Priorities for EU research

Analysis of the ECSO Strategic Research and Innovation Agenda (SRIA)

DECEMBER 2017

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use opsec@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA 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

© European Union Agency for Network and Information Security (ENISA), 2017
Reproduction is authorised provided the source is acknowledged.

Table of Contents

Executive Summary

The Digital Agenda[1] proposes to better exploit the potential of ICT technologies in order to foster innovation, economic growth and progress with the objective to develop a Digital Single Market to generate smart, sustainable and inclusive growth in Europe. Cyber security is an essential enabling factor for the development and exploitation of digital technologies and innovation and is, therefore, linked to future prospects for growth, job creation and Europe's response to environmental and societal goals. To facilitate the EU's ambition, Horizon 2020, the biggest ever EU research and innovation programme is under way to foster R&D and innovation across Europe.

As part of the H2020 programme, the EC signed a contractual private-public partnership (cPPP) with the European Cyber Security Organisation (ECSO), an industry-led contractual counterpart in July 2016. The aim of the partnership is to bridge the gap between capacity building and the deployment of trusted European cybersecurity solutions on European and international markets. The cPPP can be regarded as a key element of the master plan in structuring and coordinating cyber security industrial resources in Europe. As part of the contractual obligations, the ECSO drafted a Strategic Research and Innovation Agenda (SRIA) that identifies seven priority areas of R&D in the field of cyber security, each of them broken down to headings that analyse the given priority in detail, making suggestions for potential topics for calls for proposals in the framework of H2020. (Annex II outlines the priority areas.)

From another aspect, Europe has also an opportunity to put policies in place to ensure that minimum security requirements are put in place in digital products and services to ensure safety and security of the European citizens and their data. There are two concurrent EU legislations, the General Data Protection Regulation[2] (GDPR) and the NIS Directive, [3]that will have an ultimate impact on the next generation of goods and services in the cyber domain in Europe and beyond. Both legislations are enablers of the Digital Single Market, and with this, Europe should capitalise on the state-of-the-art cyber security to give Europe a competitive advantage.

The objective of this current document is to provide an analysis of the research proposals of the ECSO SRIA document by briefly summarizing each research priority, and highlighting the areas where the priorities have to be aligned with the provisions of the GDPR and the NIS Directive. The document endeavours to identify the most research intensive vertical domains and transversal infrastructure, and match these with the most relevant areas of cyber security research. The document also places the European cyber security environment in the global context, and identifies the inhibiting factors of European leadership in the market.

[1] https://europa.eu/european-union/file/1497/download_en?token=KzfSz-CR&usg=AOvVaw3RadlBjrZ19TcVzB4VsXOc
[2] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf&usg=AOvVaw36C2K-6DsRW98BUZ3iYgI5
[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

1. Introduction and background to the ECSO SRIA

1.1 Objectives

The objective of the current report is to provide an analysis of the areas and priorities identified by the European Cyber Security organization `Security research & innovation agenda` [4]report. The document also looks into the alignment of the priority areas with global cyber security trends and current EU legislation.

The background to the Security Research and Innovation Agenda report is the European Commission's contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union and the stakeholder organisation represented by the European Cyber Security Organisation (ECSO)[5] association.

The following sections introduce the cybersecurity specific legislative environment of the EU that impact the future research activities and the available funding schemes that foster R&D activities in the EU.

1.2 The EC approach to cyber security

The current approach to CIIP and resilience within the EU has its roots in the Commission communication of 2009, entitled 'Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience[6] . In 2013, the Commission released the Cybersecurity Strategy of the EU[7] , which laid down a number of fundamental principles underlying the EU approach to cybersecurity, including the need of achieving cyber resilience, strong and effective legislation on the cyber domain, the promotion of a Single Market for cyber security products, and fostering R&D investments and innovation.

The key challenges and priorities of the EU Cybersecurity Strategy are each addressed by separate but coherent actions and legislations detailed below.

1.3 Digital Agenda

The Digital Agenda (2010-2020) proposes to better exploit the potential of info-communication technologies (ICTs) in order to foster innovation, economic growth and progress.

The Digital Agenda's main objective is to develop a Digital Single Market (DSM)[8] in order to generate smart, sustainable and inclusive growth in Europe, and it consists of the seven pillars below:

- Achieving the digital single market
- Enhancing interoperability and standards
- Strengthening online trust and security
- Promoting fast and reliable Internet access for all
- Investing in research and innovation
- Promoting digital literacy, skills and inclusion

[4] http://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf
[5] http://ecso-org.eu/
[6] Commission Communication of March 2009, "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009)149.
[7] Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[8] https://ec.europa.eu/digital-single-market/en

- ICT-enabled benefits for EU society

1.4 The GDPR and the NIS Directive

This document takes two concurrent pieces of EU legislations into consideration, namely the General Data Protection Regulation (GDPR) and the NIS Directive. Both pieces of legislation are enablers of the DMS, having an ultimate impact on the next generation of goods, services, and content and cooperation models in the cyber domain in Europe and beyond. The NIS Directive is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the EU. By imposing a certain number of obligations for all Member States, the Directive will help ensure a consistent approach to cybersecurity. This in itself represents a very significant step in the approach to securing EU information systems and improving the functioning of the internal market.

The GDPR is designed to control the processing of personal data. Its rules are in the form of a Regulation, imposing data protection standards that will be the same in all 28 EU Member States. Enforcement will be the responsibility of each Member State, but the GDPR also encourages centralised co-ordination of enforcement across the EU. The GDPR focuses on the protection and processing of personal data, and does not address the critical infrastructures.

The GDPR and the NIS Directive are complimentary initiatives with the shared goal of modernizing and harmonizing system and data protection frameworks across the EU. The GDPR will give EU citizens stronger rights, empowering them with better control of their data and ensuring that their privacy remains protected in the digital age. The NIS Directive is complementary to the GDPR, aimed at the protection of IT systems in critical national infrastructure for the EU. Table 1 provides a brief comparison of the two legislations:

	GDPR	NIS DIRECTIVE
Primary Goals	Regulation to achieve a general EU framework for data protection Directive on protecting personal data processed for prevention, detection, investigation or prosecution of criminal offenses and related judicial activities	Improve cyber security capabilities in the Member States Improve Member States' cooperation on cyber security Directive concerning measures to ensure a standard high level of network and information security across the EU
Organizations Impacted	Data controllers and data processors Essentially any organization with 'Personal Data'	Operators of essential services in the energy, transport, banking and healthcare sectors Providers of critical digital services like search engines and cloud computing
Enforcement	Data breaches must be reported as soon as possible and, where feasible, no later than 72 hours after discovery of a breach. Regulation will apply to companies headquartered outside of Europe as long as they have operations in Europe. Data Transfers to third countries and international organizations may only be carried out in full compliance with this Regulation Requires Data Protection Officer	Requires operators of essential services in the energy, transport, banking and healthcare sectors, and providers of critical digital services like search engines and cloud computing, to take appropriate security measures and report incidents to the national authorities Member States will be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as CSIRTs responsible for handling incidents and risks

Penalties	Maximum penalties for data breaches are now 4% of global revenue or 20M Euro, whichever is higher	Penalties and fines yet to be clearly defined
Effective Date	May 25, 2018	The NIS Directive was published in the Official Journal of the European Union on July 19, 2016. Member States have until May 9, 2018 to implement this Directive into national laws and a further six months to identify "operators of essential services."

Table 1 A brief comparison of the GDPR and the NIS Directive

1.5 eIDAS[9]

Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market. The eIDAS Regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. It also creates a European internal market for eTS - namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication - by ensuring that they will work across borders and have the same legal status as traditional paper based processes. With eIDAS, the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access services and do transactions online and across border in just "one click". In terms of relevance to this document, the eIDAS Regulation bears several overlapping provisions with the GDPR and the NIS Directive in setting a secure environment for eID and eTS. Privacy-by-design and data breach notification are appearing in the GDPR, while security requirements of trust service providers, compliment the aims of the NIS Directive in building resilient infrastructures and services. The intent of eIDAS is to drive innovation. By adhering to the guidelines set for technology under eIDAS, organizations are pushed towards using higher levels of information security and innovation.[10]

[9] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, adopted on 23 July 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[10] more details on the topic: https://www.enisa.europa.eu/topics/trust-services?tab=publications

1.6 R&D activities and funding schemes

As a key priority to foster R&D and innovation across Europe, a structure of research facilities and funding schemes is in place to provide expertise and management to research and innovation projects and to promote synergies between these activities, to benefit economic growth and EU citizens. The beneficiaries of the funding programmes include SMEs, research centres, universities, large companies, the types of funds range from supporting start-ups to various clusters.

The Connecting Europe Facility (CEF) is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level. It supports the development of high performing, sustainable and efficiently interconnected trans-European networks in the fields of transport, energy and digital services. CEF investments aim to fill the missing links in Europe's main infrastructural backbone. The Innovation and Networks Executive Agency (INEA) is responsible for the technical and financial management of the programme.

Horizon 2020 is the biggest running EU research and innovation programme. Almost €79 billion of funding is available over seven years (2014 to 2020). H2020 will help to achieve smart, sustainable and inclusive economic growth. The goal is to ensure that Europe produces world-class science and technology, removes barriers to innovation and makes it easier for the public and private sectors to work together in delivering solutions to big challenges facing our society. In the course of implementing the programme, H2020 will build on the experience of public private partnerships. The programme objectives are coordinated by various European bodies and agencies.

Funding schemes by EC General Directorates: The European Commission makes direct financial contributions in the form of grants to projects or organisations which help implement EU programmes or policies. Amongst others, DG CONNECT[11], DG JUSTICE[12], DG Migration and Home Affairs[13] run various funding programmes in the field of cyber security.

1.7 The European Cyber Security Organization (ECSO)[14]

The European Cyber Security Organisation (ECSO) ASBL is a not-for-profit organisation under Belgian law, established in June 2016. ECSO represents an industry-led 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 such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and associations as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries. The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity, and in particular to:

- Foster and protect the growth of the European Digital Single Market from cyber threats;
- Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position;

[11] Digital Single Market-related topics and projects, https://ec.europa.eu/digital-single-market/en/funding
[12] Rights, Equality and Citizenship Programme 2014-2020, http://ec.europa.eu/justice/grants1/programmes-2014-2020/rec/index_en.htm
[13] Security programmes, https://ec.europa.eu/home-affairs/financing/fundings_en
[14] http://ecs-org.eu/about

- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader[15].

As part of the EU cybersecurity strategy, the European Commission and the ECSO signed a contractual private-public partnership (cPPP)[16] on 5 July 2016. The aim of the partnership is to foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European ICT products and services. The cPPP can be regarded as a master plan in structuring and coordinating digital security industrial resources in Europe. It includes a wide range of actors, from innovative SMEs to producers of components and equipment, critical infrastructure operators and research institutes, brought together under the umbrella of ECSO.

1.7.1 Security research and innovation agenda (Working group 6)

Within ECSO there are 6 working groups dealing with different topics:

- WG1: Standardisation, certification, labelling and supply chain management
- WG2: Market deployment, investments and international collaboration
- WG3: Sectoral demand
- WG4: Support to SMEs , coordination with countries (in particular East and Central EU) and regions
- WG5: Education, awareness, training, exercises
- WG6: Strategic Research and Innovation Agenda (SRIA)

Relevant to this paper is the working group 6, Strategic Research and Innovation Agenda (SRIA). The objectives of this group are:

- Coordination of results and expectations from European Commission and R&I projects
- Coordination of cybersecurity activities across cPPPs and EU Initiatives
- Support cPPP implementation and H2020 cybersecurity projects
- Detailed suggestions for the Work Programme 2017-2020 using an updated and focused SRIA

1.8 ECSO – Security research and innovation agenda (SRIA WG 6)

1.8.1 Structure of the SRIA working group 6 publication[17]

There are seven priority areas identified in the Security Research and Innovation agenda, each of them broken down to headings that analyse the given priority in detail. The technical projects are ment to deliver basic capabilities (building blocks), on top of which both large cyber infrastructures (cross domains) and domain specific pilots can be leveraged. The general structure of each heading includes a discussion of the specific challenge and a description of the current status, including previous and ongoing projects in the fields. The market specifics and their European relevance are also detailed, and the scope of research & innovation is suggested at each heading, followed by the anticipated targeted users and the expected impact. A budget line is referred to each of the headings at the end of each section, to be funded from the H2020 framework. Along the discussion of each heading, especially at the challenge, status, and market descriptions, the current environment with special attention to market trends is

[15] such as defence, automotive, and process industries, mechanical engineering, utilities (including utility equipment vendors), telecom, and financial services
[16] A cPPP is not specific for the cyber security industry. Any industry can set up a stakeholder interest group. The cPPP is set up in the framework of the Horizon 2020 and is open to all organisations from the European Union and the partnership countries. All eligible organisation can be beneficiaries of grant agreements for projects within the cPPP irrespective of their affiliation.
[17] http://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

detailed. References to the GDPR are common, as data protection and privacy regulations have an impact on most priority headings. Relevance to the NIS Directive can also be found throughout the document, as the various priority areas need to be operational in the regulatory and cooperation environment set by the directive.

1.8.2 Alignment of the ECSO SRIA priority areas with the GDPR and the NIS Directive

In terms of aligning the research objectives of the ECSO SRIA document with the GDPR, the primary remark regarding the legislation is that it addresses the overall protection of European citizens and is therefore not sector-specific by nature. The regulation does not reference cyber security, critical infrastructures, or any of the vertical sectors defined in the SRIA document, however, provisions of the regulation must be applied in relation to the products and services implemented as the result of the R&D activities. The GDPR employs a risk-based approach to data protection. Organisations are encouraged to implement organisational and technical measures suitable for the activities they engage in, following a risk assessment.

As for the NIS Directive, it specifies measures with a view to achieving a high common level of security of networks and information systems within the EU so as to improve the functioning of the internal real and digital market. It sets the baseline capabilities for each Member State to make sure they are well equipped to face cyber threats. In addition, it aims at increasing EU-wide cooperation, both at strategic (Cooperation Group of national authorities) and operational (CSIRT network) level and sets the requirements for notification of incidents. These provisions of the directive mostly apply for the cyber transversal infrastructures, defined later in this document.

The following sections detail the areas of research work proposed by the SRIA document. The main sections are the cyber Eco-system projects; the pilot projects for vertical application sectors, the cyber transversal infrastructures, and the cyber technical projects. All these projects describe the priorities identified. Each priority includes subsections of the key areas of research. (Annex II outlines the seven Strategic Research and Innovation Agenda priorities.)

1.8.3 Ecosystem for Education, training, market growth and SME support

The Ecosystem for education, training, market growth and SME support requires an organised approach of collaboration. Creating an operational (technological and human) eco-system is key to address the many issues that contribute to an overall increase in the level of cyber-security. 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.

Cyber Range and simulation are techniques that implement a wide number of complex scenarios and on-demand countermeasures to address emerging cyber-risks. The cyber-range and simulation concepts are of relevance to all stakeholders, regular users, professionals and experts to be able to adapt their expertise to a constantly evolving attack landscape, a widening range of IT-impacted services, and changing regulations. The current challenge is to extend the capabilities of cyber-ranges to user domain specificities, such as SCADA, ICS, mobile devices, health related devices and IoT devices etc., to the integration or federation of solutions for different simulation environments, to the development of tools to automate the preparation for large-scale simulation scenarios.

The existing simulation infrastructures are often government funded and operated, as well as defence focused, while start-ups, universities, SMEs and large companies, critical infrastructure providers also need to have access to such capabilities to reach the objective of higher competitiveness of European cybersecurity industry as well as a more secure digital society in Europe. The EU provides an ideal opportunity for creating a world leading ecosystem for simulation and cyber range platforms, given the common rules for digital society, data protection and business environment, as well as a currently distributed cyber-security experience and actionable knowledge base. The scope of the projects should focus on the piloting of networked cyber-ranges and the extension of the cyber-ranges network. The impact will improve resilience of the ICT infrastructure, organise collaboration between a network of cyber-ranges and Europe-wide initiatives such as the CSIRT network of the NIS Directive.

Security education and training needs to supply cybersecurity professionals and needs to provide a constant learning process in a complex and fast-evolving field. There is a lack of suitable training and testing environments available for the commercial sector to satisfy the 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, and the existing ones focus on their specific needs.

The scope of the projects should focus on increasing the dynamics of the education and awareness methods, to match the rate of evolution of cybercrime; and integrating awareness into the eco-system of people, competences, services and solutions, that is able to rapidly adapt to the evolutions of cybercrime or even surpass them. The impact will create better prepared professionals to emergent cyber-attacks, improve the resilience of infrastructures to attacks, help to understand and to limit cybercriminal relationships.

Certification and standardisation of security products and services needs a unified position of Member States in order to move towards the digital single market. There is no label, seal or certification scheme that is standard for European security services and products. It is essential to promote the development of basic knowledge on information security for users to raise awareness related to the risks posed by the use of products of unknown origin. The challenge is to define a unified criterion for certification of cybersecurity products and services. This is a strong demand to be reflected with the increase of the market size of IoT, intelligent cars and the overall role of IT across all domains of our lives.[18]

The scope of the projects should focus on the development of mechanisms that ease the process of certification at the level of services, designing solutions by defining and exercising metrics that should be related to a set of threat models, and addressing the evolution of the level of certification with respect to the dynamicity of the deployed environment.

Dedicated support to SMEs is designed towards SMEs as users and as solution providers. User SMEs need to be supported in democratizing access to tools & solutions of varied sophistication level for SMEs to enable them also to benefit from innovations and solutions that are currently reserved for larger organisations. 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 include easing the piloting and field-testing to foster a collaboration between SMEs, large providers and users and ease the delivery of joint competence. The specific challenge therefore addresses the full value-chain for both provider and user SMEs. The scope of the Fast Track and Full Access to Innovation projects should focus on the involvement of provider SMEs into cyber-ranges as solution providers and ease their access to user environments, as well as increasing the level of cyber resilience of user SMEs.

Another area of support for SMEs is to create a cybersecurity certification scheme for them, promoting a system of "light" requirements for software/hardware/solution/system, enabling them to adapt their certification to the actual environment/user context in which their solutions are deployed.

1.8.4 Demonstrations for the society, economy, industry and vital services:

Demonstrations for the society, economy, industry and vital services a description of the vertical sectors (application domains) and their specific needs concerning cyber security.

Industry 4.0 is the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems (mainly ICS), the Internet of things and cloud computing, touching on the issues of digital intelligence, smart sensing, advanced system modelling and machine learning technology, enabling enhanced autonomy & efficiency of robotics. Projects addressing this topic should propose, design, validate and demonstrate technological and organizational solutions enabling enhanced digitalization & modernization of existing and new

[18] more details on the topic: https://www.enisa.europa.eu/topics/standards?tab=publications

industries in Europe in a secure way. The challenges of the current approach to the security of ICS pose a number of considerations relevant to GDPR and the NIS Directive. Innovation in the sector means a higher level of exposure, adding new attack surfaces to the ICS environments[19].
Privacy and confidentiality become a security issue with the requirements of the GDPR, while smart objects handle a range of sensitive user data, service providers use Big Data solutions. The scope of R&D in the field should focus on the secure and privacy-considerate transition of the manufacturing industry, and securing advanced manufacturing labs. Information sharing mechanisms will support the implementation of the NIS Directive by building horizontal, vertical and cross sector information exchanges, where the national CSIRTs and relevant authorities play a coordinating role.

Energy: it is crucial for energy operators to ensure the safety and security of the whole interconnected energy chain, from generation to supply as society relies completely on energy. Interconnected smart devices, such as sensors and actuators, are widely deployed in households to measure energy use and reduce energy equipment consumption and it is predicted that the number of these smart devices, known collectively as the Internet of Things, will amount to several billion in the coming years. At the same time, energy infrastructures are increasingly exposed to cyber threats due to the massive use of ICT and of new data interfaces and smart devices which offer new points of entry to attackers[20].

The energy systems could be structured around three main domains.

Smart Grids are the digitalization of electricity infrastructure and the transition from a closed, centralized, analogue infrastructure to an open, largely decentralized, digital infrastructure, 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.

Distributed Energy Resources (DER) are small-scale power generation sources located close to where electricity is used (e.g., a home or business). They provide an alternative to or an enhancement of the traditional electric power grid. The DER represent an important part of the whole electricity generation due to their massive integration in the grid. Attacks targeting a large number of renewable energy sources (e.g. windfarms) could have a severe impact on the smart grid and thus on electricity supply.

Centralized electricity generation plants with a significantly long lifespan, are now introducing the use of new ICT technologies. Legacy systems have constrained resources and sometimes rely on old software that cannot always be changed. As safety is a major requirement of these infrastructures, security solutions have to mitigate security threats which can have an impact on safety, while potential interdependencies between security systems and safety systems need to be managed. Due to the use of new technologies such as IoT, privacy issues have to be addressed and solutions proposed.

The scope of research in the field should address control and management of cascading effects in power grids to avoid major supply disruptions, control and management of increased cyber threats over time in the context of the digitalization path of the energy system, and advanced access control schemes (logical and physical) for strategic energy facilities. The GDPR impacts the energy sector by providing guidelines for dealing with privacy and data protection issues when using smart devices and IoT. Privacy-by-design should use appropriate technical safeguards e.g. encryption and pseudononymisation that provide the expected level of data protection of the customers.

[19] more details on the topic: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada?tab=publications
[20] more details on the topic: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids?tab=publications

According to the NIS Directive, Member States are requested to identify the operators of essential services and the energy providers fall under this provision. As such, the specific energy subsector need to address the common threat and risk landscape and be able to react to unexpected events. The NIS Directive addresses this issue by implementing national CSIRTs and establishing reporting and information exchange capabilities between CSIRTs and the essential service providers. Establishment of CSIRTs specializing in the energy domain (i.e. ICS-CSIRTs) are beyond the scope of the cPPP, and must be handled at the Member State level. Specific actions for the energy operators are to implement crisis management frameworks, supply chain integrity frameworks, awareness raising frameworks and information sharing mechanisms that are independent of the research areas and must be applied to the energy sector in general.

Smart Buildings & Smart Cities reflect an urban development vision to integrate ICT and IoT technologies in a secure way to manage a city's interconnected assets, such as the information systems of local departments, schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services. Like any other ICT system, the smart city's technological and communication environment is vulnerable to cyber-attacks and a large amount of data is at stake. 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. Innovation and research should focus on the simulation and detection of the additional security threats created through the inter-connection of smart systems, the delivery of 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, 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.[21]

As smart cities & buildings are data driven, organizational implications of the GDPR will be a major challenge with all the obligations imposed on data processors and controllers. A network of data protection officers will have to be trained, data security programs and processes, including privacy notices and information disclosure statements have to be documented. On the technical side, the city's critical assets need to be segmented, a common approach of privacy-by-design should be adopted to limit insecure products and data leakage.

In terms of alignment with the NIS Directive, smart cities need to focus on governance. A strategy with oversight and organization over a city's cyber preparedness, especially in terms of cross-function vulnerability assessment and incident response planning should work out mechanisms for information sharing, both horizontal and vertical. Certification mechanisms will ensure interconnected devices meet standardized requirements, thus building more resilient networks and information systems.

Transportation covers all security aspects of transport systems (people and freight) whose compromise, as a result of coordinated attacks, may have serious impact at national and/or European level (e.g. cyber-physical attack accompanied by a large-scale terrorist attack). Transportation covers four areas: unmanned aerial vehicles, smart cars and trucks and road-side infrastructure, maritime units and their infrastructure, and the railway system, all of which exhibit specific challenges to security research. In terms of economic power, European Automotive industry is currently leading innovation worldwide, European railway companies currently lead the world market, European shipbuilding is the world leader in building complex ships.

- ***Vehicles*** are becoming another consumer smart device. This will require the ability to update the cryptographic algorithms and, in general, any part of its software, to adapt to upcoming challenges (e.g. revocation of cryptographic material and certificates, revising protocols and blacklisting, upgrading and patching of software, 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.

[21] more details on the topic: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cities?tab=publications

Pedestrians, vehicles and the infrastructure need to be able to trust each other. Cybersecurity attacks targeting smart cars may have severe consequences through life-threatening accidents but also through smart-car based or assisted terrorist attacks. Besides the societal impact, smart-car based cyberattacks pose a severe economic threat since trucks cover 75% of the European domestic good transport.[22]

- ***Maritime Vessels*** (cargo or cruise ships) 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. The maritime domain, including ports, faces cybersecurity challenges that are similar to those affecting ICS based industries The increasing connectivity of smart port systems, cargo tracking and cargo identification are increasingly subject to cyber security incidents resulting from cyber-attacks.
- An ***unmanned aerial vehicle (UAV)*** - or drone - is an aircraft without a human pilot. UAVs may carry out surveillance and response missions for border security, homeland security, and critical infrastructure protection, but on the other hand may call for attention to accidental, malicious, or criminal misuses. Interest in cyber-weapons embedded in defensive UAVs is growing, but there are a number of technical and operational challenges to face. Projects addressing this topic should propose innovative security frameworks to support the design of robust cost-effective Sentry UAVs, tailored to surveillance missions towards Rogue UAVs.

Railway is considered as a safety critical application. The railway infrastructure is highly distributed per Member State, the networks don't fulfil the usual cyber security requirements in terms of sustainability, protection and attack detection. Some encryption protocols have already been standardized but their application is restricted to particular ETCS interfaces. The lack of standardisation is a major impediment for the development of a cyber-secure signalling system. 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. In terms of aligning research areas with the GDPR, special technical controls need to be developed in the transportation sector to meet the data protection requirements and at the same time create state-of-the-art products. The focus of innovation and investment should put more strength in lightweight cryptography for reliable and timely authentication of vehicles, multimodal authentication schemes to identify and authenticate driver and other humans, tamperproof communication protocols to avoid channel hijacking, privacy preserving authentication.

Transportation is regarded as a critical sector in many of the Member States. As such, there is special attention on the sector constituents by the competent authorities as well as national or sectoral CSIRTs. If constituents of the transportation industry will be designated as operators of essential service, mandatory information exchanges will be applied to the essential service providers. Standardization of various technology elements (e.g. communication, data protection) in the course of the innovation activities also enhance the resilience of the transportation industry, adding to the safety and security of the European citizens. Governance aspects of the NIS Directive will be fulfilled by laying emphasis on business continuity of the transportation services.

Healthcare faces many security challenges, most of them common to any critical infrastructure. Major concerns in the field of e-health are associated with the high privacy and confidentiality requirements of sensitive healthcare data[23]. Cyber-attacks targeting the Health sector are on the rise. Lack of adequate IT spending by healthcare organizations and lack of awareness about cybercrime have exposed the vulnerabilities of healthcare organizations. The designated Operators of Essential Services under the healthcare sector within European Union fall under the stringent rules of the NIS Directive, being considered one of the critical infrastructures in many of the Member States. Pilot projects in the field should focus on existing e-Health services involving as many stakeholders as

[22] more details on the topic: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cars?tab=publications

[23] more details on the topic: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health?tab=publications

possible, including but not limited to patients, healthcare service providers, doctors and other professionals. The integrity of healthcare data being distributed among these many actors should be one of the key research areas. The e-Health service should involve interconnected systems and data transfer, mobile services, smart devices and data analytics, digitalisation of all the healthcare levels, the development of Assisted Living systems, wearable devices, IP-enabled medical devices.

Specific challenges include eHealth service resiliency against cyberattacks (especially in new technologies like telemedicine, home care systems, remote monitoring, mHealth), prevention against data-leakage and loss of patient data and identity theft. Systems availability and business continuity is another key component of eHealth. Privacy-by-design should be another focus area to ensure data security and integrity, especially in terms of big data originating from clinical trials and healthcare digitalization. These challenges all align with the requirements set out in the GDPR and the NIS Directive.

E-services for the public sector 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 operating costs to Governments. 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. Specific needs to achieve this status include privacy enhancing data handling tools and technologies that ensure confidentiality, integrity and availability.

Governments are the largest data controllers and processors, so ensuring confidentiality, integrity and availability is the primary challenge. Failing to do so can lead to political unrest and the lack of inclusion of citizens in the digital society. The provisions of the GDPR and NIS Directive place a special responsibility on the Member States to deploy seamless technical controls to protect the data of its citizens and businesses, as well as taking part in national and international cooperation via the national CSIRTs and the competent authorities to enhance the resiliency of the governmental infrastructures.

The financial sector is considered to be the backbone of the economic development and competitiveness of Europe. The implementation of a Single Financial Market and the aim of strengthening Europe's cyber resilience will highlight some of the risks and challenges in order to reach a Single European Digital Financial Market. The increasing number and frequency of sophisticated cyber-attacks against the banking sector highlights the need to develop a cyber security framework to protect the integrated financial market and to combat cyber fraud. This requires a comprehensive approach against emerging risks that takes into account the rise of digital banking via new devices, the developments of innovative solutions based upon a collaborative integration such as DLT and blockchain[24] and concerns over privacy and data protection issues.

To reach an appropriate and consistent level of risk mitigation, it is important to foster awareness through data and information sharing, even to the extent of sharing common infrastructures and to implement awareness raising and training programs to overcome the negligence of the human factor. The investment into cyber solutions in the financial sector represents a huge opportunity to boost European economy, by overcoming the customer fear and enhancing their trust in digital means. The financial sector is mentioned in both GDPR and the NIS Directive. Failure to protect customer data can lead to unforeseen effects. Data protection by means of technical innovations should focus on new methods of authentication and authorization, whereas the infrastructure protection should focus on building resilience through information sharing and cyber crisis simulation. The financial sector is a critical infrastructure and CSIRTs are already engaged with the traditional financial institutions, however, with the opening

[24] more details on the topic: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/finance?tab=publications

of the financial market under the PSD2 Directive, the newcomer service providers also need to be involved in the governance strategy of the financial sector.

Telco, media and content providers are closely related market sectors with great financial importance, mostly listed among the critical sectors in Member States. Telco networks are a core component of the current and future digital infrastructure, so ensuring their security and dependability is vital to the European and global economy. Europe has a good reputation in both privacy protection and in reliable high-quality system management, which justifies for hosting data and systems in Europe despite of relatively high labour costs. Telcos, ISPs and large hosting companies are amongst the more sophisticated types of companies investing into cybersecurity as they are high profile, high value targets for cyber attackers and the consequences of disrupting operations are highly visible and have widespread impact. For this reason, the scope of innovation and investments are focused around the areas of mobile and IoT security, detection of threats and illegal content, cloud services and platforms, network virtualisation, encryption, and 5G networking technologies. Telco, media and content providers are likely to become operators of essential services based on the NIS Directive, so their reporting obligations in terms of data breach and security incidents will impact their daily business. With regard to the GDPR, these operators will have to lay special emphasis on their activity as data processors and controllers, especially with the enhanced notice and information obligations before collection and to adhere with the consent and ability to withdraw information.

1.8.5 Collaborative intelligence to manage cyber threats and risks

Cyber Transversal 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. As the vertical elements depend critically on the digital infrastructure, it must be highly resilient and trustworthy. The challenge is to secure that the infrastructures serving the applications are resilient to attack, accident and error, and assure them of the trustworthiness of the infrastructure. There are two 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 include protection, detection, response & recovery and Governance, Risk and Compliance (GRC). These components apply to individual elements of the digital infrastructure as a whole, and to the applications and organisations that depend on the infrastructure, incorporating aspects of cooperation and coordination, both laterally and vertically.

Governance, Risk & Compliance: Security Assessment and Risk Management uses an integrated approach involving people, processes and technology; 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 viewed, consolidated and reconciled in an integrated manner. At the same time, security risk management must be aligned and interlinked with enterprise risk management and cost factors. 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.

Risk management is a major catalyst for cyber security. The GDPR and NIS Directive will be driving forces for risk management in Europe in the upcoming years, both are seen as important tools to drive adequate protection of data. GRC is a tool that provides 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, and provides an organisation's senior management with means of assessing and improving its security posture. The output of the GRC should facilitate inter-organisational cooperation and cooperation with supra-organisational institutions. This includes trusted information sharing mechanisms on threats, vulnerabilities and incidents, perhaps on an industry basis, to help the creation and coordination of preventive and corrective plans. Information sharing is mandated for operators of essential services by the NIS Directive. 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.[25]

Innovations in the area should address risk-based situation awareness, assessment and decision support, automated assessment mechanisms, cyber risk governance, the use of cyber ranges, simulation & training, and the certification of operators.

PROTECT: High-assurance prevention and protection against attacks in modern ICT components, infrastructure, and systems remains a complex task, so there is justifiable need for the design, implementation, and verification of high-assurance components, systems, and infrastructures. Solutions for end-users also require high-assurance security as they are considered a key security vulnerability. To achieve high-assurance, investments on cybersecurity initiatives to protect PCs, mobile devices, and IoT devices will need to be increased. The scope of innovation and research should cover means to protect digital infrastructures and the applications that use them by preventing cyber-attacks on them being successful. Security, privacy and trust considerations should be involved from the very beginning in the design of digital infrastructure, systems and processes. Trustworthiness should also cover secure execution environments and systems.

By preparing the infrastructures to better resist advanced attacks and their consequences, protection capabilities will target the users of ICT and ICS infrastructure. This will result in the increase of trustworthiness of European ICT services and products and the competitiveness of the European industry.

DETECT: Information Sharing, Security Analytics, and Cyber-Threat Detection are advanced processes that enable 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. Intelligence driven detection can improve the ability to anticipate breaches before they occur and respond quickly, decisively and effectively to confirmed breaches. 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. So they need more intelligent and effective approaches for integrating and using the mass of data available. It is essential to establish how information should be shared and which level of abstraction is effective. The analysis should be done across different information sources both unstructured (textual content and multimedia) and structured ones, and for this natural language analysis must be taken into account. Machine learning technologies could be helpful in obtaining Cyber Security Intelligence from the Dark/Deep Web. The sharing of security information requires trust mechanisms among the entities involved in sharing their data. A common, normalised terminology and framework is important in facilitating sharing of information and reducing response and processing times.[26]

Proposals on this subtopic need to 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. The complementarity between end-point and network detection capabilities should be enhanced, and scalability to big data should also be enabled. A native European threat intelligence feed should be established, and a mechanism created for distributing this information effectively among the stakeholders, especially operators of critical infrastructures as defined by the NIS Directive.

RESPONSE and RECOVERY: Cyber threat management is concerned with planning and executing appropriate actions following the detection of a security event, and restoring the system to 'business as usual' status. Digital Forensics

[25] more details on the topic: https://www.enisa.europa.eu/topics/threat-risk-management?tab=publications
[26] more details on the topic: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing?tab=publications

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

Proven and standardized techniques and practices of security log management, incident reporting, cost-based Response and Recovery decision-making, and incident information sharing will also enable more effective and timely cooperation in resolving incidents and higher preparedness of the users to dealing with incidents and their consequences. The technological and operational enablers of cooperation in Response and Recovery will contribute to the development of the CSIRT Network, which is one of the key targets of the NIS Directive.[27]

1.8.6 Remove trust barriers for data-driven applications and services

Data security and privacy is a very wide field. Europe has traditionally been very conscious about protecting user privacy. In this aspect, it has developed the technical expertise to lead the area of data protection and it has developed the political will that can help push innovative solutions into the market. As an impact, it is expected that companies will turn to solutions that ensure better data protection and better privacy for the end users. The scope of innovations in the topic will create secure and privacy aware data processing and storage, balance privacy needs and business demands, and facilitate the implementation of the regulatory context (e.g. the GDPR).[28]

ID and Distributed trust management (including Distributed Ledger technology) refers to the future of authentication/authorization. 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 may lead to significant innovation in the market. As an impact of the innovations in the field, flexible authentication and authorisation schemes will come to existence, authentication will operate in a distributed fashion without single points of failure on critical paths, distributed trust management frameworks will be largely adopted. This impact will satisfy the ambitions of the GDPR in terms of enhancing data protection, and the NIS Directive in building more resilient information systems.[29]

User centric security and privacy solutions aim at guaranteeing the privacy and security of citizen's data. 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. 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. 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, invoked by the GDPR or the Privacy-by-design provisions of the eIDAS regulation. Investment in the area should result in increased awareness in privacy leading to a decrease of identity theft, new best practices and usable technologies in authentication for both digital service providers and end users that enable user-centric security and privacy.

1.8.7 Maintain a secure and trusted infrastructure in the long-term

ICT infrastructure protection is one of the most challenging dimensions of cyber security, considering the speed and scope of cyber-attacks or incidents. The increased interconnections created within the Internet as well as between

[27] more details on the topic: https://www.enisa.europa.eu/topics/csirt-cert-services?tab=publications

[28] more details on the topic: https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data?tab=publications

[29] more details on the topic: https://www.enisa.europa.eu/publications/blockchain-security

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. In addition, the ICT infrastructure has become increasingly flexible, scalable and open.

Member States must be in control of their state-based critical networks, systems and platforms, and must be able to protect them from threats. Otherwise, the risk is high that citizens become reluctant to use these services. Privacy remains a key issue that can only be supported if the entire architecture of ICT services is considered secure, safe and resilient to threats. Given the expected impact of the density of devices and users in the infrastructures, virtualization of the resources in the infrastructures seems the more sustainable option that need to deal with security and scalability problems among others. Research with particular interest in ICT infrastructure protection focuses on services; cloud infrastructures, including all the computing, networking and data components; and trusted networking infrastructures and virtualization. The scope of innovations should focus on areas of threat management, network security, protocol transition / migration to secure systems, secure execution environment, and device and system security. The impact of the innovations will result in a higher security level of infrastructures, supporting the implementation of the NIS directive.[30]

Quantum resistant cryptography aims to solve the emerging threat that large-scale quantum computers will be able to break current standard asymmetric cryptographic algorithms in a matter of hours. As cryptographic functionality is a core component for cybersecurity, this will have serious implications, in particular to medical data and data in classified systems related to national security. In addition, the number of IoT devices will grow significantly in the next decade, so the development of software, hardware, and key management technologies is core to address the emerging threat.

The scope of research should focus on quantum-safe cryptographic methods and algorithms for both asymmetric and symmetric cryptography, transition from present-day cryptographic systems to quantum-resistant cryptography, and developing evaluation criteria for quantum-resistant public key cryptographic standards and implementations.

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

Trusted supply chain for resilient systems focuses on trust and dependency on consumed Cloud Services from third parties. There are many solutions developed to ensure not only the security and dependability aspects but also the data protection and privacy provisions of the Cloud Service Providers. Industry advocates cloud SLAs for transparency and applied security controls, but the lack of models, mechanisms and tools for supporting dynamicity in SLAs is still a challenge. Evidence based Cloud certification is a new approach to be explored.

The Digital Single Market will require collaboration and open innovation from stakeholders to create competitive added value. An average single company in Europe (i.e. SMEs) can hardly address the whole service supply chain by their own in the environment of IoT, inter-cloud environments, Industry 4.0, etc. The scope of innovations should focus on methods for developing resilient systems out of potentially insecure components, their certification and security assurance methodologies, enhancing open source security. The impact will be increased trust along the supply chain, with solutions for certified systems instead of certified components.

Security-by-design is the concept that software and hardware must be designed with privacy and security in mind from planning to implementation. This best practice is already mandatory in certain industries especially those involved in embedded, industrial, technical and scientific software like defence, aerospace, energy, hi-tech and spreading to telecom and finance. Europe enjoys a high reputation for Privacy and Security-by-Design, as enforced by the GDPR and the Privacy-by-design provisions of the eIDAS regulation. The scope of developments should focus on methods and tools for developing privacy enhancing and secure software and hardware, security and privacy

[30] more details on the topic: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/internet-infrastructure?tab=publications

	INDUSTRY 4.0	ENERGY	TRANSPORT	EHEALTH	SMART CITIES & BUILDINGS	EPUBLIC SERVICES	FINANCE	TELCO/ISP/ CONTENT PROVIDERS
IoT/IP enabled devices	x			x				
Access and Identity management				x		x	x	x
Cloud based infrastructure/SDN/NFV	x					x		x
Big Data / data science	x			x	x			
Authorization/Authentication	x		x	x	x		x	x
Automation/Robotics	x							
Privacy/Data Protection	x	x	x	x	x	x	x	x
Cryptograpy/encryption	x			x		x		
Embedded systems	x		x	x	x	x		
Tamperproof communication protocols	x	x	x	x	x	x	x	x
Navigation systems			x					
Anonymization/pseudonynamization		x		x		x		
Machine learning/AI	x	x				x		
Cyber crisis simulation								x
Cross domain sensing and analysis	x				x			
Cascading effects of disruptions	x	x	x		x			x
Risk and impact on human health and safety	x			x				

Cyber risk modelling and management	x					x	x	
Awareness and incident response						x	x	
Vulnerability testing	x			x				x
Cyber insurance							x	

architectures, and secure deployment. Impacted beneficiaries will be software developers and suppliers within vertical market segments, as well as the security consumers and the end-users by measurable improved security and privacy levels and efficiency gain and increased trust both by developers using the components and by end-users.[31]

1.8.9 From security components to security services

Advanced Security Services focuses on the processes required to provide, manage, measure, certify, restore, etc. privacy and security, and the tools required to support them. Any entity, from individuals to large enterprises and governments, has a need of cybersecurity functions of certain types. Most common services include consulting and IT outsourcing, managed security services, managed detection and response. The cybersecurity services market is at the moment led by North American players, however, the availability of cybersecurity services from European providers is often of high importance due to such matters as trust, requirements of laws and regulations, existing business relationships, subtle cultural aspects, etc. 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. 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. 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. The efforts should support the implementation of the NIS Directive in enabling and shaping collaboration between service providers, CSIRTs, and other relevant organizations.

1.9 Impact analysis of the R&D proposals in the context of the GDPR and the NIS Directive

The objective of this document is to provide an analysis of areas covered by the NIS Directive and the GDPR where R&D activities would achieve the greatest impact. The ECSO SRIA document proposes a complex system for areas of research, which allows to suggest concrete areas for funding with rationale for their choice. The impact analysis maps the cyber security related research needs of the vertical sectors (application domains), and makes an assumption on the priority of research topics based on their reusability, and their importance in the security/privacy-by-design concept.

Table 2 The vertical domains and their anticipated fields of research

Table 2 provides an overview of each sector in terms of their technological needs. By the description of each sector given in the section above, the following assumptions can be made:

[31] more details on the topic: https://www.enisa.europa.eu/topics/data-protection/privacy-by-design?tab=publications

- The prime area of interest by the vertical sectors in terms of R&D activities is privacy/data protection. This is a broad topic that can be broken down to technological components. Most of the topics in the matrix can be regarded as enablers of better privacy/data protection solutions.
- By selecting more specific areas of R&D, secure communication protocols and authentication/authorization methods seem to be the common interest for the verticals. Both topics can be regarded as technical safeguards that will ensure more resilient infrastructures and information systems, thus adhering to the measures of the GDPR and the NIS Directive.
- The matrix also shows that the Industry 4.0 and the eHealth sector seem to be the most research-intensive sectors.
- An interesting observation is that cyber crisis simulation and the research of cascading effects also exhibit an outstanding area to be explored aside the technical related topics.

The impact analysis further maps the cyber security related research fields in Table 3 based on the needs of the cyber transversal infrastructures. Contrary to the vertical sectors, the transversals focus their research needs more on trust and resiliency, as the stakeholders represent a horizontal cross section of the digital society. The areas of interest support in the implementation of the NIS Directive. The table below indicates that the main interest in all transversals is in usable and actionable information on threats, whereas high-assurance prevention and protection requires the biggest number of security components.

	GRC	PROTECT	DETECT	RESPONSE & RECOVERY
Threat intelligence and analysis	x	x	x	x
Cascading effects of disruptions	x			x
Information sharing	x		x	
Risk management and governance	x		x	
Cyber ranges	x			
Certification of operators	x	x		
Trusted systems & secure environments		x		
Secure verification		x		
Privacy-by-design		x		
Operating system security		x		
Secure integration		x		
Cryptography / encryption		x		
Enhanced visualization			x	
Machine learning / automation			x	x

Forensics				x

Table 3 Security specific components of the cyber transversal infrastructures and their research needs

The beneficiaries of the research activities in the cyber transversal infrastructures include (service and technology) vendors, managed security providers, CSIRTs, system integrators, certification authorities, and end-users. The NIS Directive puts emphasis on cooperation and collaboration on national and international level, so strengthening these beneficiaries with the implementation of the innovation and research results will enhance European cyber security resiliency, as well as raise the European competitiveness on the global cyber security market.

Both vertical sectors and transversal infrastructures define their needs in terms technical research. To address these needs, the ECSO SRIA document defines the scopes of cyber technical projects with a given set of themes and technical topics. By conducting research in the given topic, its product can be used in either the verticals or the transversals. The scope of the cyber technical projects is listed below with the anticipated topics of research.

- Remove trust barriers for data-driven applications and services: authentication, AIM, privacy, encryption;
- Maintain a secure and trusted infrastructure in the long-term: awareness raising, threat intelligence and management, network security and secure environments, cryptography;
- Intelligent approaches to eliminate security vulnerabilities in systems, services and applications: certification, open source security, privacy-by-design;
- From security components to security services: security analysis, security monitoring and management, incident response, forensics, threat intelligence, certification.

The outcome of the research projects will be the building blocks for the vertical sectors and transversal infrastructures from which they can leverage their respective needs.

1.10 Importance and alignment with global trends in cyber security

The ECSO SRIA makes suggestions to research and innovation in the context of the global cyber security landscape. In 2016, the EU Cyber Security Market was estimated at €20.1bn and compares favourably with the cybersecurity market of other global regions. The CAGR of the EU market however is 6%, whereas the average growth rate is around 8%, and is growing slower than all other major regions[32], so Europe needs extra effort to catch up with the global trend. The document identifies the current characteristics of the European market that inhibit leadership as listed below:

- Europe's share of the global economy is declining due to slower growth.
- The EU market is fragmented in practice, making growth difficult.
- Funding shortages and entrepreneurial support.
- Europe procurement policies focus too much on short-term savings without promoting customer-vendor partnerships needed for innovation.
- Less investment in R&D and little market success.
- Skills shortages.
- European companies favour execution over strategic vision.

[32] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler, p1

On the other hand, however, Europe places special emphasis on safeguarding its citizens and securing its infrastructure, by means of the overarching legislations, such as the GDPR and the NIS Directive, to reach toward a sustainable Digital Single Market. The objective of the cPPP is to bridge the gap between capacity building and the deployment of trusted European cyber security solutions on European and international markets. To address the global trends and to overcome the current European gaps, there need to be coordinated cyber security actions within the EU that call for the swift implementation of cyber security strategies at the EU, national, and regional levels and the promotion of European cyber security and privacy research and innovation. Parallel to this activity, there is a need for a more active outreach to the world-wide research communities to promote international cyber security and privacy research and innovation activities.

2. Conclusions

Cybersecurity is an essential enabling factor for the development and exploitation of digital technologies and innovation and is, therefore, 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.

The ECSO SRIA report highlights the potential topics for research and innovation related to cyber security for the H2020 Work Programme that fosters the consolidation and growth of the European cyber security market and industry. It describes 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, further reasoning is included on how to better motivate the choice of the suggested topics, including the market, the rationale for covering the specific areas at European level, the target users and other elements. The document in itself also refers to the currently dominant EU legislations and guidelines that need to be adhered to, specifically the GDPR, the NIS Directive, the eIDAS or the Digital Agenda.

According to the ECSO SRIA, the success factor to meet the overall objectives are the capabilities and competences of the human resources involved within the process and the ability of all the involved stakeholders to collaborate and cooperate across public and private organisations, Member States and at international level. The ECSO proposes a contractual public-private partnership (cPPP) to address the main strategic objectives to be achieved, 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.

Although the ECSO SRIA sets the objectives for the cPPP, its focus remains on the context of the H2020, and it will not be able to solve policy activities and research and innovation funding that goes parallel or beyond H2020. There are gaps remaining, especially with the alignment of the European regulatory framework, namely the GDPR and the NIS Directive.

2.1 Gaps in EU legislation

The GDPR addresses the overall protection of European citizens and is therefore not sector-specific by nature. The regulation does not reference cyber security, critical infrastructures, or any of the vertical sectors defined in the SRIA document, however, provisions of the regulation must be applied in the process of personal data collection and usage. The GDPR aims to encourage innovation, as long as organizations implement the appropriate safeguards. The regulation adopts a “broad” definition of research, encompassing the activities of both public and private entities. However, it remains unclear whether research for product improvement, corporate beta-testing or market research purposes would be considered scientific research. This important interpretative question is likely to be taken up by data protection authorities and advisory bodies. In the age of big data, where the data analytics activities of many organizations may qualify as research, it is unclear exactly how far the GDPR’s research exemption will extend. Involvement of legal expertise will be crucial as the regulation does not provide exact definitions that can be applied out of the box.

The NIS Directive specifies measures with a view to achieving a high common level of security of networks and information systems within the EU to improve the functioning of the internal real and digital market. It sets the baseline capabilities for each Member State, however many of the definitions of these capabilities still remain open in the context of set-up, methodology or content. While the priority areas are set by the ECSO SRIA, the implementation of research and innovation will only be successful if the regulatory environment will have a common definition and implementation of the provisions under the NIS Directive. By way of examples[33]:

- A common European threat and risk landscape to understand and address the threat and risks, inclusive of all vertical domains is still missing.
- The information sharing on threats, risks and vulnerabilities is not well defined and lacks a common classification scheme applicable to the vertical domains.
- The harmonization of criteria for the identification of operators of essential services is not available.
- A EU-wide accepted cyber response framework is missing that should include the necessary processes in case of cyber attacks.
- A minimum level of maturity has to be agreed when a maturity framework is available.
- The harmonization of security implementation across the European Union is not sufficiently addressed.
- A supply chain and integrity framework is not available as of the date of writing.
- There are no common incident reporting criteria defined that the vertical sectors can refer to.
- The cooperation with EU and Non-EU countries and international organisations is not or only partially defined.
- Crisis management frameworks do not address cyber security incidents and attacks for all vertical domains.

2.2 Alignment with previous Strategic Research Agenda

Identification and prioritising of forthcoming research and innovation topics should be performed in close collaboration with industrial stakeholders across Europe towards a more focused and coordinated approach. In the previous years, the European Network and Information Security (NIS) Platform was the vehicle where the key challenges and desired outcomes in terms of innovation-focused, basic and applied research in the fields of cyber security, privacy, and trust were identified. As an outcome of the NIS Platform's work, a Strategic Research Agenda (SRA)[34] was published, that outlines the key objectives of the desired research priorities as follows:

- Fostering assurance
- Focussing on data
- Enabling secure execution
- Preserving privacy
- Increasing trust
- Managing cyber risks
- Protecting ICT infrastructures
- Achieving user-centricity

The Digital Single Market strategy together with Horizon 2020 introduced the concept of cPPP that will focus on Research and Innovation but also go beyond and address measures that can help impose connection to end users, improve the reporting of validation activities with users of research results and promote participation of relevant EU Industry. In case of cyber security, this is realized by the ECSO, and the SRIA document clearly follows the key

[33] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf
[34] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/at_download/file

objectives of the SRA document of the NIS Platform. In terms of the fields covered among the focus areas of the SRIA, it can be stated with high confidence that the complementary projects proposed will cover all aspects of cyber security. The cyber security eco-system will create the baseline capabilities, the cyber pilots will address various vertical sector-specific needs, the cyber transversal infrastructures will enhance the cooperation requirements of the determinant EU cyber legislations, and the technical projects will provide the innovative technical solutions, as building blocks, for vertical domains and the transversal infrastructures.

2.3 Governance and promotion

When discussing the potential research areas that are designed to lead or regain European competitiveness in the cyber security market, the concept of governance needs to be taken into consideration. This is a task that goes beyond the scope of ECSO and their research proposal. However, the governance of ECSO provides some insight on how the organisation approaches involvement in research. The Bylaws of ECSO[35] sets the roles and responsibilities of its members and governing bodies, with special attention to the cPPP. The cPPP encompasses a Partnership Board (PB), which comprises of ECSO and EC representatives. The main objective of the Board is to discuss the annual priorities of the Horizon 2020 Cybersecurity Work Program, the implementation of the overall R&D program related topics and the monitoring of the cPPP commitments. The ESCO representatives to the PB undertake not to influence the implementation of the H2020 programme, or be involved in the preparation or evaluation of related calls. This should limit any conflict of interest from ECSO's behalf.

Furthermore, the ECSO recommends the formation of a European Cybersecurity Council, which would be a high level advisory body not belonging to the ECSO but closely linked to it. A European Cybersecurity Council would assess at a high level the work of the cPPP as well as provide the ECSO Board and the cPPP Partnership Board with guidelines and commitment for a longer term strategy. It would be composed by relevant CEOs/executive decision makers from Association Members, members of the European Parliament and of National Authorities as well as the relevant Commissioners and high-level representative from the European Institutions. The European Cybersecurity Council is yet to be established.

2.4 Areas not covered by the ECSO SRIA

In terms of gaps or uncovered areas, it is important to bear in mind that the ECSO was established to foster cyber security R&D within the H2020 framework. There are some areas, e.g. national security, defence, nuclear energy, aviation, online content development, online child protection, or general awareness raising that do not fit in the context of H2020, therefore the ECSO SRIA does not take this into consideration. However, through other funding schemes (as listed in previous section) the EU provides mechanisms to fill these gaps to ensure that all cyber related societal challenges are addressed. Promotion and dissemination of R&D results falls out of the scope of ECSO, thus it is not covered by the SRIA document. By nature, all research projects plan with dissemination activities, but the SRIA does not include any overarching promotion and dissemination plan to position ECSO as a technology transfer or research brokerage platform in the EU R&D landscape. These activities are to be carried out in other existing mechanisms, such as CORDIS[36].

2.5 What is already in place

Regardless of the cPPP between ECSO and the EC, H2020 is ongoing with its calls in the digital security focus area. Up to date, seven calls in digital security have been published, and two calls are open at the time of writing. Three calls were specifically addressing the cPPP for proposals. The areas of focus for the cyber security related calls are:

- Assurance and Certification for Trustworthy and Secure ICT systems, services and components;

[35] http://www.ecs-org.eu/documents/uploads/591d55b9be0a6.pdf

[36] Community Research and Development Information Service, http://cordis.europa.eu/guidance/home_en.html

- Cyber Security for SMEs, local public administration and Individuals;
- Increasing digital security of health-related data on a systemic level;
- Economics of Cybersecurity;
- EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation;
- Cybersecurity PPP: Cryptography;
- Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors;
- Cybersecurity PPP: Privacy, Data Protection, Digital Identities.[37]

Preceding H2020, a number of initiatives and cooperation mechanisms have been started in the field of critical information infrastructure protection and combatting cybercrime. There are a number of existing national and EU-wide information exchange mechanisms[38], mainly being formed on a voluntary basis. Most Member States have national/governmental CSIRTs that cooperate with each other and with various critical sectors. There are European agencies, such as Europol or ENISA that foster multilateral cooperation in the field of information security and combatting cybercrime. The number of best practices built up over the past ten years led to the considerations laid down in the NIS Directive. All this provides a firm background to the current and future implementation of research activities carried out in the context of the ECSO SRIA.

[37] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-ds-2016-2017.html#c,topics=callIdentifier/t/H2020-DS-2016-2017/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc (opened on 15 August 2017)
[38] more details on the topic: https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts

3. Annex I - Acronyms and abbreviations

The following acronyms and abbreviations are used in the document:

- AI Artificial Intelligence
- CAGR Compound Annual Growth Rate
- CEF Connecting Europe Facility
- CIIP Critical Information Infrastructure Protection
- CORDIS Community Research and Development Information Service
- cPPP Contractual Public Private Partnership
- CSIRT Computer Security Incident Response Team
- DER Distributed Energy Resources
- DLT Distributed Ledger Technology
- DSM Digital Single Market
- EC European Commission
- ECSO European Cyber Security Organization
- EEA European Economic Area
- EFTA European Free Trade Association
- eID Electronic Identification
- eIDAS Electronic Identification and Trust Services for Electronic Transactions
- ENISA European Network and Information Security Agency
- EP European Parliament
- ETCS European Train Control System
- eTS Electronic Trust Services
- EU European Union
- FI Financial institutions
- GDP Gross domestic product
- GDPR General Data Protection Regulation
- GRC Governance Risk Compliance
- ICT Information and Communication Technology
- IoA Indicator of Attack
- IoC Indicator of Compromise
- IoT Internet of Things
- ICS Industrial Control System
- ISAC Information Sharing and Analysis Center
- ISP Internet service provider
- IT Information Technology
- NFV Network Function Virtualization
- NIS Network Information Security
- OT Operational Technology
- PB Partnership Board

- PC Personal Computer
- R&D Research and Development
- SCADA Supervisory Control and Data Acquisition
- SDN Software Defined Network
- SIEM Security Information and Event Management
- SME Small-Medium Enterprise
- SOC Security Operation Center
- SRA Strategic Research Agenda
- SRIA Strategic Research and Innovation Agenda
- SW Software
- UAV Unmanned Aerial Vehicle

4. Annex II - An outline of the priority areas in the ECSO SRIA report

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

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu