EUROPEAN CYBER SECURITY ORGANISATION

Input to the Horizon Europe Programme 2021-2027

Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity

WG 6 – SRIA and Cybersecurity Technologies

December 2020

www.ecs-org.eu

Input from the European Cyber Security Organisation (ECSO)

to the Horizon Europe Programme – 2021-2027

Priorities for the definition of a

Strategic Research and Innovation Agenda in Cybersecurity

Final

18 December 2020

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO federates the European Cybersecurity public and private stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and association, as well as the local, regional and national public administrations across the European Union (EU) Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. The main goal of ECSO is to develop European cyber security ecosystem, support the protection of European Digital Single Market, ultimately to contribute to the advancement of European digital sovereignty and strategic autonomy.

More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

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

Table of Contents

PREAMBLE

Cybersecurity is fundamental for the Digital Transformation of the Digital Single Market aiming at protecting the European citizens, enterprises, infrastructures or institutions against cyber-risks as well as developing the competitiveness of the cybersecurity sector.

The growing political awareness about the societal and economic consequences of digitalisation has provided the necessary ground to define and structure a comprehensive cybersecurity strategy. Cybersecurity is now recognised to be an essential enabling factor for the development and exploitation of digital technologies and innovation and is, therefore, inextricably linked to future prospects for growth, job creation and Europe's response to environmental and societal goals. The significance of cybersecurity is an ever-growing issue with political, societal and economic implications.

Taking stock on the European added value, this cybersecurity strategy should be structured to meet the immediate, mid and long-term security requirements at national and European level to strengthen the European ecosystem, protect critical infrastructures and to build the capabilities needed to ensure a satisfactory level of strategic digital autonomy, both in terms of new technological developments and of mastering digital technologies.

ECSO has identified four main strategic areas for investment in order to develop a comprehensive cybersecurity R&I strategy in Europe to increase digital autonomy and respond to the needs of our industrial sectors, while protecting the European fundamental rights. These investments could be supported by the coming Horizon Europe Programme, from 2021 to 2027.

The **first pillar** of the proposed R&I strategy identifies the importance to **create a sustainable ecosystem in Europe** where a cybersecurity culture and best practices need to flourish to address the needs of the citizens, society and develop the needed skills to cope with a fast-changing digital society or even digital world powered by cyber technologies. In this context, it is key to look at the societal impact of cyber technologies and moreover the threats that the use of insecure cyber technologies or the misuse of them can bring to citizens as individual entities or society as a whole. This may provoke a lack of trust and, subsequently, of acceptability of the digital world, and what can be done to build a more reliable and secure digital society. Moreover, the citizens' perception of cyber technologies may differ considerably from the actual state of the affairs and is connected closely with education and awareness.

The **second pillar** of the R&I cybersecurity strategy focuses on the **digitisation of vertical sectors** and the need for **resilient infrastructures**. The economic sectors identified in the ECSO SRIA v1.0 have been clustered into Industry, Finance, Health, Construction, Energy, Transport, Public services and Telecom. These sectors have grown in a process of vertical integration which was largely triggered by the key technological and organisational trends that characterise the 4th industrial revolution. To some extent, the digital transformation may potentially blow up or at least shaken historical siloes which today do not necessarily find a technological relevance. An interesting example to consider is the penetration of IT vendors into very structured industries like automotive. A shift of power that may lead to a redefinition of market segments for cybersecurity as well. In addition, we may have to consider sectors which are not yet tagged as "critical" from a cybersecurity perspective but are still vital for the human and may need to enter into the frame if we consider the technological changes affecting them.

The **third pillar** builds on **data and economy**. Data will be the key driver to our digital economy and has attracted a lot of discussion for its implication in the digital transformation

of the society and the digitalisation of the vertical sectors. Securing the data, the algorithms that operate on top of them, as well as their final results will be of paramount importance for the future of the data-driven economy in the Digital Single Market. The innovative aspect driving the need for investment should deal with data security, privacy aspects and how data interacts with the economy, requiring the definition of specific data economy models.

The **fourth pillar** is the development of **basic and disruptive technologies** that are expected to have a strong impact on markets, industries and citizens in the future and which will efficiently support the three strategic pillars mentioned above. Some identified prominent technologies are Artificial Intelligence, Blockchain, IoT, and Quantum Computing.

The list of priorities detailed below still needs to be consolidated and discussed further within the ECSO community. A detailed description is reported in the Annex.

Main levers to drive the priorities

- Ecosystem, social good and citizens
    - Development of resilient systems, including software, with a security by design approach to reduce the financial impact of zero-day attacks.
    - Definition of risk management strategy and countermeasures to manage future unknown (evolving) attacks or fast-adaptable attacks that changes their behaviours exploiting vulnerabilities and potentially weak countermeasures.
    - Vulnerability management and development of tools to support cybersecurity assessment, evaluation and certification.
    - Develop measures for a trustworthy supply chain.
    - Development of adaptive digital forensics mechanisms to cope with new emerging threats and increasingly heterogeneous distributed devices and technologies.
    - Develop cyber range technologies and services and maximization of the benefits of the usage of cyber ranges within training contexts.
    - Develop sector specialisation of cyber ranges as an enabler of the simulation and defence scenarios of critical infrastructures, essential services and application domains.
    - Cybersecurity pervasive technology and management of cybersecurity challenges related to this machine economy based on the Internet of Things and Cyber Physical Systems
    - Develop methodologies, tools and platforms to develop human body embedded devices with security by design.
- Cyber resilient infrastructures and services for ICT technologies and vertical sectors
    - Enhance the security level of highly critical infrastructure, including, energy (electricity, gas, oil), water distribution, telecommunications, etc.
    - Improvement of the reaction to cyber incidents, sharing information among the relevant stakeholders involved in critical infrastructure management and operation.
    - Increase trust in the 4th industrial era to reduce the impact of cyber threats on business continuity.
    - Develop cyber secure communication systems and networks of the future.
    - Manage security orchestration in heterogenous systems and networks
- Data and economy to provide the foundations for a trustworthy and reliable Data-Driven Economy of the future.
    - Support the needs of digital services with new trustworthy privacy preservation techniques to protect the economic growth and European digital transformation.

  - Provide tools and mechanisms for supporting the processing, mining and dissemination of personal data and models with privacy guarantees.
  - Verify the correctness of the information to increase trust in digital services.
- Technologies, methodologies, and building blocks to develop and a secure and resilient Digital Single Market.
  - Model and validate security properties for AI-driven systems, inherently dynamic and dependant on the availability and quality of data
  - Define trustworthy AI-based systems to increase trust in the decision process and foster society at large to obtain the expected social benefits.
  - Design and implement procedures that can produce concrete security guarantees for the overall system along the product chain, from hardware implementation to product deployment.
  - Design and implement technologies for trusted electronics and continuously assess their quality and security
  - Design of cryptographic schemes and systems.
  - Develop procedures for the secure evaluation and efficiently implemented cryptographic algorithms
  - Design new digital-based currency that is as secure and privacy-friendly.
  - Address IoT challenges at all layers in the stack (device, connectivity, platform and application), and a across different layers or IoT systems as a whole.
  - Design a new family of applications, aware of relevant adversarial behaviour and capable of both detecting when they are under attack and adapting their behaviour as needed.

Detailed list of priorities

Ecosystem, social good and citizens

Approaches, methods, processes to support cybersecurity assessment, evaluation and certification

Horizon Europe – HEU.1.A	
Specific Priority	**Approaches, methods, processes to support cybersecurity assessment, evaluation and certification**
Description of the challenges – why is it important?	The EU Cybersecurity Act establishes the European Cybersecurity Certification Framework with the intent to increase the level of cybersecurity within the Union, enable a harmonised approach at EU level of European cybersecurity certification schemes, and improve the conditions for the functioning of the internal market by creating a Digital Single Market for ICT products, services and processes. Under the framework, schemes will be developed in the coming years targeting different technologies, system architectures and verticals. One key aspect will be the definition of certification schemes, assessment and evaluation mechanisms to attest that the ICT products, processes and services comply with specified security requirements. As such, there will also be the need to equip the designers of certification schemes, the vendors of products, services and systems to be certified, and evaluators, including Conformity Assessment Bodies, as well as certifiers with the necessary means to conduct such certifications, focusing on new and disruptive technologies and new software and systems design and delivery paradigms. The expectations in the application of the new cybersecurity certification schemes are quite high, but it is reasonable to assume that several challenges need to be tackled, for instance, to ensure consistency of the assurance levels across schemes or even define metrics to measure the security levels. Other relevant challenges linked to support a useful, comprehensive, and continuous cybersecurity assessment is how to address complex systems as security cannot be considered additive and how to integrate the notion of privacy and data protection in practice, since certification schemes might have a potential impact on data, both personal and industrial. Security assessment and certification so far focus either on products that can be well separated from their environment (e.g., IoT devices, processors, firewalls, even OSs, with the majority of the software and hardware owned by the vendor) or best practices and security management (e.g., for cloud service provisioning). The long-term objective of the European Cybersecurity Certification Framework is to provide a broad set of schemes extending this focus towards more complex systems as they are used by citizens and businesses – a connected car, a digital manufacturing line or a home automation system. Future economy scenarios, where product lifecycle can become even more relevant than today, e.g. circular economy, might bring additional complexity due to the potential reuse of components, leveraging on an extended lifecycle. Complex systems are characterised by:

- their distributed nature connecting different components / systems from different vendors ("systems of systems") over multiple nesting levels, as well as by their software relying on third-party development, build, deployment and execution environments and open source software components;
- the strong integration of Artificial Intelligence technologies including machine learning, natural language processing, robotics, image processing and more;
- their strong dependency on large sets of data which include business sensitive and personal data, and which are governed by regulations, e.g., the GDPR or sector-specific requirements;
- frequent changes and updates enabled by new development and deployment paradigms (agility, containerisation, dynamic loading of code).

To enable the assessment, evaluation and certification of systems like those described above, new metrics, methods and tools are needed that:

- are able to assess risks stemming from both HW/SW vulnerability and human and organizational capabilities;
- take technology specific threats and risks into account, e.g., adversarial machine learning, bias in ML models, fake data, deep fakes, and more;
- allow for objective risk assessment by introducing standardised metrics, data sets and test suites for measuring cybersecurity as well as methods for aggregating risks up to system level;
- explicate the security promises made by system constituents and allow to draw conclusions about full systems based on these promises;
- characterise the evidence needed to assess the cybersecurity of complex and dynamic systems and provide the tools to collect and evaluate such evidence, assuming modern, agile development and deployment environments, and considering aspects of both the effectiveness and correctness of implementation of security socio-technical measures;
- support continuous security assessment over the lifetime of a product, service or process, acknowledging technology (e.g. dynamic software systems where only parts of the code are known at design-time) and environment (e.g. different lifetime of, say, microservices and energy distribution systems) specifics;
- increase the efficiency and effectiveness of evaluation and certification activities by applying rigorous methods in an automated fashion and supported by processes that may be (in some cases) leverage a model-driven approach;
- allow to scale assessment and evaluation according to the assurance levels as defined by the Cybersecurity Act while maintaining adequate security claims;

	• support the definition of schemes aiming at data protection (GDPR) compliance certification. Measuring the cybersecurity is crucial to compare and assess different systems and devices, and to find mitigations against the failures encountered. Risk assessment is still subjective, as the metrics used to measure the security level can be affected by the expert judgement and depend on the understanding of potential threats vectors and impact. In addition, some of the metrics, such as the likelihood are difficult to measure. In this sense, security testing provides an objective and empirical way to assess a system. Nevertheless, the testing process is still performed manually and the integration between the testing and risk assessment still remains an open issue. Furthermore, there is a need for risk assessment approaches capable of aggregating the risk of a system of systems, reusing as much information as possible from the components assessment. The heterogeneity existing in the assessment and certification mechanisms makes this situation even more difficult. Each scheme uses different criteria and metrics that can lead to different interpretations according to the expert evaluator. Well-defined metrics and criteria to measure security will also enable moving from a qualitative to a quantitative analysis making it easier to understand the impacts of potential attacks, a better prediction of the possible impact of security countermeasures to strengthen services and products. The complexity of the cybersecurity assessment increases when data protection could be impacted, for instance in cloud service assessment and certification. Thus, it will also be important to understand how the different certification schemes expected to come up under the *GDPR and the EU Cybersecurity Act* will relate to each other. Furthermore, in some sectors, where safety is a primary concern, cybersecurity considerations need to be coordinated with other aspects such as functional, safety, quality, etc., requiring additional an effort to coordinate with sector directives and other relevant standardization initiatives for ICT/IoT systems. In order to support the definition and deployment of such schemes, cost-efficient methods and tools need to be developed and deployed on system device, service and process level. While providing innovations in the areas indicated above, solutions should pay particular attention to the economic viability of the novel approaches they investigate in. Security certification as a means to increase consumer trust and to boost the level of security of European product and service offerings requires a broad adoption of the respective schemes, which will only be achieved if processes are simple, the degree of automation in the evaluation is high, costs are low and timelines are short. Activities under this priority are expected to contribute to these objectives.
Digital Living & Working	Certification and tools supporting assessment can be a driver for improved trust in digital services and products. The specific market needs of the different sectors, such as transport, finance, education, medical research to name a few can open new scenarios requiring improving systems integration for urgent needs, e.g. the collection and study of COVID pandemics related data.

BASELINE	
What has been done so far (in EU and in the World – EU position)	In the context of the EU cybersecurity framework, ENISA is tasked to propose the certification schemes. ENISA has established already 2 AdhocWGs of experts who started drafting the first certification schemes under the Cybersecurity Act covering the SOGIS Common Criteria and the cloud services. Many assessment technologies have been researched in the past, including formal analysis, testing, static and dynamic analysis tools, and more. These techniques form the foundation of security assessment. Initial attempts for reasoning on system level have been made, by investigating into machine-processable assertion formats (project ASSERT4SOA) and using them for security claims on system level (project OPTET). Initial attempts for IoT security formal verification have been made in recently started projects (IoT4CPS, SPARTA) in order to make different private life and business IoT environments more secure. The ECSO document “Assessment options” explains how to benefit from the right mix of security assessments, and what constraints to be aware of when organisation are building their cybersecurity capabilities and need to choose how to assess security. The CSPCERT group from the European Commission has identified recommendations for the implementation of a Certification scheme for cloud services. Still on cloud, the project EU-SEC already provided a reference implementation for continuous auditing-based certification in cloud computing, including tools like Clouditor. ENISA has recently published a report which explores 5 distinct areas, which have frameworks, schemes or standards that can potentially be evolved to EU candidate cybersecurity certification schemes: IoT, cloud, threat intelligence in the financial sector, electronic health records in the healthcare and qualified trust services. The study reflects on the standards currently available on these areas of interest and identifies existing gaps. Regarding risk assessment, there are a high number of general security risk assessment methods managed by both commercial and non-commercial organisations. However, they are often subjective (such as the SANS vulnerability analysis scale or the DREAD scheme), specific for web applications (e.g. the OWASP Application Security Verification Standard (ASVS) Project), or too large and complex, such as OCTAVE. The Common Vulnerability Scoring System (CVSS) consists of three metric groups, base, temporal and environmental, like the Common Weakness Scoring System (CWSS), base finding, attack surface and environmental. These approaches are widely used, for example in CWE/SANS Top 25, OWASP Top Ten or in the National Vulnerability Database created by the NIST. However, the metrics are still subjective, depending on the person who perform the assessment. In addition, these proposals do not offer a mechanism to aggregate and reuse the assessment of the system components in a way the system could be assessed in an easy and non-expensive way. For what concerns testing, it is worth mentioning the ICSA Labs IoT Security Testing Framework on specifying security testing

	requirements for different types of IoT devices. Ideally, mature and standardised cyber-ranges could be a key element for testing in any cyber-security certification schema. Their usage in this direction is quite limited so far (in Europe but also worldwide), since cyber-ranges are actually mostly perceived for training purposes only. Within the ECHO project, a dedicated task will explore in detail how to better include cyber-range in the EU Certification Framework. In terms of addressing data protection, the EU Commission has recently published a report on certifications. It is a sector where, thanks also to the GDPR the EU could take a leading role in the world. https://ec.europa.eu/info/study-data-protection-certification-mechanisms_en
Effort until now	Past and current EU projects have worked on specific issues related to assurance and security assessment without fully addressing the challenges above: ASSERT4SOA, OPTET, IoT4CPS, SPARTA, ARMOUR. In the area of risk assessment, RASEN project proposed an integration between risk assessment and testing later standardised by ETSI. In the H2020 programme, ARMOUR developed a certification methodology based on the ETSI proposal by combining the two approaches of testing and risk assessment. The EU-SEC project aims to create a framework under which existing, certification and assurance approaches can co-exist. The ongoing project ECHO is currently working on the definition and implementation of a multi-sector risk assessment framework with the aim of approaching the risk analysis from a horizontal perspective (sector-neutral, in order to find commonalities) but being able to add sector-specific elements (taxonomies, methodologies) and find interdependencies. Specific certifications schemes for data privacy have been developed in the context of EU funded research projects, for instance Europrise or Europrivacy.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Cybersecurity assessment will greatly benefit from automated tools (when possible) that help in assessing the risks, define objective security requirements and security assurance activities, continuously monitor the effectiveness of security countermeasures and the associated technical and organisational measures. Those tools should incorporate vulnerability management procedures and analysis of the impact of the vulnerabilities both on the security and business levels. This should be implemented at different levels. • There is a need of security risk assessment schemes able to cope with all the challenges inherent to security, easy, and automatic if possible, facilitating a posterior assessment, and coping with the dynamicity inherent to security. A broader acceptance of what “security auditing” is should be enforced, where bug bounty (also named crowdsourced security) has

	equal status with current penetration testing approaches in terms of compliance. • There is a need for new knowledge and tools for the assessment and improvement of cybersecurity culture, both among vendors and users. • A system composed by devices could be composed by several components with different levels of security, so security composition could be a desirable design feature, as well as multilayer assessment, dealing with the different threats that could be derived from each layer. Since security is known to be non-compositional in general, such approaches need to be carefully characterised in terms of their contributions and limitations, as well as the strength of security claims resulting from them. The context in which the device will operate must be considered, in order to make devices comparable among each other and to specify the boundary conditions of the context where the security risk assessment was applied. • To address the need to measure the security properties, objective and easy to measure security metrics must be established. A security risk assessment scheme has to take into account the protocol stack in order to have an overall cybersecurity label that covers the entire configuration and the different threats that could be derived from each layer. • Specific testing procedures should be designed and executed for each assurance level and domain as the baseline for cybersecurity certification. The tests results could be used to create a dataset to establish a benchmark, compare the security achieved and continuously assess the security attained. • Methods and tools to relate risks and test scenarios to provide a means to characterize coverage of security testing. • Tools and guidelines for risk management and assessment: define a scientific approach and methodology for reproducing results and compare the results over time and across the sector. • Tools and methodologies to address organisational measures: it is not trivial to find reasonable metrics for an automated measurement of organisational controls, since they are mainly describing the need for processes or the existence for specific documents. Novel techniques based on NLP are necessary to analyse large number of documents for a semantic match to organisational measures. • Tools to analyse system behaviour, identify potential risks and vulnerabilities, and continuous evaluation of security strengths. • Tools for security analysis and assessment in specific disruptive technology domains, for instance, in Artificial Intelligence • Combination of security risk assessment with security testing in order to estimate and validate in an objective way the security level of a system. Prediction analysis of possible security countermeasures and their potential impact should be investigated.

	• Combination of assessment methods and tools to ensure sufficient expertise and organisational capabilities to cope with diverse threats. • Usage of cyber-ranges to support cyber certification and test schemes should be greatly encouraged and studied. • The result of the assessment should be communicated to the user in an understandable but enough informative way. Other aspects that could help in the security assessment include formal verification whenever possible to support the evaluation of complex systems originating from contributions of different provenance. Approaches need to be optimised regarding effort, costs and duration, aiming at a maximum degree of automation. Testing tools can operate in a grey-close-to-black box approach testing, for example, communication protocols' stacks, some embedded security-critical software implementations based on, say, scanning or fuzzing techniques, may the feedback loop data be logical or physical.
Expected benefit; strategic or economic impact **➔ What can be achieved?**	The development of certification schemes can bring immense benefits to the market by increasing the trust of end-users and the governance of data processes. Solving this challenge widens the scope of security assessment and certification significantly, extending it to products, services and systems beyond critical infrastructures, which still bear a major risk for being exploited for attacks. This, in turn, significantly increases trust in information infrastructures and can position Europe as demonstrating leadership in protecting citizens' daily lives. • A suitable risk assessment scheme would help to assess and compare different security technologies, in order to provide a more harmonised security view to be leveraged by end consumers. It will allow to compare the security of different products in an objective and homogeneous way. • Harmonisation in the assessment process will enhance the objectivity of the measures and facilitate the process of the evaluation. • A standardised set of tests will help to increase the development and adoption of new technologies, and the enforcement of current EU cybersecurity regulations. • Better comparison of the security level achieved by similar products, allowing the consumer to choose one based on the security that they provide. • Real time information about security based on the results provided by testing procedures. • Reliability of the assessment process, as it is meant to be repeatable. • Furthermore, an assessment approach able to deal with composition, implies a significant time and cost reduction due to the reusage of the components' assessments. • Improved cybersecurity culture, better skills, expertise and organisational cyber-security capabilities.
Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 7

Timeline (2025/2027/beyond)	2023/2025

Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP

Horizon Europe – HEU.1.B	
Specific Priority	**Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP**
Description of the challenges – why is it important?	Most of the recent cyberattacks usually depend on some kind of programming error, a bug which, when exploited, may give control of the execution to the attacker, compromising in this way the victim computer. Buffer overflows, heap overflows, dangling pointers, etc. have all been used in the past to hijack the program's execution and enable the attacker to gain control of the victim computer with no explicit user interaction. Unfortunately, it is not easy to find these software bugs, since by definition, they are mistakes made inadvertently by computer programmers, and thus they are not known. One way to deal with these unknown bugs is to "harden" the executable (without introducing significant performance overhead) so that when/if the bug is triggered it will not allow the attacker to compromise the computer. Recent trends have shown that, as the security of the higher stacks of the software has improved, software attacks have been exploiting "lower level" vulnerabilities down to the interaction between the hardware and the software. A hardware-software co-design approach to the software hardening objective needs to be studied to make sure the definition and implementation of the underlying hardware does have the adequate features for ensuring security at any level of the stack of the software. It is reasonable to assume that even with best-practice security technology and processes in place, one cannot completely prevent security breaches like, for instance, credentials being stolen or zero-day attacks happening. While this calls for increased efforts on security research and innovation, it also draws attention to a complementary approach to security: runtime application self-protection (RASP). RASP means that applications are aware of relevant adversarial behaviour and are capable of both detecting when they are under attack and adapting their behaviour as needed. The RASP paradigm results in defensible, resilient applications that can protect themselves even in cases where other security mechanisms and controls fail. In addition to software vulnerabilities, the research community recently discovered that, much like software, hardware also can suffer from bugs exploitable by cyber attackers. Hardware bugs, such as RowHammer or Spectre, can be triggered by malicious software and, as a result, can compromise computers (or data) by reading from or writing to arbitrary memory locations.

	While software bugs may be fixed by releasing and installing software updates (patches), hardware bugs are much more difficult to mitigate, as no such hardware updates exist. For example, if a processor has a bug, there is no easy way to fix it. Currently IT-Systems need to be constantly monitored, since they are under attack by adversaries (e.g. 'hackers'), as well as subject to system failures and crashes due to software bugs, network failures, hardware issues, etc. As IT-Systems continue to pervade all branches of modern lives, this monitoring proves to be an inhibiting factor which does not scale, thus limiting the applicability of IT-Systems, even making them prohibitively costly. Thus, the amount of human monitoring needs to be limited to an absolute minimum, and such techniques as self-healing and self-protection are instrumental in achieving that. On the one hand, new technologies will provide new ways to protect against attacks, and on the other hand they will bring in new potential vulnerabilities or also tools to perpetrate new complex attacks or easily accessible and low-cost attacks, including new forms of attacks against cryptographic procedures and their implementations through quantum computers. Current countermeasures typically target specific attacks in the short-run and gradually improve technology. Instead, however, the objective should be to develop more robust architectures and algorithms that deliver an inherently increased level of protection. Since we cannot assume that attacks and system failures will decrease over time, we need systems, which are resilient to such attacks through more robust and resilient polycentric architectures and algorithms at design phase, implementing software hardening technologies, developing systems that have self-healing capabilities and run-time application self-protection and self-healing, such that less human intervention is needed in the event of failure.
Digital Living & Working	
BASELINE	
What has been done so far (in EU and in the World – EU position)	Chipmakers fixed the vulnerabilities of processors to attacks like Spectre, Meltdown and their offspring but did not fundamentally change the architectures and how these type of attacks can be mitigated in a structured way with a moderate performance cost. High-assurance products covered under high Common Criteria Evaluation Assurance Levels are well-protected against advanced attacks. However, this protection does not propagate down to commercial and industrial grade devices while the attacks become easier and cheaper over time. There is a need for methods and tools to support resistance against advanced attacks during the design phase as well as automated evaluations, and to understand the potential impact of attacks and potential associated risks and how those risks evolve during the attacks, for example through the implementation of digital twins. There are some self-healing mechanisms, such as Docker, which have the ability to restart crashed servers. However, these systems

	have only limited understanding of what humans would consider a 'system failure'. Systems with a broad understanding do not exist as of now. *AI-based* solutions have not yet been able to develop a human-like understanding of system failure. Even anomaly detection driven by machine learning has, as of now, only a very limited scope, and is not yet able to survey and manage whole infrastructures. Consequently, there are no holistic approaches to AI-driven self-healing systems. In the case of Software Hardening although the initial ideas may be traced back to the 80's, real work in the area has blossomed only in the past decade, after the realization that software security is much more difficult that what was originally thought.
Effort until now	There have been some projects related with self-healing and SW hardening like: • ASPIRE; establish trustworthy software execution on untrusted mobile platforms that have a persistent or occasional network connection to a trusted entity at their disposal. • HDIV: SELF-PROTECTED WEB APPLICATIONS; HDIV, a technology that follows a security by design approach, generating self-protected web applications • SECRET; automated early detection and warning of known and unknown network-based cyber-attacks facilitating a distributed passive monitoring infrastructure, and to investigate the automated reaction alternative strategies for self-reconfiguration and adaptation of the security system • SHARCS; a framework for designing, building and demonstrating secure-by-design applications and services, that achieve end-to-end security for their users. • CyberSec4Europe; design and develop technologies to harden programs against cyberattacks. • STANCE; define, implement and validate a set of program analysis tools capable of verifying the security of complex software systems made in C, C++ and Java • ROSETTA; reverse engineering of complex software that is available only in binary form; automatically hardening software without requiring any access to the source code • SHADOWS; targets the problem of growing software complexity and its detrimental impact on software reliability by introducing a new model-based paradigm for the development of self-healing software systems automatic detection, localization, and healing of faults • WS-DIAMOND; developing a framework for self-healing Web Services monitoring, detection and diagnosis of anomalous situations, due to functional or non-functional errors. • REACT; forecast where attackers will strike next and to use this information (i) to fortify potential targets to withstand the attack and (ii) to wire targets up with forensic hooks and make them "forensics ready" immediate delivering effective patches by selectively armouring the vulnerable part of a program • WOMBAT; new types of sensors, especially in the domain of client-based honeypots semi-automatic generation of metadata associated with the raw data collected

	• SISSDEN; development and deployment of a distributed sensor network based on state-of-the-art honeypot/darknet technologies and creation of a high-throughput data processing centre • NEMESYS; adopt the honeypot scheme for the main types of smart phones and devices, develop an infrastructure to gather, detect and provide early warning of attacks on mobile devices and, eventually, understand the modus operandi of cyber-criminals that target mobile devices • YAKSHA; develop and introduce the innovative concept of honeypots-as-a-service which will greatly enhance the process of gathering threat intelligence • NoAH: a European Network of Affined Honeypots; development of an infrastructure for security monitoring based on honeypot technology It is possible to say that efforts till now are sparse and patchy, with not very well-connected results and not resulting in popular practical technologies. There is some work on anomaly detection but only with very limited applications and in narrow domains. Holistic anomaly detection or failure detection remains future work. On the other hand, Software Hardening is very recent and there are only very few projects underway, that have been previously mentioned https://www.cybersec4europe.eu/ and http://react-h2020.eu/
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Application self-protection needs to be adaptive, taking the history and context of the interaction with the attacker into account when protective actions are taken upon detection of an attack. It also needs to be intelligent, not letting the attacker know that it has been detected even when it is, for instance, diverted to a honeypot. This requires capturing the information and knowledge an attacker might already have gained before detection, the creation of believable but safe data for simulated application environments in a honeypot, the risk assessment of an application context and state, the automated generation of effective honeytokens, and more. Concerning the design of self-healing systems, AI-based agents are necessary to alleviate the task of IT-infrastructure monitoring. At the first stage, it would be necessary to design agents that detect failure in an abstract sense, which comprises more than the binary notion of ‘server up/down’ or ‘service responding/not responding’, but understands the IT-systems and their purpose. Matching the system’s purpose against its current state, the agent should be able to detect failures. At the second stage, it would be necessary to design agents which correct these failures, leading to self-healing systems. More research is necessary in order to understand the potential and cost of software hardening and in the case of embedded systems, it will necessary to investigate about run-time on-chip or on-board monitoring techniques that would detect abnormal behaviours linked to software or hardware attacks. It is also essential to incorporate the secure-safe and resilient-by design methodology within the research and development of a any future technology to be deployed into digital products. This

	methodology would encompass the practical analysis of the resistance of any new technology (hardware or software) against known attacks in order either to identify whether this new technology is capable of repelling such attacks or to identify to what extent the technology need to be modified to offer intrinsic resistance. Finally, the design and implementation of resilient computer polycentric architectures supported by advanced tools during the design and evaluation phases is still necessary.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	Self-healing systems will greatly promote the use of IT-systems, leading to enhanced productivity in all sectors. It will reduce workload on human experts and improve uptime. It will also make systems more resilient to attacks, which will be more easily detected, and countermeasures be taken. RASP is an important element in a comprehensive security strategy for software applications, providing increased protection from attacks caused by unknown vulnerabilities or by attacks using channels outside the application or system scope (e.g., credentials stolen via social engineering). Sound and complete detection mechanisms (e.g., by tracking data flows at run-time) allow for automated mitigation and adaption. Altogether, the practical security of applications and systems is significantly increased. Protection of software against unknown bugs with low performance overhead and reducing the financial impact of zero-day attacks, not allowing those to compromise the victim computers. Making sure future processor definitions encompass the adequate instruction set or hardware mechanisms to implement hardening techniques at all levels of the software stack.
Starting TRL / Expected TRL	**Starting TRL:** 2 **Target TRL:** 6
Timeline (2025/2027/beyond)	2030

Development of digital forensics mechanisms and analytical support

Horizon Europe – HEU.1.C	
Specific Priority	**Development of digital forensics mechanisms and analytical support**
Description of the challenges – why is it important?	While digital forensics generally deals with the acquisition and investigation of any material found on digital devices, our focus here is on the important special case of data related to cyberattacks and extracted primarily from breached devices and systems of attack victims. Digital forensics is always evolving, as it needs to adapt to new contexts formed by increasingly heterogeneous distributed devices and technologies, growing data volumes, and requirements of high reliability and performance. Issues of digital identification and attack attribution, crucial for providing a solid foundation for assigning legal responsibility, and protecting personal information, connected to such

	key GDPR requirements as data privacy and right to erasure ('right to be forgotten'), must also be addressed in forensic investigations. All these challenges are exacerbated by the wide use of cloud services, with their multi-tenancy and high level of anonymity, CPS and IoT devices. Hardware security analysis tools need to be developed to adapt to the legal and technical constraints of digital forensics so that digital evidence can be extracted from CPS and IoT devices in a forensically sound manner. Digital evidence management (DEM) principles should be followed in design and production of such devices. Digital forensics operations are currently highly time-consuming and involve large amounts of manual work, so AI-based data analysis approaches must be explored to support investigators. Furthermore, correlation across multiple digital evidence and threat intelligence sources and use of meta-data are important to take full advantage of contextual information. At the same time, evaluation of the veracity of automated results is often crucial in the forensics domain. Most of the solutions commonly used for digital forensics today are reactive or post-incident. Synergies among forensic investigations, threat intelligence efforts and security monitoring and attack detection methods and operations must receive attention, as well as forensics-by-design approaches to developing systems, running security processes and training personnel, to increase the level of forensic preparedness. Countermeasure decisions often need to be considered based on results of forensic investigations and attack attribution efforts. Those involve complex technical, legal and ethical matters, and guidance for organisations that have to consider such decisions is required. A serious challenge slowing down developments in the domain that should be noted is the lack of availability of forensic datasets for research and tool validation. Law Enforcement Agencies (LEAs) and Incident Response (IR) service providers and teams, which have access to relevant data, typically cannot share such data with security and data analysis experts even within their own organizations.
Digital Living & Working	Wider use of remote access to organizational systems, online / team collaboration tools and cloud-based services extend the attack surface and set higher requirements for aggregating and analysing forensic evidence across multiple devices and platforms under multiple ownership.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Currently there are many digital forensic tools, commercial and open source, for data acquisition, evidence discovery and examination, forensic data analysis, and cybercrime datamining (e.g., EnCase Forensic, AccessData FTK, Magnet Axiom, Rekall, Volatility, SIFT Workstation by SANS, Sleuthkit, Pyflag). Some of the tools are adopted by LEAs and IR service providers and teams. There has been progress in such directions as live memory forensic, network forensic, event timeline reconstruction, support for simultaneous examination of multiple sources of digital evidence, data carving, and some others.

	However, the available tools have numerous limitations, including reliability and performance problems, and the efforts in different aspects of forensic analysis appear widely scattered. Given the very high expectations of expertise and practical experience applied to digital forensic investigators and high amounts of their work required in majority of IR cases, we believe that significant improvements to the tools and – even more importantly – a consistent and concerted integrational effort are required. On the information representation side, which is also crucial for successful integrations, such initiatives as Unified Cyber Ontology (UCO) should be considered. Training in specific commercial forensic tools and certification programs for experts in digital forensics exist, but it is challenging to keep those up to date.
Effort until now	Among the projects on digital forensics, only a few focused (fully or partially) on forensic investigations of cyberattacks, while the emphasis in the others was on analysis of digital evidence extracted from devices of criminals, for various forms of physical crime and cyber fraud. The relevant recent projects are: • *LOCARD* (Lawful evidence collecting and continuity platform development), 2019 – 2022. The project aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain, supporting permission policies for selectively sharing access to digital evidence with other platform nodes. This will be powered by an immutable storage and an identity management system to protect privacy and handle access to evidence data using a Trusted Execution Environment. • *PRIVACY4FORENSICS* (A Formal Rule-Processing Engine for Privacy-Respecting Forensic Investigation), 2015 – 2018, Marie Curie Action: "International Incoming Fellowships". The key goal was to develop a rule-processing engine that extracts privacy properties of collected data and investigation search warrant(s), detects conflicting or uncertain situations and labels collected data accordingly, and monitors and controls investigator access to collected data in accordance with the assigned labels. • *VIS-SENSE* (Visual Analytic Representation of Large Datasets for Enhancing Network Security), 2010 – 2013. Combining and supporting attack attribution techniques with visual analytic technologies, including interactive visualization of massive amounts of data, was one of the items in the project scope. • *RAMSES* (Internet Forensic platform for tracking the money flow of financially-motivated malware), 2016 – 2019. The objective was to design and develop a holistic, intelligent, scalable and modular platform for LEAs to facilitate digital Forensic Investigations, from the Threat Intelligence standpoint, analysing, linking and interpreting information extracted from Internet related with financially motivated malware, identifying patterns of fraudulent behaviour. The focus was on ransomware and banking Trojans. • *ASGARD* (Analysis System for Gathered Raw Data), 2016 – 2020. Will develop, maintain and evolve a best-of-class tool

	set for the extraction, fusion, exchange and analysis of Big Data, including cyber-offense data for forensic investigation. LEAs prioritised needs in the fields of multimedia big data acquisition, processing, fusion, mining, visualisation and collaboration. • *INSPECTr* (Intelligence Network and Secure Platform for Evidence Correlation and Transfer), 2019 – 2022. Will develop a shared intelligent platform and a novel process for gathering, analysing, prioritising and presenting key data to help in the prediction, detection and management of crime in support of multiple agencies at local, national and international level. The project will deploy big data analytics, cognitive machine learning and blockchain approaches to significantly improve digital and forensics capabilities for pan-European LEAs and will ensure that analytical tools are used proportionally and in line with relevant legislation (including fundamental rights), with extended options for multi-level and cross-border collaboration. As we can see, only ASGARD and INSPECTr include actual forensic data analytics in the scope but focus more on evidence extracted from devices of criminals. VIS-SENSE worked on visual analytics for attack attribution, but the efforts were limited to network traffic analysis and date back to 2010 - 2013.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	The diversity problem, where a greater variety of devices – including CPS and IoT – become candidates for digital forensic investigation and require appropriate data acquisition mechanisms, needs proper attention, with emphasis on devices that are likely to be targeted by attackers. Addressing forensics-related challenges of cloud services and correlating evidence of incidents collected in cloud instances and client devices used to access those instances are important work directions. One particular challenge to address is ensuring trustworthiness of collected evidence in devices and cloud platforms. Performance of forensic tools is often a serios bottleneck, aggravated by the increasing data volumes. HPC options for expediting data pre-processing, storage, analysis, correlation, and reporting should be explored, including use of GPUs and Field-programmable Gate Arrays (FPGAs) for exploiting algorithmic parallelism. AI-based methods should be developed for supporting forensic investigators in information retrieval and analysis, including: • detecting relevant patterns and anomalies in large forensic datasets; • filtering out irrelevant details; • correlating evidence across multiple sources; • clustering events and pieces of evidence; • explaining evidence and reconstructing attack scenarios. It is important that implemented AI methods allow to achieve a desirable balance between the competing goals of precision and recall, which is often case- and goal-specific.

	AI-based approaches should be complemented by visualisation ones, e.g., ranking and clustering, to support forensic experts in combining automated and human analysis. Threat Intelligence, data collected by security monitoring systems and detections and alerts produced by attack detection logic can be indispensable in forensic investigations. At the same time, results of forensic investigations can extend and enrich Threat Intelligence and allow to improve monitoring and attack detection mechanisms. So, appropriate integrations and information exchange should be considered a high-priority work direction and a key ingredient of forensic preparedness (proactive forensics). Other important ingredients are: • Forensic-by-Design, i.e., integration of forensic requirements into relevant phases of system development lifecycle, in cost- and system resources-conscious ways; • reliability and security of digital traces; • approaches to digital identification, which plays a critical function in the context of "smart society" and similar and poses significant challenges; • methods of attack attribution (connected with digital identification) and understanding the extents of their accuracy and reliability; • trained personnel and processes for handling incidents in a way that satisfies legal, privacy and forensic requirements. New methodologies and platforms must be developed to enable cooperation among teams and organisations involved in digital forensics activities. Also, forensic intelligence sharing could be supported by existing popular threat intelligence sharing platforms, such as MISP, OpenCTI, EclecticIQ, Anomali, and communities around those. In all activities and technology development, privacy issues must be taken into account to protect citizens' rights, in particular, forensic-by-design mechanisms must respect privacy-by-design principles. Multi-disciplinary efforts in the technical, legal and ethics domains are required to provide guidance on countermeasures that can be considered as a result of attack investigation and attribution.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	• Increased traceability of attackers and protection of their targets. • Improvement of the security mechanisms due to intelligence and insights produced by forensic investigations. • Discouraging cybercriminals by effective digital forensic operations, including court cases and penalties. • Better effectiveness and efficiency of forensic investigations, better societal services by LEAs, more affordable commercial IR services. • Improved protection of resource-constrained devices and ecosystems and businesses relying on those. • Increased sense of security and justice for citizens and organizations using the Internet and digital services.

Starting TRL / Expected TRL	**Starting TRL:** **Target TRL:**
Timeline (2025/2027/beyond)	2027 and Beyond

Cyber ranges and simulation environments

Horizon Europe – HEU.1.D	
Specific Priority	**Cyber ranges and simulation environments**
Description of the challenges – why is it important?	At present, society has realized that the risks of cyber security can have a global impact when the sector or infrastructure affected offer an essential service to the population. This new type of attack, more specialized and sophisticated, includes very specialized computing and communications devices, which use their own standards, closed designs and a high economic cost. To solve these problems, it is necessary to invest in research on simulation technologies and emulation of highly complex systems that allow to prepare, identify and mitigate current and upcoming threats in an effective and cost-efficient manner. These new systems will extend the capabilities and scope of the current Cyber Ranges and will act as an enabler of the evidence-based simulation and defence scenarios of critical infrastructures, essential services, and various other vertical sectors. Cyber ranges are rapidly raising up in importance within the security domain. The capability to support R&D, training, threat simulation, AI/ML, and test & certification enables cyber ranges to become one of the key technological elements in the future cyber security landscape. While cyber ranges capabilities shall be universal and horizontal, they have the capability to be vertical on single sectors (e.g., “energy cyber range”, “healthcare cyber range”, etc.). This capability gives a number of different possible applications of the concept and also paves the way for showcasing dependencies between sectors and supply chain threat modelling allowing decision makers to make strategic decisions based on evidences. Modern cyber ranges can also support physical appliances, resulting in “hybrid” environments even more flexible in their possible usage.
Digital Living & Working	
BASELINE	
What has been done so far (in EU and in the World – EU position)	Currently, most of the Cyber Ranges offered in the Market present a generic architecture of IT services, fully virtualized and flexible, require human interaction to set up scenarios, evaluate performance of participants and the creation of challenges. Scenarios and targeted competence buildings are based on individual/organisational ideas, rarely on evidence based approaches. The scenarios that include industrial or specialized equipment require the integration of physical

	elements with the limitations that this entails: lack of access to the device because it is key in the production process, impediment to perform exercises with real attacks that can damage temporarily or permanently said device, lack of flexibility and scalability of the training scenarios, especially compared to the maturity of traditional IT architecture, etc. The underlying technologies (private/public cloud, virtualization platforms) are becoming mature, contributing to enhance the cyber range offers. However, the market seems to be still scattered and not particularly coherent. The concept itself of cyber range is not standardized and it seems to get different declinations and offered features depending on the provider. Standardization and classification efforts seem important in order to allow customers better understanding the market offer and the technology limitations of the different provided services. The concept itself of cyber range provider is still not really defined. No standards are defined for cyber ranges and related technical elements. Attempts on standardization of the scenario description meta-languages has been taken (Tosca, as an example) but basically failed their purpose, up to now. Another clearly weak area is related to the optimization of the usage of cyber ranges. How to transform the competence building needs of an organization into practical cyber range scenarios (whose configuration is usually extremely technical)? Some EU funded programs (H2020-DS-07-2017 and SU-DS01-2018, as example) partially covered this issue but definitely additional efforts should be spent on maximising the benefits of cyber ranges within training curricula. Also the ease of integration into existing educational or training activities is still a challenge. In terms of offered services, the actual market seems to mainly focus on the training capabilities, while not much is available on the market directly supporting R&D, threat simulation and test, verification & certification (while potentially the EU Digital Single Market and the Certification Frameworks could benefit of cyber ranges as relevant test beds for security certifications and also for simulating the impact/potential threats when modifying a network or assets on a network). While technically feasible, the diffusion of sector specific cyber ranges seems still limited both from technical and content perspective. The European concept of cyber exercising and facilitating cyber ranges as true means of metrics for resilience buildings shall be developed and adapted. Within the very last years the concept of “federation” and “interconnection” of cyber ranges gained diffusion within the cyber security landscape. A federation of cyber ranges seems to be a possible solution to better organize the market offering (since a federation of ranges would standardize and organize the service offering of the single federated ranges), optimize the resources utilization (some analogies with the EU Govsatcom initiatives can be easily found, in relationship to the concept of “pooling & sharing”) and allowing the creation of complex multisector scenarios, of great interest from military, commercial, an d research/academic

	perspective. Technology and governance model issues are still relevant within the concept of federation of ranges. Some EU initiatives (funded by EDA or by different H2020 calls) are providing the initial ground to improve the technical understanding of the problem and also rationalize the output. EU is not behind in cyber-range technologies and their application, with respect to the rest of the world which is facing a similar situation as described above. An initial market comparison between cyber range offering performed within the ECHO project shows that there is not significant gap in the domain between the rest of the world and Europe. It seems, however, that the EU has more diversity in product and offering. These elements give EU the possibility to take a leadership role in the domain, if properly stimulated by the governments. Cyber ranges on a technological level – as stated above – are more and more frequently used by organisations. Yet from the soft-skills part cyber ranges are still lacking easily available and affordable content (scenarios, VMs, traffic simulations, automated attacks, evidence-based threat generation, AI based analytics, etc) and a uniform view on curricula to be aligned both at HEI and industry levels. There are initiatives to tackle this challenge, yet clear steps towards this direction still needs to be done.
Effort until now	As previously stated, main efforts until now are related to the technical development and the implementation of the underlying necessary technologies, which can be considered mature for single range installations. Initial effort related to the maximization of the benefits of the usage of cyber ranges (in particular for what regards the training aspect) has been made. Initial effort on the analysis of benefits and technology challenges of federation of cyber ranges has been made. Running projects cover different aspects of cyber ranges. CYBERWISER.EU project seeks develop an educational, collaborative, real-time civil cyber range platform, while CYBER-TRUST seeks to address the security of IoT devices with the intent to develop a cyber intelligence platform. REACT project focuses on the proactive measures to identify and reach to potential attacks and on the fortification solutions to the potential targets with passive and active defence approaches. Cybersecurity training in specialized environments, is addressed in “SU-DS01-2018 - Cybersecurity preparedness - cyber range, simulation and economics”. The call is considered a continuation of the topic DS-07-2017, with the intent to develop, test and validate highly customisable dynamic simulators serving as knowledge-based platforms accompanied with mechanisms for real time interactions and information sharing, feedback loops, developments and adjustments of exercises. The three projects funded under this call address different domains. SPIDER addresses the 5G network and its services. The FORESIGHT project aims to develop a federated cyber range solution that collaboratively brings unique cyber security aspects from the aviation, smart grid and naval domains. The third project Cyber-MAR focuses on the maritime logistics value chain.

	Cyber ranges is also addressed in a more comprehensive way in projects that support the creation of a European network of cybersecurity centres of excellence, such as SPARTA and ECHO, one of whose objectives is the creation of a federated Cyber Range at European level.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	An interconnected and secure system requires understanding the implications of the relationships between devices, services, humans and a correct evaluation of cascading risks and effects. Currently cyber ranges are used in an ad hoc manner, meaning the "customer" knows it is important to have hands-on experience in a simulated environment, yet there are no clearly set competence building guidelines and expectations, cyber exercises and drills usually focus on either segments of cybersecurity measures (e.g., Detecting attacks with end-point security solutions) or on how to carry out attacks (hacking and understanding offensive tools and tactics (TTXs)). While these aspects and competences are important, they don't simulate real life situations and usually are not accompanied with a learning curve. Investments should be targeted on several layers and levels and enforcing implementation of cyber range and simulation-based competence building to be addressed as an overarching investment. Also supporting legislative environment development should be researched and implemented to foster the usage of cost-efficient cybersecurity measures. **Economical/strategical R&D.** Currently there is no standard how to measure cyber resilience of any given organisation as a whole (people, processes, technologies). There are frameworks (ISO27001, NIST, ITIL, etc), however the actual true level of resilience of the organisation is only based on questionnaires and not on measuring evidence based operative capabilities and capacities. Cyber ranges and cyber exercises should serve as "security-as-enablers", meaning they should highlight where the focus point should be when enhancing cyber resilience at any given organisation. Having the proper underlying knowledge transfer methodology and supporting technical capability, organisations should be able to understand their current level of cyber resilience in the context of current and future cyber threats affecting business continuity. This can be achieved by researching methodologies and technologies to cost efficiently create simulation environment of a client infrastructure (like a Digital Twin in manufacturing), have Cyber Threat Intelligence (CTI) based threat simulation, where current and future threats are identified and mimicked along with accompanying tools and tactics and the different possible prevention, mitigation, BCP/DRP solutions can be modelled and evaluated along with the technical and human operative capabilities. To support this concept R&D efforts more improvements need to be done on the technological and soft offering of cyber ranges: **Virtualisation and contextualisation.** Efforts should be spent on improving the flexibility of the private and public cloud from a virtual

	networking perspective and a virtual machine contextualization perspective. How can the actual networks be cost efficiently mimicked, how can cyber ranges secured (simulation results contain vulnerability and sensible information!), how can technological, methodological best practises be publicly shared, how can current and future asset investments be tested and evaluated (eg. before investing in hardware or software solutions they can be tested in a cyber range how their integration impacts the current network, etc). Specify an Open API for data interoperability in AI processing of heterogeneous sources of data that will ease threat detection and the implementation of coordinated reactions to attacks by using a standardized interface for various sources of data from different system owners. The open API shall also enable AI engines to combine complementary data sets, such as security logs from real deployments, honey pots, cyber range activity logs, as well as human generated data, such as breach identifications by CISO, Data Protection Officer or end-users. It shall enable AI engines to process larger data sets to identify and share new patterns and signatures of cybersecurity attacks. It shall also enable to replace and test various AI engines without altering the underlying deployments, enabling easier comparative analysis and benchmarking. This API shall serve as cornerstone for standardization. **Hardware.** From a hardware perspective, modern storage solutions can offer important benefits to cyber range platform. The applicable cyber ranges should allow easy integration of any hardware for quick implementation of a given scenario. At the same time, the hardware (e.g., smart-meter or RTU in energy sector) needs to allow (either by standard or guideline) easy self-virtualization from a given state/snapshot or ideally come with a digital-twin template (which would be run/deployed over a digital-twin engine present with upcoming modern cyber-ranges). However, this is still a non-standard approach based on isolated experience from cyber range providers but without a real understanding and dedicated support from the hardware vendors. This requires often “home-made” solutions to optimize the usage of dedicated performant hardware with cyber range platforms. **Software.** Software challenges are twofolded. There are the softwares that operate the cyber range and then there are the software solutions that are simulated in the range itself. For the later there is a clear gap on adapting existing licensing schemes to the need of cyber range services: for example, it is extremely complex to find feasible solutions to leverage on multiple Microsoft licenses, reusable on many different scenarios and covering different version of operating systems and products (a necessary feat to simulate a plethora of different real environments). Actually, all solutions need to be “home-made”, since no direct support on cyber range specific needs is provided by most vendors. From and R&D objective out of the box solutions are missing for automated CTI/evidence based background scenario generation with AI support for addressing competence building based on organisational features and assets, supporting automated technical scenario setup based on the background scenario and participants (provisioning, networking, human/machine interactions, etc), automated participant evaluation based on competence building KPIs,

	supporting tools for AI based attack simulations (injects, dynamically adapting scenarios based on performance and cyber killchain, etc). Also the aspects of obsolete/legacy softwares that might be used in the infrastructure (especially in the OT environment) shall be investigated, how to simulate a SCADA/PLC solution from a vendor already unavailable, etc. For the software managing the cyber range it is necessary to have easy to use UI/UX and a good user experience in order to make cyber ranges as a generic tool for upskilling, competence and resilience building. **Big data and AI.** Research and develop AI that supports CTI based scenario generation, analyses potential threats through simulations, analyses performance and evaluates participants. AI should also be able to aid organisations by constantly monitoring and setting up simulations of attacks affecting their current (and before integration: the future) network and services enabling cost effective risk evaluation. Data along with threat intelligence collected through cyber range activities (simulations, exercises, etc) shall be used for improving cyber resilience, sharing best practices (anonymised) and enabling cyber ranges service providers and consumers to benefit from a common knowledge base (and/or access to it). **Harmonisation and interoperability.** Effort on standardizing key technological aspects of cyber range (for example, the definition of cyber range scenario as a meta-language) could simplify the development of new cyber range technologies. Given the potential benefits of the usage of cyber ranges for R&D and for testing & certification, ad-hoc research should be made in order to properly explore these possibilities, eventually within the Digital Single Market initiative and the EU Cybersecurity Certification Framework. Consistent effort should be put on researching for the maximization of the benefits of the usage of cyber ranges within competence building contexts. The impact and the interoperability of cyber ranges and exercises should be researched in a holistic approach, measuring impact on interconnected level of the different aspects of cybersecurity (people, processes, technology). A common standardised language (meta, technological, competence building) shall be developed enabling potential cyber range users to benefit from the various available soft content with a high return on investment. Creation of "cyber-range content ecosystem" for creation, sharing and updating training scenarios and past completed exercises (e.g., replay/review the exercise to improve strategy or find gaps in personnel, technology, policies later on), which are the key asset, not the technology itself. Taxonomies/methodologies for cyber ranges, trainings and cyber defence exercises (CDX) to setup and foster common base of communication. Create open format for content to support sharing and encourage development of open source cyber ranges and related tools to reduce costs and support competition.

	Methodology. Effort should be put on using cyber ranges and exercises as enablers for the organisation in order to map their current capabilities and capacities, providing a strategic plan and a clear understanding of the current and future threats and company's performance at the end of a cyber exercise for decisionmakers. Research is needed to develop the supporting shared methodology serving as a cornerstone of strategic decisions and prevention tool. Exercising and drilling methodologies shall be developed identifying risk assessment KPIs and supporting simulation solutions. **Emulation capabilities**: while virtual/hybrid cyber range platforms are rapidly improving their capabilities in terms of scenario definition, the availability of advanced tooling to better emulate the reality is somehow behind, Advanced traffic simulators, for example, are available in the market, but usually out of an acceptable cost for most providers and exercises. Cyber-range industry could highly benefit from additional research in the field, spanning from IT to sector-specific emulations. R&D&I efforts are required for virtualisation classed (HW/SW, OT, protocol/interface, etc) emulations as currently such solutions are either unaffordable for majority or not covering their needs. **Competence building.** Cyber ranges should be an integrated part in the digital competence building programs within Europe, both in high level education and training sector, providing the hands-on knowledge base for the participants. Cyber ranges should help the targeted skills and competence development of the participants along with the extended thinking when approaching IT infrastructures and functions. Simulation based competence building should be easy to integrate into existing educational and training curricula, **Legislation, policy making, insurance, risk assessment and national security.** Integration of simulation-based cyber resilience measurement and competence building should be integrated into cybersecurity requirements within the Digital Single Market, a common classification system shall be developed allowing organisations to understand the potential cybersecurity risks when connecting/making business with each other. Insurance companies and companies responsible for compliances shall research the risk assessment framework to develop the capability of understanding evidence-based risk assessment and develop accompanying solutions. CSIRTs/CERTs shall become ambassadors of simulation based competence and capability building, enabling them with tools and solutions.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	Benefits related to the usage of cyber ranges are actually not well understood/researched and only barely perceived, mainly due to the fragmented usage of it. The capability to leverage multisector training, R&D and testing & certification activities, at a fraction of cost and much increased agility with respect to any testbed based on physical assets or on old virtualization approaches seems to be crucial in the actual days and even more in the next future. A greater knowledge about the cybersecurity of the programmable electronic and radio/communicating systems that we can currently find

	ubiquitously can be achieved, especially in those critical sectors that benefit most from digitalization: Healthcare, Energy, Finance, industry 4.0, Smart cities, 5G or Autonomous Driving. Each of them has its own technical challenges, but humans are reaching a point where the lack of cyber security may be affecting the transfer of technology to the Market due to low confidence in safety. Having technologies and training services, operated internally or by third parties, should bring the social and technical perception to a higher level of confidence, both in the initial authorization and in the quick response to new challenges. Otherwise, it will be difficult to comply with the implementation roadmap of these technologies with the enormous economic and social impact that this can imply for Europe as a global competitor. On an EU level a common framework and understanding of the level of cyber resilience of any given organisation can be achieved. Also decision making can be based on outcomes of actual performances and simulations enabling stakeholders to invest into the domains where the highest return on investment can be achieved and enabling them to measure those investments. Cyber ranges and exercises are not just a great tool to cost efficiently understand the possible impact of a potential cyber-attack, but also can outline the ways to enhance resilience in the most cost-effective way, providing capability and capacity insights along with required improvements. Also cyber ranges and cyber exercises enable new business services and solutions while raising the level of cybersecurity within the EU. Organisations responsible for national security shall benefit from the results also as they can be informed of what potential threats critical infrastructure operators pose and can also make recommendations before applying certain vendor's solutions into national infrastructure.
Starting TRL / Expected TRL	**Starting TRL:** 4 **Expected TRL:** 7-8
Timeline (2025/2027/beyond)	2025

Cyber-physical systems security and cyber secure pervasive technology

Horizon Europe – HEU.1.E	
Specific Priority	**Cyber-physical systems security and cyber secure pervasive technology**
Description of the challenges – why is it important?	The advent of technologies like IoT, 5G or Cloud/Edge Computing promises to realize the vision of a hyperconnected society, in which humans and devices compose complex interconnected systems leading to strong cybersecurity interdependence. We could also imagine a machine economy in which multiple objects (either legacy devices or new operational technologies), even objects embedded in our body, will be able to connect with other, make transactions, take decisions by themselves and even exchange tokenized value among them. It is in this context where we need to consider Cyber Physical

	Systems (CPS) and the cybersecurity challenges associated with them. Indeed, a CPS is composed of: (i) a cyber part, mainly based on software and control elements, (ii) an interconnection part composed of interfaces between the software world and the physical world, and (iii) a physical part that interacts with the physical world via sensors and actuators. These different parts communicate via different kinds of wireless and wired networks. Complex cyber-physical systems include several components and establish multiple relationships, which in turn complicates not only the integration of security mechanisms but also the measurement of their effectiveness. Security vulnerabilities in one component could affect other components and trigger cascading effects due to unforeseen threats, which might compromise the whole system. Since CPS are often integrated into critical systems, like industrial, transportation or healthcare ones, these systems have to be protected from external and internal threats that come with Internet connectivity. Traditional "physical" devices such as HVAC, lights, video surveillance, ID cards, biometrics, access control systems and more are now IP-enabled. This creates an entirely new set of vulnerabilities that hackers are already exploiting and will continue to exploit, so as to access a company's network, e.g., to steal business or customer information. In the case of critical systems that have safety properties, it is critical to understand how the violation of security properties can affect safety properties. This interaction between safety and security properties must also be analysed in a certification context (EU Cybersecurity Act). The convergence between safety and security issues needs to be further studied to build appropriate models, and corresponding implementations and techniques for testing and validation in order to ensure the resilience of such systems. Resilience in this context is critical, and response and recovery approaches are still considered a challenge for the community. Disruptions in the operation of EU countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems. Recent events demonstrate the increase of combined physical and cyber-attacks due to their interdependencies. For example, a cyber-attack may be leveraged by a physical attack, or vice-versa, resulting in the amplification of the overall impact on the target organization and, potentially, on the civil society. Nevertheless, we should not limit the role of CPS in critical systems, we should consider the specific threats and challenges associated to various domains. To give an example of the scale of the challenges, it is worth considering the healthcare domain, as more and more of these devices are starting to be embedded in our bodies, such as pacemakers to treat cardiology problems. Other novel technologies, such as nano-sensors and nano-robots, are being developed to detect diseases and put medicines in proper places inside our body. In this very critical domain, challenges are not only limited to the protection of these technologies and – by extension – the well-being of the users, but also assuring that the information of the users remains private.

Digital Living & Working	Exceptional situations such as the recent Covid19 pandemic reflect the importance of protecting CPS systems, especially medical systems and devices that can collapse due to a security breach, putting many people's lives at risk. Furthermore, some of the technologies mentioned, such as nano-robots, can help in these types of situations to fight the virus and even create vaccines, so security flaws in them could not only slow down or reduce positive effects, but could even be fatal. The security of CPS systems is crucial to protect critical infrastructures that support essential services, such as electricity, water or gas, and even the supply of food that allow an adequate quality of life and an adequate working environment. However, working from home also increases the attack surface and the security controls that are normally implemented in a workplace may not be available from home, providing easy targets for attackers who want to get sensitive information or cause damage to the systems. Employees will be exposing companies to greater risks to the extent that they are not mindful of workplace safety and security. In the case of Covid19, the number of people working from home has increased considerably, dramatically increasing digital activities and, therefore, the number of nodes that can be attacked and the information that can be leaked.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Current modelling tools do not capture the complexity and high variety of relationships inside a CPS. Some schemes, such as the NIST cybersecurity framework, take into account the relationships between different security properties and requirements. NIST CPS framework proposes a formal language to describe security assets in a standardized way. This language has been further used to develop a formal reasoning tool about the security of a system. Cascading effects are contemplated in different areas, such as the recovery part and in other aspects related to response and protection, where controls should be considered to avoid the possible risks associated with cascading effects. Other tools following the model-based testing techniques use high level models to generate tests, facilitating the security measurement. However, none of these tools allow for capturing all the complexity of CPS. Another aspect to consider is that critical systems and CPS are often dependent on complex supply chains, which adds an entire class of threats that must be taken into account while assessing and treating risks. Therefore, supply chain protection (physical and cyber) is nowadays mandatory when managing the security of a critical infrastructure. At present there are various recommendations and standards in this area, yet they mostly focus on performing risk analyses and integrating traditional security procedures. While the overall security governance for critical infrastructure is slowly converging towards a horizontal security model, involved teams and tools remain separated.

	Moreover, to model such vulnerabilities, models of the system under test, and of the devices and components constituting it, need also to be researched and developed.
Effort until now	There have been a number of European projects around the topic such as AMASS (https://www.amass-ecsel.eu/) that aim to lower certification costs for CPS in face of rapidly changing features and market needs, and the ongoing project certMILS (https://certmils.eu/) that aims to develop a compositional security certification methodology for CPS. On the other hand, the H2020 ARMOUR project (https://www.armour-project.eu/) applies model-based testing approaches to large-scale IoT systems. However, ARMOUR is focused on protocols and simple devices, and does not capture the complex interactions between different components and vulnerabilities. Finally, it is worth mentioning the set of H2020 calls (SU-INFRA) specifically targeted the correlations between cyber and physical security within different sectors.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	It is necessary to think how to build cybersecure CPS from the start with secure architectures and communications means, being able to trace the identities of objects that take part in specific transactions, to know the level of cybersecurity of an object (as easily as we know the level of energy efficiency of a device), how it is updated and how liability issues are resolved if something goes wrong. It is also necessary to develop methods for better resilience and security co-design of products and services, including support for safety/security certification from the beginning of the design process. There is also a need for the development of a modelling framework able to capture the properties and dependences of the CPS systems. This modelling framework should allow to model components inside CPS and their relationships, and should be able to represent the complexity of interconnected ICT systems, dependencies of vulnerabilities, propagation, modelling of any asset and ways to link abstract models with their corresponding real systems. It should also provide a way to generate tests from a model in a way to be able to measure the security of CPS, facilitating this process. Finally, of real interest is using approaches able to capture key security notions (assets and their value, components vulnerabilities, relationships among components and consequent impact, attacker profiles, privacy) to exchange information about rules/requirements/threat-intelligence, for example, using the NIST CPS framework language or Meta Attack Language. Also, we need dynamic and autonomous approaches for prevention, situational awareness, resilience and traceability, all of them working in highly automated manner.
Expected benefit; strategic or economic impact	Improved protection of critical systems in industrial, healthcare and transportation domains, that are currently vulnerable to many different types of attacks, and more secure interconnected objects with better

➔ What can be achieved?	knowledge of the level of cybersecurity of autonomous and connected objects and the corresponding cybersecurity of systems of systems. Other potential benefits are: • Automation of the security testing in order to increase its usage in the industry and facilitate the security comparison among different CPS, allowing the consumers to decide on what to buy depending on required security properties. • Improvement of the security assessment of CPS, due to the capability of capturing collateral effects of an attack and dependencies among components. • Security improvement, since it will be possible to know the weak points of CPS, allowing to protect them better. • Models can be used during the whole lifecycle of CPS to detect vulnerabilities, apply security measures and generate forensic reports, as models enable the formal definition of security properties, cyber-physical attacks and incidents, physical and cyber behaviours, assets, as well as the system composition and effects of attacks at system-level. • The creation of competitive market in which business continuity is guaranteed regardless of the type of context.
Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 6
Timeline (2025/2027/beyond)	In the case of improved and model-based threat / vulnerability identification with the consideration of effects from safety towards security the timeline could be 2025-2027. In the rest of the cases BEYOND is the expected timeline.

Application domains and infrastructure

Cyber resilient digitised infrastructures

Horizon Europe – HEU.2.A	
Specific Priority	**Cyber resilient digitised infrastructures**
Description of the challenges – why is it important?	Due to their vital importance to nations' societies, security and economies, the cyber-physical protection of critical infrastructures is a challenge of utmost importance. While technology enables innovation, efficiency and effectiveness, critical infrastructures need to have state of the art IT security and risk management systems that is at the same level and do not hamper the new services/benefits technologies bring. This challenge is even more complex due to the following specific requirements of the digital era: • requirements for high-availability and controlled performances of such infrastructures; • presence of legacy systems / components that are not secure-by-design or may become untrustworthy over time, and that can endanger the whole system

	• high complexity of modern systems, interconnecting heterogeneous technologies (including IT, OT, edge / cloud computing, IoT, etc.) and stakeholders across levels and organisations; • a heterogeneous regulatory scenario, where there is limited enforcement and insufficient alignment across sectors. In order to meet this challenge, the most urgent needs we have identified are: • developing monitoring, reporting and mitigation solutions that take advantage of advanced data analytics and artificial intelligence capabilities, always taking into account privacy issues; • new approaches for data protection such as data-centred security. This would allow the data exchanged between organizations or users to be always protected cross-country; • addressing and establishing industrial resilience (from prevention to response / recovery) embracing the whole CI lifecycle management process. This includes the distributed supply chain, while not interfering with operations; • devising lightweight, robust, autonomous, and isolated virtualization environments capable of securely orchestrating appliances in heterogeneous hardware and software architectures with or without a central trusted authority. It should also pay specific attention to integrating and balancing the security and privacy of innovative architectures and the need of increasing trust in services, especially edge computing.
Digital Living & Working	The digital era has brought many benefits to organizations. On the one hand it allows their employees for more and better remote working at different levels (e.g. developers, managers, business, etc.). On the other hand, data acquisition, manipulation and management can be done cross-country, which made possible to share and use it in different places. These two basic functionalities have attached cybersecurity and privacy issues that, if not fulfilled, would harm their evolution and adaptation to new technologies. Therefore, having a change of paradigm to data-centric security (so the data is always protected wherever it is located), better tools for sharing and communicating supporting different legislations (e.g. country-based, organization-based, etc.) is mandatory if we want society to move forward in the digital era. Digital transformation and market changes in case of exceptional events, such as a pandemic, demand for increased agility and improved visibility in the entire value chain to react to changing needs of the critical infrastructure in an agile manner. A global visibility of the supply and production chain, and a fine-grained management of the digital infrastructures could be important to allow for reconfiguration and adaptation to a hard-to-foresee situation.
BASELINE	
What has been done so far (in EU	At research level, the employment of data (and Big Data) in the security field is relevant, especially concerning cybersecurity. Unfortunately, its application in the CI area remains relatively limited.

and in the World – EU position)	Advanced data analysis techniques available in other research sectors (such as Artificial Intelligence for Natural Language Processing) are proving to be helpful in increasing the situational awareness of operators and players. It is important to acknowledge that Europe has not yet succeeded in creating solid references neither in big data and hyper computing technology nor in public cloud services. This lack of a strong trusted European value chain in digital technology limits adoption of such technology by critical infrastructures and operators of essential services in Europe. Indirectly, it also penalizes the European Cybersecurity industry by creating a competitive disadvantage against North American or Asian vendors who benefit from a greater synergy effect between computing and security technologies. As an example, when the cloud computing started its way in the digital word, the lack of European leadership has brought as a result that nowadays almost all cloud providers are from outside of Europe. This allows them to take advantage of the data generated of Europe and lead any initiative in this field. Therefore why it is necessary Europe push the different technologies for the future digital society. However, the cybersecurity perimeter is being constantly redefined by the convergence of IT and OT, as well as by the progressive spread of new information sources, e.g. IoT. This evolution brings a tight integration between physical- and cyber- security, setting the need for innovative approaches considering the combined effects of the cyber-physical integration. European industries are working to adapt the IT technologies and to open the OT domains. This is currently being done at the level of each single provider and/or protocol, while still lacking a domain-level approach needed to proactively protect the next IT-OT infrastructures. Breaking silos and improving interoperability will be essential to enable collaboration: characterizing systems/components assumptions and guarantees in terms of security will favour a more secure integration and more objective evaluation of risks and attribution of responsibilities, including a clarification from the legal perspective. While we have highlighted above a certain disadvantage of European industry in matters of digital technology, it is to notice that such a disadvantage does not apply in traditional OT. In particular, European players own the largest share of the ICS market, slightly ahead of US vendors and far ahead of Asian players. The convergence of IT and OT into IoT must be taken as an opportunity for Europe to step back into digital technologies with an advantage in sensitive and critical IoT inheriting the tradition of excellence that European players have sustained in OT. Concerning the application of edge computing to CIs, Europe has been leading the definition of Edge Computing infrastructures through the development of the ETSI Multi-Access Edge Computing (MEC) set of standards[1], which focus on the deployment of the Edge over cellular infrastructures.

[1]Industry Specification Group (ISG) on Multi-access Edge Computing (MEC), https://www.etsi.org/committee/1425-mec

	Also, the integration of Edge infrastructures in 5G deployments is being actively studied from the research community[2,3]. European companies are actively participating in consortiums, such as the OpenFog consortium (now joined with the Industrial Internet Consortium) and the Linux Foundation-managed LFEdge organization, whose goal is to establish interoperable IT frameworks for Edge computing for different scenarios. As security and privacy is a priority for these consortiums and organizations, various security components have already been defined. Other active lines of research in Europe in this domain include fully homomorphic encryption, computing on encrypted data, secure multi-party computing, and protection of machine-learning models. Please refer to the priority on Cryptography and Data protection for additional details.
Effort until now	The most significant efforts towards secure infrastructures have been made in the frame of H2020 INFRA calls such as INFRA01 and INFRA02 and preceding CIP calls. While the protection of critical infrastructures against cyber and physical threats has been intensively addressed, it is important to note that few of the funded projects have effectively addressed the area of research that lies in providing intrinsic security of cyber-physical systems which form the new attack surface of critical infrastructures. A general confusion has been to think that cyber-physical threat scenarios would be addressed effectively by simple aggregation of physical and digital security layers. Concerning data analysis for the security of CIs, complexity and huge amount of data to be processed still require the intervention of human experts to effectively evaluate the real seriousness of a warning or alarm, even when sophisticated data analytics tools are employed. However, the H2020 INFRA01 topic encourages the convergence of the cyber and physical world through a holistic security perspective. To show an example, the INFRA01 project INFRASTRESS is focused on exploiting the overall information space, including relevant data and events from both cyber and physical landscape. The adaptation of new IT technologies to OT domains has been explored mainly through public financing, as in the case of the H2020 project ECOSSIAN. As an example of technologies applied in CIs, the work done in Edge computing has been explored in several EU projects. A short list is: • 5G deployments (SESAME, 5G-ESSENCE, 5G MiEdge) • specific scenarios including manufacturing (FAR-EDGE, QU4LITY, FORA, COLLABs), vehicular systems (Hailo-8), smart grids (ENIT Agent 2.0), healthcare (InteropEHRate), and data analysis (DITAS) • security: ESCUDO-CLOUD, Secure-SCM, PAPAYA, mF2C

[2] 5G AT THE EDGE, https://www.5gamericas.org/wp-content/uploads/2019/10/5G-Americas-EDGE-White-Paper-FINAL.pdf
[3] A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art, https://arxiv.org/pdf/1906.08452.pdf

	Although it must have been in scope of many initiatives, the problem of addressing mismatching lifecycles between IT and OT doesn't seem to have been solved. In particular the lack of applicable methods for system-level qualification and change management across software and hardware layers continues to slower down the adoption of digital technologies by critical infrastructures. In many cases, this plays against both efficiency and security, as it forces critical infrastructures to keep using obsolete equipment and operation modes for much longer than they were designed to and wait for the failure to upgrade instead of anticipating and preventing disruptions. The INFRA02 project IMPETUS works on enhancing the resilience of cities in the face of security events in public spaces. There is a growing concern of security and ethical threats that exploit interconnected city grids of sensors and big data technologies, and the project will address this within the complete physical and cybersecurity value chain (detection, simulation & analysis, intervention).
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	Effort should be focused on: • **achieving effective, real-time situational awareness** through advanced (big) data analysis: automating the detection / mitigation of exploitable vulnerabilities and the evaluation / assessment of legacy systems; introducing real-time analysis for CI security, data correlation among different stakeholders, forensic tools for cyber incident analysis. Digital Twins and Distributed Ledger Technologies should be also supported; • **securing the whole CI lifecycle**, by means of: developing suitable and usable processes and tools to assess the security of systems and protect components; establishing interoperability standards, secured infrastructure and component integration (including legacy components); foster cybersecurity training and education for all end users accessing/maintaining the systems (e.g. developers, technicians, operators, etc.); • **addressing the security issues introduced by 5G deployments and other IoT/edge computing architectures** by: integrating existing security/privacy components, distribute decision making and collaboration solutions into real-world Edge infrastructures and architectures; improving situational awareness, edge forensics and digital evidence management; supporting security- and privacy-as-a-service solutions by means of orchestration services and the creation of a community in the field of edge nodes; researching on P2P protocols; contextualising and updating the current results on computing and querying over encrypted data, its relevance in cloud-based deployments; multi-party secure computing, and related fields, with a focus on infrastructures rather than applications.

Expected benefit; strategic or economic impact ➔ **What can be achieved?**	• **Improvement of the identification and reaction to cyber incidents** through the sharing of information among the relevant stakeholders involved in critical infrastructure management and operation. • **Increasing trust in the 4th industrial era** where the risks of cyberthreats and vulnerabilities can considerably grow and impact business continuity, economy and, most importantly, social well-being, improving global control and optimization of the value chain, increased preparedness to changing markets and ability to withstand to production reconfiguration at a global scale. • **Creating an ecosystem of secure, resilient and privacy-friendly Edge infrastructures** (for research, industry, university and society at whole) that serve as a foundation for advancing strategic areas such as the Industry 4.0, vehicular networks, and the Internet of Things. • **Promote European leadership in secure and privacy friendly advanced IoT applications** and even beyond, towards any type of distributed applications.
Starting TRL / Expected TRL	**Starting TRL:** 3-4 **Expected TRL:** 7-8
Timeline (2025/2027/beyond)	2025 / 2027

Secure Quantum Infrastructures

Horizon Europe – HEU.2.B	
Specific Priority	**Secure Quantum Infrastructures**
Description of the challenges – why is it important?	In contrast to classical cryptography where information is protected by relaying on the computational hardness of mathematical problems, in quantum cryptography it is based on the physical layer and can, in principle, provide for information-theoretic communication security. In particular we speak about Quantum key distribution (QKD) as a form of Quantum information communication. This is allowed for by the laws of quantum mechanics (in particular Heisenberg's uncertainty principle and the no-cloning theorem) which renders undetected eavesdropping virtually impossible. The promise of un-hackable long-term security, even at the presence of fully-fledged universal quantum computers is sparking a growing interest in quantum security, from several perspectives. After significant progress has been made on the technical fundamentals of QKD, the next step is to bring it into larger systems[4]. While 5G certainly is a topic for security developments at high TRL levels, it is important that Horizon Europe also supports the development of communication infrastructures targeting the era of quantum computing and post-quantum communication. This requires significant investment in topics such as Quantum Key Distribution (QKD) which is likely to be the most realistic application of quantum

[4] The topics of post quantum or quantum resistant crypto appear in the Cryptography priority.

	communication in a near future, but also computational security alternatives such as post-quantum cryptography, a field where Europe has been underinvesting for now compared to US or China.
Digital Living & Working	
BASELINE	
What has been done so far (in EU and in the World – EU position)	Attempts to build a pan European started with the initiated "Quantum Communication Infrastructure" – an initiative (backed by the European Commission and currently signed by 24 EU member states) aims to build a pan-European quantum-communication infrastructure based on both fibre and satellite links. At the same time there is still not complete overlap between the QKD community and the classical ICT security one, and efforts should be devoted to the integration of the communities as well as of the corresponding technologies. China has already spent nearly 1bn US$ on quantum research with significant progress on establishing long-range QKD links[5]. To avoid global dependency in highly sensitive application, it is necessary to develop independent European technology. It is important to note that efforts in the development of a European Quantum Communication capacity has been yet hampered by the lack of coordination between initiatives addressing Space and Terrestrial segments. Also, while unconditional and perpetual security appear to be the promises of quantum communication technology, it is to be noted that the challenge has been up to date fostered by physicists, while security professionals essentially remain aside of leading initiatives in the field. A possible consequence is that state of the art QKD experiments fail to address a number of basic attack scenarios such as Denial of Service (DoS) attacks and side channel attacks on repeater nodes.
Effort until now	The European Commission has launched the Quantum Flagship initiative. In matters of quantum communication, it is important to highlight the leading initiatives of Austrian and German Governments as well as some theoretical studies carried ESA and the European Commission, including the project launched early 2020 by EC for the definition of Overarching System Architectures of the European Quantum Communication Infrastructure. Preceding projects are known: • in terrrestrial segment as OpenQKD, CiviQ Quantum Internet Alliance, Qrange, UNIQORN • in space segment as ESA LEO Mission studies Quartz and QKDSat. Some initiatives in field of Optical Comms come in support of QCI development such as TELEO – GEO feeder Demo.

[5] https://iopscience.iop.org/article/10.1088/2058-9565/ab4bea/pdf

	In particular, the European Commission has also launched the OpenQKD project, a pilot project for the QCI infrastructure aiming to demonstrate a wide range of QKD use-cases around Europe. Recently, CEN CENELEC has recently launched a Focus Group on Quantum Technology to ensure support the support of standards for the deployment of Quantum Technology in industry.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	Consolidated the European Backbone for QKD (reaching all the member states) connecting the main critical infrastructures and strongly integrated with classical security environments. Innovations in the area of adaptation of classical cyber security for quantum advent will focus on the analysis of quantum technologies and their impact in classical security mechanisms as well as how classical mechanisms (including crypto) can help in quantum computing and communication security. This entails the study and development of scenario-based risk assessment frameworks. Based on those, mitigation strategies should be developed. Innovations in the area of QKD protocols and Quantum Communications, for instance: • Device independent QKD • Satellite quantum communications • Continuous variable QKD • System Architectures for Quantum repeaters and secure endpoints • Hybrid (classical-quantum) communication architectures • Large scale demonstration of QKD infrastructure Other areas are: • Develop a Quantum Technologies supply chain in Europe to strengthen European autonomy. • Develop appropriate risk assessment and architectural frameworks for a resilient European QCI across space and terrestrial segments • Develop Quantum Key Management technology to support European Quantum Communication Infrastructure deployment • Launch European hybrid cryptography developments and establish European standards.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	The global quantum cryptography market is expected to grow from USD 285 million in 2018 to USD 950 million by 2024, at an Annual Growth Rate of 15% during the forecast period. Quantum cryptography market includes the growing incidents of cyber-attacks in the era of digitalization, increasing cyber security funding, rising demand of next-generation security. A European QCI will enable unconditional security of communication between Governments, Institutions and Essential Services in Europe.

Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 7
Timeline (2025/2027/beyond)	2025 – 2027

Cyber secure future communication systems and networks

Horizon Europe – HEU.2.C	
Specific Priority	**Cyber secure future communication systems and networks**
Description of the challenges – why is it important?	New autonomic and context-aware security frameworks are needed to be orchestrated and enforced dynamically, at various scales and layers in future communications systems and networks. Virtualized defence mechanisms (either proactively or as reactively) are to be enabled, according to the circumstances, in upcoming heterogenous networks (e.g. 5G), systems (CPS/IoT) and computing architectures (Fog-Edge and Cloud). The orchestration will need to face the challenge to interface with diverse and distributed control elements, e.g. IoT Gateways, (network orchestrators (e.g. NFV-MANO), Fog-Edge entities, SDN controllers, thereby enforcing dynamically the security enablers in the network/systems to mitigate evolving kinds of large-scale distributed cyber-attacks. Additionally, security solutions are supposed to be resource-aware and –efficient security management for scalability, reduced environmental footprint and wide applicability in future networks. 5G and Beyond 5G networks are intended to offer the possibility of integrating different kinds of networks, including IoT, with the possibility of using 5G backhaul to ease the deployment of these technologies. This calls for a redesign, optimization or adaptation of the existing protocols and processes, to secure the communications whilst maintaining interoperability. In fact, security design patterns able to manage IoT/Fog/Cloud specific vulnerabilities and their interactions are currently lacking at EU level. Security patterns should be developed with relation to the growing complexity of the future telecommunication networks, enabling: the integration of connectivity, computing and control; interoperability in convergent networks; cognitive, autonomous and automated network management. Moreover, future communication networks should address the growing concerns of availability (ultra-high service availability against nefarious or unintentional-but-harmful activities/event) and integrity (e.g. impact of untrusted suppliers and supply chains) at EU level.
Digital Living & Working	In COVID-19 ongoing situation, cellular communication data (location/identities) for localization/emergency services is widely used by several countries. Share such data for improving other societal services or create new business opportunities by balancing privacy/anonymity should be defined consistently at European level.
BASELINE	

What has been done so far (in EU and in the World – EU position)	So far Europe has successfully invested effort in cyber-security frameworks that orchestrate security services. For instance, H2020 CIPSEC creates a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of CIs. Likewise, H2020 Anastacia EU project is researching, developing a cybersecurity framework that provides self-protection, self-healing and self-repair capabilities through novel enablers and components. The framework dynamically orchestrates and deploys security policies and actions that can be instantiated on local agents. Thus, security is enforced in different kinds of devices and heterogeneous networks, e.g., IoT- or SDN/NFV-based networks. Similarly, H2020 INSPIRE-5Gplus EU project initiated at the end of 2019 is working on intelligent and autonomous end-to-end cyber security services to be integrated in the 5G networks. It aims to predict, detect and mitigate the impact of current and upcoming threats targeting next-generation networks and leverage on existing tools, techniques and concepts as well as embracing new ones gaining momentum (e.g., AI and ML, Trusted Execution Environments (TEE), Zero-Touch management, liability concepts, DLT). The H2020 5GZORRO project targets a security and trust framework, integrated with 5G service management platforms, to demonstrate Zero-Day trust establishment in distributed multi-stakeholder environments and automated security management to ensure trusted and secure execution of offloaded workloads across domains in 5G networks. The Internet Engineering Task Force (IETF) is working at different fronts to secure the so-called Internet of Things, comprising in some cases very constrained devices and networks. The IETF working group such as LPWAN has not yet focused on security, which leads to the gap of bringing interoperability and security to these networks as part of the future integration of these networks in 5G. IoT/Fog/Cloud security solutions require expert knowledge that can be gathered by means of security patterns providing specific solutions to known/unknown vulnerabilities using secure elements such as Trusted Platform Module (TPM). European standardization organizations ETSI and CENELEC have recognised legitimacy in Europe. ETSI TC CYBER develops standards in order to fill the existing gaps and provide support for defining certification schemes e.g. for trust services, consumer IoT security, 5G networks. ETSI NFV Group is working on security of future networks from the network softwarisation perspective. CENELEC JTC13 provides coordination of stakeholders to ensure consistency and optimize the effort in evolving standardization ecosystem.
Effort until now	Security orchestration of virtualized network functions has been properly achieved in specific domain/silos but has not been yet realised holistically, at scale, in upcoming heterogenous networks and systems, to counter and mitigate cyberattacks. Besides, the autonomous nature of upcoming systems, as well as the new cyber-threats and increased attack surface appearing from new disruptive

	technologies/networks (e.g. SDN, NFV, Cloud, Edge, Fog, 5G, LPWAN…), have given rise to new kind of cyberattacks and security issues, that cannot be solved with the current state of the art in cybersecurity management. In the scope of the European H2020 initiatives, Smartie laid the foundations to securely manage IoT deployments such as Smart Cities. ANASTACIA brings another level of management and security by leveraging SDNs and deploying VNFs related to security on demand. The project SliceNet presents an integrated FCAPS (Fault, Configuration, Accounting, Performance, and Security) framework for end-to-end management, control and orchestration of 5G slices by secured, interoperable, and reliable operations across multi-operator domains. However, several issues still need to be addressed, including authentication, key management, data integrity and storage, risk assessment and management, intrusion detection and prevention.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	• Dynamic and cyber-situational awareness security orchestration of Virtual Network Security Functions (VNSFs). • Deal with security orchestration in heterogenous and cross-border networks and systems, and in any segment of the 5G networks. • Optimal allocation of ultra-lightweight virtual security appliances. • Evaluation of new security protocols are being proposed, for example, in the IETF. • Leverage similarities of some types of networks to the cellular networks (i.e., LP-WAN) and the existing security infrastructure of cellular networks such as Authentication, Authorization and Accounting (AAA) and the use of the Extensible Authentication Protocol (EAP) in 4G and the next, 5G. • Adaptation or integration of novel protocols in these scenarios through the aforementioned established protocols and frameworks (EAP and AAA). • Cognitive, autonomic, end-to-end orchestration of future network services, supporting secure, dynamic computing resource pooling and balancing between the edge and the cores. • Resource-aware and –efficient security management for applicability at various scales and layers in future networks. • Evaluate the security (including risk) at different layers and the dependencies they bring to the deployments. An example could be to leverage model-driven and semi-automated formal approaches to keep risk assessment results up-to-date on change of infrastructure, publication of novel vulnerabilities, observed security events, with minimal effort and high consistency.

	• Define and implement unified certification schemes to justify certain security levels for networks and services to ensure security policy unification across multiple domains. When possible, formal approaches could be leveraged at different layers to certify security with high assurance and manage the flow of security requirements down to implementation and to the different layers of communication. • Holistic security assurance and management across multiple domains including unified threat, risk & vulnerabilities management. • Risk assessment and security/trust assurance in 5G and beyond public network-based emergency critical communication systems. • Privacy/anonymity preserving frameworks for utilization of cellular communication data (location/identities) for localization/emergency services. • Better understanding of cyber threat actors for aligning both high level strategies and company / organization level cyber security strategies and implementation of routine forensics tools in cyber defence environments, enabling legal responses and making cyber-crime more easily actionable by law enforcement. • Security-by-design approach shall be the taken into account as a best practice for developing security and network architecture together.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	• Security defences are orchestrated dynamically and optimally enforced, mitigating in near real-time distributed cyber-attacks. • Holistic security orchestration in heterogenous and fragmented 5G and beyond networks. • Increased trust in the cyber world for supporting digitalization. • Coordinated security management and orchestration across Member State borders. • More trustworthy, reliable and resilient on-line systems, networks and services. • Assured minimum security levels in heterogenous deployments. • Standard based developments and deployments. • Homogenization of the security processes in the convergence of IoT/Fog-Edge/Cloud in 5G. • Scalable and explainable security in diverse, dynamic and fragmented future networks • Integrated mechanisms for seamless root cause and liability analysis to support security governance • Future communication systems and networks applying intelligent software (artificial intelligence, machine learning) for decentralised and automated network, enabling the future data economy • Management, data analytics and shared contexts and knowledge for pervasive threat intelligence and situational awareness. • Increased trust among Member States supported by validated security patterns and certification schemes.

Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 7
Timeline (2025/2027/beyond)	2027

Vertical sectors cyber challenges

Horizon Europe – HEU.2.D	
Specific Priority	**Vertical sectors cyber challenges**
Description of the challenges – why is it important?	While we expect digitization to impact critical infrastructures and communication infrastructures horizontally under the thrust of a bottom-up technology push, we acknowledge that there will remain some sectorial peculiarities which need to be addressed by vertical in a more top-down demand-pull. For this, it is essential to build user-driven initiatives reflecting the needs of future industries in terms of security and digitization. Some foreseeable changes must be addressed here such as: • The advent of recursive and collaborative design techniques enabled by connected product life-cycle management approaches • The enhanced use of digital twins in design, manufacturing, operation and maintenance for monitoring, control, optimization and security purposes • The cognification of industrial activities and related challenges to maintain accountability of supply chain actors, whether they are organizations humans or machines • The multiplication of autonomous objects and vehicles which will populate our homes, cities and territories by 2027 • The deployment of smart electric grids and the diversification of energy sources across European territories • The modification of population density, standards of living and age structure which will exert unpreceded pressure on healthcare and civil security sectors • The development of new ecosystems and business models enabled by data economy, circular economy and smart manufacturing trends These changes have significant impact on security needs and requirements which must be addressed with a good understanding of both sector specificities and commonalities. Some specific challenges are identified below for an initial list of vertical domains.
BASELINE	
What has been done so far (in EU and in the World – EU position)	The maturity level can vary a lot across verticals when it comes to security considerations. Some sectors like aerospace have a long-lasting culture of security, mainly driven by safety considerations. Some sectors such as banking have historically been more advanced in preserving confidentiality and privacy. In terms of secure smart

	manufacturing one of the leading industries seems to be the pharmaceutical sector. A number of sectors and subsectors are lagging behind, with noticeable weaknesses both in terms of digitization and security. With consideration for the above highlighted challenge of aging society and population density, investments in secure digital transformation of healthcare infrastructures and other essential services such as water utilities or food industry have been severely lacking. While European Member States like to remind that security is a matter of sovereign relevance, the public sector and namely services to citizens are not always prepared in terms of digital security. Compared to the US landscape and the prevalence of strong sectorial ISACs, the European landscape is particularly weak in terms of security adoption by vertical sectors. To our knowledge, only finance, energy and aerospace have the start of an official ISAC, enabling to grow sectorial maturity in security. Most worrying is the absence of such incentive in public investment programs. A start of initiative was launched in 2019 to build an ISAC for maritime sector. However, this project was only partially sponsored by member states and apparently suffered from extremely low funding incentive, which kept major player aside of the initiatives.
Effort until now	In terms of publicly funded research, the main initiatives seem again to be found in CIP and INFRA call of H2020 Secure Societies. Some useful initiatives driven by sectorial DGs can be mentioned like the EPES call for security of European Electric Power and Energy Systems or the ICT8-2019 call for secure collaborative manufacturing.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	Some important topics for research would be the following: • **Cyber and physical world convergence** – while **cybersecurity** provides trust, protection and safety to all **cyber assets** (i.e., software and information), IT systems are even more interconnected with physical devices. That means cybersecurity can significantly impact physical risks: this aspect should be addressed at any level in any critical sector (clear examples are healthcare and autonomous vehicles). Secure recursive design of autonomic cyber-physical systems of the future will play an important role. • **Interdependencies between critical sectors** – when focusing on the cybersecurity of a certain sector, utmost attention should be paid to considering cascading effects between different critical sectors. To show some examples, energy and telecommunications are well-known event-originating infrastructures that generate cascading effects in many other domains (e.g. transport, healthcare, smart cities, etc.) • **Interoperability and information sharing** – information sharing multi-organization and cross borders (where possible due to GDPR and national policies) should be supported. Sharing cyber-threat information and collaborate on cyber intelligence is an effective way to identify risks and

	responsibilities as well as detect, mitigate and prevent incidents • **Cybersecurity approach at supply chain level** – even in a single critical sector, cybersecurity information is not shared at supply chain level. To show an example, in finance sector sharing information is commonly done for specific areas of the chain, but not across all players of the payment chain. Instead, cybersecurity measures, training and approaches should address all actors and stakeholders, including final users • **Standardisation and strategic autonomy** – standardization efforts are being carried out outside Europe; also, Europe is falling behind in the production of ICT components. Effort should be focused on standardizing cybersecurity practices and approaches cross-sector and cross-boundary, in order to influence the design of the ICT components. • **Circular economy** – decentralized cryptographic developments supporting sharing economy and circular economy. Areas of interest for certain specific sectors would be detailed below.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	The above proposed initiatives would provide Europe with a strategic advance in technological fields of vital importance of the Economy and Society. Economic impacts include the development of new business models for example in the context of Industry 4.0, with potential redistribution of supply chains in favour of European countries. It will reduce dependence towards untrusted Asian hardware and American software. It would potentially contribute to greater independence from Oil and Gas supplies from Middle East and Russia thanks to the deployment of secure smart energy and power systems. It will also enable the development of European Cybersecurity value chain in close connection with lead vertical sector champions which Europe owns in fields of aerospace, automotive, industrial automation, food and pharmaceutical industry. The envisaged solutions will greatly extend the monitoring and protection of the supply chains in operation. Societal impacts include the reinforcement of healthcare system and simplification of social security mechanisms in Europe, in a context of aging population, demographic concentration and migratory pressure. Also, the adoption of modern, safe and secure transportation means, the enablement of more environmental-friendly standards of living and the renaissance of local production enabled by the shift from transport of goods to transfer of data will certainly have a positive impact on well-being and serenity of European citizens. The solutions will provide an improved analysis over the interconnections between physical and cyber security and interdependencies. As a result, they will improve citizens/final users safety, trust and wellbeing.
Starting TRL / Expected TRL	**Start: TRL 3-4** **End: TRL7**
How much funding is required?	

Timeline (2025/2027/beyond)	According to TRL maturity targets. 2025-2027: focus on hyper-connected & hyper-virtualized systems Beyond: focus on autonomic systems

Industry 4.0 and ICS

Horizon Europe – HEU.2.D1	
Specific Priority	**Industry 4.0 and ICS**
Description of the challenges – why is it important?	The main challenges for industry are distributed in the IT and OT areas of application, targeting for each of them specific types of attacks. Additionally, Security requirements of CPS (Cyber-Physical Systems) are growing in parallel to the evolution of their threat landscape. CPS security goes under the umbrella of the Operational Security (OT), a branch of computer security that differs from IT security by several points of view. IT security typically builds up from the Confidentiality-Integrity-Availability paradigm (CIA), while OT cybersecurity starts from the Safety-Reliability-Productivity (SRP) properties. Hence, the safety and security aspects in the CPS systems are tightly connected to each other. Ten years ago, OT systems were physically separated from IT systems and the threat environment was limited. Today instead, we witness a convergence of IT and OT systems: protecting modern CPS installations requires both information technology (IT) and operational technology (OT) expertise[6,7]. Gartner, in its hype cycle for the internet of things 2019, reports the IT/OT alignment at the beginning of the plateau of productivity[8]. Recent literature in the industry area reports that **the cybersecurity approach must be holistic, including cyber, physical and cyber-physical**. In addition, its **governance model must be the same spanning across IT and OT domains[9]**. This is a challenging area still in the focus of the research. This category of problems gained its first momentum with the case of Norsk Hydro[10], where an IT attack provoked OT consequences that rolled into the company up to the governance level, which took the decision to stop the production line[11]. The most critical context where these problems are present today is in the data-intensive industry 4.0 context, where data collected,

[6] A. Gary and U. Prananto, "Cyber Security in the Energy World," in *Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*, 2017.
[7] E. D., "IT+OT Cyber security experts?," 2018. [Online]. Available: https://www.linkedin.com/pulse/itot-cyber-security-experts-daniel-ehrenreich.
[8] Gartner, "Hype Cycle for the Internet of Things, 2019," Gartner, 2019. [Online]. Available: https://www.gartner.com/en/documents/3947474/hype-cycle-for-the-internet-of-things-2019.
[9] N. Benias and A. Markopoulos, "A review on the readiness level and cyber-security challenges in Industry 4.0," in *South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, 2017
[10] G. Fouche and T. Solsvik, "Aluminum maker Hydro battles to contain ransomware attack", Reuters, 2019. [Online]. Available: https://www.reuters.com/article/us-norsk-hydro-cyber/aluminum-producer-hydro-hit-by-cyber-attack-on-tuesday-idUSKCN1R00NJ
[11] E. Kovacs, "Industry Reactions to Norsk Hydro Breach: Feedback Friday," SecurityWeek, 2019. [Online]. Available: https://www.securityweek.com/industry-reactions-norsk-hydro-breach-feedback-friday.

usually at the edge, are passed along a relatively complex chain of technologic handlers. In this context, cybersecurity is mandatory. Unfortunately, the scenarios of modern Industry 4.0 are complex due to all the critical cybersecurity and functional properties that has to be satisfied (CIA and SRP)

IT and OT security are missing a unified security model that spans from the physical up to the governance layers. A unique cybersecurity model that integrates all the layers up to the governance one improves IT cybersecurity in complex organisations. The IT security experts generally agree with this problem (e.g., the Integrated CyberSecurity Governance Model -ICGM- based on the Plan, Do, Check & Act -PCDA- model[12]). However, the miss of an integrated approach affects more OT than IT systems. An attack to a hybrid IT and OT systems usually hits different departments or units of an industry, which are historically not used to exchange information with each other. Consequently, an attack on a hybrid IT/OT system may lead to taking the wrong decisions at the governance level and underestimate the attack's effects (either technical or economic). The problem is the difficulty of estimating the safety state of a cyber-physical system while an intrusion is underway or afterward.

Putting together all the layers of industry that are affected by a cyber-threat leads to a relatively complex model, made of fifteen layers, which starts from the root (the physical layers) and ends with an integrated governance model. The so-called **cyber-terrain model**[13], originated in the military area[14] is gaining its momentum as one of the most complete models for cybersecurity in mixed IT-OT data-intensive contexts.

Furthermore, the Industry 4.0 innovation core is represented by data, in which we find technologies very related to cybersecurity: Artificial Intelligence, IIoT, and Big Data. On the other hand, the innovation vehicle is represented by B2B data exchange. It is crucial to define technical and organizational measures (TOMs) to adequately protect data spaces against attacks from cyberspace.

Finally, another crucial distinction, as we identified at the beginning, is the difference between the IT and OT threat landscapes[15]. The risks and threats of these two worlds are very different, as are the professional communities involved in dealing with them. For example, one relevant ICS threat is the miss or delay of required traffic: while in an IT system this would not be a critical issue, in a CPS it becomes a threat because of the anomalies injected into the system[16]. Literature

[12] T. Cornelius, "Integrated Cybersecurity Governance Model (Plan, Do, Check & Act)", 29 Apr 2019. [Online] Available: https://www.linkedin.com/pulse/integrated-cybersecurity-governance-model-plan-do-check-tom-cornelius

[13] S. Riley, ""Cyber Terrain": A Model for Increased Understanding of Cyber Activity," 7 Oct 2014. [Online]. Available: https://www.linkedin.com/pulse/20141007190806-36149934--cyber-terrain-a-model-for-increased-understanding-of-cyber-activity

[14] R. David, G. Conti, T. Cross and M. Nowatkowski, "Key Terrain in Cyberspace: Seeking the High Ground," in *6th International Conference on Cyber Confl ict*, Tallinn, 2014.

[15] G. Fink and P. McKenzie, "Helping IT and OT Defenders Collaborate," *ArXiv,* 2019

[16] Two significant categories split the threat landscape of CPS: (i) malevolous agents that are injecting anomalies and, (ii) malevolous agents that are injecting normalities. The type (i) refers to agents that, more or less rapidly, shift the operational parameters of the CPS or the entire production floor into the direction planned by the attacking entity (e.g. a malware's deliberate and slow alteration of a turbine speed or an oven's

	reports that anomaly detection solutions for CPS should handle different, real anomalies (i.e., coming from defective processes or actual exceptional events) and injected anomalies (i.e., resulting because of a cyber-attack) in order to cover each of the areas and their joint work. An example of this issue is the study done by Stuxnet[17] in OT security, which demonstrated that malware can inject anomalies n the processes. In addition, the IT/OT convergence involves an increasing need of collaboration between IT and OT professionals in risk management processes. This means that the development of cybersecurity around ICS needs to address the human and organizational side of the IT/OT joint work.
Digital Living & Working	**Impact on Digital Business Ecosystems**. Due to recent COVID surge supply chains will shorten and merge into resilient ecosystems. Global supply chains have long been geared towards keeping quality relatively constant while driving lower costs at every step. This has resulted in significant concentration risk in terms of geographies and vendors for most companies. For example, China scaling down due to Covid-19 and creating a knock-on supply impacts we see today has exposed the lack of resilience in this approach. There is a sharp need for a more distributed, coordinated and trackable supply of components across multiple actors. The shortening of the supply-chains and the foreseen merging of most supply chains into resilient ecosystems is, therefore, a clear trend and a surging threat for cybersecurity. Two important aspects are related to this: the cybersecurity resilience of digital business ecosystems and the technologies to support it. For example, blockchain can guarantee resiliency or data integrity, also for smaller entities. This trend is true for any supply-chain based business but Industry 4.0 is probably the most impacted one. As an example, the International Data Space Association (IDSA) promotes a technological reference architecture for the ecosystems across the EU, but its main scope is the big industries (i.e., I.40). A resilient ecosystem means an ecosystem where the nodes (e.g., small companies) shares data (and value in general) on the base of a measurable trust (i.e., cyber trust) also guaranteeing the data sovereignty.
BASELINE	
What has been done so far (in EU and in the World – EU position)	The work and agendas for Industry 4.0 have been mostly centralized in the different member states, which created their own plans for the digital transformation of their industries depending on the needs and specific area of application. Germany has been one of the bigger supporters as the first country that adopted this strategy. The European Commission has created initiatives to support organizations and member states in the transition to Industry 4.0 and beyond. The Digital Transformation Monitor describes several initiatives of member states in the area in order to facilitate the work between them. Among others, they list key technologies and challenges of this sector. The Commission also proposed a new set

temperature). The type (ii) refers to agents that, controlled by the attacker, are reporting to the monitoring sensors a normal behaviour in the face of a malfunctioning.

[17] D. Denning, "Stuxnet: What Has Changed?," *Future Internet*, vol. 4, no. 3, pp. 672-687, 2012.

	of measures to equip European industry and society with the right tools to deal with cyber-threats. These include a proposal for an EU Cybersecurity Agency to assist Member States in dealing with cyber-attacks, a new European certification scheme for products and services, and further actions to step up the EU's cybersecurity capacity. Additionally, the European Technology Platforms (ETPs) are forums of industry stakeholders, recognized by the European Commission, formed to support the development of innovation agendas and technology roadmaps for several sectors at national and EU levels. The ETPs launched the European Factories of the Future Association (EFFRA), a Public-Private Partnership of industrial associations which regularly publishes strategic technology roadmaps that form the basis for research and technology development call topics.
Effort until now	Until 2020, almost the only specifically purposed EU call, which posed the question of I4.0 security in IT and OT, was the ICT-08-2019 Security and resilience for collaborative manufacturing environments. This call was relatively generic and posed omni-comprehensive arguments. Indeed, a lot of open questions were addressed generically, and no specific arguments were indeed mentioned in the call. As described above the IT and OT threat landscape changed rapidly, OT is now where IT was 10 years ago. Among others we could describe the following projects of Industry 4.0 that are active: Industry4EU (Industry 4.0 for the future of manufacturing in Europe): this project aims to bring together social partners and institutions in an effort to identify concrete actions to turn Industry 4.0 challenges into opportunities. C4IIOT (Cyber security 4.0: protecting the Industrial Internet Of Things):its main objective is to design and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm for minimizing the attack surfaces in Industrial IoT systems. COLLABS (A COmprehensive cyber-intelligence framework for resilient coLLABorative manufacturing Systems): will develop a comprehensive cyber-intelligence framework for collaborative manufacturing, which enables the secure data exchange across the digital supply chain while providing high degree of resilience, reliability, accountability and trustworthiness, and addresses threat prevention, detection, mitigation, and real-time response. COLLABS solution will be validated on 3 real-world use cases from complementary I-4.0 domains: automotive, aerospace, consumer. QU4LITY: it is the biggest European project dedicated to Autonomous and Zero Defect Manufacturing in the Industry 4.0. It will build and demonstrate an open, certifiable and highly standardised, solution for ZDM products and service model for Factory 4.0. It is supported by a cybersecurity framework for protecting the systems and communications between the factories.
DESIRED SCENARIO	

What more should be done? What gaps to be filled? For what reason? How can it be done?	The main gap overall on data security is that it must be guaranteed along the entire data-lifecycle: at acquisition time (where the data is generated), at motion stage (while moving from sensors to the final destination) and at rest phase (once stored, for example in the database). Moreover, security solutions must guarantee CIA or SRP paradigms across all the layers from the physical lowest to the governance upmost layer. Several big players are increasingly getting interested into the market (e.g. FireEye, Dragos among others), however there are several areas of improvement. • **Regulations**. Cybersecurity in the CPS systems and Industry 4.0, in general, have still a low maturity. Regulations such as ISA99/IEC 62443 (Network and system security for industrial-process measurement and control) are still not complete, for example, the Part 3-2 (Security risk assessment and system design and technical requirements) is still in draft. • **Vulnerability assessment, penetration testing and certifications**. With the emergence of the Internet of Things paradigm (and its contextualisation to the industrial IoT context), the ability to connect and communicate of the automated devices via the Internet is becoming pervasive[18]. The transition from closed networks to enterprise IT networks and then to the Internet is increasing issues and alarms about security. As we increasingly rely on intelligent and interconnected devices, a new question related with security comes up: how can we protect all the appliances to avoid the intrusions and interferences that could compromise personal security and privacy? The confidence in these devices has become essential, and it is a crucial factor to guarantee cybersecurity. Vulnerabilities usually are based on software failures that are used to force the device and to change it is normal behaviour or operation. These vulnerabilities are intrinsic to the software, but it is possible to reduce them with a good design and implementation of the software. • **Connectivity between IoT devices (or rather Industrial IoT) or new software and legacy systems**. This issue is usual in the industry sector, like embedded programmable controllers and *automata* operating systems that sometimes are integrated into enterprise IT infrastructure. In this sense, it is vital to protect them from human interference while preserving the investment in the IT infrastructure and the leverage on the security functions. Besides it is crucial to ensure that these systems receive software updates and patches without risk in terms of safety. Moreover, the channels must be secure to protect the information from unauthorised disclosure and usage. • **Secure interaction with the Internet for enabling the B2B data exchange** is guaranteed by the IDS Connector. The technical requirements have been defined in the DIN SPEC

[18] M. Lezzi, M. Lazoi and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Computers in Industry*, vol. 103, pp. 97-110, 2018

	27070 standard. Organizational measures will complement the technical ones for data spaces protection. • **Distributed Ledger Technology.** DLT can be a key enabler in building secure-by-design IIoT and ICS in complex scenarios characterized by connectivity and near-real-time collaboration within a diverse ecosystem of factories and value chain stakeholder. However, DLT is not just a novel technology but also requires a radical redesign of system architectures, often to the extent of reshaping or even reinventing business processes. This means that new DLT-specific cyber security threats are likely to emerge • **Human element**. Helping IT and OT defenders to communicate is becoming a security issue on its own. Papers[19] reports that IT defenders and OT operators have to common problems with cybersecurity: o the difficulty of coordinating detection and response between defenders who work on the cyber/IT and physical/OT sides of cyber-physical infrastructures, o the difficulty of estimating the safety state of a cyber-physical system while an intrusion is underway but before damage can be affected by the attacker Solving cybersecurity problems requires coordinating defences between cyber security staff and physical plant operators. Human effectiveness is a challenge for cyber physical systems (CPS) security, but human influence adds both resilience and complexity to cyber-physical systems. Every control system is a unique combination of sensors, actuators, controllers, and computers connected by excessively many semi-interoperable proprietary protocols. OT staff specialize in knowing the idiosyncrasies of these highly diverse systems and their protocols. Usually they do not know how to recognise cybersecurity problems. • Finally, other cybersecurity challenges are: o Edge security o Create specific ISAC centers for Industry 4.0 o Vulnerability and penetration testing for OT devices o Cybersecurity issues when integrated with 5G SDN and NFV o Monitoring and protection for distributed industrial systems o IIoT gateway security o Efficient and secure communication networks based on optical wireless communication Protection of data aggregated through usage control technologies
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	Creating a secure cross-company exchange of industrial manufacturing data is necessary to implement many scenarios in digitization and modern distributed value chains. **The adoption of state-of-the-art security measures fosters the B2B data exchange for large and**, mostly, for **SMEs**, filling the lack of standards and skills.

[19] Fink, G. and McKenzie, P., 2020. *Helping IT And OT Defenders Collaborate*. [Online] arXiv.org. Available at: https://arxiv.org/abs/1904.07374

Starting TRL / Expected TRL	**Starting TRL**: 3-4 **Expected final TRL**: 6-7
How much funding is required?	40M
Timeline (2025/2027/beyond)	2020-2025: IA projects covering new industry technologies with cybersecurity. RIA projects could also be possible. 2025:2030: lighthouse project and IA projects covering 2-3 cybersecurity technologies applied to Industry 4.0. Projects in this phase should use as basis results/work of projects of the first phase

Energy (oil, gas, electricity), and smart grids

Horizon Europe – HEU.2.D2	
Specific Priority	**Energy (oil, gas, electricity), and smart grids**
Description of the challenges – why is it important?	The term energy indicates different sources such electricity, gas and oil fundamentally, and energy distribution refers to the infrastructures that offer services that enable the normal functioning of other industries and citizen life. Smart Grids are the digitalization of electricity infrastructure and the transition from a closed, centralized, analogue infrastructure to an open, largely decentralized, digital infrastructure. The functioning of the society and industry relies completely on energy and on a continuous electricity supply to the infrastructures belonging to other sectors such as health, transport, telecommunications, banking, etc. An interruption of the electricity supply can leave us without light for a certain time with the consequent discomforts, but if the interruption of the service is prolonged it can end up having a cascading effect since it would impact services offered by other sectors and dependent on the electricity supply such as telecommunications , water distribution, hospitals, banking services, etc. A problem in energy supply can have a cascading effect that can affect other sectors, other networks and even other countries given the interconnection that energy networks have. In this cascading effect, the close relationship that exists between smart grids and telecommunications networks must be highlighted, since smart grids offer the energy necessary for the operation of telecommunications, but at the same time they are necessary for the proper functioning of the smart grid and this relationship will become increasingly dependent as 5G technology is implanted in the industrial world. To the importance of the energy sector for our economy and society, it must be added that the world of utilities and electricity grids is facing major challenges such as decarbonisation by reducing fossil fuels to the maximum, decentralization through technologies decentralized control systems and digitisation throughout the value chain from generation to distribution to the consumer. Renewable and distributed generation in low voltage, photovoltaic solar energy, storage and electric vehicles, all connected at consumption points, are real trends in the sector. To this must be added the new role of consumers, who now can not only consume energy but also produce it, which implies changes in the relationship with companies and in the business model

	of distributors, turning them into market facilitators exploiting the large amount of information available to them and offering new related services with high added value. The integration of smart devices and the Internet of Things (IoT) deserves special attention since the volume of electronic devices that will be integrated or connected to the smart grid will increase exponentially in the coming years. Electric vehicles that will require specific equipment to be integrated into the infrastructure, such as charging stations and stations for electrical vehicles, or distributed generation with domestic photovoltaic panels, wind generation, etc. are some examples. We can think of future threats that may come from IoT devices connected to the smart grid and how to detect massive attacks from IoT devices coming from, for example, HVAC systems or home devices. Clearly, we must think about how to consider its safety from the design so as not to encounter future problems. The digitalization, especially with the increased use of automated controls, connected industrial and IoT devices, presents new challenges for the energy sector. Digitalization is both a product (an "end" state), and a process[20] with its corresponding transition risks related to the process itself. The transition toward smarter grids is a sociotechnical change process where the alignment between technical capabilities and organizational readiness is key to the development of resilience. Every operation within a power plant could be affected and the worst risks are, outage or cyber/digital production disruption and Safety Instrumented System (SIS) disruption, that could have impact on the interruption of an essential service, cascading effects on other industries and in the worst scenario employee's health or life. Similar consequences could be faced in case of outage or cyber disruption in a grid control centre, here the outage can lead to cross-border power outages within the European grid. As supply chains are digitised, the integration and interdependence among actors in the supply chains is another big challenge for that sector. Any suppliers, if compromised, could be a threat for any utility company, for instance an attack to the electric infrastructure could have consequences for an Oil & Gas company. The energy sector shares similar cybersecurity challenges to other sectors, and it is characterised by intrinsic and interlinked challenges such as cascading effects, mix of legacy and new technologies, and real-time requirements. A global approach should be adopted to secure energy systems and security solutions should address equipment not designed with cyber security, energy systems which have a very long lifetime as resource constrained legacy systems. Moreover, the energy sector differentiates from the others for the higher complexity due to the variety of energy sources and different kind of energy systems (from generation to supply) which have each one of them its own characteristics and specific cybersecurity

[20] Antonsen, Grøtan, Gjerde & Istad (2020): Security of electricity supply in the transition toward smarter grids. Proceedings from the ESREL conference 2020.

	challenges. For instance, some energy sectors are subject to heavy and strict regulations. Other challenges that deserve attention are: • Privacy and data protection concerns: possibility of creating behavioural profiles of customers if their energy consumption is transmitted into the Smart Grid especially in small time intervals. • Increased attack surface: heterogeneous data interfaces such as new and connection-oriented meters, collectors, and other smart devices (IoT technologies) which cause new entry points for attackers as well as the SCADA system used to monitor these software components. • Interdependency between safety and security. • Highly distributed and resource constrained systems. The fight against industrial espionage and terrorism, linked to sabotage and/or hacktivism, certainly remains among the most relevant challenges for the Oil & Gas sector. While espionage is aimed at stealing sensitive and confidential information, causing brand and reputation damage to the affected company, terrorism, sabotage and hacktivism are aimed at interrupting the availability of a specific service causing malfunctions and damage, including physical damage, to infrastructure, supply reliability, people and the environment. These actions are mainly perpetrated by threat actors driven by the interest in acquiring strategic confidential information and intellectual property, organisations with an unlimited amount of time, money and resources, or characterised by strong economic and motivational incentives, cyber-terrorists, who act to sabotage networks or infrastructures with the aim of causing damage to people or things, and hacktivists, who act for political ideals or to challenge the ethics and activities of multinationals. The energy sector is essential in a developed economy and society, so the resilience of the energy ecosystem to different types of security threats or accidents must be ensured with a holistic cybersecurity and safety vision.
Digital Living & Working	Developed economies depend for their operation on energy in its different forms and for this reason the objective of energy infrastructures is to offer a continuous and uninterrupted energy supply, and this can only be achieved if the energy chain, from generation to supply, works properly. and safely. Resilience is a challenge for any organization but given the characteristics of the energy sector and its important role in the digital living and working, the resilience of the energy ecosystem to cyber-attacks is of vital importance. Moreover, the CVID-19 pandemic is showing that cybercriminals and state agents are trying to compromise critical infrastructures in an attempt to create more chaos in the current situation, so the importance of having a resilient to cyberattacks energy sector is fundamental.
BASELINE	

What has been done so far (in EU and in the World – EU position)	The energy sector is considered in the EU Cybersecurity strategy developed by the European Commission and it is one of the critical sectors addressed by the EU Network and Information Security directive. The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation which is already enhanced across the EU providing a baseline of cybersecurity regulations. The NIS directive is now implemented in every national law EU wide and addresses the following aspects: 1. National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc. 2. Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc. 3. National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines) The NIS directive ensures a baseline security for all Operator of Essential Services (OES) in the EU Member States. In April 2019, the European Commission has adopted the recommendation on cybersecurity in the energy sector with the intent to increase awareness and preparedness in the energy sector. This recommendation sets out a series of actions to consider the particularities of the energy sector such as cascading effects, real-time requirements that pose challenges for standard cybersecurity solutions and legacy systems. In this last case, the challenges are due to the integration of new technological solutions with IoT devices and systems that were implemented and put into operation when there were no cybersecurity requirements, posing challenges in managing the life cycle of products and facilities. Cybersecurity solutions should be implemented on an old and geographically dispersed infrastructure with thousands of legacy devices in a context in which the life of products will be drastically reduced and continuous revisions of products due to vulnerabilities will affect not only the manufacturing, but also the updating and certification process. This same recommendation urges relevant agents such as energy network operators, technology providers and especially essential service operators to take appropriate measures in relation to cybersecurity in the energy sector, recommending standards such as ISO / IEC 27001/27019, IEC62443, IEC62351 and ISO / IEC31000. The Smart Grids Task Force - Expert Group 2 – Cybersecurity (SGTF EG2) has drafted its recommendation for the implementation of a Network Code on Cybersecurity, which proposes a harmonized cybersecurity baseline across the European Union. It provides clear requirements for process implementation, offering the flexibility for the

	stakeholder to follow individual approaches on technology and implementation. The recommendation of SGTF EG2 is based on well stablished mature International standards used worldwide that will continue to evolve with the participation of Energy stakeholders. Specific standards have been defined regarding cybersecurity issues for industrial and power systems (see ECSO State of the Art Syllabus for a list and specific details), but there is still a lack of a unified regulation and certification framework at European level for network operators and technology suppliers. New certification schemes covering all aspects from the product to services, process and people could be defined in the framework of the Cybersecurity Act. In this sense ENISA is working in the definition of a unified regulation for the electric sector and the definition of the regulation should be more agile in order to speed up the harmonisation at EU level and the certification process should be more agile and similar to the need of the device actualization requirements. A summary of the different initiatives related to the energy sector are the following: • Cybersecurity Act that ENISA will materialize in different certifications. • NIS Directive in its Group of Cooperation with Member States (Work Stream 8 on Energy). • Exchange of information at the EE-ISAC technical level in its Task Force on Smart Grids. • Regulation on Preparation for Electrical Risks. • Regulation on the Security of Gas Supply • Actions to raise awareness and mobilize the community in collaboration with the Thematic Network for the Protection of Critical Infrastructures (TNCEIP) and the European Gas Infrastructure (GIE) involved in the construction of European energy infrastructure. • Commission recommendation on cybersecurity in the energy sector.
Effort until now	Few European project have been funded in Horizon 2020 to address cybersecurity challenges in the energy sector. The call SU-DS04-2018 focuses on the cybersecurity challenges in the Electrical Power and Energy System (EPES). The objective is to make those systems more resilient to cyber-attacks and reduce their exposure to potential vulnerabilities. The EnergyShield project will develop an integrated toolkit covering the complete EPES value chain. The toolkit should include technologies for vulnerability assessment, monitoring and protection, and learning and sharing. PHOENIX will offer a cyber-shield armour to EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimise cascading effects on the infrastructure itself, the environment, the citizens and the end-users at a reasonable cost. The SDN-microSENSE project will focus on a set of secure, privacy-enabled and resilient to cyberattacks tools to address the normal

	operation of EPES as well as the integrity and the confidentiality of communications, thus looking at SDN-based technology. A second call for projects related to this topic, "Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches" is scheduled for August 2020 with projects potentially starting in 2021. There are other projects like CoordiNET that has the objective to establish different collaboration schemes between transmission system operators (TSOs), distribution system operators (DSOs) and consumers to contribute to the development of a smart, secure and more resilient energy system and is under the umbrella of the BRIDGE project that is a cooperation group of Smart Grids and Energy Storage H2020 projects. The project SecureGas, funded under the a call linked to the protection of critical infrastructures, focuses on the European Gas network covering the entire value chain from production to distribution to the users, providing tools and guidelines to secure existing and incoming installations and make them resilient to cyber-physical threats. In particular, the project will also look at the interdependent and interconnected European Gas grids to understand the impacts and cascading effects of cyber-physical attacks.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	The energy sector is facing a rapid pace of innovation and integration of new technology into legacy systems, thus increasing dramatically the complexity of managing the infrastructure. The increasing demand of energy supply, but also the interconnectivity of the infrastructure, clashes with the lack of security design in old ICS systems, increasing the need to secure legacy systems in a digitised world. The resilience of the digital infrastructure is an attribute tightly linked to different and important factors and resilient capabilities such as business continuity, which extends to physical security and organizational capabilities. In terms of **assurance**, specific processes need to be defined as they are important for managing internal know-how in relation to in house-built software, employee's awareness of rules and procedures and for compliance to international standards and best practices. An Energy Sector Commercial Product Assurance Scheme should be implemented to provide TSOs and DSOs with a way of having their systems independently tested to show that security features demanded by both the functional and non-functional security requirements can be assured. A European common framework would allow efforts to be focused, avoiding addressing potential conflicting requirements and create a unified Digital Single Market based on well established, mature international standards and certificate schemes based on widely accepted standards and best practices. The security certification of energy infrastructures should consider the security of the whole infrastructure, otherwise it cannot cover the whole security needs and would give a misleading impression of security. The management of the **product life cycle is a key aspect.** Cybersecurity innovative solutions created in R&D projects should be deployed in an old and geographically disperse infrastructure with thousands of legacy devices. We have to think in life cycle products of

	20-30 years with continuous vulnerability revision (defence that works now may not work tomorrow) that will affect the manufacturing, upgrading and certification process. To deal with emerging threats, such as 0-day exploits or new threat actors, a well-structured **risk assessment and management system**, with a resilient organization (to be understood as infrastructures and procedures) and with a secured by design hardware and software, can help to do this challenge. **Cyber physical systems (CPS)** are an important cycle/model. They will empower our critical infrastructure and have the potential to seriously impact our daily lives (consider, for example, the protection of assets like power grid and oil plants). They also place the basis for future smart services. Pervasive technology like work smartphone or GPS, used to operate within the companies' facilities, also should be secured. **Cyber secure future communication systems and networks** (5G/Fog/Edge/Cloud) enable the digitalisation of the infrastructure (i.e. IoT tools and devices used by the technicians), as well as the remote control of the assistance services and also the capabilities of an HPC (high-performance computing) technologies. Specific solutions need to be defined to ensure integration with the energy infrastructure. **Cybersecurity solutions** (firewalls, IDS, SIEM, IPS, honeypots, …) for the smart grid need to fulfil the real-time requirements in the energy sector: some elements of the energy system need to work under high-performance conditions (response times are about milliseconds). **Data protection** and the counter action against malicious use of data is a critical factor, particularly if we consider the retail and marketing divisions of oil and gas companies, where hundreds of thousands of users are potentially exposed to this risk. Not least is the priority protection that must be ensured for data relating to intellectual property and other sensitive corporate information. **IoT security** is especially important for its potential and for future applications that are expected to be implemented. For instance, current objectives in the Oil & Gas sector are predictive optimization and maintenance as well as optimization and tracing of the supply chain. For example, sensors inside the wells can collect data in real time and by analysing pump data companies can identify when the pump could fail or if it is malfunctioning. This could be done in real time. The challenges with long-lived legacy systems include difficulties to patch security vulnerabilities for fear of system malfunction. One approach to this would be to faithfully mirror complete systems in a **digital twin cyber range**, where security updates and other changes can be tested out (including accelerated testing) in a realistic but safe environment before deployment. Another aspect is the preparedness to cyber-attacks and the development of skills by defining cybersecurity exercises and awareness specific for the energy sector, e.g. by involving companies that belong to the same sector across Europe in cybersecurity exercises.

Expected benefit; strategic or economic impact ➔ **What can be achieved?**	The implementation of cybersecurity solutions will have major impact in • Guaranteeing the continuity of energy supply, 7/7 24/24, for the benefit of the society • Building a resilient energy sector to cyber and privacy attacks. • Avoiding cascading effects due to the interruption of the energy supply • Securing legacy equipment to coexist with new technologies. • Enhancement of the security level of the Smart Charging • Easier implementation of the NIS directive. • Development of more robust and secure products, increasing trust in the new technology and charging systems and ensuring that new devices, including IoT devices, have and will maintain a level of cybersecurity appropriate to the Smart Grid. • Increase the sharing of information among the relevant stakeholders: for instance, provide a better and faster response to cyber incidents. • Avoiding money losses caused by cyber-attacks: cf total amount generated by Cybercrime > 1000 Md$ (worldwide, annually) • Developing a European top industry and reaching excellence on cybersecurity for energy • Increasing trust in security and safety of energy infrastructures and respect and protect European values.
Starting TRL / Expected TRL	**Starting TRL:** 4 **Target TRL:** 7
Timeline (2025/2027/beyond)	2027

Transportation (road, rail, air; sea, space)

Horizon Europe – HEU.2.D3	
Specific Priority	**Transportation (road, rail, air; sea, space)**
Description of the challenges – why is it important?	**Automotive** The automotive sector is rapidly becoming reliant on digital technologies for connected and autonomous vehicles. The ongoing trend towards software-controlled assistive / automated / autonomic functions inside vehicles and the storage of personal information raises the potential risks. Besides that, several services and technologies are increasingly vulnerable to cyber-attacks: • ***In car decision support / autonomy.*** Cars rely on a wide array of sensors, processing capabilities and decision support systems to provide assisted driving and autonomous driving. These sensors and algorithms are vulnerable to attacks, in ways that human drivers were immune to. It is important to address issues such as physical manipulation of on-board systems which compromise vehicle safety of driver privacy.

- ***In-car communications.*** Cars rely on a large number of interconnected devices for command and control. These significantly increase the attack surface, both in risk occurrence and potential impact. While there are upcoming regulations, certifying modern vehicles with up to 150 ECUs and 100 Million lines of software is still a unsolved challenge.
- ***Car-to-car communications.*** Cars share the same space. As such, they must be able to communicate with each other safely and securely, to ensure that the algorithms used for decision support rely on accurate external data. Issues such as attacks on vehicle interfaces and functions for external connectivity, attacks on in-vehicle network or software of on-board systems, attacks exploiting software update, social engineering exploits vulnerabilities and weaknesses introduced by human errors have to be addressed.
- ***Car-to-infrastructure communications.*** Optimal management of the road infrastructure and safety require that the infrastructure communicate with cars, and exchange information in a reliable manner. Here existing regulations like the required usage of an automated emergency call service[21] has the potential to increase road safety, if the security can be guaranteed. However, it is also possible that global optimization of infrastructure usage will be contrary to the interests of individual drivers. There thus might be incentives to cheat (provide false information) or ignore requests from the infrastructure, leading to unsafe (or sub-optimal) situations. On 5G-enabled mobility an important issue is cybersecurity and data privacy, especially when it comes to ensuring the integrity and authenticity of the exchanged information. For example, spoofing V2X messages, tampering with transmitted data or code, attacking data integrity, exploiting the trust relation, gaining unauthorized access to data, jamming the communication channel on the protocol or RF level and inject malware or malicious V2X messages are important issues to focus on.

Rail Transportation

Some of the main challenges of the rail transportation sector are:

- **Interoperability**: railway sector is moving away from standalone proprietary systems and is increasingly relying upon open/wireless networks shared with other domains. The European Rail Traffic Management System (ERTMS) is being deployed to replace traditional heterogeneous structures across different countries to increase interoperability. The trends are relevant for increasing efficiency, capacity and cost-competitiveness of the sector. But, on the other hand, they also increase concerns on cybersecurity by broadening the attack surface. Greater connectivity and interdependence between countries, without a finalized approach on how they asses and tackle cybersecurity makes railways a more vulnerable target.

[21] https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en

- **Digitization**: digitalization is already impacting the railway sector and is going to further transform it offering better digital services to the commuters; increasing integration with other modes of mobility, leading to multimodal journeys in urban setting; providing digital services for rolling stock and predictive maintenance; and leading to automation and integration of train control systems. While this will attract more passengers and goods to this mode, threat actors will also find it more viable to attack rail systems, reinforcing the security concerns.
- **Security profiles:** improving the ERTMS robustness against cyber threats and reinforcing operational homogeneity. This can be achieved by addressing gaps and vulnerabilities identified by experts in ECTS; by fostering a faster upgrade path to Future Railway Mobile Communication Systems (FRMCS), which should also incorporate security by design; and by issuing specific rules and regulations to ERTMS-users regarding security measures, ERTMS-components robustness, as well as monitoring, detection and response capabilities.
- **Collaborative incident response:** Reinforcing collaboration between different stakeholders and entities (such as national cybersecurity agencies, ENISA, ER-ISAC, CERTs & CSIRTs etc.) to establish common understanding and policy for risk assessment and mitigation measures across Europe. Here the European Union Agency for Railways (ERA) can play a role to foster cooperation.

Maritime Transportation

We consider here broadly maritime transportation systems such as cargo or cruise ships to transport goods and people **and their infrastructure** at land (ports). Some of the main challenges of the maritime transportation sector are:

- **Bottlenecks**: a major proportion of the goods transported between Asia and Europe navigate through the Strait of Malacca, which is a narrow stretch of water between Indonesia and Malaysia. Thus, a cybersecurity attack in the maritime domain can trigger perturbations on the economy at a global scale. This also applies to Red Sea areas although traditional piracy is more widespread there.
- **Customs control**: The International Maritime Organization (IMO) required all member nations to implement *electronic single windows* (ESW) from April 2019 to facilitate the release and management of controlled goods under the mandates of Customs and Other Government Agencies (OGAs). Other types of communication between ship and ship/shore are undergoing digitalisation.
- **Cyber-piracy:** an increasing technical knowledge is demonstrated in piracy acts which follow a general trend towards cyber-piracy. GPS Spoofing is increasing used to place ships in vulnerable positions. Attacks to on-board communication networks are rapidly spreading.

- **Maritime ICS Security**: A vessel is indeed a floating system of systems where ICS and standard IT networks are operated. For instance, the propulsion system, the navigation system, the energy generation system, the HVAC system of a vessel such as a cargo vessel all rely on ICS. The operation of a port relies also on ICS, for instance for the automatic loading and unloading of cargo vessels.
- **Ship data system**: the complexity of the ship data systems is relatively high with many infotainment, administrative and technical networks with different types of interconnections. Ship systems develop over the ship's lifetime which may be as much as 35 years. The result is very inhomogeneous data systems.
- **Cargo tracking**: cargo tracking and cargo identification are increasingly subject to cyber security incidents resulting from cyber-attacks. The same applies for the automated systems handling the cargo in ports. Data theft, for criminal purposes, may also increase as a direct result of insufficient cyber security measures or measures not sufficiently matching the complexity of the ICT environment involved.
- **Vessel autonomy: t**he maritime domain has also to tackle specific cybersecurity challenges. The isolation of the vessels and its limited crew is a factor that needs to be taken into account. These specificities imply technical and training cybersecurity challenges. The crew, if any, must manage the security of the data systems on the ship without support from on board specialists.
- **Bandwidth limitations**: communication bandwidth for ships is at a premium due to high costs and limited availability. Security mechanisms for shipping need to be very bandwidth efficient.
- **Ship-shore information exchange**: through e-navigation, ships are increasingly reliant on exchange of information between ship and shore and this opens up new attack vectors targeting conventional data exchanges as well as special purpose data exchange systems used only by ships.

Civil Aviation

The Aviation sector is undergoing big changes in terms of growing demand (including improved safety and integrated controls, as shown by the SARS-Cov-2 emergency), new connectivity services for customers across their entire journey (from airport, to flight, including interaction with all the intermediate transport services), new communication infrastructures such as the ATN/IPS. All these ongoing changes enhance the role of cybersecurity, The growing integration with other transportation subsectors also broadens the attack surface as civil aviation at state of the art benefits from a greater culture of security than other transportation businesses. The principal challenges are in the following:

- **A multi-actor domain**: Aviation security by itself is sub-divided into four main areas: airspace security, air traffic manage-ment (ATM) security, airport security, and aircraft

security. Each is handled by a variety of actors. It is important to notice the collaborative nature the engagement for flight safety which involves Air Traffic Control (ATC) authorities, Airports, Customs, Airlines, Aircraft manufacturers and Aeronautical Maintenance companies. Such collaboration requires information systems to gather highest interoperability and security standards.

- **A growing reliance on information systems**: ground-air communication infrastructures (e.g. ATN/IPS) are becoming more open, sophisticated and flexible to cope with the complex scenarios of modern aviation. Across the different national regulations and the heterogeneous communication means, there is a need to guarantee highest security standards and continued availability for these infrastructures, in front of a growing threat landscape.
- **Time-sensitive safety-critical systems**: unlike most terrestrial vehicles, aircraft are not in security conditions when the system is down. Safety procedures and requirements for safety are of extreme importance and while cyber-risk is now generally acknowledge, it remains ancillary to safety requirements and to some extent underestimated. A classic provision for safety is the use of “fail open” technology which simply skips security mechanisms such as encryption or network filtering when safety mode is activated. A growing risk is that skilled attacks exploit such mechanisms to their advantage.
- **A complex certification framework:** providing usable and maintainable approaches to support novel certification frameworks is a challenge. The combination of vertical certification frameworks from air transportation domain and critical infrastructure protection frameworks driven by national or European (NIS) regulation lead to redundant certification practices without fully preventing the existence of security gaps. A coherent approach to physical and cyber-security across embedded and non-embedded parts is required.
- **A need for collaborative incident response**: security information disclosure needs to be managed in a controlled manner. We need to promote the development and complementarities between initiatives such as the A-ISAC, EASA-ECCSA, EUROCONTROL CERT and ED-204 Continuing Airworthiness. Consistent threat modelling, risk assessment across organizations, tools to support post-EIS incidents investigations, vulnerability management, methods and tools, are required to enforce transparency, accountability and liability in this sector.
- **A growing population of unmanned aerial vehicles:** the advent of Unmanned Air Vehicles (UAVs) disputing the airspace with traditional aviation sets major challenges for Air Traffic Control (ATC) and Air Traffic Management (ATM). This new population can hardly be kept out of reserved flight zones and their population may not be centrally managed with preplanned flight routes and predefined schedule as

regular aircraft once were. UAVs, but also Urban Aircraft (UA) such as flying cars and air taxis form a new class of Air Vehicles (AVs) for which airworthiness criteria remain inequally defined. They depend heavily on commercial ICT, Air-to-Air (A2A) and Air-to-Ground (A2G) data links, Global Navigation Satellite System (GNSS) and/or Detect and Avoid (DAA) systems. All off these are vulnerable to cyberthreats. And we lack of experience to properly anticipate the broad range of risk scenarios which this new population of AVs may cause.

Space

While a number of transportation subsectors are subject to caution for impact of the current health crisis, it is important to notice that, whatever the future designs as a scenario for human development; space will be a sector of upmost importance. If our societies switch to a structurally less geographically distributed supply chain, increased pressure will exert on space-based telecommunication systems to maintain global activity. If they return to an era of international trade, comparable means will be needed to provide geolocation, traffic control and transport systems connectivity.

- **Secure autonomous GNSS**: in a context where a growing number of nations let themselves be tempted by nationalist and populist policies, it is essential that Europe gains and sustains a relative autonomy in supply of space-based navigation services and ensures required resilience of such capacity towards attacks which could be initiated by malicious States or organized criminals. State of the art space systems supporting GNSS services have not been thought to operate in a context of cyber-warfare and are extremely vulnerable to cyber and cyber-physical threats. Such vulnerability should not be left unaddressed in the coming years.
- **Secure satellite communication:** in a world were the vast majority of world communications are routed via satellite, even when it comes to extremely local connections, it is of major concern that such communication service be exposed to cyber-threats. The densification of SatCom constellation, notably in Low Earth Orbit (LEA), is part of the answer to this risk, but creates another risk that the orbit becomes crowded with satellites and debris, leading to collisions and environmental damage. Security of up and downlinks needs to be enforced as well as a resilient space traffic management capacity to support future growth in in EU and the World.
- **Spacecraft Control Systems**: space craft control systems such as Attitude Determination and Control Subsystem (ADCS) or Telemetry, tracking, and command (TT&C) systems have been designed for operation in non-competitive and non-hostile environments. With the democratization of space and the growing importance of space-born systems in state and corporate strategies, this situation is likely to change. We observe a growing interest

	from malicious states and actors in space systems while the cost of offensive means literally collapses. As the attack surface grows and the attack toolsets get more affordable, we must expect a growing threat towards these systems to materialize in the coming years.
Digital Living & Working	Besides the specific sectorial challenges exposed here over, the digital transformation of transportation sector is likely to drive a number of cross-cutting challenges such as the need of protection of geo-localization systems, V2X communication protocols, autonomous driving technology, edge computing, novel multimodal transportation services, unmanned vehicles and the environment. **Geolocation systems:** More than any other, the transportation sector strongly depends on the availability, accuracy and resilience of geolocation systems, notably GNSS and alternative inertial navigation system, but also a growing use of IoT-based sensing and tracking technology which provide complementary means for geospatial positioning and navigation. Each technology has its strength and weaknesses. • **IoT-based geolocation jamming:** a growing trend towards the adoption of light IoT devices or tags and beacons is observable in transportation industry. These provide cheep means for indoor and outdoor location with variable levels of accuracy and reliability. 5G deployments will accelerate this trend by enabling extension of this technology to more time-sensitive applications. A major concern however is the vulnerability of these systems to rogue device intrusion and jamming attacks. • **GNSS spoofing:** a risk inherent to satellite based navigation systems is their exposure to spoofing attacks, which may only be mitigated by costly active counter-spoofing techniques or basic (but fallible) return to base control orders. This vulnerability is particularly detrimental to the adoption of unmanned and autonomous flight systems. • **Inertial navigation:** while being immune to the above identified threats, inertial navigation remains a costly solution which suffers from integration drift. For this reason, they require another system such as GNSS to regularly correct positions. **V2X communication:** In order to reach the vision of self-driving vehicles (SAE L4/L5), some of the key enabling technology components are multimodal sensors and artificial intelligence/data fusion, high-end edge and centralised computing capabilities, precise location/navigation and Vehicle-to-everything (V2X), i.e., Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N). While V2X in the wording comes from automotive, we acknowledge here that the need for it across different sub-verticals. Protocols are under definition. Yet the following challenges are already identified: • **Vendor policy and sectorial siloes**: the automotive sector is characterised by competing and no-synergistic culture. In the CCAM case several players like automotive companies,

OEMs, road operators, telecom vendors and operators, etc., have to collaborate to come up with an efficient, safe, secure, and privacy preserving architecture that spans the automotive environment from sensors up to application software control. Eventually, in dense areas, it would be of certain interest to enforce V2X beyond the automotive and road transportation domain to enable more comprehensive safety and optimization potential with urban transportation systems for example.

- **Lightweight communication security**: unlike office computers, cars and other vehicles do not accept latency or uncertainty in communication. For the vital safety-critical functions like anti-collision, assisted/ autonomous driving / braking, communication, if required, must be near real time and suffer no uncertainty. In the mean time, V2X communication must be protected against jamming, sniffing, or spoofing attacks which would compromise passenger safety or confidentiality. An acceptable trade-off must be found between communication security and latency.

Autonomous / assisted driving:

Safety-critical vehicle control decisions presumably assigned to humans are being increasingly transferred to computers, and a plentiful of new types of connected and autonomous vehicles are currently being designed. Beyond secure connectivity, this requires proper assurance of robustness of decision-making algorithms which support flight autonomy functions. Though it looks legally reassuring, assisted driving potentially retains even higher risks with consideration to the effects of computer support on human psychology and attention.

- **Autonomous driving**: the main concern with autonomous driving relates with the non-deterministic nature of AI algorithms which support it. Several demonstrations have proven the vulnerability of autonomous driving algorithms and other machine-learning based applications to adversarial AI and pollution of learning data. Beyond that, the problem of accountability and liability for accidents caused by autonomous driving vehicles remains unsolved. While machines greatly understand other machines' intelligence, it is now generally admitted that the cooperation of autonomous and non-autonomous vehicles in shared spaces presents the highest risk level.
- **Assisted driving**: current regulations leave little room for autonomous vehicles to operate without minimum provisions of manual fall-back procedures. However, the recent accidents show that today's pilots/drivers are of little help when flight/driving control automation really fails as they tend to loose vigilance due to a phenomenon known as cognitive underload. Interesting developments in automotive and aeronautics provide artificial means to ensure the cognitive load on pilot/driver remains between defined lower and upper limits which guarantee vigilance.

Edge computing:

Because of the previously described need for time sensitive machine decisions making, novel transportation systems may not be subject to processing and communication latencies as current information systems are. Yet, to unload power and processing constrained embedded systems, in a context where vehicles become more and more talkative, analytic functions must be distributed between central cloud, edge and endpoint in an agile manner.

- **Vehicular security analytics:** whenever driver/passenger safety is at stake, security analytics must be enforced at closest from the vehicle to prevent decision latency and loss of connectivity. Yet, they should not affect the core critical vehicular control functions. Considering that vehicles have limited computing power and processing capacity and constraints in weight and vibrations, it can be clever to place these analytics at the edge of the supporting cloud infrastructure.
- **Fleet security analytics:** yet when it comes to cyber threats potentially affecting a complete fleet of vehicles or using more stealthy approaches such as APTs which would remain inactive for long, we should exploit the ability to detect and correlate weak signals from a central point and deploy countermeasures on a larger scale. This requires complementary analytics to be placed on central cloud to perform longer term surveillance routines.

Multimodal transportation:

A major limitation of existing transportation infrastructure is the lack of comprehensive understanding of passenger journey from door to door and the contingencies due to poor multimodal transportation planning. This lack is addressable by the use of state of the art ICT technology and a minimum of human intelligence. However, it is important to anticipate potential cross-sector effects which tighter integration of transportation systems can have.

- **Passenger information and IT risks**: a first step in multimodal transportation is probably the integration of passenger information systems of different transportation means (airport, urban, rail, road…) to provide real time estimation of passenger journey schedule and recommendation for optimal routes taking potential hazards or traffic perturbations into account. A number of applications provide this information, to date without commitment from infrastructure operator, but with already a strong adoption rate. We can only encourage such practices which enable greener and leaner commutation in large cities. Yet we observe that they become vital to a point that they were not initially designed for. Because a wrong information can create chaos in an ever growing passenger flow, it is important to consider these information systems of public interest and enforce minimum security guidelines.
- **Adaptive transportation systems**: a more radical application of intermodal transportation principles goes beyond information towards dynamic scheduling and real

time communication across different transportation subsectors. Such practices can lead to significant economies, traffic reduction, increased customer satisfaction and reduced environmental impact. However, they trigger harsher requirements or time-sensitive information sharing and cybersecurity assurance, as attack scenarios on such infrastructures would affect not only their information layer, but system integrity and availability or even passenger safety.

Unmanned vehicles

The use of Unmanned Aerial Vehicles is becoming very popular; a trend supported by dropping prices and enhanced capabilities. This success calls for attention to accidental, malicious, or criminal misuses. Security is a key factor to obtain public acceptance of UAVs, especially considered the potential safety risks related to the highly connected and highly automated nature of provided services, especially in densely populated areas. Proper mitigating actions are required to assure that these risks are on acceptable levels.

- **Surveillance**: UAVs can carry out surveillance and response missions for border security, homeland security, and critical infrastructure protection, as well as support goods and people transportation. For infrastructure such as energy, telecommunication, or water/transport networks over wide, unsupervised areas, UAVs can be used for surveillance and protection, to detect, intercept, and neutralize rogue drones. In this context, cyber-interception requires even higher resilience against malicious or criminal intruders.
- **UAS resilience**: considering the growing adoption of UAVs in all those domains, it is important to guarantee superior robustness, autonomy, detection, response, recovery, collaborative and cognitive capabilities. UAV platforms shall be extremely secure, resistant to different forms of physical attacks (like GNSS spoofing, wideband jamming, MEMS disturbance, other electronic countermeasures) as well as against all the traditional digital threats to communication and HW/SW platforms. In this area, it would be important to develop security frameworks to support the community in the design of robust cost-effective UAVs, tailored to critical applications.
- **Unmanned Traffic Management (UTM)**: another important area concerns communications supporting air traffic management, in particular with shared airspaces. There is a compelling need to support air traffic management by an underlying, fully secured global high bandwidth data network, hardened and resilient by design to cyber-attacks. It is important to consider resilience by design to current and future threats, both affecting the ground bases and the on-board communications. An additional concern is the requirement for dynamic geo-fencing capabilities enabling to enforce air traffic control measures on demand, taking consideration of particular operational / security situations.

	Environmental challenges Transportation is responsible for 24% of direct CO2 emissions from fuel combustion. Road vehicles – cars, trucks, buses and two- and three-wheelers – account for nearly three-quarters of transport CO2 emissions. A growing concern for environmental challenges will bring novel developments aiming at reduced environmental impact by improved energy efficiency or alternative transportation usages. In both cases, ICT and security are key enablers to this transformation. • **Enhanced energy efficiency**: interesting perspectives are open in this field by the performance of electric engines, battery technology, alternative modes of propulsion and hybrid vehicles. Notable is the role of software and computing technology in the optimization of vehicle propulsion techniques and so is the requirement for cybersecurity. While traditional propulsion methods are relatively immune to electronic hazards, more efficient power trains cannot be trusted without proper consideration for cybersecurity threats. • **Novel transportation usages**: perhaps the most effective measure against environmental impact of transportation sector is a shift from vehicle owing to side-sharing or collective transportation practices. These usages do not only save on gas emission but broadly the environmental impact across the whole life-cycle of transportation systems. Here again, such usages require real time computation, optimization and communication technology which will tend to become more and more vital to transportation practices of the modern times.
BASELINE	
What has been done so far (in EU and in the World – EU position)	**Automotive** Concerning the area of Secure Product Development Lifecycle, SAE Cybersecurity Guidebook for Cyber-Physical Vehicle Systems J3061 is currently the relevant guideline for the automotive sector. Its development benefit also foundations build during a number of EU projects, including EVITA and HEAVENS. The automotive domain is currently developing its first international cybersecurity standard ISO/SAE 21434 “Road vehicles — Cybersecurity engineering”. While the introduction of a standard describing cybersecurity engineering from HW and SW up to the system level is still a challenge. UN-ECE developed also a regulation which requires cybersecurity for the type approval of vehicles (current WP.29 draft is of February 2020). While this is a major challenge for the European Automotive industry there is also the opportunity to enable the European Automotive industry as standing for secure and privacy-aware vehicles. The European Automotive Industry needs support in (1) introducing cybersecurity engineering, this ranges from the development of methods to tools for supporting cybersecurity considerations in the complete lifecycle (security-by-design), and (2) cost-efficient

cybersecurity solutions in HW and SW. Cybersecurity auditing is a relevant area, for which ISO is in the preliminary phases of preparation of a guidelines document (ISO/WD PAS 5112 “Road vehicles - Guidelines for auditing cybersecurity engineering".

In terms of wireless communications, the IEEE 802.11p is the de-facto technology standard for V2X communications. It is a relatively mature technology, validated by over a decade of field trials. At the same time, 5G-based V2X, from the Third Generation Partnership Project (3GPP), is a relatively new alternative solution to the IEEE 802.11p-based V2X communications.

Concerning infrastructures, the area of Cooperative Intelligent Transport Systems is of extreme importance. The EU commission supported an initiative[22] to develop studies around C-ITS challenges. The final report (2019) indicates a number of cybersecurity challenges related to handling privacy-sensitive data, securing payment services, strengthening security of interoperation across national infrastructures, clarification of risks and obligations of different stakeholders.

Rail

As the rail sector across Europe becomes more interconnected, standardization of railway cybersecurity has become relevant to reduce heterogeneity across different countries. To this end, some relevant work is being conducted by European Committee for Electrotechnical Standardization (CENLEC) where the WG26 of Technical Body TC9X is working on Draft Technical specifications 50701 “Railway Applications – Cybersecurity”, which adapt and interpret the emerging Cyber Security Standard IEC 62443 to railway sector’s specificities.

However, since the IEC 62443 series is still evolving, it is challenging to comprehensively adapt these standards for the railway sector and it is an ongoing work. Currently, IEC 62443 2-1 / 3-2 / 3-3 are considered relevant with regards to the common understanding and assessment of the cybersecurity, -risks and -threats landscape and processes. Instead, IEC 62443 3-3 / 4-1 / 4-2 cover component security level. Finally, IEC 62443 4-1 covers verification and validation, while IEC 62443 2-4 / 3-3 / 2-3 are considered relevant for maintenance objectives to provide standardised services profiles for the cybersecurity service provider, standardised patch management processes as well as general requirements and processes for threat detection, prevention and response.

On a parallel track, the CYBER Technical Committee of European Telecommunications Standards Institute (ETSI), is working on defining protection measures for critical infrastructures and guidance on implementation of NIS directive in different contexts.

Maritime

[22] https://ec.europa.eu/transport/themes/its/studies/its_en

	The Maritime Standardization landscape is quite articulated. There are several groups of organizations driving standards in cybersecurity topics relevant for Maritime: international and UN bodies like the International Maritime Organization (IMO)[23], the International Convention for the Safety of Life at Sea (SOLAS), the Global Maritime Distress and Safety System (GMDSS), and the International Ship and Port Facility Security code (ISPS). The principal driving factors are related to safety and autonomy. The Maritime Safety Committee, at its 98th session in June 2017, adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, encouraging administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code). IMO has given ship owners until January 1st, 2020[24] to incorporate cybersecurity risks management into their Safety Management Systems (SMS) or the ships will be subject to be detained by the port authorities. To drive trade facilitation, the IMO required all member nations to implement *electronic single windows* from April 2019. Similarly, other types of communications between ship and ship/shore are undergoing digitalization. Another area of current focus for IMO is Maritime Autonomous Surface Ships (MASS), for which the Maritime Safety Committee (MSC) is currently considering challenges related to state and non-state threat actors, considering also the increased risk posed by cyber pirates and risk of spoofing of Navigation systems like GPS/GLONASS/BEIDOU to place ships in vulnerable positions. In particular, the Navigation Communications and Search and Rescue Subcommittee[25] (NCSR) of the IMO deals with Ship to shore and Search and Rescue communications. Besides, the Facilitation Committee[26] (FAL) is specifically focused on cybersecurity issues related to the transmission of documents to Ports and between ships. Both NCSR and FAL are both concerned with vessels systems being affected by Cyber attacks. The MSC-FAL.1/Circ.3 *Guidelines on maritime cyber risk management* provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO. Concerning radio links, ETSI standardization work (in progress[27]) is considering requirements coming from all the relevant stakeholders in the marine sector (among which, IMO SOLAS, GMDSS and MED directive) to provide guidelines for the new maritime radio equipment. Also trade associations have issued guidelines and codes of practice for sharing information on risks and incidents.

[23] http://www.imo.org/en/About/strategy/Pages/default.aspx
[24] https://maritimecyprus.com/2019/12/05/ism-code-cyber-security-changes-coming-into-effect/
[25] http://www.imo.org/en/MediaCentre/MeetingSummaries/NCSR/Pages/default.aspx
[26] http://www.imo.org/en/MediaCentre/MeetingSummaries/FAL/Pages/Default.aspx
[27] https://www.etsi.org/technologies/maritime?jjj=1590405181834

Civil Aviation

Civil Aviation telecommunications are under profound transformation with the new communication infrastructures called ATN/IPS, in discussion in EUROCAE WG-108. Moreover, there are new regulations to provide guidance and security objectives for Aeronautical Systems Security as discussed in EUROCAE WG-72. These discussions gave rise to novel standards that require to prove due diligence has been done for guaranteeing an adequate level of security: ED-202 (Airworthiness Security Process Specification), the companion ED-203 (Methods and Considerations), and the ED-204 (Continuing Airworthiness), which are complementary to the existing ARP-4754 Aircraft Development process. Finally, EUROCAE WG-72 SG3 is working on guidelines to regulate incident management and information disclosure in the Civil Aviation sector to foster collaboration across stakeholders (A-ISAC, EASA-ECCSA, EuroControl CERT, and similar institutions in EU).

Another very important regulation under discussion is ED-201A, Aeronautical Information System Security (AISS) Framework Guidance, which is in charge of defining the overarching context of shared responsibility for AISS. The responsibility is shared across multiple stakeholders of the civil aviation sector. The domain is quite articulated: it covers all relevant areas, including aircraft design, production and operation (passenger and cargo), air traffic management, airports, maintenance repair and overhaul operations (MRO), aviation service providers, components & information, and the supply chains which these use and comprise. Adoption across the entire civil aviation sector will pose significant challenges and the full benefit will not be achieved until a critical mass of stakeholders will be engaged.

Space Systems

Existing standards applying to space systems only partially address the requirements for cybersecurity assurance. The ISO group ICS 49.020 provides standards for aircraft and space vehicles in general Including aircraft performance, flight dynamics, etc… Group ICS 49.140 provides specifications for space data and information transfer systems, yet without an explicit consideration for cybersecurity risks. The ISO document Nr 11231:2019 provides insights on probabilitic risk assessment for space systems, yet with a clear focus on physical risks and hasards. Possibly some threats are being addressed in ISO document Nr 14302:2002 which establishes performance requirements for the purpose of ensuring space systems electromagnetic compatibility (EMC). ISO 14620-1, 14620-2 and 14620-3 documents address the safety requirements applying to respectively space systems, launch site operations, and flight safety systems. Yet again, without an obvious consideration for cybersecurity. ISO/DIS 24129 Network layer security adaptation profile is under construction.

	Cross-sectorial Besides considering sector-specific institutions, it is important to align regulatory efforts to EU-wide regulations such as GDPR and NIS, and to establish relations with national institutions supporting management and reporting of cyber incidents, such as ANSSI (FR), NCSC (UK), DIS-CSIRT (IT), etc.
Effort until now	**Automotive:** SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of 'Connected Vehicles' and V2I communications seeking to improve the cyber-physical security ecosystem of Connected Vehicles in Europe. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles. CARAMEL proposes to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques, and also to continuously seek methods to mitigate associated safety risks. The ICT4CART project proposes an ICT infrastructure to enable the transition towards road transport automation looking at cyber-security and data privacy aspects. **Rail:** In addition to the technical specifications and standard setting efforts described before, several projects specifically focusing on cybersecurity in the railway sector have also been funded. Under the Shift2Rail initiative, there is specific focus on cybersecurity in Innovation Programme 2. Technical Demonstrator 2.11 aims to achieve the optimal level of protection against any significant threat to the signalling and telecom systems in the most economical way. In this context, some of the main projects focusing on cybersecurity in railways include – CYRail (Cybersecurity in the RAILway sector); MISTRAL (Communication Systems for Next-generation Railways); X2Rail-1 (Start-up activities for Advanced Signalling and Automation Systems); X2Rail-3 (Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication); and 4SECURAIL (Formal Methods and CSIRT for the Railway Sector). In addition, entities such as the International Union of Railways (UIC), European Rail Research Advisory Council (ERRAC), Association of the European Rail Industry (UNIFE) along with expert groups/bodies like EU Rail Passenger Security Platform (RAILSEC), Land Transport Security (LANDSEC), and European Rail – Information Sharing and Analysis Centre (ER-ISAC) are also contributing through regular discussion and facilitating collaboration on the topic.

Maritime

Within the pilot project CyberSec4Europe there is a dedicated demonstration case on *maritime transport,* where the cyber security capabilities of the participants are combined and applied to emerging maritime services and operations.

The Cyber-MAR project focuses primarily on cyber range in the maritime logistics value chain but also look at decision support tools to cybersecurity measures, by deploying novel risk analysis and econometric models.

The Project SeCoIIA addressing cybersecurity of collaborative manufacturing systems includes a use-case for Naval construction, where remote third party maintenance is made possible through the implementation of fine-grained access control and anomaly detection techniques.

Civil Aviation

The SATIE project is working to build a holistic, interoperable and modular security toolkit to be exploited by the next generation of Airport Operation Centre and Security Operation Centre in order to protect critical air transport infrastructures against combined cyber-physical threats. Additional aim is to update security policies in favour of a simplified change management. This area of the Transportation priority will be developed in synergy with the CleanSky 3 initiative[28] (in particular for what concerns high-bandwidth. high security, resilient communications) and (the continuation of) the SESAR initiative. It is also in synergy with the current ACARE SRIA, which provides high-level objectives aligned with the currently proposed scope.

The SESAR JU CORUS project has performed a preliminary cyber-security risk assessment for the inclusion of UAVs in cohabitation with other users of very low level airspace.

The project ALADDIN intends to design, develop, and evaluate a counter UAV system, yet involving essentially physical detection and neutralization means.

Space

The most structuring initiatives addressing security of Space systems have been Copernicus, Galileo and Govsatcom. Copernicus addresses space-based security missions rather than security of the space systems themselves. Galileo contributes to European autonomy in GNSS services, thus, indirectly supporting security of transportation systems which rely on geolocation services. Yet the consideration for cyberthreats applying to the Galileo constellation itself is not in core scope of the program. Govsatcom program does address bothways security of space systems and space-based security services? It is however focused on governmental market.The ESA4S initiative was launched with the objective to develop Secure Satcom for Safety & Security. At this stage the ambition and budget support to this initiative remain uncertain.

[28] http://www.clean-aviation.eu/

	Cross-sectorial The C-MobILE project enables large-scale, real-life C-ITS (Connected Intelligent Transport System) interoperable deployments across Europe. The project defines operational procedures leading to decentralised and dynamic coupling of systems, services and stakeholders across national and organisational borders in an open, but secure C-ITS ecosystem, based on different access technologies, the usage of which is transparent for service providers and seamless and continuous for the end-users across different transport modes, environments and countries. nIoVe aims to deploy a novel multi-layered interoperable cybersecurity solution for the Internet-of-Vehicles (IoV), with emphasis of the Connected and Autonomous Vehicles (CAVs) ecosystem by employing an advanced cybersecurity system enabling all relevant stakeholders and incident response teams to share cyber threat intelligence, synchronize and coordinate their cybersecurity strategies, response and recovery activities.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	**Automotive** Car safety has come a long way. From the first padded dashboard to seat belts and from rear-view cameras to active safety measures such as autonomous emergency braking (AEB), technological advances are picking up speed. Nowadays, cars are becoming smarter and 'greener' through connectivity and artificial intelligence, and cybersecurity is emerging as a new concern able to stop such huge potential for more sustainable safer roads with zero fatality. For the automotive sector, it is important to define tools and methods integrating cybersecurity in the development and engineering of vehicles. While there is a first draft standard, the implementation of this standards needs major efforts and support from research. As cars and road infrastructures have relatively long lifecycles, it is important to define standards which ensure security and safety of a car fleet gathering vehicles of very diverse levels of autonomy (from 1 to 5) on road infrastructures of equally diverse connectivity levels. From a technological perspective, we will have to face the following challenges: - The need for ligtweight authentication and encryption mechnisms to secure V2V and V2I communication under time-sensitive constraints. - The need for vehicular network segregation techniques compatible with weight and cost constraints applying to automotive. - The need for privacy-preserving and scalable cyber-security monitoring techniques, potentially leveraging edge-computing to support anomaly detection and automated reaction to cyberthreats. **Rail**

Historically, several attacks have deliberately targeted the rail transportation, especially metro systems, within major European cities. These attacks have been specifically de-signed to cause maximum disruption and a high number of fatalities. Attacks on subways and local trains have shown that the rail network is an attractive target for attackers to spread fear and terror in the population. The terrorist attacks of the 2004 Madrid train bombings and the 2005 London bus bombings claimed the lives of 191 and 52 innocent civilians, respectively. Furthermore, criminals and terrorists have taken the transport sector to be an easy target. According to TAPA, the theft of high value and high risk products moving in supply chains costs business about € 8.2 billion a year in Europe.

Actually, due to the advancing integration of ICT (Information and Communications Technology) technologies into land transport, mobile units and infrastructure alike, the number of potential cyber risks has steadily risen during the last decade. With the generalization of automation and computerization in the rail vehicles and signaling systems, we will most likely see attacks, motivated by financial gain, political or terroristic intends, or simply vandalism, using these techniques. This could become a high potential risk. Additionally, the increasing use of wireless techniques as a basis for the communication infrastructure also poses additional risks. For example, in the ERTMS framework, GSM-R techniques are used for on-board/Track-side communication, where safety relevant information is exchanged. Therefore, this new channel can be target of jamming or spoofing attacks. It is worthwhile to notice that the cyber threats increase as the train control systems are more and more relying on ICT systems and radio communication, even for automatic train control systems. As railway systems are designed according to the fail safe approach, interrupting of signals would lead to train stops, but the failure of communication operation makes the trouble caused much more complicated.

Maritime

While the IT world includes systems in offices, ports, and oil rigs, OT is used for a multitude of purposes such as controlling engines and associated systems, cargo management, navigational systems, administration, etc. Until recent years, these systems were commonly isolated from each other and from any external shore-based systems. However, the evolution of digital and communications technology has allowed the integration of these two worlds, IT and OT. The maritime OT world includes systems like: Vessel Integrated Navigation System (VINS), Global Positioning System (GPS), Satellite Communications, Automatic Identification System (AIS), Radar systems and electronic chart. hile these technologies and systems provide significant efficiency gains for the maritime industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance, and design of cyber-related systems as well as from intentional and unintentional cyberthreats.

When addressing these cyberthreats, it is important to consider the uniqueness of OT systems, as these assets control the physical world. OT systems are responsible for real-time performance, and response to any incidents is time-critical to ensure the high reliability and availability of the systems. Access to OT systems should be strictly controlled without disrupting the required human-machine interaction. Safety of these systems is paramount, and fault tolerance is essential. Even the slightest downtime may not be acceptable. OT systems present extended diversity with proprietary protocols and operating systems, often without embedded security capabilities. They have long lifecycles, and any updates or patches to these systems must be carefully designed and implemented (usually by the vendor) to avoid disrupting reliability and availability. The OT systems are designed to support the intended operational process and may not have enough memory and computing resources to support the addition of security capabilities. In addition to the ongoing integration of IT and OT, the future will bring MAS – Maritime Autonomous Systems. Based on artificial intelligence and Internet of Ships and Sea Services, the new generation of ships will be remotely controlled from the shore. MAS has a “disruptive” potential with implications in terms of technical, economic, environmental, legislative and social impacts in the years to come. This development may also provide opportunities and new concepts which could improve logistics and, therefore, also improve the overall environmental impact of transport.

Maritime companies still need to become more aware of the above risks and significant investments are required to enforce best practices: identify the threat environment to understand external and internal cyber threats to the ship; identify vulnerabilities by developing complete and full inventories of onboard systems and understanding the consequences of cyber threats to these systems; assess risk exposure by determining the likelihood and impact of a vulnerability exploitation by any external or internal actor; develop protection and detection measures to reduce the likelihood and the impact of a potential exploitation of a vulnerability; establish prioritized contingency plans to mitigate any potential identified cyber risk; respond and recover from cyber incidents using the contingency plan to ensure operational continuity. Maritime industry and its digital exposure have many similarities with industrial systems and the broader OT. In this context, these companies must move very fast to the direction of protecting their systems, providing a reliable operating environment not only from performance perspective but also from security perspective. Both proactive and reactive measures must be developed and applied with the real-time security awareness and visibility being possibly the most critical solution, since OT environment remains extremely sensitive in providing timely and accurate services. The creation of a European Maritime ISAC, initiated by recent EC calls, needs to be supported further to reach a more concrete application. In parallel, further research in OT security and convergence of safety-security risk management needs to be fostered to ensure safe & secure development of maritime sector in Europe.

Civil Aviation

The following actions should be taken to strengthen security of Civil Aviation and UAVs:

- Strengthen authentication and authorization of information flows between services, and integrity verification of data (e.g. registration and geo-fencing data)
- Strengthen integrity of information flows coming from external, critical services (e.g. GNSS signal, authentication and use of lightweight encryption)
- Protect the integrity of software/firmware upgrades, increase guarantees on integrity for information flows coming from external, critical services (e.g. GNSS signal).
- Protection of navigation and surveillance comm.s (ADS-B)
- Multiple, different security functions at different levels in the communications end-to-end system, supported by clear regulations
- Enforcement of regulations across stakeholders, to ensure trust in the infrastructure and guarantee appropriate monitoring of UAVs when they become a risk for the entire infrastructure
- By-design support to event handling and incident reporting, with methods and tools to simplify cooperation among stakeholders
- Strengthen command and control links, potentially with redundant communications leveraging a network of ground stations
- Strengthen layer-2 security solutions and promote wide adoption across the heterogeneous infrastructures
- Improve authentication infrastructures worldwide, coping with different national regulations, cross-border and cross-infrastructure handoff, leveraging PKIs
- Infrastructures able to guarantee continuity of service and acceptable performance levels, prevent disruption, adapt to changing conditions and recover rapidly from disruptions.
- Applications of post-quantum crypto in the aviation sector
- Support detection and analysis of threats propagating across transport infrastructures

Specifically in Civil Aviation sector it would be important to support the following developments:

- High-assurance communication links, e.g in the datalink layer, continued availability, and resilience against emerging threats;
- Support certification needs in the area of cybersecurity risk assessment (as per ED-202), in the context of safety, with novel methods and tools (as per ED-203) also leveraging model-based and semi-automated approaches to improve scalability and consistency, and support changes in architectures and environment (as per ED-204);
- Design-time methods and tools to verify adequate assurance is provided with respect to elicited cybersecurity requirements (as per ED-202), with potential application of formal methods form the specification, to design and to the

	implementation, on applicable layers of the communication stack; • Support to cross-organization threat models and a common approach to risk assessment, to improve understanding of shared risks and responsibilities, formalize mutual assumptions and guarantees, support more effective sharing of novel threats and their impact on infrastructures; • Support to vulnerabilities impact assessment with rigorous methods and semi-automated approaches, possibly leveraging shared vulnerability databases for the domain; • Development of methods and tools to support the creation and maintenance of vulnerability databases relevant to the domain of Civil Aviation, with secured and tracked access, considering constraints and limitation in incident management and disclosure (as per EUROCAE WG-72 SG3 ongoing work); The following developments whoudl be fostered for application to UAS and UAs: • Strengthen authentication and authorization of information flows between services, and integrity verification of data (e.g. registration and geo-fencing data). • Strengthen integrity of information flows coming from external, critical services (e.g. GNSS signal) • Protect the integrity of software/firmware upgrades. Increase guarantees on integrity for information flows coming from external, critical services (e.g. GNSS signal). • Methods to guarantee continuity of service and acceptable performance levels, prevent disruption, adapt to changing conditions and recover rapidly from disruptions. • Multiple, different security functions at different levels in the drone end-to-end system, supported by clear regulations. • Enforcement of regulations across stakeholders, to ensure trust in the infrastructure and guarantee appropriate monitoring of drones when they become a risk for the entire infrastructure • Besides the event handling and incident reporting services, an independent monitoring service is required for certain areas, to identify (rogue) drones. In addition, measures are needed to counter these drones, supported by the appropriate regulations. • Strengthen command and control links, potentially with redundant communications leveraging a network of ground stations **Space** GNSS is identified above as one of the main threat vectors to transportation systems in general. Greater resilience can be provided by signal-based anti-jamming techniques, densification of trusted GNSS constellations, miniaturization of intertial navigation systems but also through the development of more disruptive

techniques like magnetic anomaly navigation technique should be investigated.

The role of space segments in secure communication should be reinforced, in particular with consideration for the role of satellites in Quantum Communication Infrastructures as envisaged to support high grade communication for commercial and dual uses. Developing secure space nodes will be needed to ensure long range communication with minimal exposure and reduced cost of infrastructure.

The densification of Low Earth Orbit (LEO) SatCom constellations comes with a new upsurge of risks, including increased collision lieklyhood, augmentation of space debris and expansion of the cyber-attack surface. These risks, physical or logical also tend to be more and more interdependent, so that traditional safety instruments become practically ineffective whenever the cyber layer does not equally upgrades. With satellites becoming a commodity, it is no more ecluded to watch cyberthreat actors getting equipped with space-born tools as well. This threat is already reality in the case of state-sponsored attacks. Hence the cost, complexity and specificity of space systems is no more a sufficient defence against cyberthreats to space segments. Dedicated research and innovation actions should be fostered in this field.

Cross-cutting challenges

SW / HW components to build secure future mobility

- Automotive (and maritime) systems are outside of a controlled environment and potentially accessible by an attacker. Therefore there is a need to provide a secure hardware-based root of trust.
- Approved and shared crypto-libraries are essential to ensure an uptake and high level of security
- Both can be used to build up secure reference architectures (layer of defense)
- Attack detection and mitigation system for connected cars.
- Safety and security co-design for certification of connected cars.
- Solutions to address potential attack surfaces of communication systems used for the connected and cooperative mobility
- Utilization of network softwarization, mobile edge computing, cloud native applications and advance radio access technologies to reduce cost and complexity of cybersecurity services for future mobility
- In vehicle anti hacking and data privacy solutions
- Vulnerability management and certification of sensors and algorithms

Today, much work is targeted at making ship hardware systems more resilient to cyberattacks, but digitalization of work processes and by that electronic messaging has been mostly overlooked by authorities. Furthermore, little action has been taken to safeguard

	maritime communication solutions (satellite, digital VHF) against cyber-attacks.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	**Automotive** While automated transportation is able to offer benefits like a retained and self-determined mobility for elderly people there are ongoing discussion regarding privacy and also increasingly regarding cybersecurity. Here the ethics of such systems are also an important topic, connected to cybersecurity. The European Automotive Industry has the opportunity to establish itself as Automotive Industry with the highest level of security and protecting the privacy of its customer. In Europe around 13.8 million people are direct and indirect employed in the Automotive Industry and the turnover represents over 7 % of EU GDP. Automated and connected mobility represents the next step of evolution in the Automotive Industry and cybersecurity is essential for future challenges. The list of vehicles that are expected to become autonomous include, apart from private cars, taxis, buses, and trucks. Automotive manufacturers have already solved complex problems like collision detection and avoidance, and navigation. However, a lot of work on defending against a full spectrum of malicious attackers, wielding both traditional cyberattacks and a new generation of attacks employing techniques from the rapidly advancing area of adversarial machine learning, is still to be done. As consensus grows that autonomous vehicles are just a few years away from being deployed in cities as well as highways, the risk of cyberattacks has been largely ignored. The situation resembles numerous articles promoting e-mail in the early 1990s, before the newfound world of electronic communications was awash in unwanted spam. Back then, the promise of Machine Learning (ML) was seen as a solution to the world's spam problems and indeed, today the problem of spam is largely solved. However, it took decades because the danger was underestimated and because the right ML tools were not mature enough back then. The damaging effects of cyberattacks to an industry like the Cooperative Connected and Automated Mobility (CCAM) can be tremendous. From the least important to the worst ones, one can mention for example the damage in the reputation of vehicle manufacturers, the increased denial of customers to adopt CCAM, the loss of working hours (having direct impact on the European GDP), material damages, increased environmental pollution due e.g., to traffic jams or malicious modifications in sensors' firmware, and ultimately the great danger for human lives, either they are drivers, passengers or pedestrians. The current timing is ideal to address these issues because the critical Original Equipment Manufacturer (OEM) and Tier-1 components of interest (e.g., 5G, autopilots, smart charging controllers) are mature and they are ready to be integrated in the modern vehicles. On the other hand, the cybersecurity solutions are based on powerful AI tools and algorithms to combat security risks in modern vehicles that were not possible to be hosted on embedded

processors and platforms some years ago. Sooner or later, European roads will be overwhelmed by CCAM vehicles with SAE layer 3 and above, and this is a unique opportunity for Europe to promote research required to provide the highest possible robustness against attacks, thus having the first movement advantage in the emerging field of automotive cybersecurity.

According to the European Road Safety Observatory car accidents were responsible for over 25,000 fatalities and 1 million injuries in Europe and notably, 94% of these car accidents are due to human errors. Inevitably, autonomous vehicles, which are already technologically feasible and in the commercial horizon, will gain ground in an effort to increase transport safety and to reduce casualties. Moreover, people that are aging, visually impaired, or not fit to get a driver's license will get enormous benefits from the introduction of autonomous vehicles, being able to travel independently. The most advanced commercial autonomous vehicles have reached the Society of Automotive Engineers (SAE) level 3, and they are able to travel without human intervention with speeds up to 60 km/h. Cybersecurity here stands as a crucial enabler for progress towards safe autonomous cars towards SAE levels 4 and 5, which will undoubtedly open a new cycle of expansion for the automotive sector. Having EU industry at the forehead of this revolution is more a question of survival than an opportunity to seize.

Rail

While pioneering the industrial transformation of modern societies in the nineteenth century by setting up the first mechanized transportation networks, the rail sector has since then been inclined to a certain conservatism and ICT technology has essentially been adopted by progressive replacement of legacy systems subject to obsolescence. Formerly isolated mechanical systems have thus been replaced by more communicative and automated systems with insufficient consideration for related risks. The rail supply industry is however a crucial component of European industrial growth, jobs and innovation. This industry includes: the manufacture of locomotives and rolling stock, tracks, electrification signalling and telecommunication equipment, parts and services. Both SMEs and major industrial leaders are active in the sector. European rail supply industry invests 2.7% of its annual turnover in R&D and represents 46% of the world market. It employs about 400,000 people in Europe and accounts for more than 1 million direct and 1.2 million indirect jobs in the EU with a turnover of EUR 49.2 billion and a value added of EUR 15.2 billion in 2017. The European RSI remains a major player in the global RSI market, despite slowing down between 2009 and 2013, it recently recovered its growth rate to approximately 5% per year.

The EU remains the largest net exporter since 2000, with the only exception of 2005 in which Japan presented a higher value of net exports. However, the global RSI market is changing. China started to become a key player. Fuelled by strong internal demand, often of public investment nature, the Chinese RSI has seen its production grow exponentially. Combined with investments in R&D by Chinese companies in the RSI, this indicates a new role for Chinese RSI not

only in terms of ability to satisfy the internal demand, but also as a role of exporter. Innovation remains one of the key elements of success of European RSI. R&D, ad-hoc cooperation projects to share knowledge and capabilities between companies, as in the case of ERTMS, appears to be an excellent way to maintain the innovation. The joint participation of the railway industry in the development of the ERTMS technical solution and standards was essential for its success. Despite the technical standardisation, operation rules remain national based and are still a barrier for seamless cross border rail operations. ERTMS has been successful in its implementation outside Europe, but deployment in the EU remains low due to the additional costs required to ensure compatibility with national legacy systems. Nonetheless, the sector managed to maintain a leading position globally thanks to various initiatives related to stimulation of R&D&I, e.g. by means of the Shift2Rail Joint Undertaking. This investment in R&D&I may be necessary in light of the significant investments taking place in other regions, most notably China. Initiatives in the field of digitalisation will support the RSI in maintaining a leading position in the near future.

A necessary corollary to sustained digitization of rail systems and to the achievement of interoperable systems across EU is the reinforcement of cybersecurity standrads applicable in that field. Being particularly risk-averse, the sector would suffer from incidents occasioned by the exploit of vulnerabilities in ICT and ICS components. Also the development of traveler-centric and intermodal services, an important trigger for future growth, requires due consideration for information security issues. Noticeably is the public extremely sensible to rail accidents. Also the development of trans-urban and peri-urban ssegments requires greater attention to the request for connectivity and data services to passengers. A condition for such development will be the strengthening of data security and privacy protection mechanisms.

Maritime

90% of the international trade of goods are transported overseas, within Europe approximately 60% of goods are carried by maritime transport, and 3 European ports account for around 10% of overall traffic volume. The importance of ship transport is expected to grow with increased trade and the future must make transport more energy efficient to reach climate goals. Ship operations represent high values and incidents can have severe consequences, in the case of large container ships in the range of billions of euros. If cyber-crime caused a ship to block, e.g. the approach to Rotterdam, Antwerp or Hamburg, direct and societal costs could become much higher. This illustrates the huge damage that errors in navigational information or interference with ship data exchanges can cause. Of particular concern is threats directed at key navigational information such as electronic charts and navigational data exchanges between *Vessel Traffic Services* and the ship. In this sector, European actors are already much threatened by the competition of Asian ship

owners and shipyards. Providing greater security assurance could be a strong differentiator for EU maritime sector.

Aviation

"*At a time when the average cost of a cyberattack is now estimated at $1 million (some recent aviation cyber incidents cost much more e.g. The fine of €204 million imposed on British Airways by the UK Information Commissioner, ASCOS being closed for 3 weeks), the objective of "just" complying with new various cyber security regulations, either aviation related, such as EC 373/2017, or not, such as GDPR or the national implementation of the EC 1148/2016 (so-called NIS Directive), is now overcome by events*"[29] The expected benefit of the proposed research agenda (in close synergy with DEP.2.A, HEU.1.A, HEU.2.C, HEU.4.B, and other related areas) is to develop methods and tools to support cybersecurity evaluation at all stages of design, at a system/system-of-systems scale, in a repeatable and transparent manner. Model-based approaches have already proven their effectiveness in the Aviation domain and formal approaches are applied (and recognized by avionic certification standards) for high-assurance and safety-critical applications. Both capabilities are extremely useful for functional and safety related considerations and their maturation to support broader application in the cybersecurity domain has the potential to bring a significant contribution in the domain.

The development of Urban Air transportation systems including manned and umanned vehicles is critical for further development of dynamic cities able to compete with the attraction power of Asian and American megacities. Such development is hampered by surface traffic congestion which limits activity, expansion and service offering to citizens, also causing unbearable pressure on prices of real estate. Cybersecurity thus stands as an enabler for further urban development, attraction of talents and enterpreneurs to European cities. Novel air vehicles, typically electric Vertical Take-off and Landing (VTOL) systems may not gain access to the market without prior definition of security standards applying to them and the construction of adequate certification frameworks. Taking the lead in this field would help Europe remain competitive in field of transportation systems and urban development.

Last but not least, it is important to acknowledge the severe harm caused by COVID crisis to the aviation sector in general. In this context, we have seen the development of new practices wich move the lines between transportation sector, e-citizenship and e-health. The generalization of passenger health checks and follow ups, now triggers needs for harmonization of practices across countries, secure cloud access to patient data, and enhanced collaboration between healthcare, aviation and security practitioners in the management of pandemic risk. Unless adapted identity and access management mechanisms are set up, such practices may in many ways contradict the principles of privacy protection. Without proper measures, it will be difficult for the aviation sector to regain

[29] https://www.eurocontrol.int/publication/cybersecurity-aviation

passenger trust. To this extent, cybersecurity stands as an enabler for the recovery of aviation sector from COVID crisis.

Space

The global space economy reached EUR 309 billion in 2017,1 having grown on average by 6.7 % p.a. between 2005 and 2017. With approximately one quarter of this amount attributed to government budgets and three quarters to commercial revenues, the global space economy is significantly influenced by the global economy, thereby subjected to periods of stagnation and of growth. The most recent economic upswing happened in 2010–2014, providing an average growth of 6.2 % p.a., a value that surpassed the growth of the overall global economy, which grew at 4.4 % p.a. over the same period. The overall space economy consists of both revenue-generating commercial space activities and government investments in space. While governments were the driving forces in the 20th century (e.g. the Apollo programme, International Space Station (ISS) and the Global Positioning System (GPS)), commercial activities are now setting the pace, accounting for EUR 229 billion or 76 % of the global space economy in 2016. In contrast, the US government spent EUR 39.8 billion on defence and non-defence space efforts in 2016, while non-US government space investments made up EUR 28.9 billion.

Starting with the emergence of the private spaceflight industry and miniaturised satellites, traditional boundaries and business models are changing radically. This rise of new entrants has brought with it new opportunities for innovations in products, services and processes, which, in turn, have created spillover effects to various industries both inside and outside the space sector. To adapt to technological changes, established space companies increasingly are forced to seek revenues outside the traditional realm of institutional space. Many space companies find it difficult to engage on commercial terms or have limited financial reserves for the necessary investments. The period 2011–2017 accounts for nearly two-thirds of the investments in NewSpace over the last 15 years. This is not a singular trend; in 2016, space generated nearly EUR 1.42 billion in venture investment in a single year, a remarkable figure, bearing in mind that the space arena had never reached over EUR 95 million in venture investment annually prior to 2014. Agile design, commercial-off-the-shelf, digitalisation and miniaturisation, dual-use, spin-in, venture capital and valley of death have become keywords synonymous with the ongoing change within the space realm. Today’s business models thrive not only on technological improvements, but also on shorter generation cycles, aggressive spin-in approaches and a consequent trade-off between risk, cost and time to market. Eventually, securing digitized manufacturing processes for space system production may be of equal importance with efforts made to enhance security of space systems themselves.

In the global space economy, satellite services represent the largest sector (around 37 %), closely followed by ground equipment. Earth observation is the biggest user of satellite manufacturing and launch services, and remains a key driver for the overall industry. Space

hardware and space applications have been important users of innovations in industries outside of the space industry. Advances in manufacturing technologies, miniaturisation, nanotechnology, artificial intelligence and reusable launch systems have driven market disruption in the space industry, for example, through falling costs in satellite manufacturing and launch vehicles. Scientific and technological progress go hand in hand and can lead to disruptive innovation, resulting in a new market with a radically different value proposition. Space is therefore an enabler for several industry verticals. For example, space-based infrastructure projects such as Galileo serve as precursors for many space-related applications in segments such as location-based services and agriculture. Thus, even though some of these technologies may be competing with the space industry for investment, the space industry in fact provides important incentives for other technologies. It is important to note that 40 % of the companies in space sector seek public funding as it is a precondition for private investment. It is a sector where public funding serves as a seal of approval in the market.

Unlike aviation, space is essentially unharmed, even possibly boosted by the consequences of COVID crisis, as the development of remote working practices and restriction towards physical transportation will esstentially increase pressure on SatCom capacities which are essential to these practices. It is noticeable that space sector is bound to grow, whatever the scenario is for world exchanges in the coming years. Space segments essentially support both distant communication and transport in physical space. For this very reason, they might well become the Achilles heel of modern societies. Investing in secure space systems is thus a recommendable decision. Space systems will play a growing role in the defense of European interests both from a geopolical and economic perspective. Importnant is to acknowledge that they have been for long exempt of investments in matters of cybersecurity. As space systems and space-born services are getting more and more commoditized though, they will become an attractive attack surface to cyber-offenders of all kinds. For this reason, substantial effforts must be drawn to the establishmet of minimum security standards in that field.

Cross-cutting challenges

Modern vehicles require about 100 million lines of code, more than e.g., a Boeing 787 (14 million) or Facebook (61 million), making them some of the most complex systems available today. The new capabilities and functions increase dramatically the complexity of a vehicle’s systems, and although these complex systems have vastly improved vehicle performance, safety and fuel efficiency, the probability of breakdowns has also increased. Indeed, the more interdependent and complex parts existing in a system, the higher the probability that the system will fail. More importantly, cybersecurity rises out as a necessity to protect these systems and the information contained inside. Applied to the vehicles of today and the near future, cybersecurity needs to take on an even more important role: to protect systems and components that govern

	safety from harmful cyberattacks, unauthorised access, damage, or anything else that might interfere with safety functions.
Starting TRL / Expected TRL	**Starting TRL:** 3-4 **Target TRL:** 6-7
Timeline (2025/2027/beyond)	2027 and possibly beyond

Financial Services, e-payments and insurance

Horizon Europe – HEU.2.D4	
Specific Priority	**Financial Services, e-payments and insurance**
Description of the challenges – why is it important?	The financial sector is slowly adopting new technologies in order to improve or create new business. This implies that the threat environment is also rapidly evolving, becoming more sophisticated and complex in nature. This will cause, in the next years, an increase in security breaches and cyberattacks, therefore requesting more expert technologies/processes for prevention and protection, both in the technological and human area. Enhancing cybersecurity awareness for all employees will be critical for financial organizations. Financial Institutions have always been one of the most attractive targets for cyberattacks due to their economical appeal. Nowadays, due to their owned high volume of personal data, more malicious actors are targeting them with innovative and unknown attacks. Due to all these factors, although new technologies and digitalization bring so many benefits to this sector, it also has increased exponentially the attack surface. Additionally, another critical issue for the financial sector is the growing attention from European legislators, regulators and standard bodies on cybersecurity issues related to the financial sector. The high volume and complexity of regulations, together with the fragmentation arising from different EU laws across national EU Jurisdictions causees inefficiency and loss of profitability. Also, the high number of requirements imposed by both national and regional regulators, which often conflict with regulations, requirees banks to enhance their cyber-resilience while at the same time fulfilling all different regulations. Therefore, it has been identified as a critical challenge to develop processes and solutions that deal with multiple mandatory incident reporting requirements. Cooperation and cyberthreat intelligence sharing are nowadays also a critical necessity in this sector. Information sharing and the support of global cybersecurity main initiatives on Financial Services, e-payments and insurance will allow European players to be part of the decision-making process and to represent their best in class solutions. An example of the need for this action is that insurance companies do not have adequate tools for an objective measurement of cyber risks in the financial sector. This is even more complex if it is a multinational

	organization that has to fulfill different legislations. Financial Institutions strongly encourage the setting up of a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States. The emerging new paradigm of Open Banking has arisen several challenges. While this will push banks to aim at being fully digital and make customer data more accessible for the ecosystem to build superior products on, it could also create an environment that would enable more fraud and risks. Finally, new legislations continue to appear in the European ecosystem (e.g. PSD2, 5MLD, PAD), which have influenced and will continue to influence the landscape of Financial Services (and especially e-payments). These legal developments need to be supported by technical innovations and European Infrastructures to have large-scale effects in the fields of cybersecurity, with the appearance of not yet mature solutions on the market that may impose a cybersecurity risk for users. These infrastructures will support, on the one hand, the EU sovereignty with the increasing adoption of solutions from non-European market players, and, on the other hand, the EU market integration, against the risk of fragmentation of the European market due to the emergence of proprietary local solutions that do not allow pan-European reach.
Digital Living & Working	The COVID-19 has impacted the financial sector in different ways. On the one hand the workforce is now divided, working remotely, and the virtual communications have become they day-to-day life. Although it brings benefits it also creates new challenges such as 24/7 secure communication channels and how to work with confidential information in a non-secure environment. This brings the emergence of new services and solutions that expand the current functionality of existing online/sharing platforms to seed new experiences for large virtual workforce while respecting security and privacy policies. On the other hand, an important aspect has been the achieving of a cashless economy and inclusive banking as part of a global financial system. The demand for online banking and virtual customer services has been increased greatly, as shown by the rise of download rates of mobile banking apps. Regulators have to adapt to this new reality for it to succeed. Also, only payments and requested services has quadrupled, evidencing that customers demand reliable and secure digital banking and financial management.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Digital finance includes a variety of products, applications, processes and business models that have transformed traditional banking to a more sophisticated integrated, distributed and open financial services. Investment in new technologies has substantially increased in recent years and the rate of innovation is exponential. In March 2019 the European Commission adopted an action plan on FinTech to foster a more competitive and innovative European financial sector. This plan identifies 19 steps that the EC intends to take to enable innovative business models, support new technologies such as blockchain,

	artificial intelligence and cloud services and increase cybersecurity in the financial sector. This action plan is part of the EC efforts for building a Capital markets union and a true single market for consumer financial services (therefore, part of the Digital Single market strategy). The European Commission has created a consultation about financial services for improving resilience against cyberattacks. The target audience is key stakeholders of financial institutions, market infrastructures, etc. and the main goal is to gather stakeholders' views on the need for legislative improvements as a way to make the financial sector more secure and resilient. ENISA supports the financial sector as it was identified as a critical backbone of the European economy. For this reason, ENISA created a new expert group for finance (EGFI 2.0) with the objective of raise awareness of the sector to ICT risks, promote good practices and standards and develop cybersecurity profiles specific to different financial market institutions. Together with the European initiatives, the European Banking Federation (EBF) is the voice of the European banking sector, uniting 32 national baking associations in Europe (large and small, local and international). The EBF is engaged in different activities for secure digital innovation in banking. This includes contributions to the work in the data-driven economy, supporting cloud adoption in banks, use of big data, AI and actions to increase cyber resilience. The main objectives of the EBF in this area are to contribute to shape the European legislative, regulatory and supervisory environment in its fight against cybercrime, active promotion of information sharing and cybersecurity awareness for bank employees and customers.
Effort until now	Few European project have been funded in Horizon 2020 to address cybersecurity challenges in the finance sector. The call SU-DS05-2018-2019 addresses data security and protection for the critical sectors. This included the financial sector as one of the identified critical ones The 2018 call focuses only on the financial sector and in particular addresses the need for technologies for digital security, privacy and personal data protection. Among other projects, as an example of work done till now, the SOTER project aims at increasing cyber resilience by providing a comprehensive set of tools to increase the cybersecurity level. Also, the CRITICAL-CHAINS project focuses on the integration of Cyber Physical Systems in the financial sector by delivering a novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations. In the area of critical infrastructure protection, FINSEC aims to provide a mature implementation of the reference architecture (RA), based on the enhancement and integration of the novel solutions from the partners (e.g. Anomaly Detection, AI CCTV Analytics, Risk

	Assessment Engines, Collaborative Risk Analysis & Management, Compliance), in order to strengthen the security of the financial sector. Finally, due to its importance in Europe, the finance sector is one of the main areas of effort in the European pilots. More specifically, cybersecurity solutions are researched for applying in this sector for covering information sharing and protection against cyberthreats in CyberSec4EU and CONCORDIA.
DESIRED SCENARIO	

What more should be done? What gaps to be filled? For what reason?
 	
How can it be done?
	• ***Cybersecurity exercises and awareness.***
	  ○ Define a common regulation for cybersecurity exercises across Europe.
	  ○ Define cybersecurity exercises and simulations for testing the whole financial system readiness, identify weakness on actual process and define specific guidelines.
	• ***Regulatory Harmonization.*** Defining common controls framework and tools for international players operating in EU market in order to improve compliance to European regulations.
	• ***Competences and certifications*****.** cybersecurity common and recognized certifications should be a must-have for working in the sector and be globally acknowledged.
	• ***Specific harmonization on incident reporting.***
	  ○ Need for the harmonisation of incident notification practices by exploring the differences and synergies that exist between the most relevant incident reporting schemes and each of their aspects.
	• Cybersecurity intelligence sharing
	  ○ Need of common tools and practices for facilitating cybersecurity intelligence sharing.
	  ○ Common format for data sharing supporting data protection and controlled access
	• Main European infrastructures are still missing*:* Critical Infrastructures for Financial Activities are not under European Governance or are not yet developed at European Level (e.g. e-payments, Federated IDs, DLTs)
	• Cyber-attacks are particularly challenging for several reasons: they rapidly increase in sophistication and complexity; they are persistent; they exploit both technological and human weakness and vulnerabilities and the entry points can be external to the organisation.
	• Harmonize and unify resilience strategy on a global level, enhancing interconnections and interdependencies in the EU banking and financial system.
	• Other relevant challenges are:
	  ○ Cryptocurrency
	  ○ Enhanced e-payment security
	  ○ Integration of eIDAS Digital identity
	  ○ Cyber insurance and risk modelling

Expected benefit; strategic or economic impact ➔ **What can be achieved?**	**Streamline and enhance current incident reporting practices through harmonization and risk-based approach for regulations** • Increase efficiency of coordination between organizations and to reduce reporting burden. • Effective and simplified regulation, with advantages, for financial institutions, in terms of profitability and improvement of the general security situation. • Harmonisation in terms of strategic objectives, structures and practices in the fields of Incident Response. • For Financial entities is essential to improve a risk-based approach on requirements definition or support an overall compliance to regulations. **Increase awareness and create cybersecurity professionals** • Increasing awareness could reduce cyberattacks and their impact both in economic terms and consumers' trust. The outcome will be a more secure and reliable European ecosystem. • Ensure a new and prepared generation of cyber specialists is necessary for maintaining and increase the cybersecurity maturity level of the sector. • A regulatory framework applied to all players (EU and non-EU working in EU) to reduce uncertainty, ensure comparability and allow competitive solutions on a global basis. **Increase prevention of and response to cyber incidents through collaboration and information sharing** • Develop and increase the cyber capacity of the EU financial sector by contributing to create a proper customization of a tested methodology and operating models in order to support the development of financial sectorial CERTs. • Increase the capacity to support for prevention, preparation and response to cyber-attacks and security incidents of the CERTs. • Necessary to have continuously updated information relating to the current trends in fraud in the financial sector. Also, to have tools and design operational contexts for sharing information for a correct assesing and adequately classification of the potential risks arising from cyberattacks. • Rationalize and share the experience of individuals bringing to common factors the elements that can improve risk management from every point of view including the identification of minimum requirements to enable insurance coverage, the preparation of a shared taxonomy and a common glossary. • Swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks, making the financial community – and thus law enforcement – more effective at understanding the threats and pursuing the perpetrators behind fraud and cybercrime.

Starting TRL / Expected TRL	**Starting TRL: 5** **Target TRL:** 7
Timeline (2025/2027/beyond)	2020-2030: 3 calls every 3 years, 3 projects each 2020-2023: cybersecurity solutions for specific topics (e.g. information sharing, cybersecurity awareness and simulation of attacks, etc.) 2024-2027: solutions covering two or more cybersecurity topics, initial interaction between financial entities of different countries 2027-2030 and beyond: solutions at European level for the financial sector. Collaborations between three or more different member states

Public services, e-government, digital citizenship

Horizon Europe – HEU.2.D5	
Specific Priority	**Public services, e-government, digital citizenship**
Description of the challenges – why is it important?	The current evolution of today's society needs and expectations is closely linked to the digital transformation and its pervasive impact in every aspect of everyday life. **Public administration and public services need to define innovation** roadmaps to address the emerging needs of citizens (including the diversity and unequally distributed vulnerability between different groups), improve the effectiveness of the services provided as well as their security, transparency and interoperability (nationally and cross-border). Following the European strategy of a Digital Single Market, a truly digital European society should be based on the development of cross-border digital public services, improving access to eGovernment for citizens and businesses, promoting innovative initiatives at local level and then scale up at the European level. In this context, security and privacy issues are a growing concern, especially as the internet and new technologies have made personal information more accessible and easier to collect, access and repurpose or manipulate. From a security perspective, some of the main challenges introduced by the digital transformation are: • Physical connectivity, related to the diverse devices which are connected to the egov infrastructure, with multiple stakeholders having access and potentially increasing the attack surface. That could compromise even parts of the infrastructure which are well managed and controlled • WiFi security - devices with default passwords or/and unencrypted connections can increase the threat landscape. There are also vulnerabilities related to the compromission of wifi encryption technologies • Hardware security – this refers both to not considering the built-in security of devices (e.g. a switch not properly configured) and weak encryption in IoT devices (due to low computational power) as well as lacking standardisation which can also introduce an attack vector • Bandwidth consumption – in an environment where the amount of sensors, systems, users and interactions grows exponentially, a flexible environment capable to support high traffic levels is critical

	• Application risks – in the context of egov services, there are software applications used by different organisations to access corporate data. In case of security vulnerabilities, they introduce a relevant risk. As regards privacy concerns, among the most important ones are: • Data privacy and protection - E-government systems collect a huge amount of confidential information about individuals, products, and financial transactions. Therefore, it is the responsibility of a government to ensure an individual's information is secured and the users' privacy is preserved during data management lifecycle. • Balancing data aggregation and privacy – when integrating systems each of which holding its datasets, data aggregation could enable behaviour tracking of an individual, affecting his/her privacy • Interoperability: when data is translated and transferred to different components of an egov infrastructure (which is expected to increase), potential vulnerabilities arise. Moving to the risk identification and management in local Public Authorities, the maturity of the Risk Management Systems in local public entities seems to be at a very low level, and there is still a long way to go to get closer to the level known in banking or insurance sector. That is partially related to employees' lacking awareness concerning cyber-risks, as they are usually not informed in the correct way (or at all) about the importance of security and privacy issues regarding the data of the citizens. It also contributes to the lack of investments in systems and tools for effective protection against the attacks. Poor security/privacy awareness is also experienced at organisation level: many organisations of public sector simply do not know which data are critical for them and so try to protect everything, but actually it brings them to protect nothing.
Digital Living & Working	During an unprecedented event like the COVID-19, governments at any level experience an enormous pressure, being the authority supposed to inform and lead the population through an unknown crisis. They have to force their procedures and burocracy to immediately respond to the emergency stage, e.g. ordering business closures, reorganising resources and industry to meet medical needs, providing financial assistance. All of this, indeed, must mainly be performed by using digital technologies. After the emergency, governments have to deal with the fallout of the economic crisis, balancing it with keeping in force sufficient measures to keep the virus spread under control. They have also to assess the effectiveness of the technologies used during the crisis (including telehealth, remote work, etc.) and be prepared to respond to future risks through digitalisation. While bolstering cybersecurity is an essential reactive measure during the emergency stage (e.g. tackling online misinformation and disinformation, protecting citizen privacy, securely providing public and government services, organising community responses, building trust and transparency), it becomes a fundamental pillar when

	planning actions for the mid-long term (e.g. accelerating digital government, implementing digital ID, enhancing telework capabilities, improving data availability and management, improving system resilience). Sharing technologies, expertise and tools through cross-border public-private partnership can represent a concrete support to governments in restarting the economy and rebuilding societies.
BASELINE	
What has been done so far (in EU and in the World – EU position)	In 2016, the Commission published the "EU eGovernment Action Plan 2016-2020", following the previous one (2001-2015), containing several actions to advance the modernisation of public administrations across the European Union. Examples are: accelerating the take-up of eIDAS services (including eID and eSignature), introducing the Single Digital Gateway, enforcing the interconnection of all Member States' business registers, setting up the Electronic Exchange of Social Security Information (EESSI), etc. One of the key principles supporting the Action Plan implementation is "Trustworthiness & Security", meaning that personal data protection and privacy and IT security are preconditions for increasing trust in and take-up of digital services, and they should go beyond mere compliance with the legal framework. In 2018 benchmark report, the Commission introduced the cyber security assessment, highlighting that less than 10% of the 3500 analysed European public websites passed the basic tests performed. The GDPR introduces the obligation to ensure appropriate measures for data security, including protection against the risk of destruction, loss, alteration and unauthorised disclosure or access. In addition, Public Administrations in some countries are identified as operators of essential services, therefore they subject to the NIS Directive.
Effort until now	The following H2020 projects provide a contribution to increase Public Administrations cybersecurity: • COMPACT, innovating at both technological (real time security monitoring, security awareness training, information sharing, cyber-security gamification, risk assessment, and threat intelligence) and process (adapting the Plan-Do-Check-Act cycle for LPAs to do iterative removal of security bottlenecks and achieve compliance to EN ISO/IEC 27001 and BS ISO/IEC 27005) level. • CS-AWARE, proposing a cybersecurity situational awareness solution for local public administrations that, based on an analysis of the context provides automatic incident detection and visualization, and enables information exchange with relevant national and EU level NIS authorities like CERTs.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason?	• **Privacy and Security by default and design.** The EU privacy regulation is based on the fundamental and human rights to privacy and the protection of personal data and relies therewith on globally valid rights and principles. Citizens value the high level of protection granted by the GDPR and ePrivacy

How can it be done?	legislation. In particular, Article 25 of the GDPR provides an obligation to adopt both technical and organizational measures. This assures security on personal data processing and at the same time solutions for automatizing support to data subjects so they can exercise their centric role and rights. Nevertheless, these measures suffer from the absence of technical tools and standards that make the exercise of their rights simple and not overly burdensome. It is important to stress that technical and organizational measures addressing the current regulations shall be adopted by design and by default. They should also cover all the phases from design to implementation of privacy related applications, taking also into account the "state of the art", by staying updated on technical advancement in privacy technologies, standards, regulations and recommendations. • **Interoperability between legacy and new systems.** Every new systems or applications integrated into the Public Services environment may represent a potential gate for attackers. The level of interoperability between legacy and new systems could represent the level of criticality of the overall system: the more connected is the network, the more vulnerabilities for the attackers to exploit. It is necessary to provide validated and precise interoperability recommendations and specification; define specific governance; provide on-line verification and validation means for promptly identify the possible security risks and even more in particular privacy risks. In parallel, data should be encrypted both at rest and in transit. Indeed, encrypting prevents attackers from misusing the data in case of a breach. • **End users trust management:** This encompasses different solutions: i) assuring transparency, i.e., openly communicate what data is collected, what data is stored, how it is processed, who it is shared with, and how it is protected; ii) managing consent and control, i.e., make the end users aware about the data held about them; provide the end users the right to view, update, and delete their data, and ensure that data is handled according to each user's privacy settings; iii) implement auditing and accountability, i.e., hold the Public Administration accountable for the usage of end users data and compliance with privacy policies, and promptly detect misbehaviour. • **Trusted Identify Exchange:** Advanced identity management functionalities based on the Self-Sovereign Identity model should be further evolved and supported in order to improve the overall personal data sharing process, so fully aligned with GDPR goals. Data processors will be able to verify at any time consumer identities and verify the authenticity of the data the person provides; individuals will be able to manage their digital identities and take advantage of progressive disclosure of data (zero knowledge proofs). Relevant technologies, competences and organizational capabilities considering human centre design and trust related to: • **Privacy Enahncing Technologies.** Privacy preserving tools and models are needed to liberate the potential of personal

data, facilitate citizens visualization and control of their data and open innovation in public service provision in compliance with GDPR. “Once Only” principle needs solutions acting as an intermediary between data subjects and data controller and processors by providing functionalities for lawful data sharing processes, with the ability to grant and withdraw consent to third parties.

"Consent" is the basis to authorize Data Provider to provision data to Data Consumer and authorizes Data Consumer to process that data by referring to a Data Usage Policy. It is important to support the entire end-to-end process in personal data processing, from the definition of policies to personal data sharing among an ecosystem of data driven services. To assure automation and interoperability among all the parties involved, consent and policies have to be semantically described. This **semantic harmonization** permits that a semantic description of usage policies is attached to data and travels with it allowing to manage usage policies.

- **DLT and Crypto-currency.** The Digital transformation, that is pushing Government towards an open, transparent, citizen centred, decentralised, multi provider and co-operative model, can be supported by cutting-edge blockchain and distributed ledger technologies (DLTs). Blockchain technologies and its combination with other technologies could support governments to reduce fraud, errors, and by design can provide transparency over government data and transactions. Governments worldwide are experimenting with blockchain to better meet the needs of public-service users and steward coherent use of resources to maximise public value. Blockchain and DLT technologies are not yet fully established in public services and it is therefore necessary to experiment with their integration into the public innovation ecosystem. European Council has promoted an European approach to blockchain in order to harness the many opportunities of blockchain, support actions at government level to avoid a fragmented approach. In the “Declaration of Cooperation on a European Blockchain Partnership” it is recognised the potential of blockchain to transform digital services in Europe:

    - to change the way citizens and organisations collaborate, share information, execute transactions, organise and deliver services.
    - to enable more decentralised, trusted, user-centric digital services, and stimulate new business models benefiting our society and the economy.

  The close cooperation between Member State towards a European ecosystem for blockchain services will reinforce the chances of developing the right conditions for this technology. The European Blockchain Partnership (EBP) is working on establishing a European Blockchain Services Infrastructure (EBSI) that will support, in a first stage, the delivery of cross border digital public services while meeting the highest

	standards of security, privacy, sustainability and compliance with EU laws. Within EBSI, the European self-sovereign identity framework (eSSIF) is one of the use cases supported. It aims to implement a generic self-sovereign identity (SSI) capability, allowing users to create and control their own identity across borders without relying on centralized authorities. In particular, eSSIF will allow an EU entity to "obtain" verifiable credentials, to "register" verifiable mandates/consents, and to "obtain" verify verifiable claims, which then can be used to identify/authenticate relying parties and provide those with required claims/attestations.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	• Create innovative data-based knowledge and services, without compromising privacy nor adding to the amount of personal data in circulation. • Provide deep personalisation in public service provision and put citizens as active actor in personal data management with more transparency and more control over data • Improve interaction with public services, adhering to the "Once-Only" principle and addressing privacy and security requirements. • Raise citizens/customers trust and strengthen engagement to support Single Digital Market strategies.
Starting TRL / Expected TRL	**Starting TRL:** 4 **Target TRL:** 7
Timeline (2025/2027/beyond)	

Healthcare

Horizon Europe – HEU.2.D6	
Specific Priority	**Healthcare**
Description of the challenges – why is it important?	***Secure medical Internet of Things.*** Hospitals are increasingly relying on connected objects to deliver care and monitor patients. Yet, recent incidents have shown that cyber-attacks can disable the care infrastructure (e.g. medical imaging devices). In the future, connected objects will be provided to patients outside of controlled environments (hospital), such as patient homes. These medical objects will be critical for the medical staff to take care of the patients; they will also be a possible mechanism to carry out cyberattacks more easily. ***Secure health data.*** Medical staff is increasingly relying on data workflows for diagnosis, care delivery, surgery, follow-up. These medical workflows are also interleaved with building and resources management on one hand, privacy, insurance and financial aspects on the other hand. Securing these multiple data and workflows, including with privacy technologies, is of the utmost importance for the accuracy and efficiency of medical care. Privacy-by-Design and Security-by-Design will also be a key assumption for the creation of European Health Data Spaces and development of European health data services.

	New data-based care protocols. With the availability of large volumes of data will come customized medical protocols, tailored to the specific needs of the patient. The digitalization of the medical world will thus move from relatively passive monitoring and data collection to active delivery of substances, controlled remotely over the network. Even simple denial of service attacks may significantly impact the proper carrying out of medical protocols, compromising patient integrity. New methods are thus needed to control and secure data and algorithms integrity, up to command and control of medical objects. ***Smart Hospitals of the future:*** for the sustainability of the healthcare system in Europe and elsewhere, the hospital centric ecosystem of healthcare delivery models need to be shifted to home and community-based care. Secure communication and data use would be of utmost importance when we start delivering many care processes outside of the hospital buildings, e.g., for assisted living. This implies that we depend even more on the ICT infrastructure so that we need to step up the efforts in security i.e. when we use video for consultations. Moreover, in the coming years we will have much more access to real-time data on each patient and these data sources will stem not only from the hospital systems but also from municipality and home and third-party applications and many of the data might be prone to hacking. Effective measures are needed to secure such distributed and socially connected infrastructures. Furthermore, such a shift in care delivery model is also relevant to prevent / address future pandemics, where prevention, diagnostics, treatment and monitoring can be done at community level. ***Human and organizational performance.*** Threats and opportunities to smart hospitals can be intended and unintended. Organizational, human and system performance as well as dependency to other systems, limited resources and trade-offs also play an important role. The risks that result from these threats and corresponding vulnerabilities are typically mitigated by a combination of organisational and technical security measures taken by smart hospitals that comprise good practices. With respect to organisational measures, compliance with standards, staff training and awareness raising, a sound security organisation, and the use of guidelines and good practices are particularly relevant. Relevant technical measures include network segmentation, asset and configuration management, and network monitoring and intrusion detection. However, manufacturers of information systems and devices used in smart hospitals have to take certain measures to design secure systems. Among them are, for instance, building security into products from the outset, adopting secure coding practices and extensive testing together with sound training. ***Scattered cybersecurity and privacy technology knowledge in healthcare in EU.*** While scattering of knowledge and research in cybersecurity is a general, recognized problem in the EU, it is even more evident in healthcare. Recent H2020 projects on cybersecurity for healthcare are showing how different is the cybersecurity and privacy posture of healthcare organizations in different EU nations and how diverse is the perception of the importance of cybersecurity in the sector from a governmental and organizational perspective. ***Blockchains, privacy technologies and healthcare data.*** With the widespread use of blockchains/DLTs and increased use of secure

	computing and anonymisation to store and exchange healthcare data, it becomes increasingly important to further explore interoperability, privacy, data visibility, access control in the context of DLTs and Health Data Spaces. ***One European Electronic Health Record (EHR).*** A secure, privacy-aware mechanism to have de-facto a single federated pan European Electronic Health Record which allows European citizens to effectively grant access to parts of their EHR to any European health organization to receive the same level of health service as if in their home country. This, in turn ,would reduce administrative and medical errors and improve the pan-European patient experience.
Digital Living & Working	Cybersecurity challenges: • Preventing cyberattacks that manipulate human perception, and dynamic and adaptive attacks • Keep pace with the increasingly sophisticated attack methods • Simulating human cognitive behaviour to anticipate and respond to new and emerging cybersecurity and privacy threats • Preventing cyberattacks by reducing the attack surface through increased deployment of Secure-by-Design and Private-by-Design services. • Intelligent real-time monitoring and assessment
BASELINE	
What has been done so far (in EU and in the World – EU position)	Worldwide, there has been limited deployment of advanced cybersecurity technologies for healthcare. Healthcare organisations and service providers are deploying better security procedures and technologies (e.g., stronger consent-based systems for data, increased used of encryption). However, there has been little progress in rethinking services to be Secure-by-Design and Privacy-by-Design. Increasingly, both EU and non-EU healthcare service providers have been seeking access to European healthcare data, creating a vacuum for innovation.
Effort until now	European Commissions R&D programmes have resulted in the demonstration of new technologies, solutions and pilots deployed in limited setting. These are yet to be deployed on a pan-European scale. The calls SU-TDS-02-2018 and SU-TDS-03-2018 focus on the health sector and in particular on hospitals, with the aim to reduce the cyber risks to the former and to raise awareness and develop training schemes for the latter. Under the SU-TDS-02-2018 call, the PANACEA project looks at solutions for cybersecurity assessment and preparedness of Healthcare ICT infrastructures and connected devices. ProTego will focus on advanced data protection measures to reduce the risks in hospitals and care centres. CUREX will look into GDPR-compliant solutions for the secure and private exchange of data, while SERUMS will focus on securing medical data to enhance personal care solutions. FeatureCloud will look into solutions for minimising the potential of cyber-crime and enabling first secure cross-border collaborative data mining endeavours. SPHINX will provide a vulnerability assessment toolkit and ASCLEPIOS a secure cloud encrypted platform.

	The SecureHospitals.eu project, funded under the SU-TDS-03-2018 call, aims to set up training schemes and initiate training sessions for IT staff working in hospitals with the aim of improving the knowledge of staff and in turn contribute to decreased vulnerabilities against cyber threats and increased patient trust and safety. In the area of critical infrastructure protection, SAFECARE seeks to provide solutions which aims to improve physical and cyber security in health sector by developing and promoting new technologies to enhance threat prevention, threat detection, incident response and mitigation of impact. Projects developing relevant technology include (but are not limited to) • CyberSANE: Protecting critical information infrastructure from cybercriminals. It addresses the management of cybersecurity incidents from warning to response, specifically targeting European Critical Infrastructures. • SHiELD: European Security in Health Data Exchange • KONFIDO: Secure and Trusted Paradigm for Interoperable eHealth Services • EPSOS: Smart Open Services - Open eHealth Initiative for a European Large Scale Pilot of Patient Summary and Electronic Prescription • DECIPHER: The DECIPHER Project (Distributed European Community Individual Patient Healthcare Electronic Record)
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	• Proper cyber security awareness for healthcare personnel, usually one of the weakest points of the chain. Digital training programs • New methods to protect the hospital IT infrastructure, to prevent and mitigate cyber-attacks, protecting devices, associated workflows and data. • Increased resilience and recoverability of hospital IT infrastructure. • Improved analysis over the interconnections between physical and cyber security and interdependencies. • New tools for identity and access management considering the specific needs of medical personnel (emergency access, 24x7, teams, …). Medical teams need to be able to focus on care and should be relieved of current access control mechanisms such as passwords; at the same time enforcement should enable access only to authorized personnel. • Secure deployment and maintenance for dispersed networks of medical objects. • Secure system and software development for medical systems and devices. • Secure healthcare information sharing multi-organization and cross borders with federated infrastructures (where possible due to GDPR and national policies and considering privacy technologies).

	• Secure communications with focus on integrity and availability, including command and control of the object, and maintenance (e.g. software). • Secure digitalization of standard medical procedures such as patient consent gathering and management.
Expected benefit; strategic or economic impact **➔ What can be achieved?**	• Sustainability of healthcare system by adaptation of latest advances in ICT and sensor technologies. • The EU has specific needs with respect to the medical sector. It also has global companies that are strong in the domain, yet need to strengthen their position in the global data-driven healthcare services market with regard to cybersecurity and privacy. • The expected benefit is to leverage the digitalization of the medical environment to ensure better efficiency of care while maintaining costs under control. • Facilitating secure access to medical services to citizens with reduced mobility or in remote locations. • Among the sectors, healthcare is actually one of the favourite targets of hackers and the technology and human awareness gap is evident and not constant through the EU. This condition, if properly improved, will lead to cost reduction and reduced incidents impact. • New data-driven services made possible thanks to the adoption of technologies reducing security and privacy risks to healthcare data.
Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 8
Timeline (2025/2027/beyond)	Launch up to two projects in the period in the challenge areas to focus on pan-European deployments and reach the impacts for 2025 and beyond.

Smart cities and smart buildings (convergence of digital services for citizens) and other utilities

Horizon Europe – HEU.2.D7	
Specific Priority	**Smart cities and smart buildings (convergence of digital services for citizens) and other utilities**
Description of the challenges – why is it important?	Smart Cities are an IT-enabled urban space that collects, manipulate, share and analyse data to improve citizens' quality of life. The creation of IT infrastructures that implements smart cities functionalities is a complex and always evolving process, often driven by technological progresses, and influenced by political and societal changes. Furthermore, the speed at which the IT systems are interconnected to form smart cities infrastructures is continuously changing the attack surface and thus the cyber risk for public and private smart city providers. Also, the mutual interconnection between IT systems and physical devices (traffic infrastructures, water and electric supplies, etc.) is expanding the impact of cyber-attacks and incidents from the digital world (causing data breaches, denial of services, data leaks, etc.) to the physical one, thus potentially becoming a threat for the

security of citizens. Some of the main cybersecurity challenges are detailed as follows:

- **Technical and organizational complexity due to convergence of services and utilities.** The smart city is a system with technical and organizational interdependencies between functions and infrastructures that are critical for citizens. This involves both new opportunities (e.g. innovative solutions, integrated, real time risk monitoring) and challenges (increased potential for common-cause errors and cascading failures). There is a potential for risk aggregation effects in creating tighter couplings between systems that have hitherto been loosely coupled. This potential needs to be addressed, understood and managed in a holistic/comprehensive manner, instead of considering the cybersecurity of solutions one by one. Moreover, resilient capabilities need to be integrated to cope with the increasingly extended perimeter of digitalisation, which is pervading the physical world, as well as unexpected and unintended consequences of increased digitization.
- **Larger attack surface dependent on new technologies** – Smart cities connect several infrastructures frameworks to provide a complex and heterogeneous system of services. These infrastructures offer a large attack surface: they are multi-layered, multi-operator, distributed, and often opaque. In addition, they will increasingly rely on the features of 5G (multi-device connectivity, high speed, low latency) and IoT, which not only increases efficiency but also improves citizen/consumer services by connecting products, assets, fleets, infrastructures, markets and people. Therefore, IoT cybersecurity vulnerabilities need to be addressed in the specific context of 5G implementation (e.g. radio interface security, cryptographic integrity protection, roaming security, DoS attacks on the infrastructure as well as on end-user devices).
- **Unlinkability and minimal disclosure for smart city services:** Smart cities offer access to online public services requiring user identification and, in many cases, verification of certain attributes, such as age or country of residence. To prove the veracity of the attributes users usually have to present extra information (e.g., electronic ID or credit card) that contain full name, nationality, etc. Also, service providers can collude to track users and share their data, compromising users' privacy. There is a need for an identity management system that provides both minimal disclosure and unlinkability between service providers on the same area.
- **Distributed oblivious identity management:** An Identity Provider (IdP) that generates tokens to prove users' identities for their online and offline transactions can track users' activity, learning which services they interact with and when these interactions occur. This is particularly true for regional and/or local IdP that can track online activities of the citizens in the area. Distributed oblivious identity management systems could help to deal with it, as they split the role of the online IdP between multiple authorities, so that no single authority can impersonate or track its users. This approach poses several challenges, such as: (i) the specification and development of the system architecture as well as the cryptographic tools needed to perform the role distribution, (ii) the transparency of the distributed issuance to relying parties

	and (iii) the overhead of using a distributed approach (complexity), while maintaining the same level of security as in the single IdP case. • **Privacy preservation in blockchain:** smart city services are typically enabled by processing trustworthy data from a huge number of heterogeneous sources, therefore blockchain can concretely support this type of scenario. However, blockchain is subject to different scalability, security and privacy issues such as transaction linkability, on-chain data privacy, or compliance with privacy regulations (e.g. GDPR). In the context of Smart Cities, which heavily rely on complex IoT ecosystems, blockchain needs to be adapted in scenarios with resource-constrained devices. These limitations, which affect many IoT devices acting as data sources, make difficult to implement privacy solutions. Therefore, there may be cases where a specific device may not be able to manage operations based on blockchain. • **Authentication:** users access smart city services across heterogeneous systems. As the amount of authentication data is growing exponentially, secure, effective and real-time authentication is key. Regardless of the methods adopted, user credentials should be strongly protected, in order to prevent information from passive attacks or exposure to the wrong source. Multi-token passwords or passwordless authentication are among the emerging solutions. • **Disconnection between IT and OT management in Smart Buildings** – today, building management systems rely on a combination of OT and IT protocols, improving the operation of smart buildings but also representing a potential target for cyberattacks.
Digital Living & Working	The covid19 pandemic has made us realize the importance of internet connectivity during confinement. The high demand for connection, whether for entertainment or working has exploded in such a way that internet suppliers and internet services have seen compromised their scalability, having to reduce the quality of their services as a consequence. The large amount of data and communications in turn provides a perfect scenario for attackers to obtain information and compromise critical systems such as banking or electricity. This situation also implies that any usual procedure must be done electronically, using, for example, electronic certificates, so that the security risks and the attack surface has been increased. Being most city employees forced to work on distributed devices at home, the likelihood and scale of cyberattacks on local government, which was growing anyway, has experienced an unprecedented increase. The situation is exacerbated by • the higher number of remote devices in use, the lack of a unified network and the need to continuously protect all systems the same time • the fact that, even before COVID outbreak, especially small and mid-sized cities did not have adequate internal IT staffing or resources. When adopting third-party solutions, cities must in addition be aware and careful of their risk policies and vulnerabilities.

	On the other hand, smart cities can provide useful real-time data, e.g. information on the concentration of citizens in a given area, aggregated data on symptoms received from healthcare operators and structures, or even providing information on the stock available in the supermarket, so that unnecessary displacement can be avoided. However, much of this information is highly sensitive, so protection measures are crucial to protect the privacy of citizens, while protecting their health.
BASELINE	
What has been done so far (in EU and in the World – EU position)	The major effort so far concerns the standardization of smart city infrastructures as well as to secure the exchange of data across the IT systems of a smart city (including devices and sensors). A number of bodies and associations are active on this context, including: • European innovation partnership on smart cities and communities (EIPSCC), which includes cities, industry, SMEs, banks, research and other smart city actors and is supported by the European Commission • United Smart Cities, a multi-stakeholder project coordinated, governed and implemented by the Organization for international Relations (OiER) and the United Nations Economic Commission for Europe (UNECE) • Smart America • NIST Global City Teams Challenge (GCTC), • Smart cities and Communities Framework (SCCF) series Other organisations supporting the development of smart cities are: European Network of Living Labs (ENoLL), Open & Agile Smart Cities (OASC) and the 'Join, Boost, Sustain' movement to support the scaling up of open, interoperable, cross-sector and cross-border digital platforms and digital solutions across the EU, led by EUROCITIES. There are also several finished European projects with focus on smart cities. • Secure and sMArter ciTIes data management (SMARTIE) developed a distributed platform to share large volumes of heterogeneous information for application in smart cities. • RERUM: REliable, Resilient and secUre IoT for sMart city applications, developed an architectural framework for dependable, reliable, and secure networks of heterogeneous smart objects supporting innovative Smart City applications. • CpaaS.io: City Platform as a Service Integrated and Open, which developed an open cloud-based platform that can form the basis for a smart city data infrastructure. • ALMANAC: Reliable Smart Secure Internet of Things for Smart Cities
Effort until now	There are several projects that are in process with a strong focus on smart cities: • SynchroniCity conducted and extensive review of smart cities SotA and proposes a reference architecture based on the OASC

	"Minimal Interoperability Mechanisms" (MIMs) for IoT-enabled cities • IoTCrawler focus on integration and interoperability across different platforms, dynamic and reconfigurable solutions for discovery and integration of data and services from legacy and new systems, adaptive, privacy-aware and secure algorithms and mechanisms for crawling, indexing, search in distributed IoT systems. It provides demonstrations on Smart City and Smart Energy • Fed4IoT focus on multilevel IoT interoperability for cross-domain, large-scale smart city applications • COMPACT put forward an adaptation of the Plan-Do-Check-Act model to increase the cyber resilience of Local Public Administrations (a major stakeholder of each smart city platform). • CyberSec4Europe is working on a roadmap, and a corresponding demonstrator, to secure smart city platforms.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	• Security is a shared responsibility, and this is mostly true for complex and heterogeneous systems, like smart cities. Holistic approaches to smart city protection must be investigated that consider all involved actors (including citizens). These should be based on well-defined security objectives, policies and processes that are shared, and well understood, by all smart city participants. Interoperability from a cyber security perspective should be established between the infrastructures in order to allow for early detection of cyber-attack and remediation actions to be taken. • Frameworks enabling cities to assess and reduce their overall risk for expected events, instead of only assessing the risks of singular systems and infrastructures. Moreover, resilience assessment needs to be implemented to enhance capabilities to cope with unexpected events. This requires developing the capacity for resilient performance, coordinated and collaborative governance. • Solutions for credentials privacy, secure authentication and identity management to be adopted in the specific context of Smart Cities, taking into account the amount and diversity of connected devices, the types of data accessed and exchanged (which are sensitive in several cases) and the social acceptance of the methods introduced. • Development of blockchain privacy-preserving approaches following a self-sovereign identity management approach (i.e., allowing for the possibility of using non-interactive zero knowledge proofs), while maintaining the capacity of unveiling the real identity of the owner when the inspection grounds are met (e.g. identity theft or associated crimes). Those approaches should be tailored to address the specific challenges of IoT ecosystems enabling Smart City services and envisage the application of empowerment techniques for end users to ensure privacy enforcement. • Improve the security level of smart cities by training software engineers and informing users about the security and privacy risks they could face.

	Relevant technologies complemented with sufficient expertise and organisational capabilities considering a user centre approach considering ethics and trust aspects and citizens needs: • **Privacy Enhancing Technologies:** Digital identities are necessary to unlock the potential of smart cities. However, current authentication and identity management (IdM) mechanisms have difficulty meeting the necessary security and privacy requirements while maintaining acceptable usability levels. Privacy, which is regulated by the GPDR, is key to increase user's trust and protect its identity and sensitive data, and to avoid attacks derived from its lack, such as identity theft, data leaks, phishing, extortion or forgery. To deal with it, it is necessary further research on cryptographic techniques for making cracking hard, by means of computational effort (e.g., by using several layers of encryption and hashing), protected database storage of non-text-based credentials, attribute base credential mechanisms, and password-less authentication mechanisms integrated with alternative authentication methods (e.g. biometrics) that could be device-centric. • **DLT and Crypto Currency:** DLT offer a decentralized, immutable and verifiable ledger that can record transactions of digital assets, making them a potential technology to be used in smart cities. However, there are still privacy issues that has to be solved. It is necessary research to integrate and adapt privacy-preserving solutions with technologies like anonymous credentials systems and blockchain implementations. • **Cyber secure future communication systems and networks (5G/Fog/Edge/Cloud):** 5G is designed to allow wide geographic coverage, stable connection and high-speed data sharing, therefore its employment within the smart city scenario has strategic value to increase service levels, convenience and accessibility. 5G demonstrated to function as a solid and sophisticated network, but its employment could introduce privacy and security issues. Further research is needed to assess risk, threat and security as well as privacy matters in different use cases. • **IoT Security:** IoT systems are among the key technology enablers of smart city ecosystems. Therefore, increasing security at device, platform, application levels, taking also into account the relation with new connectivity solutions is fundamental.
Expected benefit; strategic or economic impac0t ➔ **What can be achieved?**	• Fully achieving the benefits of a smart city ecosystem: improving the efficiency of public utilities, increasing digital equity, improving infrastructures, fostering economic development opportunities, performing effective data-driven decision making, reducing environmental footprint and, overall, improving the quality of life in urban centres. • Increasing alignment and compliance with GPDR regulation on data privacy protection. • Transparent, regulated and privacy preserving technologies, which avoid large-scale mass surveillance, by private companies, criminal organizations or public authorities, with all the potential negative implications if the collected data is used against the users or citizens.

	• Reduction of the threats associated to the privacy preserving identity management (e.g., identity theft, phishing, forgery, linkability and profiling or data leakage) and derived from it (e.g., DoS, surveillance or extortion). • A stronger, more innovative and more competitive EU cybersecurity industry. • Increased users' trust in European products. • Innovative (novel or improved), integrated, and incremental solutions to prevent and mitigate privacy issues within ICT systems and users.
Starting TRL / Expected TRL	**Starting TRL:** 3-5 **Expected TRL:** 6-7
Timeline (2025/2027/beyond)	2025

Robotics

Horizon Europe – HEU.2.D8	
Specific Priority	**Robotics security**
Description of the challenges – why is it important?	In Robotics, "the art of system integration" finds its paramount example. The majority of robots are equipped with the "ability" to sense, process, and act with the world around them. The field of robotics benefits from continued advancements in a variety of disciplines, such as mechanical engineering, computer science, material science, sensor fabrication, manufacturing techniques, etc. Robots are designed for specific tasks, such as assembling or repairing, which may not be readily adaptable for other applications. Over the last two decades, several researchers and practitioners have attempted to tackle this problem and explain the unusual characteristics of robotic systems. Robots have been introduced massively in the manufacturing industry as well as in everyday life. Due to their potentiality to cover several applications in our lives, the diffusion and development of new robotic systems is expected to increase day by day. In the last decade, the field of robotics has been pervaded by the emerging technologies like Machine Learning and AI (Artificial Intelligence), IIoT (Industrial Internet of Things), human-machine collaboration or autonomous and adaptable mobile systems. In this context manufacturers often overlook cybersecurity and safety aspects during the design and production phases. Robotic applications, such as autonomous cars, drones, entertainment robots, medical robots, are among the most exposed to cyber-security vulnerabilities that might negatively affect safety (if there might be implications for humans or the environment), service quality (which can be dramatically expensive for mission-critical systems or critical infrastructures), or privacy (if the robotic system manages personal data "in the edge" or "in the cloud").

	Robots are no longer standalone applications that you can forget about the relationships with the outer world. Nowadays they are rather complex system with multiple relations and collaboration where the cybersecurity is a great challenge as it could affect to safety, which should be considered a critical aspect to ensure. Therefore, it is necessary to have a good understanding of the robotics system to assess security risks and threats. The most critical challenges for a wider applicability and usage of robots are those relating to the rapidly changing consumer trends, shortage of resources and skilled workers, aging society, demand for local productions and cyber-security risks looming over the dawn of a yet immature industry.
Digital Living & Working	The connection between IT systems and operational technology (OT) is useful to guarantee the safety of plants as well as the integrity of the manufactured product even when faults, human errors, or other abnormal conditions occur. It's necessary to get cyber security and robotics experts to identify solutions to managing security aspects in robotic systems. Nowadays, manufacturers don't pay enough attention to security, but the fast-growing robotics market must focus on risks and threats in this field. Additionally, manufacturers use commercial off- the-shelf (COTS) products, which, on the one hand reduce the costs, but, on the other hand, expose them to supply chain attacks and propagation of vulnerabilities. Industrial Control Systems (ICS) use a wide variety of insecure communication protocols, such as Modbus, PROFINET, DNP3, and EtherCAT, which do not have the security mechanisms to support authentication or packet integrity. Communications are, therefore, a vital part of a robot's ecosystem. Mobile application or Internet services/cloud resources use the Internet, Bluetooth or Wi-fi without properly securing communication channel. For example, robots need to connect to the Internet to send data to cloud vendors. The literature shows that cabled communications are still used in different environments, such as: • Industrial context: smart manufacturing cells; • Medical context: Surgical and diagnostic applications; • Other context: operation of inspection and limited operational actions.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Security was already identified as one as one of the most critical factors in today's highly and continuously interconnected systems. Therefore, there have been a plethora of efforts from all actors all over the world (government, academia, industry, and standard bodies) to provide security and privacy to production ecosystems. These efforts have resulted in multiple research projects in Europe (under FP7 and H2020) and all over the world, whose results have enabled the development of several security and privacy technologies, various reference architectures aimed for specific verticals (e.g. healthcare, industrial systems), multiple standards, and many cybersecurity laws and recommendations. Robotics continues to open new opportunities and benefits in terms of efficiency and economic convenience. Not only do these advantages encourage improvements in manufacturing and trade, but also in sectors, such as transportation, medical

	assistance, education, and agriculture. However, despite these advantages, the development of robotics can also lead to severe problems in the legal and ethical sphere. For example, some issues may include civil or criminal liability connected to the use of robotic systems. The effort to regulate such a complex subject is, therefore, not exempt, among others, from a part dedicated to the regulation of trustworthiness aspects of robotics, such as safety, security, privacy, resilience and reliability.
Effort until now	SafeCOP (Safe Cooperating Cyber-Physical Systems using Wireless Communication) defines a safety assurance approach, a platform architecture, and tools for cost-efficient and practical certification of cooperating cyber-physical systems (CO-CPS) with an application to robotics. The SecureIoT provides implementations of security data collection, security monitoring and predictive security mechanisms, which can be leverages to offer integrated services for risk assessment, compliance auditing against regulations and directives (e.g. GDPR, NIS, ePrivacy), as well as support to IoT developers based on programming annotations. The TRINITY project proposes a network of Digital Innovation Hubs (DIH) for advanced robotics. In particular the network will focus on collaborative robotics and demostrators of digital tools, data privacy and cyber security technologies to support the introduction of advanced robotic systems in the production processes. Robotics is one of the domains for the applicability of the solutions. The recently funded RESPECT project will focus on creating a sustainable European and inter-sectoral network of organisations working on a joint research programme aiming to design and develop concrete defense strategies to ensure secure, safe, resilient and privacy-preserving operation of indoor mobile robotics solutions for logistic applications in healthcare environments.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	The increasing dependence of businesses and customers on robotics devices and applications is leading to an exponential growth in terms of cyber risk. Cyber-attacks exploit any type of vulnerabilities concerning robotics systems, whether they are come in the form of software or hardware, or are dependent on the person who uses them. Thus, because cyber-attacks are on the increase in this field, several scholars and experts are bringing cyber security into much prominent focus when trying to find methods to mitigate cyber threats in robotics. Challenging aspect are: • Manufacturers use commercial off- the-shelf (COTS) products, which, on the one hand reduce the costs, but, on the other hand, expose them to vulnerabilities; • Industrial Control Systems (ICS) use a wide variety of insecure communication protocols, such as Modbus, PROFINET, DNP3, and EtherCAT, which do not have the security mechanisms to support authentication or packet integrity; • Network security improvements, such as secure routing, cryptography, and network level privacy;

	• Secure connectivity and interactions with external infrastructures (e.g. edge computing); • Mitigation of DDos Attacks; • Data protection and compliance with legislations and directives; • Assuring application robustness, due to an increased attack surface and the pervasive use of the technology; • Secure and trusted interaction between multiple involved parties, such as users, device manufacturers, cloud service providers, network operators, and others; • Definition, implementation and integration of secure software engineering tools (e.g. formal verification tools) and principles (e.g. security-by-design) to allow the definition and development of secure devices, infrastructures and applications; • Security debt identification and measurement in Robotics systems; • Procedures that can produce concrete security guarantees for the overall system along the whole product chain, and means for continuously monitoring and ensuring those guarantees; • Contract-based design to automatically verify security properties in the integration of subsystems; • Supporting robot's entire lifecycle to achieve a trustworthy (safe, secure, private, reliable, resilient) robot that can demonstrate compliance with the applicable European directives • Conformity assessment and the test necessary to get CE marking • Manufacturers can inherit cybersecurity risks from their system providers in bespoke software and systems that will be integrated in the robot • Artificial Intelligence techniques can be included through the robots' development lifecycle to build and integrate more secure systems • Distributed and lightweight authorization and authentication mechanisms, including scalability of authentication in resource constrained devices and authentication in federated and dynamic environments; • Development of Intrusion Detection Systems (IDSs) able to cope with multiple devices, networks and platforms; • Detection of new vulnerabilities linked to the future evolution of consumer, business and industrial environments; • Interoperability techniques for the different security and privacy mechanisms, including trust management models; • Security audits and certification procedures for production cells and robotic platform, including platforms, services, and distributed devices; • Identification and management of tradeoffs and conflicting situations between safety and security aspects (e.g., a security measure prohibitively affecting the performance of a safety function). Effective dependability co-engineering mechanisms should be in place to conciliate and take decisions between the safety and security teams/domains of expertise;

	• Cybersecurity of intelligent swarms and swarm robotics. Finally, Robotics faces prominent challenges on security in the following areas: • Collaborative Robotics; • Autonomous vehicles; • Autonomous Robotic platform; • Adaptable robots; • Regulation and regulatory frameworks. Research and development in the robotics field shifted from a focus on industrial robots to a focus on intelligent robotics. This shift created methods of easier integration to create robotics systems, which are capable of providing promising results in different areas of robotic research, such as artificial intelligence, cognitive robotics, human-robot interaction, multi-agent systems for mobile robot collaboration, etc. In particular, the use of AI and ML algorithms led to new security and safety challenges. The introduction of mandatory regulatory requirements will probably slow down the pace of progress in robotics, but the current advanced robotics systems have enormous potential to transform many aspects of people's lives.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	As Robotics is strategic for European economy and social good, having a large impact both for mass market or industrial applications in all vertical sectors (Transport, eHealth, smart cities, industry 4.0, energy, etc.), the security of Robotics has been identified as one of the strategic topics. Solving all previously mentioned gaps and challenges will make Robotics environments more secure and resilient against failures and attacks. This will increase trust in this field, which in turn will facilitate its integration into critical infrastructures and personal life systems, not only in Europe but also in other countries around the globe. This will strengthen the position of Europe from a technological and economic point of view.
Starting TRL / Expected TRL	**Starting TRL:** 2-4 **Expected TRL:** 5-7
Timeline (2025/2027/beyond)	2025

Agrifood

Horizon Europe – HEU.2.D9	
Specific Priority	**Agrifood**
Description of the challenges – why is it important?	**1. Protect agrifood data** The European Green Deal has highlighted major strategic lines including the push for sustainable production of food, the incentive for shorter supply chains. This has a direct connection to the agrifood sector that is increasingly become digitised. In parallel, this has positioned the agrifood industry as a new target for cyber attacks,

which have increased in 2019[30], [31]. The digitisation started first within a single organisation, with farms combining local sensing with data such as weather predictions, historical information to impact their own approaches. But increasingly, the digitisation has moved to include exchange of data – used to improve local decisions based from knowledge elaborated from sharing information, used also for instance for traceability along the complete supply chain.

Therefore, this domain is increasingly relying advanced sensing and monitoring systems, Global Navigation Satellite System (GNSS) and automated machineries and robots for farming, food tracing and food quality management. This increases the need to access third party systems and components to handle huge amounts of data related to operational processes (plant growing and health, animal behaviour, quality and quantity of production, periodic yield & loss). Due to the specificity of the domain, this data can be managed along very different timelines, from real-time sensing to daily or weekly consolidations for full chain traceability. Data in the agrifood sector has therefore become a) an operational support to individual stakeholders and b) a pillar of the competitiveness of food supply chain, in terms of actors (relevant to all actors in the supply chain from farmers to consumers) and over the lifetime of a supply chain (from selection of crops to consumption of food, including in the 'farm to fork' shorter supply chains). This data is also strategic for prediction – which in the agriculture impacts the selection of crops for the **upcoming year**. The introduction of artificial intelligence (AI) components allows the exploitation of very diverse data to train predictive models able to improve the use of Decision Support Systems (DSS) to improve crop selection (based on economic potential, client base, geography, climate etc). Using sensing generated data, improvements lead to optimised environmental management of resources (water, fertilizer, pesticides etc).

In this industry, data is therefore positioned both as an **enabler** of the competitiveness of the sector and as an **asset** that has an economic value that should increasingly benefit the actors who generate the data (farmers, food transformation industries etc). Protecting both the data and the algorithms that transform it into knowledge from cyber-attacks is a strategic need.

2. Promote secure and protected data exchange.

The full potential of AI based predictive and real-time modelling can only be delivered by enlarging the scope and availability of data from a wide range of sources. To properly train models, the diversity of local conditions and markets has to be represented – and this requires sharing models at a large scale but fine tuning them to local conditions. However, there are still several factors preventing agrifood sector from achieving the full benefits of data exchange and intelligence. They include lack of perceived value of data (from several players in the supply chain), poor quality of data and/or data collection, lack of technology awareness (concerning the potential of AI, IoT, DLT, etc.),

[30] https://www.stormshield.com/news/the-food-industry-a-new-target-for-cyberattacks

[31] https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting_web.pdf

unwillingness to share (due to competitive reasons) and legal issues (e.g. data confidentiality). Furthermore, the data exchange adds a novel issue to agriculture digitization related to the security of systems and sources where data are stored or come from.

Therefore, a complete trust-based data exchange mechanism is key. Federated training approaches that are already used have to be extended to reach a point where players in the same domain (for instance farmers) or players connected along a food supply chain agree to collaborate.

Challenges are not only visible at organizational level, but are strongly chain focused with shared cybersecurity responsibility:

- digital infrastructures (of the chain)
- human errors and social engineering sources of attacks
- multiplicity of connected devices and diversity of sources (devices connected to a tractor, versus on-field devices for climate sensing etc)
- use of external data sources

3. International environment.

Many agrifood chains operate in an international environment, crossing borders, and dealing with different legislation. These are further elements of complexity to take into account when dealing with cybersecurity in Agrifood. In addition, some supply chains have very low traceability.

For example, the supply chain in the seafood industry is opaque and complex. Information is maintained in silos by separate supply chain actors, and it is nearly impossible to fully or effectively trace a product from its origin to its fate. For instance, a single fish caught in the North Sea might change hands numerous times and undergo multiple forms of processing and packaging before being sold in a distant location. This supply chain ecosystem has a very low level of transparency, and this is used by some market players to operate undermining legal and ethical standards. A study[32] has shown that up to 23 B$ of global fisheries value is lost due to illegal, unreported and unregulated fishing activities. The use of data across this chain is therefore also strategic to combat and improve the societal, economic and nutritional quality of the supply chain.

4. Agrifood is a strategic industry for cyber attackers with a wide list of motivations:

- Competition: agrifood is a domain in which reputation is a key asset. Cyber attacks can be carried out on the processing environment (food transformation sites) that in turn modify the product quality and totally destroy a company.
- Speculation: food stocks or commodities are represented on the stock market and cyber attacks on the underlying products can be used to modify the market value
- Geo-political: food is a critical resource across the world - attacks that undermine the production or the delivery in the

[32] Zabarenko, Deborah. "Fish piracy costs $10 billion to $23 billion a year." Reuters. May 8, 2013.

	agri-food sector can directly impact access to food, with impact on health and on the economy (link) • Societal: undernutrition is one of the world's plague[33], with close to 500.000 undernourished individuals at world-wide level. The key indicators in this domain are to decrease food loss (from poor harvesting) and food waste (throwing food away, lack of proper dispatching of food). Data is a key enabler of improving both food loss and food waste – and cyber security has to protect this data.
Digital Living & Working	There is a need to increase the transparency about food products from the producers, via processing and transportation companies and finally to the consumers. This requires data to move across borders, oceans and airspace in an open and tamper-proof way.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Information Sharing • USA: FBN https://www.fbn.com/ is an independent data platform which collects data from thousands of farmers (7 million acres of farmland across 17 states). This data feed the DSS features. • EU: a Common European agricultural data space will be established (EU Data strategy Communication 2020) to enhance EU agriculture competitiveness and sustainability by Big Data exploitation • EU: a set of organisations[34] have elaborated a EU Code of conduct on agricultural data sharing by contractual agreement Security Standard There is no dedicated security standard for smart agriculture, but the sector can choose from several others, e.g. ISO 27001, NIST cybersecurity framework to have guidelines for reducing cybersecurity risks. Governance • The EU Data Strategy communication foresees a legislative governance framework for data sharing by end of 2020. This governance will not be sector specific but will introduce the EU Data Spaces, including the EU Agriculture Data Space. Similarly, a Data Act is foreseen by 2021, addressing the topics of IPRs (protecting both data and algorithms), and defining the business market mechanisms for data sharing in different bilateral relationships (Governance-To-Business (G2B), B2B, G2G, B2G) Data exchange Distributed databases have been shown to be an inadequate solution as records and logs can be deleted or modified to reflect the manipulated values. Blockchain technologies, on the other hand, is a

[33] https://www.who.int/nutrition/topics/world-food-day-2019-malnutrition-world-health-crisis/en/

[34] https://www.ecpa.eu/sites/default/files/documents/AgriDataSharingCoC_2018.pdf

	more promising solution, but shown limited application in agrifood sector due to insufficient and immature mechanisms to track perishables across large geographical expanses and across multiple countries and organizations. They have also been implemented following different security and privacy regulations and standards across different countries and organizations, resulting in systems mismatching or operating in unstable network environments.
Effort until now	• Standards for Traceability: NIST U.S. Department of Commerce (National Institute of Standard and Technologies) is working on the development of new standards, tools, and guidelines for traceability and cybersecurity that increase trust among participants and customers of agri-food manufacturing supply chains. Link • Food Defence Guide (France, 2018): Food Defense Program shall be developed to reduce the risks from both internal and external threats in order to protect final customers. • Individual companies: as an example, Triskalia (a French agriculture cooperative) is an example of an organisation that adopted individual cybersecurity measures. Their IT management team have installed firewalls, antiviruses on all workstations and above all are trying to train staff as best as possible. So that they know how to manage their emails well and avoid clicking on prohibited addresses. Triskalia also made important investments in new projects launching, together with Even (another agricultural cooperative), a call for ideas to select and finance start-ups capable of providing new tools for better plant safety.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	The common EU agriculture Data Space could be a starting point to protect EU agriculture Data from cyber-attacks, not only at individual organizations level, but from a potential nation-state (EU-state) attack against the agriculture sector. The key point is the upcoming governance foreseen in relation to all data spaces, and how this governance will be the basis for the specific domain needs. Through the existing EIP-Agri and the network of DIHs, all operators of agrifood supply chains should be made more aware of a) the value of the data they generate, b) the potential use that they can do of their own and other data, c) the need to fully manage the security of this data. The employment of Blockchain technologies has proven to effectively support an increase in trust and transparency alongside the Agrifood supply chain. However, those system are too sophisticated to be implemented by small producers and they should be adopted at the level of supply chain to be really effective. In addition, there are still scalability, interoperability, privacy and data governance issues to be addressed. Therefore, the implementation of this type of technology should be achieved through a multidisciplinary perspective taking into account technical, societal, legal, safety and security factors.

Expected benefit; strategic or economic impact
➔ **What can be achieved?**
	• increased awareness of data value
	• increased trust in data
	  • increased uptake of digitisation by smaller farmers (over 90% of European farmers), shorter chains (farm to fork, circular economy, contribution to Green Deal objectives)
	  • better returns (higher quantity of food per surface) and increased food autonomy for Europe
	The fish market is a growing, demanding market where both producers and consumers demand more information about their products. Technology supporting transparency and accountability through the supply chain can improve the implementation and monitoring of international trade[35].

Starting TRL / Expected TRL	**Starting TRL:** 5 **Expected TRL:** 7
Timeline (2025/2027/beyond)	2025: • European Data standards for sharing and protect food related data • Further availability of Agri-related Open data at EU level (with a wide countries' coverage) with strong cyber protection. Agriculture Data Space populating can be the opportunity to addess this objective. • A wider spread of awareness regarding cybersecurity concerns and risks to farmers (including medium and family based ones) providing them training on how to manage cybersecurity issues and protect their business, individually and collectively (within the chian) • Food chain tracing within a selection of European countries, with a focus on protected cross-border traceability • Food traceability in short circuits: the circular economy strategy and the current COVID pandemic are accelerating the uptake of short circuits. However, any food security issue stemming on short circuits could halt this expansion and therefore the specific needs of short circuits should be considered. 2027: Food chain tracing within the whole of Europe across all profiles of supply chains

Data and Economy

Data security and malicious use of data

Horizon Europe – HEU.3.A	
Specific Priority	**Data security and malicious use of data**

[35] Tripoli, Mischa and Schmidhuber, Josef "Emerging Opportunities for the Application of Blockchain in the Agri-food Industry", Food and Agriculture Organization of the United Nations, 2018.

Description of the challenges – why is it important?	We are entering a data-driven society, where it is increasingly important to sense, collect, process and act on data. For example, most, if not all, our critical infrastructures (energy, transportation, health, etc.) rely on increasing numbers of sensors to simply deliver the services we expect. At the same time, we are currently seeing an enormous increase in the importance of electronic data on decision making. Such data are now not only at the basis of many autonomous applications, including entertainment systems, self-driving vehicles, industrial robots, financial recommendations, and advertisement systems, but are also the basis of important democratic processes including public elections. Unfortunately, data created with a specific purpose may become a driver for cyber-attacks. For example, injecting, or using, corrupted data in critical infrastructure control systems may significantly disrupt normal operations. We already have significant examples where corrupted data and systems bring down some of our critical infrastructures, with at a minimum a significant economic cost (i.e. shutting down production factories for days) and potential risk to human life (e.g. hospital shutdown). Although one may think that there is always the choice to “opt out” of all data collection processes, this is getting increasingly difficult. Take for example, connected smart meters which are slowly replacing the traditional meters in public utilities. Smart meters generate data, use data and are a requirement for the proper management of energy production and distribution. Thus, regardless of privacy aspects, we will face the fact that data will be created and used. This challenge now needs to be faced by several actors including: • Governments and regulators need to specify the proper creation and scope of data needed to operate essential services, and enable auditing and verification, potentially certification; • Service operators need (i) to deploy data-secure systems for sensing and actuating, in compliance with regulations, and (ii) to detect data-related security breaches, both incoming (attempts to attack the infrastructure) and outgoing; • Organizations providing AI-powered services need to verify the integrity of data from trustworthy sources and to detect poisoned data from untrustworthy / uncontrolled ones. • End-users need understand how their data is collected and used; need to be notified and choose to participate in essential services data collection and need to be able to selectively opt-out of non-essential services. • Everyone needs to be vigilant about the creation, propagation, and use of corrupted (or just plain false) data. Such data may include fake news, corrupted statistics and even deep fakes: synthetic media which are practically impossible for most humans to differentiate from the real ones. We need (i) to provide organisations and citizens with technologies for identifying false data (including fake news), and (ii) to empower citizens with data management tools that are geared towards their own profiles, in order to ensure, and ultimately control, the

	dissemination of private or sensitive data. The issue here is not to discourage users from sharing, but to empower them with the appropriate tools that will encourage sharing and will enable quit opt out when desired. Protecting decision making processes from disinformation and counter-information activities is a vital task for any country and on the EU level.
Digital Living & Working	Injecting corrupt, false data or modifying the original data can alter the normal functioning or even disrupt the basic services such as electricity and water supply, causing economic loses and even human life risk. Special situations such as covid19, may have adverse impact at least along two important dimensions: • false news and fraudulent statistics may proliferate because (i) people spend more time on the Internet, and (ii) confinement does not allow physical corroboration of the facts. • More people will be forced to stay at home and monitor their health through sensors reporting to their doctor/hospital. Modifying health-related data captured or transmitted by these sensors may have a negative impact of the health and well-being of monitored individuals.
BASELINE	
What has been done so far (in EU and in the World – EU position)	This is a very recent area. However, because of its crucial role in public governance, the European Commission has already started a plan to deal with fake news and disinformation: https://ec.europa.eu/digital-single-market/en/fake-news-disinformation The EU has also published high-profile policy and legislation documents including the NIS directive, the EU Cybersecurity ACT, and the General Data Protection Regulation.
Effort until now	Several projects are already underway. Some of them are: • FAke News discovery and propagation from big Data ANalysis and artificial intelliGence Operations, FANDANGO https://fandango-project.eu/ • Confidential and Compliant Clouds, CocoCloud, data sharing agreements for data management in cloud and mobile environments https://cordis.europa.eu/project/id/610853 • Newtral, real-time automated fact-checking tool to fight against the fake news and disinformation https://www.newtral.es/automated-fact-checking/ • Fake News Recognition applying Service-based Cross-Media Analytics, TRUTHCHECK https://cordis.europa.eu/project/id/854497 • EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors, ENCASE, including analysis of social web data to detect fraudulent and fake activities https://cordis.europa.eu/project/id/691025 • Privacy-Enhancing Cryptography in Distributed Ledgers, PRIViLEDGE https://priviledge-project.eu/

	• decentraLizEd Data Governance for nExt geneRation internet, LEDGER, data sovereignty and governance https://cordis.europa.eu/project/id/825268 • Pooling SME adoption and deployment of Blockchain and other DLTs, BLOCKPOOL https://cordis.europa.eu/project/id/828888 • DECODE, tools that put individuals in control of whether they keep their personal data private or share it for the public good https://decodeproject.eu/ • Transformative Impact Of BlocKchain tEchnologies iN Public Services, TOKEN https://cordis.europa.eu/project/id/870603
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	There are two main ways to deal with malicious data: policy and technology. In this work we focus on the latter. Thus, we need to develop: • automated ways to test data-driven systems for biased and erroneous results • automated recognition and filtering out of fake/bad data (in particular, training data for AI models) • mechanisms to verify data provenance and integrity • models consistent with the observations of experimental data; models which can be converted in useful tools for anyone to use. It will also be important to • Understand the depth and breadth of data collected by third parties • Understand the goals and social acceptability of data processing, particularly in the context of societal challenges (e.g. critical infrastructure or public safety) where data is a necessary enabler. • explore how Artificial Intelligence algorithms can be trained without direct access to raw data - possibly by moving the computation to the data.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	By ensuring understandable and actionable data governance mechanisms, focusing on the understanding of data use, Europe will likely become a place where data processing is stimulated by the willingness of citizens to share data. The ultimate goal will be creating trust in data sharing, in the data, and the systems based on top of them. By recognizing poisoned/ fake data (and fake news), trustworthiness of digital services and content will be significantly improved. This will also improve the protection of democracy, the mechanisms that support it (such as elections), and the protection of the European market.
Starting TRL / Expected TRL	**Starting TRL:** 5 **Expected TRL:** 7

Timeline (2025/2027/beyond)	Working solutions being ready by 2025. Market adoption a few years later.

End-to-end Privacy

Horizon Europe – HEU.3.B	
Specific Priority	**End-to-end Privacy**
Description of the challenges – why is it important?	Protecting digital privacy is an extremely challenging task even more in a world scattered with billions of smart IoT devices. In these settings, privacy must be protected end-to-end: from IoT devices, where data is collected, to backend servers, where data is analysed and disseminated. Non-savvy citizens should be able to define data sharing policies in devices which lack proper user interfaces and intuitively evaluate and understand their overall privacy protection level. They should also be able to migrate or delete data at will, when changing or terminating service providers. In some cases, privacy is compromised automatically by the leakage of information through communication meta-data. For this reason, the ability to preserve anonymity is an important factor of privacy systems. Popular Privacy Enhancing Technologies (PETs) exist and are undergoing continuous analysis. It is important to empower citizens with new mechanisms for the protection of personal data throughout the complete lifecycle of personal devices, from acquisition to disposal, preventing data leakage and indiscriminate sharing with third parties. At the same time, privacy techniques need to comply with legal requirements related to digital investigation and prosecution, supported by digital forensics. There is thus a need for privacy-respectful digital forensics in IoT devices. IoT is one important example where guaranteeing end-to-end privacy is more challenging. In this case, lightweight data sharing protocols should be developed to enable the negotiation of the quality/type of the service provided based on the granularity, format or amount of data provided by the user, that is, enabling granular opt-in and opt-out. To achieve end-to-end privacy, we must prevent the leakage of information from the metadata associated to the data being generated, transferred or processed by IoT to other devices or backend servers. One long term approach to this involves Private Information Retrieval (PIR). So far, research in this area has focused on queries with zero information leakage. Although this concept is of considerable theoretical interest, current proposals are rather unpractical, and it is likely that a practical system should use queries of with limited information leakage.
Digital Living & Working	Digital life implies a larger exchange of data and a greater number of communications. As a large number of people move this working environment from their corporate offices to their homes, they are

	exposed to a mismatch of the security controls to which such data and communications are usually subject. Corporate offices usually provide adequate levels of digital protection. It is not clear if homes provide the same levels of protection.
BASELINE	
What has been done so far (in EU and in the World – EU position)	With the enter into force of the GDPR (General Data Protection Regulation), Europe has defined one of the most advanced privacy regulations in the world. But we still lack the adequate tools to support it in a world covered with connected devices and huge processing power. From a technical point of view, there has been a number of efforts in the protection of digital privacy. Some past EU calls have separately tackled data protection and digital identities; security and privacy in the IoT; and privacy-preserving data technologies for the Cloud but they typically lack the end-to-end perspective during the whole lifecycle of devices collecting personal data.
Effort until now	There have been some recent EU-funded projects that partially cover some of the aspects here discussed. For example: The PRISMACLOUD project is aimed at protecting sensitive data during its lifetime in the cloud. It considers the application of privacy-preserving cryptographic techniques. The iKaaS project will develop an intelligent, privacy-preserving and secure Smart City Platform based on a Big Data analytics. Prior projects dealing with privacy, data protection and digital identities include PRACTICE (Privacy-Preserving Computation in the Cloud), PrimeLife (Privacy and Identity Management in Europe for Life)
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	• Define usable mechanisms for citizens to understand and decide for themselves how to protect their privacy in a smart context • Enable an end-to-end privacy protection from the definition of privacy controls to the processing and dissemination of data in the backend. • One way of improving end-to-end privacy would be to study the implementation and deployment of end-to-end encryption, from the end device all the way up to the server or the cloud. • Develop privacy-aware forensic tools that can support both personal data protection and cyberattack investigation. • Develop erasure mechanisms that fully dispose all personal data after use when recycling, exchanging or renting devices (e.g. car rental, smartphone upgrade, etc.) • Provide mechanisms for smart devices capable of enabling forensics investigations while preventing the access to personal data when the devices are borrowed or disposed of. • Developments of solutions for proving data ownership and possession as well as for tracking personal data in order to be able to access, rectify or delete it regardless of its location.

	• Providing solid user-defined mechanisms for controlling data access and execution privileges even when the data is no longer in control of the user. • Definition of privacy-preserving real-time data processing mechanisms for massive data. • Design and analyse PIR systems offering limited information leakage per single query and for combinations of queries. Continue the development and analysis of Privacy Enhancing Technologies (PETs). Evaluate the security of onion routing based systems like TOR all along its attack surface.
Expected benefit; strategic or economic impact **➔ What can be achieved?**	• Citizens will have more control over and knowledge about their personal data without. • Companies will be able to share data from their clients with each other while complying with privacy laws. • Increased trust in the adoption of the countless contexts and scenarios involving smart IoT devices • New business models based on the monetization of personal data. Larger and more harmonious adoption of open data across the EU Member States.
Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 7
Timeline (2025/2027/beyond)	2025

Economic aspects of cybersecurity

Horizon Europe – HEU.3.C	
Specific Priority	**Economic aspects of cybersecurity**
Description of the challenges	Cybersecurity is the buzzword of the day, invoked with a sense of increasing urgency in high-level political fora around the world. At a time when we rely increasingly on digital infrastructure for the storage of data and the delivery of key services, those same assets become the main, and probably among the easiest target of cyberattacks. A report published in 2018 jointly by CSIS and McAfee estimates that the cost of cybercrime to the world is about $600 billion or 0.8% of global GDP. Against this background, the sum spent on cybersecurity worldwide was estimated in 2018 in $120 billion. The huge difference between the costs incurred as a result of cybercrime and the expenses undertaken to provide cybersecurity clearly shows that the market is not delivering the necessary quantity or quality of cybersecurity, capable of preventing the damage inflicted by cybercrime. Given this under-provision of cybersecurity, we need to examine whether the market is failing to provide the right amount of cybersecurity and what role can and should the government play in this context. Some of the concrete challenges include:

	• Why the market alone is not able to supply the optimal level of cybersecurity? • What kind of economic research needs to be done to guarantee an optimal level of cybersecurity that the market alone does not supply? • What kind of taxation, if any, scheme could be used for this purpose? Tax breaks for companies that buy cyber protection products or/and lower taxation to reduce the price of cybersecurity products and services? • Will this approach solve the problem of achieving market efficiency?
Digital Living & Working	Digital life implies a larger exchange of data and a greater number of communications. As a large number of people move this working environment from their corporate offices to their homes, they are exposed to a mismatch of the security controls to which such data and communications are usually subject. Corporate offices usually provide adequate levels of digital protection. It is not clear if homes provide the same levels of protection.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Many scholars understand cyberattacks as a problem of either criminal law or the law of armed conflict, whereas others conceive of it as a software issue, or a business one involving reputation, trust and insurance. It is important to understand, however, that many firms that operate critical infrastructure tend to underinvest in cyberdefence because of problems associated with negative externalities, free riding and public goods characterising the cybersecurity market.
Effort until now	Among the research projects EU funded, IPACSO, SECCORD, and ValueSEC, completed some time ago touched upon some of these issues.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	It is clear that new conceptual approaches to cyber-security are required to make the behaviour of all players in this market more incentive compatible and guarantee an optimal level of investment in cybersecurity. The role of cyber insurance and taxation need to be explored as well as the creation of stronger trust and coordination between public and private players as two essential pillars of any future EU cybersecurity strategy.
Expected benefit; strategic or economic impact **➔ What can be achieved?**	The economic analysis of Cybersecurity should allow a better cybersecurity policy design with the objective to find the right balance between *ex-ante* and *ex-post* regulation of cybersecurity to improve resilience without stifling innovation.
Starting TRL / Expected TRL	

Timeline (2025/2027/beyond)	Answers to these questions are needed sooner rather than later. There should be calls closing in 2021 and then again in 2024.

Basic and Disruptive Technologies

Secure and Trustworthy Artificial Intelligences

Horizon Europe – HEU.4.A	
Specific Priority	**Secure and Trustworthy Artificial Intelligences**
Description of the challenges – why is it important?	Artificial Intelligence (AI) approaches, with a prevalence of Machine Learning (ML), including Deep Learning (DL), techniques, are more and more used in a large variety of application domains, affecting individual, social, corporate and government activities. Current AI-based systems rely on a data-driven approach; thus, their trustworthiness is critically dependent on the procedures used to acquire, process and represent datasets for system training and validation. Specific crafted data can be used at the training time to mislead AI-based systems in particular contexts and cases (so-called model poisoning attacks), for example, to avoid detection of cybercriminal activities or to promote a specific product in an online recommendation system. Attackers can pursue similar goals at the inference time as well, by feeding to already trained models inputs utilizing imperfections of the models. Other attacker objectives can be exposing the data used for training models (threatening privacy and confidentiality) or replicating valuable models via iterative probing (so-called model stealing attacks). The success of AI in various tasks and domains is mainly related to the availability of good training data, computing platforms, tools, and libraries. At the same time, the complexity and dependencies on data and 3rd party technology make it extremely hard to specify security properties due to the difficulty in explaining the behaviour and the lack of control, and, consequently, to define a certification process. These factors also impact the auditability, including court-admissible forensics techniques. Consequently, the compliance of AI-based systems with regulations and legislations on data privacy, on system security and safety is currently difficult to assess. The above limitations and vulnerabilities of current AI techniques have also a negative impact on the adoption of AI-based approaches in many domains, with such examples from the cybersecurity domain as situational awareness and autonomous response.
Digital Living & Working	AI approaches are increasingly used for powering personal digital assistants, recommender systems, automated information and digital content processing, and other applications supporting personal activities and collaboration. All the benefits of such applications can, however, be lost if we do not protect their underlying AI models from attacks.

BASELINE	
What has been done so far (in EU and in the World – EU position)	EU ethics guidelines for trustworthy AI have been published, as well as the Malicious AI report. Globally, there is a huge effort by many teams and organisations to get the most out of AI in a wide range of application such as image, video and speech processing, analysis, synthesis, recognition and classification; autonomous vehicles; prediction and recommendation systems; surveillance, security and safety; robotics; linguistic analysis, etc. All the EU countries contributed to the development of AI methodologies and AI-based applications through the academia, public and private research centres, public and private companies. CEPS Task Force on AI and Cybersecurity is working on a report on the market, technical, ethical and governance challenges posed by the intersection of AI and cybersecurity, focusing in particular on EU policy.
Effort until now	H2020 and other programs funded the development of AI methodologies and applications, where security and privacy issues have been addressed only partly. H2020 SHERPA project (http://www.project-sherpa.eu/) includes work on model poisoning attacks against certain classes of ML models. ITEA3 IVVES project (https://ivves.weebly.com/) is investigating approaches to verification and validation of AI-based systems as one of its focus areas.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	**Privacy-aware big data analytics/data mining.** The analysis, processing, and sharing of massive quantities of heterogeneous data bring many benefits in several application domains such as healthcare, energy, traffic management, etc. Big data analytics, however, can increase the risks of inferences that can put users' privacy at risk. Novel techniques investigating options to compute on encrypted data while ensuring data privacy are needed to address issues related to data linkage, knowledge of external information, and exploitation of analysis results. **Data Trust and Sharing.** Big data heavily interplays with trust. On the one hand, we need to trust collected data, including the providers; on the other hand, data helps to define proper trust and reputation systems, often based on recorded evidence by several parties. In particular, we need to develop and utilise techniques for trusted information sharing, provenance tracking, and data quality assessment and provide manipulation resistant algorithms. **Protection against internal and external data breaches**. The storage of vast amounts of data that are used by AI techniques for training and validation, for instance, in attack prevention and response and many other applications, requires the development of specific techniques for data anonymity and data breach and manipulation prevention. **Adversarial machine learning.** Learning-based pattern classifiers, including deep neural networks, have shown impressive performance

	in several application domains, ranging from computer vision to cyber security. However, it has also been shown that adversarial input perturbations, carefully crafted and used either at training or at inference time, can easily subvert performance of classifiers and other ML algorithms. The vulnerability of machine learning techniques to such adversarial examples, in particular, poisoning and evasion attacks, along with the design of suitable countermeasures, are investigated in the research field of adversarial machine learning. The goal here is to develop adversarial-resistant or adversarial-aware ML approaches. **Confidentiality attacks**. Some machine learning models are trained against confidential data such as medical records, purchasing history, or computer usage history. Confidentiality attacks are designed to determine the data used during the training of a model, by analysing and / or probing the model. An adversary's motive might be curiosity - to simply study the types of samples that were used to train a model - or malicious intent - to gather confidential data, for instance, for blackmail purposes. Approaches to detecting and resisting confidentiality attacks are required. **Model cloning**. Protection of AI models is essential since models are important elements of intellectual property and often the result of serious efforts in collection, analysis and processing of valuable data. A near perfect clone of an AI model can be often realised by simply querying it. Model cloning, or stealing, countermeasures are essential both to protect the intellectual property and to enforce training data privacy. **xAI – Explainable Artificial Intelligence**. Some of the most accurate learning-based pattern classifiers and other AI models are currently designed as black boxes. That is to say, as systems whose internal operations do not immediately reveal the input-output relationship. This lack of explanation constitutes both a practical and an ethical issue, complicating auditability and compliance verification and negatively affecting trustworthiness of AI-based systems. Explainable Artificial Intelligence has recently become a relevant research direction to address and mitigate these issues. In relation to GDPR, Article 22 states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." This article and other articles, Article 25 discussing privacy-aware analytics and Article 32 dealing with secure storage, seem to impose "transparency" constraints that are far beyond the state of the art of AI technologies. Goodman and Flaxman (2016) stated that the GDPR will create a "right to explanation", users could ask for an explanation of an algorithmic decision that was made about them. **AI and blockchain.** There are several characteristics of blockchains/DLTs that are of potential interest for artificial intelligence applications. It will be useful to explore the synergy between AI and blockchains, to further explore how blockchains can be used for sharing AI training data and contribute to the trustworthiness of the data that AI models work on.

	AI and physical attacks. In the case of embedded AI, the algorithms and parameters used may constitute critical assets. Initial works have shown that such algorithms and data could be retrieved through side channel attacks. The threats linked to physical attacks on such implementations will have to be further researched in order to protect those embedded AI implementations. **Resilient AI.** Interactions and interdependencies regarding introduction and utilisation need to be considered within the context of operation. It includes AI operation with legacy systems, transition towards more automation and user centred approach. AI is not always smart, so it needs to be seen in combination with expertise, tacit knowledge existing in the organisation. This will allow AI and expertise in the organisation used to train ML algorithms to have capacity to adapt and evolve. Integrating AI will require to build on existing recommendations such as EU ethics guidelines for trustworthy AI and create new knowledge and skills both in the work force and in the management.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	Possibility to use AI in different contexts without fear of catastrophic failure and with trust of all relevant stakeholders. That will bring great business opportunities as well as personal and societal development opportunities. AI-based systems are already deployed in many domains, including finance, commerce, science, military, healthcare, law enforcement, and education. In the future, more and more important decisions will be made with the aid of such systems. Some of those decisions may even lead to changes in policies and regulations. Thus, understanding of dangers and extents of attacks on AI algorithms and optimal mitigation strategies and measures is crucial not only for AI developers and adopters but also for the entire society, in order to maximize the benefits that AI systems bring and to minimize associated risks.
Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 7
Timeline (2025/2027/beyond)	2025-2027-beyond (as AI techniques spread and evolve)

Software and hardware cybersecure engineering and assurance

Horizon Europe – HEU.4.B	
Specific Priority	**Software and hardware cybersecure engineering and assurance**
Description of the challenges – why is it important?	European actors are strong in application domains such as critical infrastructure, industry 4.0, aerospace, automotive, defence, IoT or health care but rely widely on external capabilities not only in semiconductor and electronics technology, but also in software and tools. However, the progressing digitization of Europe's industry and society has to be backed through reliable IT systems, which can only be achieved if the components all the way down to the hardware

components (e.g. CPUs, SoCs, sensors, AI accelerators, memories) are available and secure.

At the moment, European industries and especially SMEs have no other option than building their products from off-the-shelf components that are only available from the untrusted, global market, which sometimes may be subject to possibly changing IP rules and licences thus limiting the availability of technology. This has to be addressed to recover European technology sovereignty in the IT sector and enable stable sources for trusted electronics and IT components for European stakeholders.

Assurance for a Trusted Lifecycle. The lifecycle of hardware and software covers different segments starting at Engineering and Development, and going over Manufacturing, Deployment, Operations and Decommissioning. Each one involves other technologies and poses individual cybersecurity risks that have to be addressed to achieve and maintain a high level of overall assurance, especially if it covers the interaction across several layers of the technology stack. Involving IP blocks, code, components and manufacturing services from several, potentially not fully trusted, external parties, methods and tools are needed to model and analyse the relation between the artefacts of the several phases and to cope with the differences in knowledge and control of the different components. This might imply a mix of glass box and black-box tools, monitoring technologies for dynamic changes and sandboxing or encapsulation methods for dealing with foreign code or cloud infrastructures, etc. With the increasing importance of green ICT, circular economy with refurbishing and retrofitting is becoming relevant, also on an industrial level[36].

Assurance for a Trusted Supply Chain. European actors currently cannot build systems without involving any external electronics technology or software, as it is much cheaper and faster for them to buy capabilities and services they are looking for, especially if it involves large investments for establishing manufacturing capabilities. However, this dependency inherits possible safety and cybersecurity risks through external designers, manufacturers, and integrators or even facilitates to become a victim to malicious actions by embedding Trojans or kill switches. Tools are needed for transparency, SLA assurance, provenance, and for the evaluation and demonstration of emerging security qualities of the overall system that can be used in a certification of the system as a whole.

Assurance for System of Systems (SoS) from a Mission perspective. Complex system of systems missions fails because a component has suffered attacks, has not functioned as it was supposed to or has found a risk scenario that was not initially thought of. Only a system and platform-oriented approach permits to assure end to end security across the entire technology stack. The secure transition from a legacy system to a state-of-the-art architecture including new and also legacy components has to consider to protect the legacy components from external threats and the system from threats through legacy systems as well. This is achieved by also

[36] https://ec.europa.eu/commission/presscorner/detail/en/fs_20_437

	integrating hardened devices to protect critical assets in more vulnerable subsystems. A resilient system also addresses the attack situation including response capabilities to maintain a secure state to the widest possible extent.
Digital Living & Working	
BASELINE	
What has been done so far (in EU and in the World – EU position)	Currently, the global electronics industry heavily relies on processor technology and major IP, software and cloud capacity that is outside of European control. While parts of the critical manufacturing can be performed within Europe, the large manufacturing capacities lay overseas and it is not within reach to create domestic counterparts on this scale. Global players providing tools to design, simulate and test electronics are also located outside of Europe. The open source community is gaining more and more commercial attraction and is working on promising hardware designs and tools, but their maturity and quality is still far away from leading commercial solutions. USA and China are in stronger positions in comparison to EU as they have access to manufacturing capabilities and also develop independent software. The US realised their shortcoming in the hardware domain and established DARPA Programs and Initatives backed by significant funding[37], at least in the defence domain. In the software domain, initiatives such as The Open Group Trusted technology forum or the OMG (Object Management Group). Software Assurance Working Group are developing specifications that enable creation secure software and lifecycles. EU through reports, such as those of the Business Innovations Observatory, recognizes the significance of a secure and ruled by standards value chain. This value chain consists of one hand of the technology companies that supply the building blocks of hardware and software and, on the other hand, of the producers, transporters, suppliers and retailers that need the transparency and traceability of the supply chain.
Effort until now	Several H2020 and national projects have developed technologies, algorithms and foundations for cryptographic and security IP. The next step is to link previous results to processors, components and larger hardware and software systems. This area is very recent, there are only very few projects underway: http://sharcs-project.eu/ https://cordis.europa.eu/project/rcn/200247/factsheet/en and http://react-h2020.eu/ Current EU initiatives such as EuroHPC and ECSEL work on related problems, but additional work with a dedicated security focus is necessary to cover the full design process and lifecycle of trusted electronics

[37] https://www.darpa.mil/work-with-us/electronics-resurgence-initiative

	Other EU funded H2020 programs that include the aforementioned critical aspects of traceability, transparency and utilize blockchain technology for trusted supply chains are https://www.efactory-project.eu/ and https://pop-machina.eu/, which research among others smart factories and circular economy scenarios as well.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	• Create the technological foundations and IP to design and improve secure systems incorporating trusted components in order to decrease the dependencies in neuralgic points and components and services retrieved from the global market. • Creating a pool of trusted IP blocks from open-source pools, e.g. RISC-V processors, and certified closed source blocks, or in addition also supporting the entire chip design., including hardened accelerators for AI, Communication or Crypto (e.g. over encrypted data), … • Entangle AI and the underlying electronic components to secure the data and processes from external attackers • Develop tools to design and verify software, trusted electronics and continuously assess the quality of open source inputs using for example formal methods and tools to easily verify IP blocks by customer to increase trust in external IP and open source components • Providing advanced system and board packaging technologies in a trusted European environment and establishing trusted logistics to ensure that no unwanted components or Trojans are integrated into a system. • New techniques, methods and tools to analyse risks from a quantitative and qualitative perspectives in the system development lifecycle and missions of systems of systems • Definition of processes and creation of tools for the overall system security evaluation and certification across a wide range of integrated technologies covering the supply chain, manufacturing process and later operation. • Combine blockchain technology with traditional and legacy software systems to fill the gap of security and identity management, traceability, non-repudiation and trusted peer-to-peer transactions without the need for a middle-man • Develop end to end transparent supply chain software solutions supported by blockchain, which provide information to and from all the participants of the network, from the producer to the end customer. Creating the corresponding software and firmware ecosystem to integrate and enable the use of the trusted hardware and the transition from legacy components to a hybrid current architecture, also including legacy components in a secure way.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	The European cybersecurity community and especially SMEs benefit by gaining access to trusted electronics and software without having to bear the development cost individually. In addition, a European community is formed.

Starting TRL / Expected TRL	**Starting TRL:** 3 **Target TRL:** 6
Timeline (2025/2027/beyond)	2027 and possibly beyond

Cryptography

Horizon Europe – HEU.4.C	
Specific Priority	**Cryptography**
Description of the challenges – why is it important?	**Quantum safe cryptography, theory and implementation.** In the first half of 2020 the new standards for PQC will be published and these need to be implemented on a huge variety of systems both new and old. Theoretical understanding is needed to select the best ones for the standard and implementation to get these adopted widely. Furthermore, new proposals for quantum safe algorithms beyond key encapsulation and digital signatures are needed to keep also the more advanced cryptographic systems and proposals safe from quantum computers **Advanced cryptographic concepts.** It is important to also research more advanced cryptographic primitives and protocols such as FHE, MPCand functional encryption. Especially looking into the quantum safety of these protocols might be an interesting venue for research. **Hardware and software implementations**. It is important to bring the theoretical concepts of cryptography to practice. To this end, there is a need to develop HW and SW implementations that are easily available to the developers of various services and products. These developers will not themselves be experts, but need tools to implement the best possible cryptographic protections in their services and products. **Protocol development and standardization**. New protocols (or revisions of old protocols) are needed to support novel concepts (e.g. digital identity) and keep also the existing technologies (e.g. wireless communications) up to date with respect to cryptography. **Measuring, assessing and certifying cryptography**. As cryptography has become more central to the functioning of many systems, it is important to understand what type of protection it can offer and to what extent. Thus, measuring assessing the “strength” and efficiency of cryptography is important topic. In many cases the implementations need to be certified in order to use them in official contexts. These certification efforts would benefit from better measurement and assessment methods. New paradigms. There should also be a venue for seeking completely new ways of thinking about cryptography and challenging the current paradigms. This research should embark on high risk, high gain ventures like the FET Open program, but more directed towards cryptography.
BASELINE	

What has been done so far (in EU and in the World – EU position)	Europe has a strong background in theoretical and mathematical basis of cryptography and on developing secure implementations. Europe also has a strong background in developing secure implementations and tools for their evaluations. For what concerns Multi-Party computation, homomorphic cryptography and other important advanced topics, there have been efforts in e.g. H2020 programmes to advance the field. NIST has launched a standardisation competition in this post-quantum cryptography and has started an initiative of standardising Threshold cryptography and in particular, threshold circuits: https://csrc.nist.gov/publications/detail/nistir/8214/final There are also many projects ongoing that develop solutions to these questions. EU has research groups that are well established in the field, but implementations are somewhat lacking. European research groups are heavily involved in the standardization processes.
Effort until now	H2020 projects (e.g. HEAT), national projects in EU and globally. H2020 projects, national and international projects. EU Flagship in Quantum computing. Secure evaluation and efficiently implemented cryptographic algorithms have started; this is a long-term effort (1 decade) COST actions in the field of cryptography in the past. NoE ECRYPT I and ECRYPT II boosted the European collaboration in cryptographic research and resulted in several important outcomes – one example is the recommendation on Yearly Reports on Algorithms and Key Lengths. NIST standardization competitions (AES, SHA-3 in the past) have provided good platforms to develop cryptographic expertise also within Europe and European research groups have been well represented.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	In some topics (such as certification) there are national or organizational silos, where work is done. Collaboration on a larger scale would be beneficial. Although identified already several years ago, there still exist large gaps between the theoretical possibilities offered by cryptography and the practical implementations. Some of the hurdles are practical (as in required computation effort, power etc.) and some are political and societal (e.g. protecting biometric templates). These gaps need to be bridged by better development of methods and requiring the adoption of better solutions, when these are available.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	Cryptography is foundational to all cyber security. Cryptography is thus necessary (but not sufficient in itself) to all cyber security solutions. Cryptography is also the key trust anchor in our digital society. Thus, the strategic impact of these initiatives is huge. The economic benefit is high as well as there is a market for dedicated cryptography solutions that is in the order of billions of dollars. Furthermore, as

	mentioned above, cryptography is necessary to realize almost all current and possible future digital services and products. In this way the impact and market potential of cryptography are much larger than merely in the dedicated solutions.
Starting TRL / Expected TRL	**Starting/Target TRL:** Everything from 1-9 In specific areas (e.g. PQC) the TRL window can be narrower (4-7)
Timeline (2025/2027/beyond)	In some areas the timeline is already from 2021-> (e.g. PQC standardization), in others the timeline is well beyond 2030 (e.g. paradigm changing systems).

Blockchains and Distributed Ledger technologies

Horizon Europe – HEU.4.D	
Specific Priority	**Blockchains and Distributed Ledger technologies**
Description of the challenges – why is it important?	Blockchains and Distributed Ledger technologies could unveil new business models and support a stronger Digital Single Market especially in the fields of dynamic data portability, public shareable auditable persistent information, data security and data provenance. These technologies must be compatible with fundamental EU values and legislation, including data subject rights (like in the GDPR Regulation), electronic identification and trust services (like in the eIDAS Regulation), cybersecurity frameworks (including the Cybersecurity Act, the NIS Directive), to support and foster the new data economy space. Blockchains and DLTs are positioned to intermediate a significant part of future world's GDP, allowing new business models to be implemented while making some of them more efficient or on the contrary outdated. A significant part of the future digital and data economy will leverage on blockchain systems and Europe should have control of these technologies that have to be "EU friendly" in terms of values and normative reference. Currently blockchain systems are not designed with an EU-first focus, resulting in systems that are not always compatible with our laws, resulting on their limited adoption. Companies face the dilemma of trying to innovate in this area while subjected to many regulations that at first seems to hinder innovation. The main goal of the Horizon Europe should be to provide the technological basis for solutions that allow for stronger and EU-friendly blockchain systems, supporting their adoption in relevant sectors and markets, integrating and expanding current solutions and initiatives in a cross-border fashion, fostering interoperability and essentially creating a new playing field for EU-actors willing to innovate with the support and in line with the current legislation.
Digital Living & Workings	
BASELINE	

What has been done so far (in EU and in the World – EU position)	**Policy framing** The European Parliament, with the Resolution of 3rd October 2018 on distributed ledger technologies and blockchain, recognized that Distributed Ledger Technologies "can constitute a tool that promotes the empowerment of citizens", "improve transaction cost efficiency", necessitating frameworks to "provide legal certainty and respects the principle of technology neutrality" and that the approach towards them should be "innovation-friendly". In relation to digital identity, the aforementioned Resolution of the European Parliament focuses on digital identity in the context of Self-Sovereign Identity but also states that "it is of the utmost importance that DLT uses are compliant with the EU legislation." In her political agenda for the Next European Commission, President of the European Commission Dr. Ursula von der Leyen, stated that "It is not too late to achieve technological sovereignty in some critical technology areas. To lead the way on next-generation hyperscalers, we will invest in blockchain, high-performance computing, quantum computing, algorithms and tools to allow data sharing and data usage", "We will jointly define standards for this new generation of technologies that will become the global norm", adding that "we have to find our European way, balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards" and that "We need to move from "need to know" to "need to share" On April 2018, the European Partnership for Blockchain was launched. Commissioner Gabriel welcomed the event with these words: "In the future, all public services will use blockchain technology. Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies." In the Communication from the Commission COM(2020), "A European Strategy for data", it is said that "New Decentralised digital technologies such as blockchain offer a further possibility for both individuals and companies to manage data flows and usage, based on individual free choice and self-determination. Such technologies will make dynamic data portability in real time possible for individuals and companies, along with various compensation models".
Effort until now	• In March 2018 the European Commission adopted an action plan on FinTech to foster a more competitive and innovative European financial sector. A Fintech Action Plan (COM(2018) 109) gives a lot of emphasis on blockchain for the finance sector. • The European Blockchain Observatory and Forum: aimed to accelerate blockchain innovation and the development of the blockchain ecosystem within the EU, and so help cement Europe's position as a global leader in this transformative new technology. • The CEN CENELEC Focus Group on Blockchain and Distributed Ledger Technologies released a White Paper on

	Recommendations for successful adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies". The Focus Group is now part of a much greater effort as the new launched CEN CENELEC JTC 19 on Blockchain and Distributed Ledger Technologies.
	• The European Blockchain Partnership joins all EU and EEA members to work together towards realising the potential of blockchain-based services for the benefit of citizens, society, and economy. As part of this commitment, the Partnership is building a European Blockchain Services Infrastructure (EBSI) which will deliver EU-wide cross-border public services using blockchain technology. This initiative is funded through the CEF programme.
	• The International Association for Trusted Blockchain Applications (INATBA) has formed, a global forum to interact with regulators and policy makers and bring blockchain technology to the next stage.
	• EU has launched an investment fund for startups in the field of Artificial Intelligence and Blockchain.
	• Many Horizon 2020 calls are requesting specifically (or hinting at) blockchain based solutions.
	  ○ PRIViLEDGE project focuses on the blockchain and distributed ledger technologies supporting privacy, anonymity and decentralised consensus.
	  ○ PHOENIX project, mainly focused on Energy infrastructures, will look into a fully decentralized inter-DLTs/blockchain platform for real-time synchronized cybersecurity information awareness.
	  ○ SOTER project, targeting the finance sector, will look at a cloud platform that will make use of blockchain technology.
	  ○ KONFIDO project adopts a blockchain based logging for not repudiation of the exchange of eHealth data in Europe through the eHDSI.

DESIRED SCENARIO	

What more should be done? What gaps to be filled? For what reason?
How can it be done?
	• Support specific research actions in this area, including:
	  ○ Privacy-friendly blockchain systems based on innovative cryptographic schemes, transforming a blockchain from a distributed storage to a distributed computing engine accessible from different parties thanks to mechanisms like delegation, selective disclosure, homomorphic encryption, zero knowledge proofs, secure multi-party computations and considering quantum threat and quantum resistance for a medium to long perspective;
	  ○ Safer and simpler key management schemes including distributed key recovery systems;
	  ○ Strong integration with current and existing trust services, rethinking, extending and complementing them, whenever

	possible, in a decentralized way (including decentralized identity management, authentication and timestamping); ○ New and innovative consensus algorithms for optimized throughput, new security features, improved decentralization and fairness; ○ Safer and more solid smart contracts languages, better operational life cycle management, security checking and advanced integration with current IT systems; ○ Integration with other innovative technologies under the unifying vision of "secure digital transformation;" ○ Interoperability protocols, still lacking nowadays, to connect multiple blockchains systems in a safe way. • Support the development of innovative payment systems (including cryptocurrencies) in the context of heavily regulated sectors including finance and banking. • Definition of legal frameworks for the adoption of blockchain systems, including domain-specific regulatory sandboxes targeting first heavily regulated sectors (like finance, banking, healthcare). • Support to standardization initiatives, especially EU-based like CEN CENELEC and ETSI. All of those above should be made in line and in accordance with EU legislation, finding creative and effective ways to have them implemented properly. Three different lines of intervention are advised, tailored for different actors and for technologies and solutions at different maturity levels: 1. Cascade grants for specific innovations, to support researchers and startups and have them capable of finalizing their ideas in a fast-moving setting. These should also include support to standardization initiatives. 2. More structured research calls, appealing for consortia, where some of these and other innovative technologies could be further developed and tested in some specific operational domains. Pilots for wide adoption and integration with other strategic technologies once the results and maturity from the previous points has been evaluated and there is more need to integration in cross-border and cross-domain settings.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	The strategic impact is having an internal European capacity of building sound, strong and safe blockchain systems reducing the cost of data exchanges and fostering new business models for ecosystems composed of public and private actors, without relying on external parties and with strong cybersecurity guarantees.
Starting TRL / Expected TRL	**Starting TRL:** 2 – 4 **Expected TRL:** 5 – 8

Timeline (2025/2027/beyond)	2025

IoT security

Horizon Europe – HEU.4.E	
Specific Priority	**IoT security**
Description of the challenges – why is it important?	At its core, the concept of the Internet of Things (IoT) revolves around connecting all kinds of physical devices to the Internet, for tasks such as relaying data or behaving as a primary source of intelligent capabilities. Yet the concept of IoT has evolved over time, provisioning novel services not only at the business level but also at the consumer and industrial level. Both this evolution and the deployment of IoT applications have shown that there are still many issues to solve in terms of IoT security and privacy. In fact, the attack surface of IoT has become larger than traditional Internet-connected systems, due to many factors such as the physical deployment of the devices, the lack of security guarantees, the inherent mobility of several devices plus the dynamic nature of certain IoT ecosystems, the large variety of device types, communication protocols, APIs, and standards, and many others. Therefore, it is necessary to address novel and underdeveloped security challenges related to areas like resilience, authentication, identity management, mobility, and scalability at all levels: not only to the different layers in the IoT stack (device, connectivity, platform and application), but also across different layers – or even IoT systems as a whole. Moreover, security by design procedures and tools (e.g. formal verification) should produce concrete security guarantees for the overall system along the product chain, from hardware implementation to product deployment.
Digital Living & Working	It is essential to highlight (also in connection with the 'Privacy' proposal) that health-oriented devices can be included here. IoT devices have invaded not only the industrial field, but also our daily life. The large amount of data they handle is an important asset to improve many facets of life. However, the management of data raises many privacy and security problems that in exceptional cases such as that of COVID19, where teleworking has increased, can be exploited to obtain data that would otherwise have been more complicated (inside the company environment). The increasingly connections and the number of devices connected to the internet has led to a greater attack surface, where the weak point of that network are the IoT devices. These devices can be used to create a botnet and attack more ambitious targets through a denial of service. When telemarketers are collapsed due to high number of current connections, a successful denial of service attack could be performed easily. Indeed, an attack to a hospital in a COVID19-like situation would be fatal to many people's lives. In other sensitive environments such as the industrial one, devices are a weak point to perform an attack because the safety of these low-cost devices is not

	always considered. However, an attack on them that could lead to an access to the central system could cause a disruption of essential services such as electricity or the connection to the internet. On the other hand, the information handled by IoT devices could be used in these types of situations to monitor symptoms or exits from the home, which also raises privacy problems versus maintaining public health.
BASELINE	
What has been done so far (in EU and in the World – EU position)	Shortly after the definition of the Internet of Things paradigm, security was already identified as one of its most critical factors. Therefore, there have been a plethora of efforts from all actors all over the world (government, academia, industry, and standard bodies)) to provide security and privacy to all IoT ecosystems. These efforts have resulted in multiple research projects in Europe (under FP7 and H2020) and all over the world, whose results have enabled the development of several security and privacy technologies, various reference architectures aimed for specific verticals (e.g. healthcare, industrial systems), multiple standards, and many cybersecurity laws and recommendations. Still, due to the heterogeneous and evolving nature of the IoT paradigm, there are still multiple challenges to be overcome – not only from a technological point of view but also from a legislation point of view. For example, as pointed out by ENISA, there are some identifiable gaps in IoT security standardization such as interoperability between security standards and the existence of certification and validation schemes. Other initiatives focused on IoT security are the document created by BITAG with a series of security and privacy recommendations for consumer IoT devices. The Online Trust Alliance IoT Trust Framework also gives recommendations and security practices to develop secure IoT devices. With the possibility of self-evaluate through a checklist our own IoT products, the GSMA developed a series of IoT Security Guidelines and recommendations oriented to mitigate common security threats
Effort until now	Beyond the previous research IoT initiatives that studied the protection of IoT infrastructures, such as various projects under the umbrella of the IERC research cluster, current European research initiatives focus on novel and underdeveloped IoT security and privacy challenges. Examples of these challenges include IoT security formal verification (IoT4CPS, SPARTA), security-as-a-service (SecureIoT, SerIoT), security-by-design (ANASTACIA), blockchain-based integrity checking (GHOST H2020 KONFIDO H2020, CHARIOT), enhanced resilience (RESISTO), IoT-Edge interactions (mF2C), intrusion detection and honeypots (SunRISE, nIoVe, SerIoT),
DESIRED SCENARIO	

What more should be done? What gaps to be filled? For what reason? How can it be done?	***Challenges at device level*** • Secure execution and trust of IoT devices and services, in order to be connected to an ICT infrastructure. • Secure migration to post-quantum cryptographic algorithms, especially for high-assurance devices or devices with a long-expected lifetime. • Firmware and application integrity, including scalable update delivery and remote attestation procedures. • Protection against advanced attacks, including physical attacks (e.g. side-channel) and micro-architectural attacks (e.g. Spectre-like attacks) in devices with low computing power constraints. • Availability of an open-source hardware that allows a European sovereignty over the deployed circuits. • Automate, facilitate and drastically speedup the overall process within IoT ecosystem through distributed ledger (blockchain-type) technologies, along with contracts that can translate conventional agreements into smart contracts (for automated transactions) ***Challenges in connectivity and network layer*** • Network security improvements, such as secure routing, cryptography, and network level privacy. • Secure key management for a high number of IoT devices. • Security and privacy (including anonymisation) of data retrieved or inferred from IoT devices and processed in external IoT platforms. • Secure connectivity and interactions with external infrastructures (e.g. edge computing). • Secure mobility where heterogeneous devices and connection technologies coexist in multiple ecosystems. • Embedding proper security capabilities in IoT communication standards. ***Challenges at IoT platform and IoT service layer*** • Secure lifecycle to establish, operate and update IoT platforms and networks, with a special focus on the secure integration and interaction with legacy systems and devices. • Enable secure self-management of IoT ecosystems by deploying situational awareness services, predictive systems, and reactive systems. • Release constraints on backend IoT applications and services by shifting certain security checks and controls to the IoT device level. Such lightweight security solutions deployed on the IoT can benefit from other enablers such as Cloud/Edge computing. • Mitigation of DDos Attacks. • Holistic integration of advanced security mechanisms in novel and existing IoT platforms. ***Challenges at application layer and related to end-users***

	• Data protection and compliance with legislations and directives. • Tackle risks of exposure of sensitive information, such as personal or business confidential data, in the IoT environment. • Assuring application robustness, due to an increased attack surface and the pervasive use of the technology. • Secure and trusted interaction between multiple involved parties, such as users, device manufacturers, cloud service providers, network operators, and others, in IoT ecosystems. • Usability of security solutions in IoT ecosystems. • Increasing awareness for both consumers and professionals. ***Cross-cutting challenges***, which affect all previously mentioned layers and levels to varying degrees. • Definition, implementation and integration of secure software engineering tools (e.g. formal verification tools) and principles (e.g. security-by-design) to allow the definition and development of secure IoT devices, infrastructures and applications. • Procedures that can produce concrete security guarantees for the overall system along the whole product chain. • Authentication and authorization challenges: • Distributed and lightweight authorization and authentication mechanisms, including scalability of authentication in resource constrained devices and authentication in federated and dynamic environments. • Scalable and secure identity management solutions, including the different identities of IoT objects: personal identity (“who I am”), core identity (“what I am”), association identity (“who is my owner”), and location identity (“where I am”). • Definition of forensics procedures in the context of the IoT from a technical and legal standpoint. • Intrusion detection and management challenges: • Development of Intrusion Detection Systems (IDSs) able to cope with multiple IoT devices, networks and platforms. • Detection of new vulnerabilities linked to the future evolution of consumer, business and industrial IoT environments. • Development of specific threat intelligence tools, able to support multiple IoT devices and protocols. • Development of simulation and cyber range tools focusing on IoT technologies and associated verticals. • Interoperability techniques for the different security and privacy mechanisms, including trust management models. • Security audits and certification procedures for all IoT elements, including platforms, services, and distributed devices.
Expected benefit; strategic or economic impact **➔ What can be achieved?**	As IoT is strategic for European economy and social good, having a large impact both for mass market or industrial applications in all vertical sectors (Transport, eHealth, smart cities, industry 4.0, energy, etc.), the security of the Internet of Things has been identified as one of the strategic European priorities.

	Solving all previously mentioned gaps and challenges will make IoT protocols and IoT environments more secure and resilient against failures and attacks. This will increase trust in this technology, which in turn will facilitate its integration into critical infrastructures and personal life systems, not only in Europe but also in other countries around the globe. This will strengthen the position of Europe from a technological and economic point of view.
Starting TRL / Expected TRL	**Starting TRL:** 2 – 4 **Expected TRL:** 5 – 8
Timeline (2025/2027/beyond)	2025

Artificial Intelligence techniques for better security and malicious use of AI

Horizon Europe – HEU.4.F	
Specific Priority	**Artificial Intelligence techniques for better security and malicious use of AI**
Description of the challenges – why is it important?	The domain of IT security has always been an arms race between attackers and defenders and naturally, with the enormous success of artificial intelligence (AI) and machine learning (ML) in a variety of application areas, these techniques are already employed by both sides. Therefore, it is not only very beneficial to further improve existing AI-supported security technologies to help security professionals to deal with the ever-increasing complexity of modern IT, Industry 4.0 and IoT infrastructure and the vast amount of data created by them, but it is rather necessary to stay ahead of attackers that are going to employ AI-supported automated attacks on these infrastructures. Common examples for the offensive use of AI are the following: • Automated information gathering using natural language processing (NLP) methods • Impersonation, Deep Fakes for Audio/Video/Text • Malware/Spyware/Ransomware Generation • Password and Captcha Breaking • Attack Automation (Automatic exploitation and post-exploitation) On the other hand, defensive techniques can be employed on almost any level of an IT (security) infrastructure: • Physical (Surveillance Cameras, Physical access control systems) • Network (IDS, Packet Inspection, Malicious Node Detection) • Endpoint (AI-based malware detection, Better Spam/Phishing Detection) • Application (Static and Dynamic Code Analysis, Fuzzing using Reinforcement Learning Methods)

	• User (Behavioural Anomaly Detection, Continuous Authentication) • Processes (Fraud Detection) The usage of artificial intelligence techniques is quite diverse: • Dynamic attack detection: endpoint, network, cloud, web app, IoT and IIoT, collaboration platforms, social networking platforms, applications... • Threat intelligence, cybercrime forecast and trends, security risk evaluation • Malware identification (and riskware, PUA, privacy-violating SW, etc.), static, dynamic, combined approaches • Malicious web resources identification • Red-teaming / pen-testing automation, attack modeling, ML-guided fuzzing • Code analysis, vulnerability identification • Response and remediation automation and support, SOC support • Forensic data analytics, attack attribution (described in priority HEU.1.C) • Fake and malicious content identification (described in priority HEU.3.A) • Context-based security • Authentication mechanisms • Attacker - defender games, GANs, reinforcement learning However, most of the so far suggested algorithms or systems are very domain-specific solutions lacking the contextual or full situational awareness of the system as a whole. Collecting, aggregating and summarizing result from the individual systems to create a full situation report or meaningful incident alarm is a big challenge. Fortunately, orchestrating multiple systems to perform automated attacks as effectively as a human attacker would do, is equally challenging but some rudimentary frameworks based on Metasploit already exist. Furthermore, current systems mainly react rather than proactively assess risks, predict or even prevent attacks. Finally, on the defender's site significantly more care must be taken with the development of robust, fault-tolerant and reliable AI defensive techniques, since otherwise also a new attack surface is created. This line of research is known as adversarial machine learning and addressed in HEU.4.A. On the attacker side, the tools and resources needed to create sophisticated machine learning models have become readily available over the last few years. Powerful frameworks for creating neural networks and other models are freely available, and easy to use. Public cloud services offer large amounts of computing resources at inexpensive rates. More and more public data is available and cutting-edge techniques are freely shared - researchers do not just communicate ideas through their publications nowadays – they also distribute code, data, and models. Cybercriminals, disinformation organizations, and nation states are technically capable of utilizing

	these frameworks and techniques, and may already be using them. For instance, data analysis techniques have been used to target specific users with political content via targeted advertising service. As the capabilities of ML-powered systems evolve, we need to understand how they might be used maliciously, which is especially true for systems that can be considered dual-use, such as in the realm of offensive cyber security (a proactive and adversarial approach to protecting computer systems, networks and individuals from cyberattacks.) Password-guessing suites have recently been improved with Generative Adversarial Network (GAN) techniques, fuzzing tools now utilise genetic algorithms (e.g. american fuzzy lop) to generate payloads, and web penetration testing tools have started to implement reinforcement learning methodologies. While better offensive tools will enable more vulnerabilities to be discovered and responsibly fixed by the white hat community, black hats may use these same tools to find software vulnerabilities for nefarious uses. ML capabilities may be used by botnets to deliver optimized DDoS attacks and spam campaigns, and to automatically discover new targets to infect. Malware in the future may be designed to learn from the host it is running on in order to remain undetected, search for and classify interesting content for exfiltration, search for and infect new targets, and discover new pathways for lateral movement. Malware command-and-control (C&C) may employ host profiling logic and deploy specific payloads to each machine, based on its profile. Data analysis techniques can also be used to perform efficient reconnaissance and develop social engineering strategies, such as spear phishing and impersonation, against organizations and individuals in order to plan and carry out targeted attacks. In August 2018, IBM published a proof-of-concept design for malware obfuscation that they dubbed "DeepLocker"[38]. The proof of concept consisted of a benign executable containing an encrypted payload, and a decryption key ‘hidden’ in a deep neural network (also embedded in the executable), making reverse engineering to extract the malicious payload extremely difficult. Sophisticated nation-state cyberattacks sometimes rely on distributing hidden payloads (in executables) that activate only under certain conditions (e.g. Stuxnet), so obfuscation techniques in the DeepLocker style may attract interest from advanced adversaries. ML-based content generation techniques can be used for automated spam and disinformation generation (see also priority HEU.3.A).
Digital Living & Working	Protecting an individual’s personal and professional digital identity has become an increasingly important goal that became even more apparent in special situations such as the lockdown caused by COVID-19. With most of the communication shifted to digital media such as (video) conference calls, disclosure of confidential information due to impersonation using deep fakes can become a serious problem.

[38] https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/

	Moreover, as AI technologies further evolve, voice-controlled personal assistant or AI-controlled dialogue and customer support system embedded in a person's home or car, or a company's IT system, respectively, become more and more ubiquitous, new and previously unknown attack surfaces are created.
BASELINE	
What has been done so far (in EU and in the World – EU position)	RAIL (Responsible AI Licenses) empower developers to restrict the use of their AI technology in order to prevent irresponsible and harmful applications. https://www.licenses.ai/ Research around Cambridge Analytica, e.g., User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, https://ieeexplore.ieee.org/abstract/document/8436400 A number of research publications on offensive security, including ML-guided vulnerability discovery and fuzzing, model poisoning attacks, and the use of Generative Adversarial Network (GAN) techniques, also studied for somewhat different purposes in: RECAP, https://recap-h2020.github.io/ HYBSPN, https://cordis.europa.eu/project/id/797223 We refer to HEU.3.A for the discussion on fake content and disinformation.
Effort until now	
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? How can it be done?	**Machine Learning for cybersecurity**. ML algorithms have shown impressive capabilities in malware detection and network security. With the increase of the computational capabilities on IoT edge nodes, ML can extend its reach to specifically address anomaly detection at the edge. **Large-scale, robust threat- and anomaly detection on highly heterogenous and incomplete data to create situational awareness.** In the domain of data analytics for security intelligence, big data capabilities are envisioned to add predictive and proactive capabilities to existing security tools and systems. By leveraging on trusted data sources, and on adequate machine learning algorithms, the threat environment and the attack surface can be analysed in real time, and appropriate countermeasures could be enforced for attack prevention and response. Such an approach allows for the analysis of long-term historical trends and forensics. Future security intelligence cannot be simply hardcoded based on a "sandbox" of aggregated history only (Closed World Assumption). It must be trained following the Open World Assumption challenges to address previously unknown potential attacks a similar way as if a human immune system meets new "intruders". Such artificial "Immunity" can potentially be enhanced with automatically generated "vaccines" (special content permanently produced and updated during adversarial training).

	New AI-enabled Security information and event management should be able to aggregate heterogenous data and results (either from multiple context-aware (AI-enabled) sub-systems or in a centralized monolithic manner) to create a meaningful real-time situational overview. **Predictive security and (semi-)autonomous incident mitigation to support active incident response strategies.** Rather than just reacting to anomalies and displaying alarms defensive systems shall act more proactively by continuously estimating risk, predicting new attacks and potentially even deploy mitigation action. Application of AI algorithms to complex, real-time strategy games such as StarCraft (featuring imperfect information, long term planning horizon and huge action space) with or beyond human performance shows that it is already possible to combine multiple ML-Systems for processing heterogeneous inputs from API interfaces and visual maps and autonomous decision making. **Protect additional attack surface created by new and emerging technologies for interacting with IT Systems.** **Understand and anticipate possible malicious use of artificial intelligence.** Discuss and develop best practices for distribution of data, code, and models that may be put to harmful use. Explore approaches to identifying patterns and traces of AI-supported malicious activities.
Expected benefit; strategic or economic impact ➔ **What can be achieved?**	On empowering cybersecurity with AI techniques, the first and very crucial benefit is not falling behind in the arms race and exposing the European community, economy and citizens through the increasing and persistent threat of (automated) cyberattacks. Secondly, there are, of course, huge efficiency and productivity gains to be made vertically, across all levels of the security infrastructure, as well as horizontally across industry sectors: Less workload for humans in the loop is required, more reliable systems and services, faster development cycles due to improved automated software testing and decreased fraud-related cost are just a few potential benefits. Preventing attackers from low-investment cost-efficient use of AI and mitigating consequences of ML-powered attacks means fewer successful attacks and lower damage to individuals and organizations.
Starting TRL / Expected TRL	**Starting TRL:** 4 **Expected TRL:** 7
Timeline (2025/2027/beyond)	2025-2027-beyond (as AI techniques spread and evolve)

ECS
EUROPEAN CYBER SECURITY ORGANISATION

> JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU