards for interfaces and data formats, enabling effective interoperability between security tools and technologies
- High level of automation of the key functions of cybersecurity services, while maintaining a proper balance between human expertise and machine intelligence
- Exemplary levels of security / self-protection for cybersecurity services and their providers, as they are clearly attractive attack targets and can be used as an attack vector to compromise their customers
- Processes and methods for ensuring privacy and information confidentiality of the customers
- Selection of technically and financially efficient service delivery platforms, which may be challenging to reconcile with the two items above (e.g., in the case of cloud-based platforms)
- Information sharing platforms and processes for security service providers and their customers

Finally, we note that while (regular) personnel training is highly important for cybersecurity service providers, this is left out of the scope of this document.

8.4.1.6 Targeted Users

Everybody can benefit from security services. We expect, however, SMEs and similar small-scale organizations to benefit the most, as they often lack expertise and resources for managing their security internally. At the same time, even very large organizations can be in need of selected third-party security services, such as digital forensics or security certification.

8.4.1.7 Expected impact

A dynamic and innovative European market in cybersecurity services and a strong global market share for European security service providers are naturally the key expected outcomes, which will yield significant economic benefits for Europe and ensure reliable cybersecurity services for European organisations. Companions and prerequisites of the market success are proven designs, business models, and technological foundations of cybersecurity service provisioning, profitability of the business for providers and cost-effectiveness for customers. The efforts should also support the implementation of the NIS directive, in particular, enabling and shaping collaboration between service providers, CSIRT's, and other relevant organizations.

8.4.1.8 Budget / Time / Instrument / TRL

15 ME, 2019, IA, TRL 7

9. OVERALL BUDGET DESCRIPTION

It is estimated that for the WP 18-20 (3 years) the Commission will provide funding for calls for projects of about €380M under several strands (as the Secure Societies and the ICT – LEIT). We tried to balance among the different instruments, including the ratio between research and innovation activities, providing more relevance to the latter. In addition, in order to obey to the constraints given by the EC on the available budget per year of ~110M for 2018, ~130M for 2019 and ~140M for 2020.

Given the current trend and the significant role of innovation in the cPPP ECS, a tentative budget sharing has been developed:

- 150M of the budget will be allocated mainly to research and innovation activities (RIA)
- 228M of the budget will be allocated mainly to innovation projects (IA), in particular
  - 108M to demonstrators
  - 78M to large transversal infrastructures
  - 44M to the development of the ecosystem (mainly IA and CSA)
- 2M to the international coordination

It is reasonable to expect a stable allocation of budget to ensure that there is continuity of the programme and its supported technologies and innovations.

	2018	2019	2020	Total
Coordination	**0 M€**	**2 M€**	**0 M€**	**2 M€**
cPPP international coordination		2 M€		2 M€
Ecosystem (incl fast track to innovation budget)	**15 M€**	**17 M€**	**10 M€**	**42 M€**
Cyber range and simulation		5 M€	5 M€	10 M€
Education and training	4 M€	**3** M€		7 M€
Certification and standardization	5 M€	4 M€	1 M€	10 M€
Dedicated support to SME	6 M€	5 M€	4 M€	15 M€
Cyber security demonstrators in application domains	**26 M€**	**72 M€**	**10 M€**	**108 M€**
Energy, including smart grids	16 M€			16 M€
Transport		18 M€		18 M€
Healthcare		10 M€		10 M€
Smart & Secure Cities		13 M€		13 M€
Public/Finance/Insurance/Telco/ Services		16 M€	10 M€	26 M€
Industry 4.0	10 M€	15 M€		25 M€
Transversal infrastructures	**38 M€**	**0 M€**	**40 M€**	**78 M€**
GRC: Security Assessment and Risk Management	18 M€			18 M€
PROTECT: High-assurance prevention and protection	18 M€			18 M€

DETECT: Information Sharing, Security Analytics, and Cyber-threat Detection			20 M€	20 M€
RESPONSE & RECOVERY: Cyber threat management: response and recovery			20 M€	20 M€
Coordination of the transversal projects	2 M€			2 M€
Basic components	**28 M€**	**43 M€**	**79 M€**	**150 M€**
Removing trust barriers on data				
Data Security and Privacy			20 M€	20 M€
Identity and Distributed Trust Management	15 M€			15 M€
User-centric security and privacy		10 M€		10 M€
Maintain a secure and trusted infrastructure in the long-term				
ICT Infrastructure Protection	13 M€		25 M€	38 M€
Quantum-resistant cryptography			16 M€	16 M€
Intelligent approaches to eliminate security vulnerabilities				
Security and Privacy by Design			18 M€	18 M€
Security Assurance along the supply chain		18 M€		18 M€
From security components to security services				
Security Services		15 M€		15 M€
Total	**107 M€**	**134 M€**	**139 M€**	**380 M€**
Target imposed by Budget constraints of the Commission	110 M€	130 M€	140 M€	308 M€

APPENDIX A – MARKET ANALYSIS

Quantitative Data on the European CyberSecurity Market is not widely available as this topic is often a sensitive one, both in commercial organization, and in the Institutional/Defence/Public administration world.

- In commercial organization, very often the spending on cybersecurity is related to cyber incidents and handled at the Chief Security Office (CSO) level. CSO come often from physical security and very often have previous experiences in the intelligence / law enforcement world, usually not inclined to public disclosure of information.
- At the Institutional/Defence/Public Administration level, Cybersecurity is in itself an issue of National Interest and often bids with strategic relevance in cybersecurity are not public.

The combination of these two effects leads to a shortage of data and different study often consider limited perimeters or combine Cybersecurity with the ICT World, given that often the boundary is blurred. Given these caveats, the present chapter is ECSO WG6 elaboration based on IHS TECHNOLOGY Cyber Security - EMEA Study, 4 February 2016, one of the most recent and reputable material commercially available.

For all estimates given in this document we consider 1.1€ = 1$

Market Segments, whenever possible has been aligned to the segmentation proposed in this document but this was not possible for some sectors.

A.1 Overview and rationale

The ECSO community Estimate the total European cybersecurity market to reach almost 40 B€ in 2020, with a CAGR of nearly 10% for the period 2016¬2020.

Europe Total Market / Classification Products/Services/Consulting
Revenues (€ million)

	2016	2017	2018	2019	2020	TOTAL 16-20	% TOTAL 16-20	CAGR 16-20
Products (including Hardware&Software)	10.317	11.138	11.901	12.632	13.296	59.284	35,7%	6,5%
Services	8.573	9.441	10.332	11.206	12.033	51.585	31,1%	8,8%
Design, Consulting, Threat Intelligence	8.341	9.539	10.889	12.401	14.086	55.257	33,3%	14,0%
Total Market EU (€ million)	**27.231**	**30.119**	**33.123**	**36.239**	**39.414**	**166.126**		
Growth Rate		10,6%	10,0%	9,4%	8,8%			**9,7%**

Products market (hardware and SW) being now the leading category in term of size, will grow less than the other category with a CAGR 16-20 of 6.5% vs 8.8% for managed services and 14% for Design, Consulting, Threat intelligence.

Managed security services in Europe will growth with an 8.8% CAGR. Threat mitigation managed services hold the lion's share of these revenues (estimated around 58% in 2016, and forecast to account for 55% in 2020).

The market in cybersecurity design, consulting, and threat intelligence will grow the fastest in EMEA, with a 14% CAGR 2016-2020. Risk assessment and threat intelligence is forecast to account for the most revenues (35%) throughout the forecast period.

Considering the market grouped by application/scope area and combing product and services, it comes clear that Threat mitigation is by far the biggest area with almost 40% of the aggregated 16-20 Market even if it is growing less than the other segments.

Design and consulting (including Forensics, Vulnerability, Risk assessment, Compliance and audit are growing strong with a CAGR 16-20 of about 14%. Within the product and service Encryption is growing the fastest also due to New European Legislation.

Custom Table, Europe by Scope Revenues ($ million)								
	2016	**2017**	**2018**	**2019**	**2020**	**TOTAL 16-20**	**% TOTAL 16-20**	**CAGR 16-20**
Encryption (Product & Managed Services)	1.564	1.818	2.085	2.345	2.598	10.410	6,3%	13,5%
Authentication and Secure Access Control (Product	3.396	3.729	4.064	4.394	4.714	20.297	12,2%	8,5%
Analysis and Management (Product & Managed Ser	2.624	2.841	3.066	3.289	3.510	15.331	9,2%	7,5%
Threat Mitigation (Product & Managed Services)	11.305	12.192	13.018	13.809	14.507	64.832	39,0%	6,4%
Forensics & Incident Response	1.990	2.305	2.656	3.041	3.463	13.455	8,1%	14,9%
Vulnerability Testing & Penetration Testing	1.938	2.228	2.548	2.898	3.280	12.891	7,8%	14,1%
Risk Assessment & Threat Intelligence	2.880	3.293	3.747	4.243	4.780	18.942	11,4%	13,5%
Compliance / audit	1.534	1.714	1.939	2.220	2.563	9.970	6,0%	13,7%
Total Market EU (€ million)	**27.231**	**30.119**	**33.123**	**36.239**	**39.414**	**166.126**	**100,0%**	**9,7%**
Grow th Rate	1,1%	10,6%	10,0%	9,4%	8,8%			

In terms of vertical markets, Banking and Finance is the largest (about 23% of the total market '16-'20) followed by the Public Sector/Intelligence/Security (about 21%), Manufacturing and Utilities – Industrial Control System (about 16% and growing strong).

Healthcare comes Third, followed by Telecommunications and Automotive Sector (small but growing fast).

Cyber Security Market Size by Vertical Market Revenues (€ million)								
	2016	**2017**	**2018**	**2019**	**2020**	**TOTAL 16-20**	**% TOTAL 16-20**	**CAGR 16-20**
Public Sector/Intelligence/Security	5.846	6.467	7.103	7.746	8.387	35.550	21,4%	9,4%
Automotive	738	821	908	1.002	1.101	4.571	2,8%	10,5%
Finance and insurance	6.344	7.017	7.715	8.438	9.175	38.690	23,3%	9,7%
Healthcare	3.209	3.543	3.890	4.252	4.616	19.510	11,7%	9,5%
Manufacturing & Utilities - ICS	4.180	4.686	5.241	5.850	6.498	26.455	15,9%	11,7%
Telecommunications	2.030	2.235	2.445	2.658	2.875	12.243	7,4%	9,1%
Others	4.884	5.350	5.820	6.292	6.762	29.108	17,5%	8,5%
Total revenues ($ million)	**29.954**	**33.131**	**36.435**	**39.863**	**43.356**	**166.126**	**100,0%**	**9,7%**
Grow th Rate	11,2%	10,6%	10,0%	9,4%	8,8%			

In the following an overview of the trends, major threats and needs of major vertical markets.

A.2 Public Sector/Intelligence/Security

A.2.1 Definition

This sector includes Government and commercial industry complex working for it, including design, production, delivery, and maintenance of government/intelligence/ military/security systems, subsystems, and components or parts. Part of this sector is outside the scope of the CPPP (Defence, for example) but has to be treated as a whole for market analysis purposes. This sector does not include healthcare to be treated separately.

A.2.2 Context

The market of Public Sector cybersecurity (i.e. securing the IT systems of Public Administration is intertwined with the growing importance of cyber capabilities in geopolitical competition and the use of cyber capabilities to collect sensitive information and face attack on critical infra-structure.

This is made clear by the fact that in most countries cybersecurity is treated at the National level involving several stakeholders like the Ministry of Defence, Interior and the public procurement entities.

The approach of National States is still in its infancy with little understanding of how the possession of offensive cyber capabilities will affect national competition and what kind of protocols and rules must be developed to regulate the use of national cyber capabilities and to what ends these capabilities can be employed.

Threat mitigation and Consulting services represented the majority of this market but Encryption, Forensics and incident response are growing faster. Overall this market is and will remain the largest in the 2016-2020 period even if it its growth is slightly slower (9,4%) than the market average (9,7%).

This sector is involved mainly in

- Protecting the security of ICT systems for Local and Central Public Administration
- Protecting the security and providing cyber defence capabilities to Strategic Segment of the public administration (Prime Minister, Parliament, Defence, Interior, Foreign Office, Secret Services, Police forces)
- Co-ordinate and guarantee situational awareness regarding the security of critical infrastructures.

Main issues in this sector are not only technical but also related to procedures and coordination

- Integrate stakeholders (both private and public), manage joint ventures and public-private collaborations
- Build on extensive experience in integrating several parties and handling complex projects
- Understand conventional projects regarding intelligence/defence and integrate them with cybersecurity
- Promoting Awareness and defining Cyber Security Guidelines/Schemas (e.g. UK Cyber Essentials Scheme)

There is a considerable number of initiatives in policy development, research, regional cooperation and strategic funding decisions overseas involving international organization like ENISA, NATO, EDA as well as the establishment of national cyber emergency response teams. At the private level there has been considerable movement of industry into the global cyber market with the establishment of overseas centres of excellence and acquisitions of specialized cyber security companies.

This market is becoming highly dual with traditional Public Administration Contractor competing with civil players coming mainly from the cyber security Sector.

A.3 Automotive

A.3.1 Definition

This sector includes companies and activities involved in the manufacture of motor vehicles, including most components, engines and bodies, connected car technology, auto infotainment, driver assist technologies and mobile devices used in the car. The sector does not Include tires, batteries, and fuel industries.

A.3.2 Context

Most of the medium term future in this industry is related to the connected car. However, as the connected car industry is still embryonic, the majority of the revenues refer to the revenues coming for the automotive industry as a specific manufacturing sector not included in other sector.

Growth in the EMEA region in the connected car cybersecurity will begin after 2018, however, the Europe auto industry has not moved yet massively on the protection of the connected car. Market estimate value that in 2015, 30% of the cars sold worldwide will be connected, while this percentage will rise up to 74% in 2022, while the first limited self-driving (in specific protect environment) will be available in 2018 and the first full self-driving or human driving cars in 2025.

Correspondingly, in the 2016-2020 timeframe market size will not be huge, even if it will exhibit a strong growth (CAGR 16-20 10.5%). Nor it will be possible to stage a real world pilot in 2018 as this pilot should involve cars, road infrastructures, integration standard not yet completely defined.

From the technology point of view, and from the social impact and life-related cybersecurity induced risks this sector will be one of the more relevant.

The connected car industry with vehicles incorporating technologies like cloud computing, wireless and GPS, radars, laser scanners, on-board computers that control most cars functions will face many risks pertaining software complexity and cybersecurity.

Cybersecurity threat will become real in the next decade and built-in security solutions will be required, including hardware-based security features, central software solution and secure exchange of data for vehicle 2 vehicle and vehicle 2 infrastructure communication.

A.4 Manufacturing & Utilities - ICS

A.4.1 Definition

This sector includes a) production, treatment, and distribution of gas, electricity, water, and sewage; b) companies involved in the production of goods; c) critical infrastructure in general assets, systems, and networks, whether physical or virtual, so vital to society that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

A.4.2 Context

This Sector is the third largest one, behind the Defence/Intelligence/Government and the Finance /Insurance. Given the Huge Scale of the infrastructure to protect and the fact that this sector is just starting to tackle the cybersecurity protection of Industrial Infrastructure, it is not surprisingly the sector with highest CAGR 16-20 at 11.7%. Main areas of growth include Encryption and Threat mitigation products managed services.

Cybersecurity concerns in these markets revolves mainly around

1. Protection of intellectual property. Industrial-scale theft of intellectual property has been a growing concern and has strained international relations. This problem becomes even more important in companies relying on a distributed supply chain.
2. Threat of cyberattacks to industrial targets especially in the oil and gas, chemicals and power industries, energy systems, water. that can lead to loss of life and impact on national economic security, national public health or safety.

Within this context the undergoing adoption of an Information and communication layer interacting with the physical production and distribution infrastructure (usually described under the umbrella-definition of IOT and Industry 4.0) will dramatically increase the attack surface.

In terms of number of breaches and cybersecurity awareness and countermeasures this sector is years behind the traditional ICT world and bears the new risk of massive physical consequences cyberattacks.

Many security vendors have started exploratory research on the types of solutions they could provide for ICS environments, but solving the security problem for control systems requires a deep understanding of the individual devices from a wide range of control system vendors (including Siemens, Honeywell, Emerson, Rockwell and ABB). Most of these vendors use proprietary communication protocols and have vulnerabilities that are unique to their individual devices.

So this sector is characterized by

- huge technology infrastructure already in place, a world that evolved for decades without ever being exposed to the level of threats and technical exploitation common in the internet
- Most of the technology employed by this sector has a lot in common with traditional ICT infrastructure, sharing concepts (computing, networking, data communication) but has also specific technologies and standard. Given this, most of the infrastructure is not vulnerable to most automated attacks and malware common on the internet, but the use of hacking technique adapted to industrial automation architecture is possible and increasingly happens.
- A global trend by automation vendors to increasingly adopt devices, standards and COST software coming from the ICT world is constantly increasing the vulnerabilities

Most network security vendors have not spent time in the industrial environments that house control systems, or with the device vendors, so they are starting almost from scratch. The emergence of the concept of IoT (Internet of Things) as a new way to frame our understanding of interconnected machines with no human interface sharing data has increased discussion around security connected devices of all types.

The total market is also extremely immature, with almost 200 vendors vying in the market and offering a variety of hardware, software, and services. Growth of the market for cybersecurity in this category over the next few years is forecast to be solid and steady.

Main topic to be addressed in this area include

1. Develop specific vulnerability and penetration testing techniques by applying hacking practices developed on the internet to the ICS world (including devices, processes and including human factors)
2. Start a widespread evaluation of device specific vulnerability and develop attack databases applying hacking techniques developed on the internet to real world cases, developing vulnerability assessment and penetration testing techniques.
3. Based on this assessment develop specific technologies to fill gaps in all security aspects, also retrofitting existing solutions (es: data encryption layer)
4. Build testing platforms the control system vendors can use to test their own products for vulnerabilities as a basis for future certification activities

As lifecycle of industrial systems is usually MUCH longer than that common in the ICT landscape a main topic is the development of technology to secure the high number of legacy systems.

A.5 Finance and Insurance

A.5.1 Definition

This sector includes financial services B2B and B2C: banks, investment funds, stock exchanges, real estate and bureaux de change, all types of insurers, such as property and casualty insurers, life insurance companies, full-line insurers and insurance brokers. Depending on its mandate, insurance enterprises may also hold international insurers, or may be restricted to domestic insurance companies only. Market data include both the cyber insurance market and the insurance companies spending on cybersecurity.

A.5.2 Context

Banks and Insurance represent together the largest market (bank ~23% of the cumulated 2016-2020 market estimate). Banks alone experience three times as many security incidents as other sectors.

- Most attacks are directed at stealing money
- Banks and insurance maintain an enormous database of customer data, including credit card information, email addresses, financial state
- Banks increasingly rely on internet and mobile technology to deliver services valued by the customer, but doing so they increasingly rely on infrastructures and technologies behind their reach
- Banks and insurance face a complex security environment as they must defend themselves and their customers from cyber-attacks comply evolving regulations an at the same time compete on the market with fast changing business requirements, speed to market pressures, expansion into new markets.

- Cyber Insurance Market are in its infancy, UK being the leading market. modelling of cyber risk has been difficult due to a lack of available data; however, there are alternative approaches to valuing the risk of cyber-attacks including using stress testing
- Main risk involved in the insurance sector is the confidentiality and privacy of the increasing amount of data/big data collected by insurers to develop more personalized products and tailored risk evaluation.

Common cybersecurity problems in banks and insurance include

- Online web banking breach, distributed denial-of-service attacks, payment card skimmers in ATM and POS.
- Malware and Trojan to steal credentials
- Social engineering (vishing and phishing) mainly to customer and to a lesser extent to employees directly.
- Botnets complemented with automation kits to scale and reduce cost of attacks.
- Intellectual property loss - trade secrets, trading algorithms,
- Personal risk profile for customers with private data such as health record

Given the scale of the risk, the number of attacks, the number of years of experience in defending their assets and the fact that essentially the ICT system, differently from other sectors are not support systems but the production engine of modern banking and insurance, this sector is at the forefront of securing Information Systems, networks and Internet/Mobile access. Insurance is a less attractive target and correspondingly the level of readiness is usually lower.

Main areas of interest are

- Mobile Security (area with largest forecasted growth, as security measures in this area are lagging behind)
- Security awareness and incident handling
- System to detect and respond to attacks
- Threat intelligence with integration of activities at bank sector level, national and international level, as the Finance and Insurance industry is highly globalized
- Pre-emptive activities to manage and study malware families most commonly used and prepare detection and reaction systems in advance or able to respond to variants; advanced decision support
- Advanced Authentication techniques to reduce reliance on username and passwords and increase convenience for customers

A.6 Healthcare

A.6.1 Definition

This sector includes all forms of healthcare companies and organizations, including: hospitals, clinics, hospital management firms, biotechnology medical products such as: medical devices & healthcare IT.

A.6.2 Context

The health sector that is handling sensitive personal information and is increasingly relying on ICT infrastructure, is an easy target for hackers. Analysts estimate that a individual health record are traded in the black market at a premium regarding to financial records and credit card numbers. IHS estimate that almost $2 billion worth of health-related records was sold on the black market last year, with growth over 20% per year. The threat is conducted both by external and Internal attackers. Stolen records may give way to litigation.

Healthcare is still relatively new to “digitalisation” in comparison to other market verticals, with the vast majority of large-scale investment and legislation occurring in the last decade. These investments are effectively creating large pool of data and increasingly network connection with little attention to cybersecurity.

The threat is escalating due to the growing importance of individual health record, that has to be shared among several stakeholders (patient, doctors, hospitals, laboratories, pharmacies service providers and manufacturers) and may include a whole range of data including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats like age and weight, and billing information as well as personal characteristics, including face photo and possibly handwriting or other biometric data. This information can be extensively exploited, for example for social engineering breaches. This information has a longer lifespan compared to other easily stolen data (like credit card).

The sector has responded strengthening policies and privileges administration, defining Compliance requirements but in the end essentially focusing more on regulatory compliance than on security. This focus on compliance reveals the main aim of protecting from litigation more than the willingness to really protect patient’s data.

This is caused by the fact that patients choose their health care provider based on proximity and medical competence; there is a limited supply of such providers in a given area and major security breaches have proved to have little to no effect on the revenue stream of the organizations, there is no economic incentive to invest in digital security.

Consequently, the cybersecurity market regarding the Health sector even if sizeable one (about 11.7% considering the period 2016-2020) grows at a rate very close to the global average (9,75) and is estimated to be less than 3% of the ICT investment from the Health Sector.

Threat Mitigation are estimated to make up around 43% of this market in 2016 but with decreasing relevance; Forensics & incident response, vulnerability testing & penetration testing and risk assessment & threat intelligence are showing the biggest growth. The product component is over 40% of the total.

The market in Europe form cybersecurity services to the health sector is still fragmented with no clear leader.

Main areas of interest include

- Encryption, especially focusing on reducing to the minimum needed the amount of time that data spends in unencrypted form during the lifecycle

- Authentication, secure privileged access control based need to know strategies is the second key component that involve technology and appropriate management to keep user records and privileges up to date.
- Early detection of breaches, containment, & response is another priority with more emphasis on behavioural analytics of internal users
- Medical device manufacturers, almost always designed without considering cyber security requirements, must be assessed to identify possible security gaps and vulnerabilities, considering not only the risk of data theft but also the risk of malfunction due to cyberattacks (consider the risk with Insulin pumps, heart monitors, x-ray…), with attack surface growing with connections and more direct access through the Internet
- Privacy and audit issues and ability of citizen to be aware of who owns that record and how to determine access rights to such data

A.7 Telecommunication (including IoT)

A.7.1 Definition

This sector includes all organisations involved in the interconnected industry using terrestrial, satellite, and wireless transmission systems, Mobile devices and networks, mobile media, operators, cellular M2M, the Internet of Things (IoT), low power wireless, mobile handsets, smartphones/mobile broadband, and wireless systems.

A.7.2 Context

The ***sector is highly interconnected:*** satellite, wireless, and wireline providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability. This sector serves extensively business as well as end users.

Telecommunication companies are a target for cyber-attacks mainly for two reasons:

- Get access to data stored or transmitted
- Disrupt connectivity with corresponding interruption of the supported businesses or consumer
- Use the telecommunication and ICT infrastructure as a mean to conduct cyber attack against other organizations.

The context is getting more complex as a consequence of several trends:

- very often in the last decade, telecom operators have expanded the role becoming providers pay TV and cloud operators.
- Mobile phone and connected devices (e.g. camera) are getting more and more complicated being essentially full-fledged computers. This increase of complexity and attack surface will accelerate with the impact of M2M communication and IoT.
- The move towards an All -IP- LTE core will bring with it new security threats, and the coming 5G will continue this trend exposing directly the core network to new attacks.

On the plus side Telecom operators are generally ICT savvy and has started protecting their networks since many years, despite this, being the fabric that connects all the systems, networks remain vulnerable, especially to attacks that may include advanced persistent treats (APTs).

Because of this, Telecom operators are focusing on

- Threat detection and intelligence capable solutions
- Mobile security and mobile device management strategies
- Enhanced protection of the carrier network and core network using sophisticated end-to-end authentication and encryption

Nevertheless, as in the finance sector the Telecommunication Sector is one of the most mature with cybersecurity Markets at 7.4% of the total and projected to increase with a CAGR of 9.1% (2016-2020), slower than the market average.

Again, threat mitigation makes up the highest proportion of revenues (roughly 40%) in 2015 but growing slower than other services like vulnerability, penetration testing, risk assessment, threat intelligence. Revenues from consulting services (combined) are projected to nearly double.

A.8 OTHER

A.8.1 Definition

Includes all other companies, not listed before, such as those involved in education, entertainment and leisure, distribution, gaming and casinos, retail, services (including professional services like law firms, representation firms, and call centers) and transportation.

Given the large variation in threats and scenario, no detailed analysis will be presented.

A.8.2 Countries considered in the provided market data

Austria, Belgium, Denmark, Finland, France, Germany, Greece, Eire, Italy, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, United Kingdom, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Russia, Slovakia, Slovenia, Turkey, Ukraine

A.8.3 Product/Service Taxonomy

Cybersecurity products are products devoted to the protection of computers, networks and data

- Hardware Appliances including pre-installed operating systems and applications
- Software
- Software solutions delivered in cloud with a subscription model
- Virtual appliance: system image equivalent to a hardware appliance

Managed Security Services

These are professional services devoted to deliver security solutions to companies. These can be delivered remotely (e.g. Remote SOC services, cloud security), Onsite at customer's premises, or in a hybrid way

Consulting Services

- Forensics and incident response,
- Vulnerability testing and penetration testing
- Authentication and secure access control,
- Risk assessment and threat intelligence
- Compliance and audit.

APPENDIX B – LIST OF CONTRIBUTORS

This document has been prepared by the ECSO WG6 (also with other WGs contributions) as input to H2020 WP 18-20. The document has been prepared starting from ECSO cPPP SRIA v1.0 and industry proposals as well as through discussions the 3 meetings of WG6 (sept. 12, sept. 14 an nov. 3).

The list of contributors (possibly incomplete) is given below (~150):

ECSO WG6 SRIA chairs

Fabio Cocurullo (Leonardo), Volkmar Lotz (SAP), Fabio Martinelli (CNR)

ECSO SWG6.1 Ecosystem chairs

Herve Debar (IMT), Javier Lopez (UMA), Veronique Pevtschin (Engeneering)

ECSO SWGS6.2 Vertical Application Domains chairs

Alia Fourati (EDF), Mari Kert (Guardtime)

ECSO SWG6.3 Transversal Infrastructures chairs

Ana Ayerbe (Tecnalia), Paul Kearney (BT)

ECSO SWG6.4 Basic Technologies chairs

Florent Kirchner (CEA), Evangelos Markatos (FORTH), Per Hakon Meland (Sintef)

Contributors

Adam Kozakiewicz (NASK Institute)	Kai Martius (SECUNET)
Adrien Bécue (Airbus DS CyberSecurity)	Kai Rannenberg (Goethe-Universität Frankfurt)
Ahto Buldas (TUT)	Kalev Pihl (SK – AS Sertifitseerimiskeskus)
Aimo Pellinen (JAMK)	Kaur Virunurm (RIA)
Albert Brignoli (Vitrociset)	Kevin Jones (Airbus Group)
Alessandro Zanasi (Zanasi & Partners)	Kim Davis (Research Council of Norway)
Alexey Kirichenko (F-Secure)	Klaudia Tani (EOS)
Alia Fourati (EDF)	Lanfranco Marasso (Engineering)
Ana Ayerbe (TECNALIA)	Laurent Manteau (Gemalto)
Anatonio Skarmeta (University of Murcia)	Leonardo Aniello (CINI)
Andrew Boyce (DCMS UK – Department for Culture	Leonardo Querzoni (CINI)
Andrzej Szyszko (Ministry of Digital Affairs – Poland)	Loic Mougeolle (DCNS)
Anthony Der Krikorian (Gemalto)	Lorenzo Pupillo (Telecom Italia)

Antonio Pellicia (IBM)	Luigi Rebuffi (ECSO)
Artsiom Yautsiukhin (CNR)	Maarten Bodlaender (Philips)
Axel Legay (Conseil Regional de Bretagne)	Magdalina Nazare (Digital Catapult)
Axel Paschmann (NXP)	Maite Alvarez (Tecnalia)
Barbara Carminati (CINI)	Manel Medina (APWG)
Bart Preneel (KU Leuven – iMinds)	Manuel Urueña (Universidad Carlos III de Madrid - UC3M)
Bengt Sahlin (Ericsson)	Marcos Alvarez-Diaz (Gradiant)
Bian Yang (NTNU CCIS)	Marcus Voelp (University of Luxemburg)
Carlos Prieto-Saiz (SGS Group)	Mari Kert (Guardtime)
Christian Derler (JOANNEUM RESEARCH)	Maria Adele Di Comite (Intesa Sanpaolo)
Claire Vishik (Intel)	Marina Soledad Egea Gonzalez (Indra)
Constantinos Tsiourtos (CNTI)	Mark Miller (Conceptivity)
Cristina de la Maza (Innovalia)	Martin Borett (IBM)
Daniel Medianero (S21SEC)	Martin Ruubel (Guardtime)
Daniela Coutinho (S21SEC)	Martin Stierle (AIT)
Daniela Fernandes Coutinho (S21SEC)	Mathias Dehm (Continental Automotive)
Daniela Previtali (WIBU-SYSTEMS AG)	Maurizio Mencarini (ExpertSystem)
Daniele Frasca (Deloitte)	Micehl Kostucki (Safran Identity & Security)
David Francis (Huawei)	Michael Montag (Nokia)
David Gonzalez (IK4 Research Alliance)	Michal Choras (University of Science and Technology, Poland)
Didier Bourse (Nokia Bell Labs France)	Mikel Uriarte Itzazelaia (Nextel S.A.)
Dieter Weiss (Giesecke & Devrient)	Mirko Panev (TüV Süd Management Service)
Dirk Stegemann (Bosch)	Natalia Vicente (ETNO)
Emmanuel Dotaro (Thales)	Nicolas Sendrier (INRIA)
Ene Visnev (Estonian MoD)	Nikolaos Tsouroulas (Telefonica)
Enrico Frumento (CEFRIEL)	Nina Olesen (ECSO)
Erkuden Rios (Tecnalia)	Olivier Bettan (Thales)
Evangelos Markatos (FORTH)	Øyvind Ytrehus (Simula@UiB)
Fabio Cocurullo (Leonardo)	Pablo Dago (Gradiant)
Fabio Martinelli (CNR)	Paolo Campegiani (AEI Ciberseguridad)
Florent Kirchner (CEA)	Paolo Lombardi (TRUST-IT Services)
Francesca Giampaolo (Engineering)	Pascal Bisson (Thales)
François Charbonneau (Altran)	Patricia Campi (aizoON)
Géraud Canet (CEA)	Paul Kearney (BT)
Gertrudis Camps (AEI Ciberseguridad)	Paul Oudshoorn (Accenture)
Gianluca Sensidoni (Expert System)	Paulo Verissimo (University of Luxemburg)

Giorgio Cusmà (Intesa Sanpaolo)	Per Håkon Meland (Sintef)
Giorgio Giacinto (CINI)	Peter Grebac (National Security Authority)
Gustavo Scotti Di Uccio (Vitrociset)	Peter Rost (Rohde & Schwarz Cybersecurity)
Hervé Debar (IMT)	Philippe Wolf (IRT Systems X)
Izabela Albrycht (KI)	Pia Olli (VTT)
Jacques Kruse Bandao (NXP)	Pieter Van Der Honing (UL)
Jani Ekqvist (Turku University of Applied Sciences)	Pietro Di Maio (Exprivia)
Janine Dobelmann (NXP)	Rainer Koch (ETNO)
Janne Jarvinen (F-Secure)	Reijo Savola (VTT)
Janusz Pieczerak (Orange)	Riccardo Masucci (Intel)
Javier Añorga Benito (CEIT- IK4 Research Alliance)	Richard Goodall (Airbus Group)
Javier Lopez (University of Malaga)	Rita Forsi (Ministry of Economic Development Italy)
Joanna Swiatkowska (KI)	Roberto Cascella (ECSO)
Jorge Cuellar (Siemens)	Rodrigue Germany (Systematic Paris-Region)
Jorge Lopez Hernandez-Ardieta (Indra)	Sebastiano Toffaletti (Digital SME)
José Aleman Hernandez (S21SEC)	Siegfried Müller (Teletrust)
José María Legido Riba (GMV)	Stefan Beyer (S2 Grupo)
Jose Ruiz (Atos)	Stefan Van Baelen (iMinds)
Josef Haid (Infineon)	Thomas Jensen (INRIA)
José-Maria De Fuentes (Renic)	Thomas Stubbings (RadarServices Smart IT)
Juan Arraiza Irujo (IK4 Research Alliance)	Ulrich Seldeslachts (LSEC)
Juan Caballero (IMDEA Software Institute)	Véronique Pevtschin (Engineering)
Juan Díez (INCIBE)	Victor Bouissou (DCNS)
Juan Gonzalez Martinez (Gradiant)	Vincent Roca (Inria)
Juan Tapiador (RENIC)	Volkmar Lotz (SAP)
Juha S. Knuuttila (Turku University of Applied Sciences)	Walter Matta (Vitrociset)
Julio Vivero Millor (GMV)	Xavier Letizia (Engineering)

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

10, RUE MONTOYER - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE: WWW.ECS-ORG.EU - TWITTER: ECSO_EU