EUROPEAN CYBER SECURITY ORGANISATION

Input to the Digital Europe Programme 2021-2027

Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building

WG 6 – SRIA and Cybersecurity Technologies

December 2020

www.ecs-org.eu

Input from the European Cyber Security Organisation (ECSO)

to the Digital Europe Programme (DEP) – 2021-2027

Priorities for supporting the implementation of policy, technology, competitiveness and competence-building

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.

Disclaimer

This document integrates the contributions received from ECSO members to produce the input to the Digital Europe Programme 2021-2027. Despite the authors' best efforts, no guarantee is given that the information in this document is complete and accurate. Readers of this document are encouraged to send any correction to the ECSO WG6 secretariat, please use wg6_secretariat@ecs-org.eu.

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

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

Copyright Notice

Table of Contents

Preamble

Cybersecurity is fundamental for the Digital Transformation of the Digital Single Market, to protect the European citizens, enterprises, infrastructures or institutions against cyber-risks as well as develop the competitiveness of the cybersecurity domain.

Europe can bring added value in all these areas as they have influence on the different critical sectors for the European society and economy. Even if some of the topics proposed could be dealt with / solved at national level, many EU countries would need such solutions and would benefit from a common effort to build a robust European cybersecurity ecosystem, to strengthen the entire value chain.

ECSO has identified some strategic areas for investment in order to develop a Capability Development Plan to increase digital autonomy and respond to the needs of our industrial sectors, while protecting the European fundamental rights.

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.

The priorities have been grouped under four main levers that drive the priorities:

1. Support to policy implementation

Main challenge

There is a growing need to define standardised and harmonised approaches to support the implementation of cybersecurity policies in Europe. The common definition of certification schemes (through the EU Cybersecurity Act) is needed to reduce the fragmentation in Europe and will bring confidence in the security of products and services. The definition and support of a federation of databases (on IoT vulnerability, incident reporting, and threat intelligence) are also needed to establish trusted and coordinated prevention and responses. To effectively combat the current cyber threat-scape, a more in-depth collaboration is required, and information sharing will be at the basis of comprehensive security analytics and applied threat intelligence. Information sharing is at the core of the NIS Directive and solutions to establish trust and confidentiality are strategic to its right implementation. Finally, the definition of a common ‘controls framework’ and tools for international players operating in the EU market would improve compliance to European regulations.

Impact

- Support to the EU Cybersecurity Act and the implementation of the NIS Directive
- A trustworthy and reliable supply chain
- Alignment of cybersecurity in the context of safety and security legislations
- Digital autonomy through the development of threat intelligence platforms
- A common taxonomy and regulatory framework across sectors and countries
- A faster and more efficient response due to harmonisation and simplification of regulatory requirements
- Increased trust among Member States
- Raised level of cyber resilience in Europe, enhanced business continuity of ICT systems and services

2. Support to technology implementation

Main challenge

Europe has a long-standing tradition in research but targeted investment in digital technologies is needed and is key to introduce breakthrough innovation into the market and support the uptake and deployment across Europe of existing critical or tested innovative digital solutions. New cost-effective digital solutions should be integrated in new platforms and services to ensure the deployment of the latest cybersecurity solutions to drive the digital transformation of the European

economy and society. Resilient communication and computing infrastructures, including 5G networks and edge computing, are needed to enable the secure deployment of applications and services of strategic importance. Identity management solutions based on decentralised technologies, self-sovereign identity and blockchain, will reduce the burden for citizens, company and governments to access services, lower the administrative costs, and speed up processes. This will also reduce identity fraud and increase user convenience. To effectively empower citizens, a platform is needed to help them manage their privacy and the information they share. Information and data are at the centre of the decision process and can have crucial political, societal and economic implications. This requires specific platforms to increase the credibility and reliability of web information. Several services and platforms should be made available to the research community and industry, such as tools for secure software development and runtime checking, platforms for the development and assessment of trusted electronic technology, adaptive honeypots to collect malware samples and link them with malware intelligence services, and tools for developing forensics capabilities. Finally, the DEP provides the ideal environment to define, exercise and deploy migration strategies for quantum-resistant crypto for larger scale deployments.

Impact

- Trusted network infrastructure developed and managed by European stakeholders and strategic for the development of resilient application domain services
- Better understanding of potential vulnerabilities in 5G technologies to anticipate cross-platform attacks
- Sovereign self-identities and better privacy-preserving digital identity
- Intelligent platforms for verification and decision making
- Development of technologies with secure-by-design principles and more resilient to zero-day vulnerabilities
- Better preparedness for the advent of quantum technology and its impact
- Better situational awareness of organisations and EU citizens about the technologies they use

3. Support to competitiveness and market development

Main challenge

Although Europe has a well-recognised industrial cybersecurity expertise landscape, the European cybersecurity ecosystem suffers from a twofold weakness: the strong fragmentation across the different market segments and a lack of private investment on a similar scale as exists in the US or China. In order to facilitate the emergence of pan-European players, the EU should be actively creating industry market-oriented initiatives. Through an EU-wide service programme made of four pillars, the cluster “Support to market development” is expected to play a key role in the development of the European cybersecurity businesses.

Impact

- An independent market analysis of the cybersecurity landscape to improve market knowledge for investors and providers
- Support to SMEs through a suite of customised services to increase their visibility to potential business partners and investors
- Leveraging the strength of regional ecosystems (smart specialisation) to accelerate the commercialisation of “Cybersecurity Solutions Made in Europe”
- European Investor Roadshow to strengthen the development of the cybersecurity investment ecosystem
- Fostering international cooperation with strategic business partners in countries such as Japan, to initiate a long-term cooperation

4. Support to competence building

Main challenge

EU policies must support the enhancement of digital competences, skills, education and awareness-raising at all ages and levels. Cyber ranges are becoming more visible and their capability to support R&D, training, testing and certification make them one of the key technological elements in cybersecurity. The use of simulation, games and virtual/augmented reality, adapted to each learning period, can also help to better understand what the risks of living in the digital world are and how to behave in it. Currently, there is a fragmentation in cybersecurity education and professional training, and there is a strong need for an aggregated European competence assessment model that is based on dynamic skills and competence building. We need to understand the demand for cybersecurity job opportunities and the motivations for involvement in cybersecurity (for women and girls in particular) and for this, a one stop shop to map competences, job profiling and job opportunities for a baseline understanding of the market would be strategic and key for addressing the skills gap.

Impact

- More cybersecure aware citizens at all ages
- EU-wide minimum curricula and common language and taxonomy of competences
- Harmonisation of job profiling (based on existing frameworks) and support to HR departments, ensuring the right people are recruited for the right jobs (more experts)
- Reducing the skills gap
- Raised situational awareness
- Fundamental (cyber)security awareness becoming a common knowledge and skill, making the EU more vigilant and resilient

Detailed list of priorities

Support to policy implementation

Develop tools to support the implementation of EU Cybersecurity Act

Digital Europe Programme – DEP.1.A	
Specific Priority	**Develop tools to support the implementation of EU Cybersecurity Act**
Description of the challenges **Why is it important?**	The Cybersecurity Act has established the European Cybersecurity Certification Framework and has set the way to create European Cybersecurity Certification schemes to reduce the related fragmentation in Europe. Trust in products, services and processes is essential to vitalise the European market and foster a minimum-security baseline and cybersecurity best practices to sustain the European industry in providing up-to-date security solutions. Validation platforms at European and national level are needed to reduce the time to markets of products and, even more critical, of software and services characterised by a shorter release cycle. These platforms will require efforts from different areas in order to satisfy the requirements and needs of different stakeholders, such as manufacturers, institutions and consumers. Specific challenges need to be addressed to support the roll-out of certification schemes: **Evidence in cybersecurity assessment.** When assessing the required cybersecurity functionalities of a system or service, different aspects need to be considered, e.g., which cybersecurity standards will apply, which party will assess that the requirements are actually met, what is the evaluation methodology, etc. The labs performing the assessment will play a key role in producing the evidence, that could be later checked, e.g. during continuous assessment, or even reused to assess products leveraging a specific component. Being able to test and analyse the security of a product in a uniform manner would provide a harmonised view to leverage and use the evidence in cybersecurity assessments. **Broader attack surface due to the impact of emerging technologies, such as 5G and IoT, and softwarisation.** Many organisations experience difficulties in integrating new technologies in their products, services and systems. The challenge is not only technological but also in the way security processes need to change to account for the emerging technologies. The advent of technologies like AI, 5G, IoT, or Blockchain promises to bring new opportunities to develop security solutions or integrate existing systems as part of the digital transformation of the society and the industry. Softwarisation will also play an important role in digital transformation. The benefits of new technologies and the shift towards a more oriented software-based approach could be undermined by the increased opportunities of attacks that could leverage potentially new exploitable or vulnerable components. **Supply chain and potential cascading effects.** A vulnerability in a component might be “inherited” in products and systems integrating the vulnerable component. Moreover, the digital transformation and the accompanying vision of a hyperconnected society, in which humans and devices compose complex and ever evolving/ever-changing

	interconnected systems, lead to a strong cybersecurity interdependence, thus increasing potential cascading effects of an attack. For instance, an attack affecting a single ICT system in a country or domain may have cascading impacts on systems in other domains or across borders. In addition to tools and services, guidance and policies should be provided, and regulatory options should be considered. **Time dimension and need to address the whole lifecycle.** One of the main problems in cybersecurity is that security is itself a very dynamic concept. As an example, the configuration, the intended use or even simply the deployment of the device in the field can exposed it to various and different security attacks. At the end of the cybersecurity certification process, a device could be tested against the defined security requirements, but the device itself can change due to the parameters' configuration or software updates, in some cases meant to also address security threats. The frequent changes in the security of the product under evaluation due to patches, updates, or even new vulnerabilities discovered, make the re-assessment of a product challenging. The security maturity of a product/service should be continuously monitored to widen the scope of the assessment and in some cases, it might require a complete re-evaluation. The certification process is very slow compared with the device updating requirements. **Vulnerability disclosure and handling processes.** Being able to check if a device is vulnerable to a particular attack or being able to share that information is crucial to improve the security. Manufactures, providers, system integrators can have in place specific programmes to improve the security of their ICT products, services and systems that can be continuously tested to discover new vulnerabilities or improved to address potentially new sources of attacks. Toward the need to improve the security, the definition and adoption of specific vulnerability disclosure programmes could be a crucial aspect. Vulnerability databases are also commonly used to gather all the discovered threats for any software, device, version, etc. The complexity of managing a unique vulnerability database could make the continuous updating and proper management of the vulnerability impractical. A security change could be provoked by a new discovered vulnerability affecting the ICT component, or a new recommended configuration or even an update or patch pushed by the manufacturer, and, therefore, it can come from different sources. In this sense, an efficient, standardised and simple way to organise that information is crucial to ensure that a user is able to ask for and receive that security information following common guidelines. Furthermore, this is already considered in the NIS directive, which is focused on the cooperation and exchange of security information among MS. **Time-to-market and cost factors are critical, especially for SMEs.** The potential large number of devices to be certified requires the design of cost-effective testing procedures. Ideally, these techniques should be applicable to different types of products, in such a way that similar procedures could serve to certify the security level of different components. Scalability could be also analysed from a different perspective; it should be a core aspect of security testing techniques by simulating real-world scenarios in order to detect possible security breaches of devices (e.g. due to a DoS attack). **Lack of common tools and testing environments.** The existing dynamism inherent to security makes testing a long and tedious

	process, which requires expensive/scarce human expertise as well as defining, modelling and implementing each test. This collides with new discovered vulnerabilities, updates or patches, that leads to repeating all processes in order to maintain the security level. Finally, as testing approaches are usually time consuming and expensive, analysing the security of recently developed technologies in a timely manner is often infeasible, and therefore not always applied to critical environments that need a particular and specific security level. In this sense, an automated and non-expensive testing approach would also help to test in an easy way the security of those non standardised protocols, helping to analyse their security level. **Market adoption of certification schemes and policy aspects.** The heterogeneity of the different certification schemes might lead to a further heterogeneity of the security certification format granted at the end of the certification process. The recently approved Cybersecurity Act brings some clarity for the definition of European cybersecurity certification schemes. Still the evaluation, the assessment, the security claims should be defined in such a way to also facilitate the comparison between different certified products, services and systems. Customers should be able to compare the security achieved by different products within the same category without feeling overwhelmed with technical details. **Skills and training to assess and operate product/services/systems.** Activities such as post-breach incident response and recovery, forensic analysis, and penetration testing are human labour-intensive and require high skills which are hard to find in the market. Training to assess and operate products/services and systems is crucial. Higher automation and integration with other security systems (e.g., for dynamic attack detection and vulnerability management) are crucial for scaling cybersecurity consulting operations in cost-efficient ways. There is the need for capacity building in conformity assessment bodies in accordance to Cybersecurity Act. **The solutions need to consider and support safety legislations (e.g., Radio Equipment, Machinery) and the Cybersecurity Act.** One of the main challenges for market adoption is the definition of vertical and horizontal certification schemes according to the different market segments, also considering the different regulations dealing with safety and regulating specific sectors. Understanding of the interaction among the different certification regimes and sector needs could also pave the way to a better understanding of the market adoption of the different schemes.
Digital Living & Working	The increased digitalisation of the society - with multiple connected objects and devices and the integration of smart technologies to support the operational tasks in the industrial sectors - has multiple impacts. On the one hand, it has reduced the human intervention; on the other hand, it has stressed the importance of relaying on trusted services and devices. As a result of the Covid-19 pandemic, particular attention will have to be paid to the way testing, assessment, and inspection could be carried out remotely while ensuring quality and strict compliance. Moreover, security assessment and certification could play an important role to increase trust, more in some sectors than others. Certification for healthcare-related/-enabling equipment could become a priority, but at the same time creating and generalising certifications for any product across the EU could be a Herculean task. Yet, this specific axis could be leveraged and consider health

	equipment (e.g. consumer electronics for self-tracking that can be mobilised by physicians) as a priority vertical to apply those new schemes and requirements.
BASELINE	
What is the situation?	The efforts towards the creation of a security certification framework have been defined at EU level through the adoption of the Cybersecurity Act. ENISA is tasked to propose the certification schemes and has already established two *ad hoc* WGs of experts who started drafting the first certification schemes under the Cybersecurity Act covering the SOGIS Common Criteria and the cloud services. ECSO has worked on the definition of the meta-scheme approach to i) help harmonising the minimal security requirements, ii) promote a uniform approach across verticals, and iii) provide a common way to define the scope and required security claim. It can act as a methodological tool to structure the landscape and "glue" together the existing schemes and specify additional steps once the first certification schemes will be available. ECSO has also worked on other aspects, including the scope of the certification and mechanisms to compare items. In addition to ECSO and ENISA recommendations, there is a need to define additional efforts to accommodate the certificate format of different European certification schemes that will coexist under a single framework. Current solutions do not take into account the sharing of cybersecurity certificate information between different stakeholders, including manufacturers and end users from different Member States. Furthermore, certificates are considered as static information that remains without any change during the lifecycle of devices. ECSO has also worked on explaining the benefits from the right mix of security assessments, and what constraints to be aware of when an organisation needs to build its own cybersecurity capabilities. The results have been published in the "Assessment options" document. 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 healthcare and qualified trust services. The study reflects on the standards currently available on these areas of interest and identifies existing gaps. ECSO WG1 has published the State-of-the-Art Syllabus (SOTA) (December 2017, now under revision), which lists all standards and specifications related to cyber security. The SOTA document gives a good overview of cyber security standards, initiatives and certification schemes, both at the European and international level (including national elements), for assessment and certification of items. Recently, the European Commission has published the Rolling Plan for ICT Standardisation indicating specific actions for standardisation bodies also in support to the Cybersecurity Act. In terms of testing, penetration testing and fuzzing testing have been highly used to stress the system under test with non-valid inputs. One of the main advantages of these two approaches is the high number of tools that can help automate the process of discovering vulnerabilities. However, common security testing techniques usually require manual

	interaction from security experts. This complexity could require expensive efforts from the manufacturer of new devices, so that the product launch is not delayed. From the point of view of certification this can represent a significant obstacle, because the update of a product will require a testing process to determine the security level of the updated device through a recertification process. Model-based testing (MBT) is a very promising alternative due to the possibility of generating tests from the system under test model in an automated way. However, MBT still have to deal with the problem of linking the high-level test specification with the real implementation of the product; operation that still remains manual. Non-European approaches for vulnerability assessment exist in the USA, such as the NIST National Vulnerability Database and CVE of MITRE. There is no European equivalent and the EU could lead the way on how to build on-top of the existing solutions and make the CVE/NVD more efficient, more harmonised and covering all aspects of cybersecurity lifecycle and Cybersecurity Act. Besides, currently IoT vulnerabilities are barely considered in vulnerability database. The existent databases do not contain enough registered IoT vulnerabilities to evaluate the risk of a device. An IoT database could help centralise and control all the current vulnerabilities for IoT and to have a starting point for certifying the security of the devices, complying with the basic assurance level. The European Database on Medical Devices (EUDAMED) initiative specifically provides a repository of information about medical devices. Regarding sharing mechanisms, Trusted Automated Exchange of Intelligence Information (TAXII) and the XML-based Structured Threat Information Expression (STIX) language provides a way to share security information in a standardised way. Indeed, it is one of the most used schemes for security information sharing. Blockchain technology could be also consider to foster a cybersecurity information framework at European level. Indeed, some European initiatives already consider blockchain to develop solutions for Social and Public Good (https://ec.europa.eu/research/eic/index.cfm?pg=prizes_blockchains and https://ec.europa.eu/digital-single-market/en/news/pilot-project-co-creating-european-ecosystem-distributed-ledger-technologies-social-and-public). There is still a lack of a unified regulation and certification framework at European level for network operators and technology suppliers. Some of them look to American standards such as NERC CIP. The existing approaches are usually expensive, slow and complex, requiring formal documentation and processes. It could potentially imply the manufacturer cannot afford the certification costs, or the delay for the release of the device in the market.
Effort until now	RASEN and ARMOUR propose different techniques and methodologies to assess the security and automate the process, making easier the usage of the certification. ARMOUR also developed a concept of label and establishes some information that should be included, such as the domain or the Evaluation Assurance Level based on Common Criteria. ARMOUR focuses on IoT and proposes a combination of risk assessment and testing based on an ETSI standardised proposal. This methodology was instantiated with tools and technologies with the aim of automating the process. In particular, ARMOUR uses model-based testing with tools such as Rational

	Software, CertifyIt and TITAN. However, some of the used tools are proprietary, and the methodology only addressed testing of simple devices and protocol, whereas the evaluation of more complex system was left as future work. OneM2M also proposed a series of vulnerabilities to be considered. The VARIoT project, funded by the CEF programme, plan to create vulnerabilities and exploits database dedicated to the Internet of Things. The ICSA Labs IoT Security Testing Framework, focused on specifying security testing requirements for different types of IoT device, also established a starting point for developing a more specific set of testable, security-related requirements for IoT devices and their components. Testing requirements in the ICSA Framework are based on six categories: communications, cryptography, alerting/logging, authentication, physical security, and platform security. TRUESSEC.EU addresses the certification and labelling problem to define recommendations on the development of European Trust-Enhancing Labels (ETEL). The ongoing project EU-SEC aims to create a framework under which existing, certification and assurance approaches can co-exist. At EU level, an example of dissemination of certificates is represented by the European Database on Medical Devices (EUDAMED). While ehealth represents a particularly sensitive context, the extension of such database embracing other devices (e.g. consumer electronics collecting health data) could increase transparency and trust in the digital era.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	The following areas should be specifically addressed. **Standards and certification for cyber resilient infrastructures – continuous assessment** • Develop tools and methodologies to deal with the heterogeneity of current standards and certificate schemes, facilitating the comparability and avoiding multi-certification. • Design and establish a platform for sharing and verifying cybersecurity certification information, in order to increase trust and transparency among stakeholders, including manufacturers and end users from different Member States. Important for the reuse of evidence. • Tools for partial and continuous assessment and lean re-certification of systems. • Tools for management of evolving threats due to the integration of new technologies and devices, e.g. IoT, with legacy systems. • Develop skills for professionals and operators of infrastructures and technical certifications. • Fostering consensus among industry, operators and policy makers to identify a common set of requirements to be considered to assess key domains. • Define common taxonomies and machine-readable formats/protocols across sectors to homogenise the landscape. • Set up an alliance integrating stakeholders of the critical sector (network operators, technology suppliers, cybersecurity solution providers, standard and certification bodies, national

	security agencies, CERTs, etc.) for defining cybersecurity standards and test procedures. **Vulnerability disclosure and handling processes** • Create a global/EU coordinated solution to re-use and update the existing vulnerability dictionaries, databases, metrics, etc., such as CVE, CWE, CVSS, CWESS, OVAL, SCAP, CAPEC to name a few, to the new digital and fast-pace realities taking into consideration what is needed to support the Cybersecurity Act. • Develop solutions for leveraging and possibly federating different European databases for known cybersecurity vulnerabilities: trusted party to maintain accurate information and access control policies to limit vulnerabilities exploitation. The solution must consider meta-data as well. • Develop an integrated cross-border and cross-sector sharing approach, so that cybersecurity information is readily available in an accurate and coherent way. • Definition of coordinated Common Vulnerability Disclosure programmes (ex. https://zerodisclo.com). • Analysis of current best practices, standards, and certification schemes that include vulnerability management and alignment with global industry best practices and international standards. • Implement a push notification system to protect and mitigate risks in products affected by critical vulnerabilities. • Define EU-level policy about clear processes and timelines how vendors or other stakeholders should respond/handle the reported vulnerabilities, and how the one reporting vulnerabilities should behave/wait/communicate/maximum-timeout. Organisations must adopt Vulnerability Disclosure Policies to encourage continuous reporting by the wider security community. Create bug bounty programmes and Vulnerability Disclosure Policies (ex https://firebounty.com). • Cyber-secure modelling via digital twin simulated environment. **Develop tools to automate evaluation compliance and checking during the lifecycle** • Tools for automated compliance checking, threat identification, system assessment and certification compatibility (static) / Most of current tools focus on dynamic analysis of software. • Tools for processing and verifying proof of fix requested under specific delays (e.g. when no bug bounty or virtual patching approach exists), especially for critical systems or particular verticals (essential services). • AI-based tools for continuous evaluation of security functionalities, impact of updates, real-time assessment, patching and lean re-assessment; automatic identification of vulnerability and patches (dynamic) / cooperation with AI initiatives. • Use of automated tools for security assessment and testing under a standard-based methodology (e.g., based on ETSI EG 203 251 V1.1.1) and tools for analysis of security certification reports (CC EAL, FIPS140-2). • Define a common taxonomy across sectors and tools to maintain cyber security in cross-sectorial systems (initial effort in some sectors such as manufacturing Semi40 and Arrowhead Tools).

	• Simulated environments for threat management: cyber range to train professionals and be reused for certification purposes, and digital twins to test security functionalities and patches • Open tools and testing certification labs to easy SME access to the precertification of products. • Develop skills for ethical hackers and professionals and bug bounty skills. • Identify compliance status for occasional penetration testing/technical auditing and for continuous security auditing bug bounty.
Expected benefit/impact **What can be achieved?**	Expected benefits: • Increase of end users' trust in EU products and competitiveness across Member States. • A stronger, more innovative and more competitive EU cybersecurity industry, fostering technological autonomy. • EU industry better prepared for the threats to ICT systems. • Common approaches across vertical sectors, and tools and platforms for SMEs entering the ICT market for a faster adoption of best practices in the related industry, enforcing the security at early stages. • An aligned vision on cybersecurity will foster the implementation of EU cybersecurity legislation (e.g. NIS, eIDAS). **Standards and certification for cyber resilient infrastructures – continuous assessment** • Harmonised vision of cybersecurity requirements and risks and traceability of security evaluation and assessment along the supply chain. • Management of the supply chain and integration into critical infrastructure. Reuse of certificate evidence to speed up the certification process. Traceability of security evaluation and assessment along the supply chain. • Cybersecurity evidence of products, services and systems and development of more robust and secure products, increasing confidence in the functioning of a critical sector. This will contribute to position European cybersecurity and critical sectors secure equipment providers as international leaders. • Increased confidence in the functioning of a critical sector, based on the development of more robust and secure products. • Improved preventive capabilities in manufacturing (less vulnerable products and services deployed). **Vulnerability disclosure and handling processes** • Increased security of products/services/systems by drawing attention to the need to update and patch. • Increasing efficiency of cybersecurity consulting through new tools, integration and higher automation. • End-users will benefit from more secure products; vendors will reduce their exposure to cyber-attacks and subsequent insurance risks. • Definition of patches and updates management process to prevent cyber threats exploiting known vulnerabilities. • Life-cycle management of security, providing a complete security support.

	• Effective and timely co-operation and information sharing between and within Member States. • Establishment and dissemination throughout the relevant user communities of incidents, threats and vulnerabilities with respect to both physical and cyber threats. • Provide mechanisms to SMEs and companies to internally assess and evaluate products. • Competitive approach on the world digital market through transparency and higher-quality products and services. **Develop tools to automate evaluation compliance and checking during the lifecycle** • Better adoption of certification process in the EU industry to increase users' trust in their products. • Management of the supply chain, cybersecurity evidence of products, services and systems for certification. • Provide mechanisms to SMEs and companies to internally assess and evaluate products. Support for SMEs in terms of awareness raising and relevance of "security by design" in practice. • Raise the bar of the security baseline by stimulating competition and better services to the market. • Harmonise the European certification schemes, avoiding duplications and facilitating the comparability of the results. Ability to compare different systems or devices certified under different schemes. • Increase the products, services and system security by determining a minimum required security level through the certification process.
Timeline (2025/2027/beyond)	2025 / 2027

Threat management and cross-vertical platforms

Digital Europe Programme – DEP.1.B	
Specific Priority	**Threat management and cross-vertical platforms**
Description of the challenges **Why is it important?**	In an increasingly technology-dependent world, providing a harmonized view of cybersecurity is crucial for the deployment of trustworthy ICT infrastructures. For this reason, cybersecurity certification has become a cornerstone concept to enhance the acceptance of the digital age. The advent of technologies like 5G or Internet of Things (IoT) promises to realize the vision of a hyperconnected society, in which humans and devices compose complex interconnected systems leading to a strong cybersecurity interdependence. Therefore, providing access to the corresponding cybersecurity information is crucial to foster the realization of a more homogeneous perspective on cybersecurity at the EU level. Information sharing will be the basis of comprehensive security analytics and threat intelligent technology, supporting effective and timely co-operation resulting in the dissemination of high-quality threat information (e.g. indicators of compromise) to prevent and detect cyber-attacks. Effectiveness will be reinforced through the proper

	tooling and staffing of sectorial Information Sharing and Analysis Centers (ISAC), providing sectors with tailored information. Most large organisations have setup a cyber defence unit (Security Operation Center or SOC). As the number of cyber-attacks increase, the resources required for each SOC team to cope is fast becoming unsustainable. This is compounded by a significant talent shortage in the area. Furthermore, these SOC rely on information shared by national (e.g. CERT) and sectoral (e.g. ISAC) clearinghouses to maintain an operational level in detecting and mitigating the impact of attacks, also potentially on improving the readiness level of the organization by obtaining early warning of cyberattacks and timely accurate situational awareness. As with many information sources, there is an increasing need to verify the integrity and correctness (truthfulness) of information and news, obtained for example in the web and social media (as well as the official ones). These SOC also rely on intrusion detection sensors and Security Information and Event Management (SIEM) systems to collect incidents for alarm correlation and filtering based on the analysis of contextual and situational risks tailored to this specific threat landscape. The current solutions struggle with the challenge of integrating multiple sources of data, including a multitude of ICT and ICS systems on one hand and diverse threat information data on the other hand. The pressure on SOCs and organizations is even increased by the speed of evolution of cyberattacks. The efficiency of sensors also relies on analysing malicious code for detection. Due to the increase in the number of malware campaigns deployed each year, it's complicated to capture fresh malware samples and to acquire the needed knowledge to perform the analysis. Beyond honeypots and honeynets, new tools and methods are required to capture and analyse malware in the wild. There is an important distinction between sensing and sensemaking. The above points have mainly to do with sensing – obtaining information about possible threats. Turning this information into a potential for action – sensemaking – requires development of tools and organizational practices that are both cross-sectoral and transboundary. Therefore, the organization of the response apparatus (not only the tools for sensing) should be seen as a challenge integral to threat management. The regulatory aspects should not be left aside. Information sharing is at the basis of the NIS directive and solutions to establish trust and confidentiality are strategic to its right implementation while not impairing or exposing sensitive information unnecessarily. Organisations in many sectors (financial, banking, energy, …) are often slowed down in their operability due to the volume and the complexity of regulations with impacts on efforts and costs, potentially causing inefficiency and loss of profitability.
Digital Living & Working	At work, the cybersecurity teams will be professionally staffed and tooled, and will rely on certified managed security services providers for additional help. Large companies and major administration have already established procedures, tools and staff, and will continue to do so.

	The situation will clearly be more difficult for SMEs and smaller regional and local administrations, which do not have the human resources and financial capability to operate such threat management platforms. The DEP should explore programs, for example with insurance companies, to support these smaller organizations. This should extend to small businesses and shops. While the practice of Security Operating Centers is largely prevalent in the professional world, the same practices are not available for private use. The increased presence of connected objects for personal use, at home, will significantly increase the attack surface. It is unlikely that Internet Service Providers will have a significant incentive in ensuring good cybersecurity practices for their customers. Therefore, the DEP program should support the development of appropriate cybersecurity tools for home use.
BASELINE	
What is the situation?	While the field of information sharing remain immature, there exist several ongoing initiatives. Multiple information sharing formats and mechanisms have been developed over the years (CVE, STIX, TAXII, OTX, MILE, to name a few), generally with little EU involvement. More recently, the development and operational deployment of open source tools such as the MISP and OpenCTI platforms is supported by the EU (e.g. through the Connecting Europe Facility program). Europe relies on third country technologies and services for many of the intrusion detection sensors, Security Information and Event Management (SIEM) platforms and cyber-threat intelligence data streams. For example, the Common Vulnerabilities and Exposures (CVE), National Vulnerability Database (NVD) and Common Vulnerabilities Scoring System (CVSS) tools are widely used, have no equivalent and are all US-based. This is not to advocate a EU-based replacement, as the worldwide reach of these tools is essential, but to ensure that we maintain access, through proxies, mirrors or otherwise. There are reputation and recommendation systems for web site and integrity checking mechanisms. Unfortunately, deep faking allows people to create pictures/movies from existing ones that at a human eye could see as real. In addition, currently most of the frameworks are human based and automation is required. Currently there many different malware intelligence services that shares knowledge about malware behaviour, command and control nodes used and files dropped by the attack. This information is submitted by malware analysts in order to share the knowledge and speed up the analysis process. Progress is needed to make regulation simpler, streamlined and efficient, especially for the Operators of Essential Services (OES) under the NIS Directive.
Effort until now	The EU has supported national CERTs and CSIRTs in adoption and deployment of the MISP platform by national CERTs through the CEF program. The most advanced CERTs and CSIRT have contributed additional functionality to the platform. ITU-T study group 17 developed a cybersecurity information exchange framework. (https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx)

	Several past and current H2020 projects are addressing the topics of detection, SOC and SIEM. Similarly, Significant research is performed on natural language processing, a pre-requisite to understand news and queries from users. Several identify and integrity management systems exists based on PKI or consensus mechanisms, including reputation and recommendation. There are many efforts to build adaptive honeypots and deception platforms, but this lacks a broader perspective. There has been no Integration effort to link malware intelligence services with adaptive honeypots until now.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Information sharing platforms could be improved through blockchain-based mechanisms, which enhance information integrity, support privacy and avoid the need for trusted third parties. This would also ensure scalability and interoperability. Security information and event management (SIEM) systems need to be extended with predictive capabilities, big data analytics for security, association of detection and remediation/mitigation, also to cope with the multiple heterogeneous sources of information. Multi-sovereign probes need to be introduced into the system to gather observational data without alter the normal functionality of the system neither to access sensitive information, but with only scope of providing actionable knowledge concerning the security situation of the system and its environment. Given the pervasive and intrusive nature of the probes, Europe needs to master the technology and develop European solutions to be fully autonomous and protect the access to potentially sensitive information vital for the European industry. Response and recovery tools are often poorly considered and / or integrated in existing systems, thus increasing the impact of potential cyber-attacks for European companies. The need to recover from and respond to cyber threats represents an opportunity to develop efficient detection and remediation solutions, ranging from artificial intelligence solutions for attack patterns learning and correlation to self-adaptive and reconfigurable algorithms to detect new evolving patterns. The technologies and solutions for incident response should make use of autonomic principles (self-*) to ensure reliability and self-preservation of the systems to minimise the risk and impact of potential future threats. Human agents are also inevitably in the look in response and recovery, making cybersecurity a sociotechnical issue. There is therefore a need to develop knowledge, training methods and organizational principles suited for rapid response and recovery. The EU could support the emergence of a framework where the integrity and correctness of information could be formally analysed and verified and the information consumer that use the DB as verification mean of credibility of information. Having also evidence of the truthfulness of the information (with the full reasoning behind, possibly explicable to humans). New deception schemes and methods should be developed to introduce malware intelligence services, providing complete analysis of malware samples as well as contextual information and possibly attribution. These services can be a strong ally to study the whole attack process, because they store fresh information about malware

	behaviour at early stage of a malware campaign. These malware analysis services should also aim at legally viable forensics. A common platform to harmonise approaches and regulatory requirements under the NIS directive could provide progress across sectors by reducing inter-sector best practices gap, improving risk management in organizations, improving regulators monitoring through standardization, streamlining and enriching incident reporting processes, and in the end defining a common framework and tools for managing cybersecurity risk compliance in critical sectors.
Expected benefit/impact **What can be achieved?**	The development of EU-based standards, tools and services, and the availability of open source alternatives for sensors, SIEM platforms and CTI, leads to increased digital autonomy for the EU. This should lead to improved detection, both in delay between attack and detection, and in accuracy. Increased reliability of web information increases consumer trust in digital services, particularly for critical infrastructures and e-government. Better malware analysis platforms reduce the time required to produce valuable information that can help to discover, stop and prevent malware attacks. This reduces both the overall impact and the risk associated with malware propagation. Improved knowledge and methods for sociotechnical response and recovery will increase the adaptive capacity and resilience of threat management. Harmonisation and simplification of regulatory requirements would lead to a more efficient risk management process, leading to a faster and more efficient response to cyber-incidents disrupting critical services.
Timeline (2025/2027/beyond)	All along the DEP lifetime.

Governance, policy and legal aspects

Digital Europe Programme – DEP.1.C	
Specific Priority	**Governance, policy and legal aspects**
Description of the challenges **Why is it important?**	The context of governance and policy is a key societal dimension: good governance[1] is related to effective institutions that provide optimal support to citizens in leading a safe and productive life in line with their desires and opportunities. Promotion of good governance goes beyond the government sector and includes all relevant actors from the private sector and society. The aims include the balance interests and focus on common goals, particularly reducing poverty and providing access to state services for all. Key challenges related to good governance include: • **Strategic autonomy** – in an increasingly digital world, technology has become a crucial enabler of governance, democracy and economic prosperity. The global race for

[1] https://www.giz.de/en/ourservices/governance_and_democracy.html

	leadership in key technologies such as Artificial Intelligence, quantum computing, 5G, as well as the global exposure of governments, critical infrastructures and companies to cyberattacks are challenging Europe's capability to decide and act independently. • **ICT supply chain complexity** – in ICT-based services, especially those relying on technologies such as Cloud Computing, it is becoming increasingly complex to determine ownership, governance structures and responsibilities of suppliers/service providers. • **Fragmented approach at EU level** – some examples are different levels of investment in cybersecurity, different transpositions of the EU legislative framework, individual National initiatives to provide cloud infrastructures, etc. • **Pursuing the "European way"** – Europe pays utmost attention to ensure that its fundamental values are respected. They include fundamental rights, privacy, gender and race equality, equal treatment in employment and occupation, consumer protection, etc. Therefore, protecting EU values in the cyberspace introduces additional challenges to be addressed. • **Legal challenges** introduced by the employment of new technologies in general (e.g. Artificial Intelligence) as well as in specific domains such as healthcare, including the responsibility model • **Fake news** has become a main undermining force for governance, institutions and democracy as a whole.
Digital Living & Working	Unprecedented, global, dramatic events like a pandemic increase the complexity of the scenario even from a cybersecurity governance perspective. In fact, when there is an urgent need to collect, process and share data and resources from a variety of locations, sources and organisations, robust, cross-border cybersecurity governance measures should be in place. In addition, the fully fledge deployment of remote working through multiple access points have increased the surface of our systems vulnerability. Ensuring cybersecure, intense and multiple telework activities may entail a paradigm change in the security of the whole system and the impact of the associated risks have all increased substantially. In the context of COVID-19: • CERT-EU published specific guidelines to support CSIRTs and its partners to better defend their respective constituencies and deal with the cyber aspects of the corona crisis. • ENISA published cybersecurity recommendations on several topics, e.g. working remotely and shopping online. • ECSO gathered several initiatives, tools and services provided by the EU Cyber Community in order to support a rapid response to COVID-19 related issues. • the European Data Protection Supervisor has published a guidance note[2] related to GDPR compliance for COVID motivated traceability of individuals From a governance perspective, the COVID-19 highlighted the lack (and the need) of EU-wide contingency plans to be put in place to

[2] https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en

	manage cybersecurity and privacy issues. This is a time when a huge amount of data is required and needs to be shared, at international level, to manage the emergency, and to face lasting changes in working practices and social patterns policies to recover from large-scale cybersecurity attacks. Specific attention should be paid to cross-border aspects and information sharing, and protection of critical infrastructures depending on the type of emergency occurred (during COVID-19, healthcare infrastructures became a specific target for advanced attackers, as health plays a strategic role for the future of EU societies and their return to normality). Recently, the EU has put forward a proposal for the European recovery plan, Next Generation EU, with the intention to create a new Strategic Investment Facility to address Europe's future resilience and strategic autonomy to enable the digital transformation.
BASELINE	
What is the situation?	Since 2013, EU policymakers have been supporting policy dialogue and legislative development on cybersecurity, with the aim to find a balance between EU values, competition and strategic autonomy. Among the most relevant results of this work are the EU Cybersecurity Strategy, the NIS Directive, GDPR, Free Flow of Non-Personal Data Regulation, e-IDAS, the EU Cybersecurity Act and the future e-Privacy Regulation. There is growing attention to linking EU policies and strategies focused on innovation to cybersecurity aspects (e.g. in the EU Data Strategy).
Effort until now	• Europe's proposal to establish the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres should be supported under the Digital Europe Programme. • Through the EU Cybersecurity Act, ENISA received a permanent mandate from Europe to carry out several tasks, including: the preparation of candidate certification schemes with relation to EU Cybersecurity certification framework; supporting cyber resilience (coordinating responses to large-scale cyber-attacks and crises); EU cybersecurity policy development and implementation; supporting Member States, Union Institutions, offices, bodies and agencies in the development/implementation of vulnerability disclosure policies • Some H2020 Security Call Topics include activities aimed at supporting the implementation, specification and further development of the current relevant policy and legal framework (e.g. SU-ICT-02-2020, SU-DS04-2018-2020, SU-AI02-2020, etc.) • The CEF (Connecting Europe Facility) Programme focused on the creation, operation and maintenance of a cooperation mechanism between a group of national and/or governmental CSIRTs. It also supported all the relevant stakeholders under the NIS Directive, including national competent authorities, single points of contact, operators of essential services, digital service providers, industry and their interactions with ISACs • The activities of ISACs, supporting information sharing in specific sectors and the implementation of the law as an advisory body (even including the participation of governmental

	bodies). They also support cybersecurity policy creation and implementation
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	• Foster collaboration between policymakers, technology providers and users to identify a proportionate regulation/policy framework, avoiding excessive administrative burden with relation to specific privacy, security, risk management, liability, ethics, transparency concerning new technologies such as IoT and AI. • Develop mechanisms and methods to identify responsibilities and requirements across the supply chain of complex ICT systems, including the end user in the loop. • Identify minimum standards and defined security-by-design and data protection by design approaches, including associated test measures, in specific domains such as critical infrastructure protection, remote working and e-governance. • Create legal structures and business rules for data sharing and management in complex, multi-actor scenarios (e.g. IoT, robotics), addressing both cross-sectoral and sector-specific issues, as envisaged in the EU Data Strategy. Foster standardisation efforts including the activities of IDSA. • Develop the European Cybersecurity Competence Centre as a platform for international public-private cooperation and information exchange on cyber threat intelligence, promoting collective cybersecurity measures. • Structure the cybersecurity certification scheme taking into account not only the “component” level, but also “process level”. • Develop a specific plan for reducing current dependence on other countries’ technologies, identifying priority investments. • Identify effective approaches to reduce the fragmentation in transposing EU legislation in Member States. To show an example, Member States shown different approaches in transposing the NIS Directive concerning the definition of security measures and incidents, risk management as well as the identification of Operators of Essential Services. • Ensure a common approach to 5G cybersecurity at EU level. • Involve Member States and industry players to ensure equal development of competencies, access to technologies (cloud federation, HPC, etc.) and participation to cross-border initiatives such as Common Data Spaces and related benefits.
Expected benefit/impact **What can be achieved?**	• Synergy across the EU concerning threat intelligence and information sharing • Achieving the full benefits of the new technologies and data sharing across Europe in accordance to European values • Improving the security of National Critical Infrastructures • Ensuring the optimal market uptake of new technologies through an increase in trust among all actors across ICT supply chains as well as end users including citizens

	• Effectively achieving strategic autonomy, while ensuring fruitful collaboration with like-minded countries • Improving the use of state-certified identity, with extended uptake of the eIDAS
Timeline (2025/2027/beyond)	2025: • full transparency mechanism implemented for citizens • increased use of electronic access for public administration • ubiquitous and secure remote working • uptake of eIDAS as the portable identity mechanism connected to commercial service providers and social networks • enlarged use / streamlined access to vast data pools 2027: • fully trusted and secure e-voting system in place (allowing democratic mechanisms to be used including through trusted digital infrastructures). • better societal inclusion / achieving digital literacy.

Support to technology implementation

Deploying resilient digital infrastructures in the field

Digital Europe Programme – DEP.2.A	
Specific Priority	**Deploying resilient digital infrastructures in the field**
Description of the challenges **Why is it important?**	New and disruptive technologies are re-defining the digital infrastructures on which society and economy depend. Their full potential can only be realised, and European digital sovereignty only be achieved if Europe will master the technology to ensure integrity and trustworthiness of (Internet) communications and services. With 5G entering the markets and promising low latency, high bandwidth, reliability and high density in terms of connected devices, communication infrastructures and technologies become more complex and more flexible. Virtualization and softwarisation of networks and network functions (slices isolation, unauthorized access or usage of assets, etc.) and the interconnection of different technologies come along with new challenges for providing end-to-end security. It is necessary to understand the synergies between these different technologies, define common security frameworks and be able to analyse attacks at different levels, facing the problem of cross-platform attacks. In fact, it may lead to both the need for designing new security mechanisms as well as utilising 5G principles and features for enhancing security and privacy, for example, to improve security policies and their enforcement on the edge of the communication. Reference policies and mechanisms need to be designed in recognition of the different business models supported for the various sectors, such as automotive, industry 4.0, eHealth, etc. it is important that these policies and mechanisms support integration across sectors, acknowledging their dependencies and allowing improved exchange of data as well as the management of complexity (e.g., caused by an expected increase of identity and authorisation authorities, or increased regulation). In addition, new trust models should be defined to address machine to machine interaction and to manage complex 5G infrastructures, including addressing liability issues. Characterizing

	assumptions and guarantees of systems and components in terms of security will favour a more objective evaluation of risks and attribution of responsibilities, including a clarification from the legal perspective. Security mechanisms across all infrastructures rely on cryptographic algorithms that are practically infeasible to be broken. With quantum computing threatening many of today's encryption and signature schemes, research has been investigating into quantum-resistant cryptography. While new algorithms are emerging, it is an open question on how society and economy can systematically, efficiently and effectively replace the current and then vulnerable schemes, used to protect vast amounts of data, by the new ones. While migration strategies might be straightforward for confined systems under single control (e.g., a database where the data is encrypted at rest with keys owned by the database operator), they are less obvious with increased degree of distribution and ownership (e.g., a national ID card equipped with individual certificates for authentication, or a public blockchain). Digital technology increases the interconnectivity between critical infrastructures. The resilience of a critical infrastructure can thus not be seen in isolation. Ensuring safe, secure and resilient European societies with improved capabilities to cope with known and unknown cascading infrastructure failures requires the development of methods for dynamic risk analysis of dependencies, as well as for increasing resilience in the increasingly complex network of critical infrastructures.
Digital Living & Workings	Resilience in infrastructures means being able to anticipate, detect and respond to disruptions that are difficult to build safeguards against, thereby sustaining operations as much as possible. It also means being able to grab and exploit the positive opportunities that can arise. "Building city resilience requires a holistic approach that includes ensuring the safety of the critical services as well as understanding dependencies among them, developing social skills to build resilient society, enhancing cross organizational resilience and collaboration efforts among city stakeholders and having good leadership and governance systems that entails proper policy decision making[3]."
BASELINE	
What is the situation?	Several European countries have started to develop a 5G plan to roll out the technology, considering the huge impact on their economy or as an enabler in recognised applications of strategic importance such as connected cars. And while the characteristics of 5G have already begun to be outlined, efficient security measures for 5G that face the specific challenges have not yet been defined. In addition, cross-platform attacks are not analysed in detail, and there are no tools or methods to perform realistic security test in complete 5G scenarios. Regarding quantum resilient cryptography, current research focuses on algorithms. As far as visible, no significant practical efforts are invested in the definition of migration strategies. The SU-DRS01 project Engage will commence in 2020, working on improving societal resilience during large disruptions such as natural hazards, terrorist attacks and industrial accidents. The overall objective

[3] How Can We Build Resilient Cities? https://www.resilience-engineering-association.org/blog/2020/04/06/how-can-we-build-resilient-cities/

	is to provide European policymakers, authorities and first responders with new knowledge and solutions for bridging the gaps between the planned, formal efforts to increase resilience (first responders and authorities), and the inherent resilience of societies. This means improving resilience by engaging citizens, communities, NGOs, first responders and authorities in the different phases of the disaster management cycle. Case studies include incidents related to nuclear power plants, tsunamis, terrorist attacks against trains and human gatherings, wildfires, floods and earthquakes. Such incidents affect a multitude of critical infrastructures.
Effort until now	Large investments in 5G (EU projects) or related (e.g., smart-cities, vehicular networks, etc.).
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	On securing 5G, we see additional needs both in terms of the design and implementation of new security mechanisms as well as on the capabilities to test and analyse security on a realistic scale. Some relevant areas for investment in mechanisms are those guaranteeing the security of the routing while ensuring control over the data and communication, mechanisms for data protection and design and development of technology for network function virtualisation, firewall and privacy-preserving network monitoring. There is also a need to investigate the development of new Software Defined Network components, especially the SDN controller. On the analysis and testing side, it can be observed that the complexity of 5G networks makes it very difficult to test new security solutions without direct access to the infrastructure. This becomes an issue when only isolated parts/technologies can be tested making it very difficult to predict or to estimate the risk of an attack to occur. In particular, cross-platform attacks can affect even more to 5G networks due the high convergence of technologies, devices and actors. Therefore, investments in order to produce realistic, open-source and configurable tools and simulators to prove new security solutions for 5G before the deployment are needed. Current simulators do not satisfy these needs. because the security expert would need to first develop protocols that are requiring a different expertise. The DEP provides the ideal environment to define, exercise and deploy migration strategies for Quantum-Resistant Crypto for larger scale deployments. Projects should focus on all dimensions and include exercises on executing different migration strategies for real use cases and applications. Lessons learned from the exercises should be transformed into practical guidelines that support entities to plan and execute their own migration, considering both the technical, economical, and legal context. While communication technologies and social media provide great capabilities, first responders and other emergency authorities still struggle to leverage and integrate information into their command and control systems and establish bi-directional channels with the public during emergencies. In addition to securing digital infrastructures, the interconnectivity between critical infrastructures needs to be understood and managed. This will require new methods for modelling technical systems in

	continuous change, and the development of resilience capabilities in the organizations managing them.
Expected benefit/impact **What can be achieved?**	• Trusted infrastructures developed and managed by European stakeholders • Better understanding of 5G for the experts. Improve the security solutions for these environments. • Avoid future problems motivated by the rapid evolution of technologies. • Increase the cooperation of different type of experts in the field. • Understand and identify the vulnerabilities in 5G technologies before these can affect to several layers of the communication architecture. • Increase the trust of the citizens in using these networks securely and privacy friendly. • European stakeholders (governments, authorities, businesses, organisations) being prepared for the advent of quantum technology and its impact. • Increased technical and organizational resilience in interconnected critical infrastructures.
Timeline (2025/2027/beyond)	2025/2027

Platform for privacy management

Digital Europe Programme – DEP.2.B	
Specific Priority	**Platform for privacy management**
Description of the challenges **Why is it important?**	Although GDPR gives users a wide set of rights with respect to their data protection, exercising these rights is very difficult as most users (i) do not record to which sites they have given their consent, and (ii) do not really know what the implications of these consents are. Indeed, as trackers and advertisers move from one site to another the implications of a given consent may change overnight.
BASELINE	
What is the situation?	With the publication and initial enforcement of the GDPR, data protection and privacy has become increasingly important for users in cyberspace. Unfortunately, when users want to access a web site, they usually have little choice but to accept cookies (or other tracking mechanisms) without an in-depth understanding of the consequences of their acceptance. Currently users have little understanding about the consequences of giving their consent. • Simple “down-to-earth” questions in the minds of users are: • If I give my consent, which trackers will get my information? What do we know about the reputation of these trackers? which of my past accesses will the trackers be able to correlate with this one? • Which trackers are currently tracking me on the web?

	• Even if I do not give consent to cookies, are there any other tracking mechanisms this site is using?
Effort until now	There have been some projects that help users understand privacy implications including: • https://www.caprice-community.net/ helps raise awareness to citizens of the privacy related consequences of digital technologies • https://cordis.europa.eu/project/id/675730 : design and develop innovative solutions to questions related to the protection of citizens' privacy • https://cordis.europa.eu/project/id/732546 develops practical alternatives through the creation, evaluation and demonstration of a distributed and open architecture for managing online identity, personal and other data
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Citizens should be provided with tools to understand (and quantify) the relationship between their acceptance of current tracking mechanisms and the importance of data that they provide. The proposal aims at developing a database of tracking mechanisms, where users could directly online understand the relationships between their actions and what happens behind the scene. Such database could contain 1) meta-information about the link between actors and the information passing schemes between them, and 2) local specific information related to the user and its credentials, that should empower him to obtain a dedicated vision of the activities tracked on him. Indeed, the database will contain information about all web sites which include a third-party tracker. This information can be used to show users how third-party trackers will track them as they move around the cyberspace. The database may also contain information about novel tracking approaches (such as cookie synchronization) that enables different sites to synchronize the information they have about an individual. For example, when a user accesses web site A and accepts cookies, the database will be able to tell the user that these cookies may be used to correlate this visit with visits to sites B, C, and D.
Expected benefit/impact **What can be achieved?**	Users will be in control of the data they provide. They will also have a better understanding of what data they give to other web sites and how these data are correlated. This platform will help with the implementation of GDPR. Indeed, although GDPR gives users a set of rights, most users currently do not know to which sites they have given their consent, simply because they do not record this information.
Timeline (2025/2027/beyond)	2027

Platform for identity management

Digital Europe Programme – DEP.2.C

Specific Priority	**Platform and processes for wide-scale digital identity in Europe: decentralised technologies, self-sovereign identity and blockchain**
Description of the challenges **Why is it important?**	Reliable identification and authentication of users as well as interoperability of identity-related information has been for decades both a major theme in cybersecurity and a concern both for public and private sector organizations, investing in such solutions to securely deliver electronic services that rely on electronic transactions. In an age of profound digital transformation across all sectors of our economy and where the economic, industrial and social relations of European and global citizens and business persons increasingly shift to the cyberspace domain and are implemented over digital platforms, from eCommerce and eBanking to cross-border eGovernment procedures, education or remote health care and social networks, secure identity technologies become the key enablers of Trust as a fundamental condition for citizens to interact safely in our Digital Society. In order to fully reap the benefits of a well-established and predictable European regulatory environment on identity, trust, eGovernment and cybersecurity (eIDAS Regulation, Single Digital Gateway Regulation, Cybersecurity Package) that decisively supports the development of our Digital Single Market and of some of its key instruments (i.e. the Single Digital Gateway and European Blockchain Services Infrastructure), research priorities need to support a new generation of identity management which puts users at the centre of its administration, enabling them to control their own identity information while effectively realizing their rights enshrined in our personal data protection legal framework (GDPR). In a context of increased cyber threats, including different forms of identity-related crimes, it becomes critical to empower users with decentralised and efficient solutions to protect who they are, revealing exactly and only the required identity information in each context of digital interactions under user control and with strong guarantees as to the authenticity, provenance and integrity of such data. Cybersecurity and strategic challenges: • Guarantee European/democratic values in the implementation of Self Sovereign identity building on previous successful experiences (CEF eID, eIDAS Trust Services, eDelivery, etc.). • Facilitate versatile, secure and trustworthy cross-border interactions (B2A, B2B, C2A, C2C), allowing public and private entities to deliver digital services more easily and building a vibrant, dynamic and rich ecosystem linking across sectors authentic public and private evidence sources, citizens/legal person representatives and service providers. • Foster a decisive competitive advantage for European industrial cybersecurity stakeholders in the market of electronic identity solutions that benefit public-private interactions, leveraging the advantages of a safe regulatory environment (e.g. eIDAS, SDGR), the strengths that European standardization/interoperability can offer to the new digital world and collaborating effectively under public (e.g. EBP), private (e.g. INATBA) and hybrid partnerships (ECSO). • Simultaneously build upon and accelerate the digital transformation in private (e.g. digital onboarding, effective KYC

	/ due diligence procedures) and public (e.g. Once-Only Principle, paperless and fully online procedures) contexts. • Contribute to the evolution of the pan-European eIDAS Network for electronic identification and authentication services as well as of EBSI towards convergence with Self-Sovereign Identity components and services and designing a strategy for the industrialisation and large-scale implementation as a European Platform of Decentralised Identity Management available to public and private stakeholders with transformative socio-economic potential.
Digital Living & Working	
BASELINE	
What is the situation?	Electronic identification and authentication have experienced over the last decades since the dawn of the Internet age an evolution from proprietary centralized solutions to federated identity schemes and protocols (SAML, OAUTH 2, OIDC) enabling interoperability across organization perimeters to state-of-the-art solutions and standards (W3C Verifiable Credentials, DIF-IETF Decentralised Identifiers) in the new paradigm of Self-Sovereign Identity which promises to realize the long awaited dream of a true identity layer for the Internet without relying on centralised authorities. This new paradigm is at the heart of horizontal efforts like ESSIF (European Self-Sovereign Identity Framework) within the EBSI (European Blockchain Services Infrastructure) an initiative of the European Commission and the Member States within the EBP (European Blockchain Partnership) that is now a CEF Digital Building Block (https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI) and will also be part of the new DEP. It will help to protect and empower not only the citizens and organizations, enabling more efficient interactions and new business models. Currently citizens need to identify themselves to different companies or to divisions from a large company, repeatedly providing personal data and information which rapidly becomes difficult to track and control and an asset that could be potentially misused without respect to its legitimate owner. Consequently, a potentially large number of entities can access this information, and in most of the cases not all collected data are necessary for their purposes. The existence of identity silos also produces issues related to quality of the information which can quickly become obsolete or inaccurate. In a self-sovereign approach which embraces a very broad definition of digital identity, users would receive certification of their identity or other valuable personal certifications (e.g. academic diplomas, professional qualifications, property entitlements) from a trustworthy source and would be able to store it on a mobile/cloud-based wallet and be able to present such credentials in a peer-to-peer exchange mode to any entity with which they need to conduct business or perform an administrative procedure. When citizen information is managed, it can be originally provided by different issuers, such as certificates issued by educational organizations, or medical records, in standardized electronic formats using public key infrastructures. The time and cost of issuing and maintaining and verifying these certificates is expensive. Furthermore,

	public key infrastructures, require using a certification authority as an intermediary to issue the certificates, creating a dependency which may be abused (e.g. inadvertently tracking user interactions). Current verification records stored in centralised databases are also liable to be destroyed in the case of natural disasters or wars. In the new paradigm, resulting from several years of research of Distributed Ledger Technology solutions for digital identity, cryptographically signed digital information will be issued to be held the citizen and by using public Blockchain, data will be notarized in fully privacy-respecting manner enabling instantaneous verification of presented proofs. It is envisaged that DLT European public sector blockchains, compliant with EU law, will support decentralised cross-border transactions between Member States, initially for the public sector and gradually for private services too thus facilitating the development of more secure and streamlined services, regulatory reporting, and data transactions between citizens and the EU institutions.
Effort until now	European Parliament's Motion for a Resolution on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP))" puts the focus on the strategic importance of these technologies and highlights their efficiency potential for public sector services and management with particular reference of the digital Once-Only Principle for reducing administrative bureaucracy and burdens, as well as the improvement of the citizens' capacity to hold governments accountable. The Motion also underscores "*how a permissioned blockchain network shared between Member States could be designed in order to store citizens' data in a secure and flexible manner*" and "*calls on the Commission to explore the improvement of traditional public services*"… "*applications that improve processes related to the privacy and confidentiality of data exchanges, as well as access to e-government services using a decentralised digital identity*". On-going efforts like ESSIF seek to empower users and realize the integration of different data sources to create an efficient interaction between public and private services. Blockchain infrastructures like EBSI have the ability to create a tamper-proof and distributed sequence of events. This allows any Decentralised Identity owner to update and keep track of the changes in the identity, as well as issuer of verifiable credentials to revoke the validity of verifiable credentials, without the need of any central authority.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Single Digital Gateway Regulation implementation and Once-Only related projects (e.g. Digital Europe For All, https://www.de4a.eu/) are of high relevance to consider in relation to this topic and can build strong synergies alongside the planned evolution of eIDAS and ESSIF in the coming years in the context of DEP. Digital identity management systems based in distributed ledger technologies (DLT) will play an important role in supporting the implementation of fundamental rights like personal right to a user-centric identity, with a strong view on self-determination and personal autonomy of natural persons. This will lead to faster, cheaper and easier ways of conducting electronic transactions between citizens, businesses and governments using standardized interchange

	mechanisms while allowing EU industry vendors to develop a wide range of products and services compliant with those standards. Some areas of action are: • Develop new identity management systems, federated, de-centralized or mixed, to manage the entire life cycle of digital identities of people, organizations, objects, processes, to provide a robust and rich semantic layer for innovative business processes • Apply these innovations in specific areas or domains, with a strong focus on regulatory compliance (e.g. fintech, healthcare), universality of access (e-government), limited computing resources (e.g. IoT) with large scale pilots • Support the adoption of digital identity systems and procedures in specific and at-disadvantage areas and scenarios (e.g. intermittent connectivity, elder people, unemployed people) focusing on usability and developing innovative trade-offs between security and usability • Support standardization efforts in European and International committees for interoperable, secure and innovative digital identity models
Expected benefit/impact **What can be achieved?**	By using verified sovereign self-identities, only the persons responsible for verifying the citizen's identity in the first instance require access to the data. Other than that, the only persons who hold and control the data are the citizens themselves. This means that, in contrast to authentication delegation systems, organisations no longer need to manage the complex systems for access rights but access a public Blockchain infrastructure which allows universally and immediately available verifications over data notarized in it. Furthermore, electronic signing/sealing of verifiable attestation allows to combine the strengths of European Trust Services that rely on qualified certificates issued by supervised trust service providers registered in EU Trusted Lists, as has recently been proposed by the EC with eIDAS-Bridge initiative (https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about). This means saving significant resources previously spent in setting up and maintaining non-universally interoperable approaches that relied only on costly PKI with centralised authorities or other siloed and proprietary solutions. Furthermore, possibilities for identity theft are greatly reduced as personal data will not be stored in the Blockchain and more importantly, risks of monitoring user behaviour and creation of user profiles on the part of the identity provider - as traditional IDM systems could allow - are now prevented. Verifiable pointers that proof authenticity of claims will be stored with full guarantees on a blockchain (permissioned Blockchain infrastructures like EBSI are backed by the EC and Member States) while data itself will be under control of the users. Better transparency and accountability will be achieved, thanks to blockchain non-repudiable and superior resilience properties. Also, third parties will be able to verify the claims directly themselves using the cryptographic material stored within a blockchain, enabling efficiency in multi-stakeholder scenarios. Recent studies (https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report) point to promising scenarios even in the short to medium terms, whereby use of notified eIDAS eIDs

	will enable issuance of Verifiable Credentials, current eIDAS nodes will be able to issue SAML assertions based on such Verifiable credentials (signed with qualified certificates using the new eIDAS Bridge developed by ISA2 Innovative Public Services Action or new eID technical specifications may be adopted by Member States based on ESSIF for (more flexible) identification.
Timeline (2025/2027/beyond)	2025

Establishing an engineering platform for trustworthy hardware, software. and systems

Digital Europe Programme – DEP.2.D	
Specific Priority	**Establishing an engineering platform for trustworthy hardware, software. and systems**
Description of the challenges **Why is it important?**	Maintaining a trusted system state from the design and manufacturing throughout the operation of a system, deployment and its decommissioning can only be achieved by interlocking activities across the entire value chain, with new challenges for reused or even refurbished components. • Secure hardware design, manufacturing and testing of trusted electronics • Secure software development and services • Analysis, technical forensics, hardware fingerprinting and incident investigation The initial trust in a system is rooted in its hardware. This requires that all critical components (CPUs, SoCs, sensors, AI accelerators, memories, …) are designed in a secure way, and it can be assured that the implementations perform the specified functionality and only this functionality. Global supply chains make it difficult to ensure this trust outside the domain of dedicated high-security electronics. At the moment, European industries and especially SMEs have no other option than building their products from cutting-edge components that are only available from the untrusted, global market. In addition, limiting access to technology IP became recently a more viable political option to enforce national interests. Therefore, one major challenge in cybersecurity is to establish cross-sectoral capabilities that provide access to the necessary technologies and tools to design European Trusted Electronics. This is a foundation to recover European technology sovereignty and enable stable sources for trusted electronic components for European stakeholders across multiple application domains such as IT, transportation, mobile devices, industrial control, and beyond. Further, a significant part of the actual cyber-security issues is due to the lack of proper security-by-design on the software and systems developed or designed during the first decades of the IT boom. A secure lifecycle has to consider how the software and the systems evolve over time in a secure way while legacy components are still in place. Such hybrid scenarios require hardware and software platforms that secure the integration also of legacy components and provide security measures with an appropriate system-level approach. However, only with advanced analysis capabilities it is possible to investigate possible attacks. Thus, digital forensics and hardware fingerprinting must evolve in improving the methodologies that consider the new IT contexts and

	the social changes and integrate lessons learned for security-by-design. Those new methodologies must consider technical, social and legal aspects, and be flexible enough to withstand a rapid evolution. This calls for integration between the fields of digital forensics (including fingerprinting) and incident investigation. The new solutions must be understandable by experts of different profile, who must be able to work cooperatively and be usable throughout the lifecycle.
Digital Living & Working	A secure living and working relies on the specified operation of critical systems. This specified behaviour can only be assured if the underlying system is in a trustworthy state. In addition, global supply chains are significantly more sensitive to international emergency situations.
BASELINE	
What is the situation?	On a global scale, Europe is falling behind in secure microelectronics and it requires immediate action to keep pace with other global actors. To give an example for the strategic relevance of the topic, the Pentagon's requested budget for 2021 allocated 1.5 billon$ for research and development only on microelectronics and 5G, where one of the main concerns is to establish domestic supply chains for the design and manufacturing of trusted electronics. (https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/) From a system design perspective, organisations from ENISA (https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/internet-infrastructure/secure-software-engineering) to several academic organization, secure software development guidelines (NIST, OWASP, ISO, private organizations such Microsoft, NASA, ESA, others) have been developed, covering all phases of software and system development. Proper secure software development and environment guidelines are both requested in order to achieve ISO27001 certification. However, they typically do not involve hardware and supply chain risks that fundamentally threaten the security of systems. Here domain specific initiatives like ISO/SAE 21434 for Automotive Cybersecurity contain first considerations. 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 analyse design, simulate and test electronics, software and systems are also often located outside of Europe. The open source community is gaining more and more commercial attraction and is working on promising hardware designs, such as the RISC-V instruction set architecture, and tools, but their maturity and quality is still far away from leading commercial solutions. The open source community is gaining more and more commercial attraction and is working on promising hardware designs, such as the RISC-V instruction set architecture, and tools, but their maturity and quality is still far away from leading commercial solutions. Open HW/SW platforms can support the creation of a secure ecosystem, leveraging common strategies across manufacturers and an improved system-level approach to trust The design, manufacturing and development, assessment and certification of high-assurance electronics, software and systems is well-established but carried out in a separated domain so that it is difficult to integrate into standard industrial and commercial electronics. European R&D is strong, e.g. in the design of advanced post-quantum cryptographic algorithms, but the

	underlying framework is missing to make the research results accessible to the end users and their products in product-grade hardware and software.
Effort until now	For the hardware part, 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 and larger systems and bring them into systems. 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. Multiple initiatives by different organizations/agencies (NIST, OWASP, ENISA, others) to standardize secure software development guidelines. Multiple tools for SAST and DAST are in the market (licensed, opensource). Tools for risk management are often developed for IT / Cloud systems and difficult to apply from the HW/SW level. Also, several communities have been created as IFIP WG 11.14 (on secure engineering (NESSoS)). Large corporate introduced several secure development lifecycle schema. Yet those are not complete and widely adopted. For the forensic part, OLAF (European Anti-Fraud Office) investigates fraud against EU budget, corruption and serious misconduct within the European institutions, and develops anti-fraud policy for the European Commission (https://ec.europa.eu/anti-fraud/). Legislative actions have been defined by the EU (https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en). Diverse standards that define both general methodologies for incident investigation and the steps to follow during the whole life cycle of electronic evidence, from when it is obtained until it is processed and communicated: Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012), Guidelines for analysis and interpretation of digital evidence (ISO/IEC 27042:2015), Incident investigation principles and processes (ISO/IEC 27043:2015), Governance of digital forensic risk framework (ISO/IEC 30121:2015).
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Security should be addressed from the beginning of the development of a new system (from the preliminary phases) and should especially cover third party components (HW, SW, Lifecycle), as they often inherit a major course of vulnerabilities and are difficult to assess (black-box components). The entire lifecycle from the development and operation as well as the system evolution and adaptation should be considered thus: security requirements engineering, secure architectures and design, secure programming and testing environment, secure manufacturing, run time monitoring frameworks, supply chain security, secure software adaptation and evolution, etc. Overall, we need development frameworks that enable assurance and certification based on continuous risk management as well as analysis. Indeed, additional efforts should be done to standardise a secure development lifecycle (potentially tailored to specific sectors) and on developing tools to support the entire development lifecycle in a simple way, from the preliminary phase to the operational phase. Such tools should be able to integrate potentially with: • Collaborative Design tools and procedures (for preliminary phases in complex systems) • Requirements elicitation and validation tools • Design and verification tools

	• Extension of SAST and DAST tools from software to hardware and system design. Reasons behind the lack of proper secure development posture are time and cost. New processes, supported by tools, should limit these two elements in order to maximise the diffusion and adoption even the small software houses and SMEs. It is also relevant to consider risk analysis and management during SDLC and at operation time. It is relevant to link systems developed according to a specific secure framework with the certification process for a potential fast track assessment. In other words, certifications must include a verification of the development process. It turns out that each piece of software should come with a trustworthy and verifiable statement of the development process that has been employed. This requires to create services for European stakeholders to design trusted electronics, especially for heterogeneous systems containing both, trusted and untrusted components. Establish a technology platform containing of a mix of open and closed source components • Processor platforms for different application levels from low-power microcontrollers to multicore application processors • IP pool containing e.g. accelerators, AI components, memories and communication blocks to adapt the processors • Fingerprinting mechanisms to track components and systems through the value chain to validate their trustworthiness during manufacturing and operation • Design flow and verification tools • Capabilities to assess and continuously monitor the security of IoT and especially open source components • Software and Firmware to securely operate and maintain the developed components • User-centric ecosystem with fine-grained access and usage control to ensure that the data sovereignty remains with the data source • Risk analysis and management tools, supporting integration with model-based engineering and addressing HW/SW/System level To increase trust on third party software, we need to create Reverse engineering capabilities to evaluate ICs with untrusted value chains Define standards within the European Union to understand digital forensics and incident investigation within a common framework, considering technical aspects, legal and human factors. These must be flexible enough to evolve and survive the IT, social and legal changes. The restrictions for the legal admissibility of digital evidence and prosecution of cybercriminals in different countries must be clarified to all the experts. Privacy must be included as part of the new methodologies due to GDPR, and new forms of cooperation between experts and citizens should be introduced. Also, necessary to define new solutions to adapt digital forensics to new use cases and scenarios, and train technical experts in legal issues for the new scenarios and tools. Define effective and intuitive open source tools and help the different experts (e.g. computer engineers and criminologist) to cooperate. Feed digital forensic tools with publicly available information.
Expected benefit/impact **What can be achieved?**	For trusted electronics, it is necessary to create a European capacity to design, integrate and assess trusted electronics to increase the flexibility and competitiveness of the European industry, and provide a technical foundation to ensure European sovereignty in trusted electronics.

	Methods for Secure Software Development Lifecycle (SSDLC) should be extended towards hardware and system design and made available to mass developers and practitioners. In particular, software scanning tools to test for the presence of known vulnerabilities or detect new ones. The goal is reduction of software released with known vulnerabilities, reduction of zero-day vulnerabilities. For the forensic, fingerprinting and incident investigation parts, we need tools and experts using those to detect and discourage cybercriminal behaviour. More responsible and civil society. Citizens will better value to experts.
Timeline (2025/2027/beyond)	2027 and Beyond

Support to competitiveness and market development

Investments in Europe and development of regional ecosystem

Digital Europe Programme – DEP.3.A	
Specific Priority	**Investments in Europe and development of regional ecosystems**
Description of the challenges **Why is it important?**	European Union and European companies face three main challenges: (1) the lack of dedicated & specialized investors in cybersecurity companies, (2) the lack of sufficient and specialized growth capital beyond the seed and A-rounds, and a sustainable path to scale-up and exit/IPO European cybersecurity companies in Europe instead of the need to access primarily the US market, (3) the lack of marketing and business development skills to support the growing phase of our competitive companies at global level. Firstly, the investment capacity of existing specialized funds in Europe is very limited, partially because of a limited awareness of cybersecurity potential amongst traditional private investors. In particular Europe suffers from an investment gap versus Israel (estimated to be circa 500 Million €) and versus the US (more than 3 Billion €). Secondly, Europe's cybersecurity lacks strategic sizable consolidators/acquirers able to facilitate competitive companies to stay in Europe and sustain valuable business and retain brains in Europe. Beyond the early stage investments, it is difficult for companies to raise sufficient funds to execute their further growth strategies due to a lack of market means. They have to rely on organic growth, which slows them down and limits their competitive advantage to continue to be market leaders. Finally, although Europe has several regional hubs (named here "Cyber Valleys") and a well-recognised interesting industrial and technological cybersecurity expertise, the go-to-market and product development capabilities of local companies remain less significant compared to its global competitors. The lack of growth acceleration facilities is revealing to be of essence to drive Europe's own start-ups and SMEs to reach out far beyond their traditional home markets and get a European dimension.

	This results in the lack of sufficient European cybersecurity eco-systems and powerhouses, stifling the competitive advantage of innovation on a European and global scale.
BASELINE	
What is the situation?	A highly fragmented market made of more than 12.000 companies with very few European accelerator programs working at local level (e.g. in Castilla y Leon, Basque Region, Estonia CyberNorth, Cube5 in NorthRhineWestflavia, Station F in France, CyLon) most of them focusing on early stage companies. In terms of investment, very few private investors are acting in the European market with a dedicated fund or action on cybersecurity (Ace Management, eCapital, KPN-TIIN Fund) while at this stage Europe Union is still facing the lack of dedicated public mechanisms for the cybersecurity market. Lack of an independent market analysis of cyber security landscape: being small and medium sized companies, a lot of the European cybersecurity solution providers lacks tools and resources to increase their visibility on the market.
Effort until now	The current activities of ECSO with private investors and regional ecosystems has been of paramount importance as initiated and sustained the interaction between private investors and the cybersecurity start-ups community throughout Europe. ECSO Cybersecurity Market Radar, designed to represent European-based cybersecurity products, vendors, services and consultancy providers, was published as a static report in November 2018 and the 2nd edition in July 2019. The market-oriented taxonomy of the ECSO Radar is used for mapping regional ecosystems in the context of the Pilot Action “Cyber Valleys” on Smart Specialisation and taken up by the Luxemburg and other regional ecosystems. Some results are available at: https://www.ecs-org.eu/working-groups/news/the-latest-edition-of-the-ecso-cybersecurity-market-radar-is-out-now ECSO Cybersecurity Business Matchmaking events have been designed to establish a unique Pan-European forum for selected promising European cybersecurity start-ups and SMEs to pitch their innovative cybersecurity solutions and to hold B2B meetings with the European and international investors. Over two years, ECSO gathered more than 150 companies during 6 events, ranging from seed and growth investment to strategic investment and M&A, as well as to support companies positioned on the entire cybersecurity value chain. 4 officials deals have been closed among participants at our events. In particular, during the last events in Madrid and Luxembourg ECSO gave exposure to European companies to American and Japanese investors. In parallel, DG CNECT launched in November 2019 the AI/Blockchain Investment Fund and call for tender (750K€ for 15-month activities) to establish the related Investment Support Program. A similar structure should be envisaged for the cybersecurity sector. In addition, ECSO coordinated the creation of the first community of regional ecosystems specialised in cybersecurity. ECSO facilitated the exchange of best practices among regional ecosystems and took the role of coordinator of the first operational scheme of a network of regions willing to support local companies to scale at European level. The proof of concept run in the context of the Smart Specialisation

	Platform Pilot Action funded by DG REGIO has validated the concepts and the tools proposed (https://s3platform.jrc.ec.europa.eu/cybersecurity). The impact of ECSO initiatives that have been undertaken over the last 2 years created momentum that can be seized over the coming years.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Two main inter-linked strengths: a dedicated investment support program and an inter-regional acceleration program. **1)** An Investment support program should carry out activities focused on supporting the further development and adoption of cybersecurity technologies and services in Europe. A dedicated program should be structured as follow: **a) Dedicated investor and investee awareness raising activities and community engagement.** To enhance the awareness and visibility of innovative Cybersecurity companies and projects with financial intermediaries and the broader investment community and to map the public and private investment programs in Europe. By strengthening the cooperation among investors (through regular workshops) and by incentivizing the creation of industry specific investment funds or funds-of-funds, private investors initiatives could be fostered or leveraged. **b) Cybersecurity Industry Market Radar.** To continuously monitor the current market developments and carry out specific market consultations with a broad range of stakeholders from the cybersecurity ecosystem, Governments and private investors and to convene and to better link the investment community with innovative cybersecurity SME, start-ups and scaleups. **c) Cybersecurity Ecosystems development.** Support the portfolio development and originate deal flow of technically and financially viable projects, identify and facilitate ecosystems to be developed, avoiding effort duplication and building on expertise and assets from each other. A critical success factor for the thematic investment platform is the development and origination of a strong portfolio of potential investment projects that are both technically and financially viable and having “smart money” investors being strategically leveraging their interests supporting their investment ecosystems. The program could run a data-driven scouting process via the use of large sample of data collected through local Investor Days and beyond. In addition, ECSO will establish a Permanent Expert Selection Committee (PESC) to continuously assess large numbers of innovative cybersecurity SMEs and start-ups. In cooperation with EC services, ECSO aims develop a methodology to identify a pipeline of potential investment projects. **d) Dedicated Matchmaking Platform.** Design and implement a dedicated platform aiming to facilitate the meeting between cybersecurity companies and private investors and extend this to matchmaking between cybersecurity companies, supporting and enabling organizations and towards end-users. **2)** Create a Pan-European “Cybersecurity Accelerator” as a network of regional ecosystems specialised in cybersecurity in order to widen the deployment of European cybersecurity tools and trigger large technology & business partnership.

	The network is made of regional excellence hubs providing scale-ups with key expertise and services on the commercialisation phase of their solutions. The accelerator structure, managed by a central structure, is aims to focus on entrepreneurial initiatives in cybersecurity. The regional hubs could be located in several EU locations that are ecosystems of emerging cybersecurity industry, academic excellence and a conducive entrepreneurial culture. 5 key European services completing the existing local acceleration layer: Potential services: • Local mapping of existing cybersecurity capabilities (SMEs, end-users, investors and support players e.g. investors) • Local immersion & regulatory support: coaching/advisory, support services for growth-stage high-impact companies to better understand the local business environments (e.g. application of the NIS directive, GDPR,) • Network of sales and resellers at regional level (link to the DIHs) in order to facilitate the access-to-market • Business- design service driving development of a shared European roadmap and vision with all relevant stakeholders to accelerate progress in order to collectively design the best solution. • European Investors Roadshow and Investors deck preparation and readiness coaching is part of this service (link with the investment support program). • A dedicated cascading fund mechanism to support SMEs to increase their cyber risk awareness and preparedness (including voucher scheme to finance training, audit, pen-testing, and response to attacks activities).
Expected benefit/impact **What can be achieved?**	This proposal aims to reinforce and consolidate the whole investment chain and thus strengthen the position of regional ecosystems as enabler of a stronger internal European market. On one side, more specialized funding capacity will a) support the emergence of new ventures addressing current market needs. Specialized investment will be able to b) better support these companies needs in industry specific expert resources, go-to-market, and supporting the developments of European cybersecurity ecosystems and eventually powerhouses to scale out beyond their national borders and gaining pan-European scale. On the other side, the Cyber Valleys program will be the unique gateway to create the future European champions in cyber security based on the conjunction of the regional specialisations, the proximity with potential customers through regional structures and four tailored services. In particular, the Program is expected to run two six-month sessions per year, with each session including ten Europeans scaleups. Over a 3-year period, the Program would be able to accelerate 60 scaleups. In addition, the Inter-regional program will support 1 technology and business partnership among scaleups every 1.5 year (e.g. cooperation among companies specialised in the ICS segment in order to build up a larger and more competitive offering).

	The objectives of the Cyber Valleys program could be supported by a dedicated fund (estimated between 75M€ and 120M€) that will invest into at least half of the scaleups participating in the Program over 3 years, which means around 30 scaleups in total. In addition, the Fund would also have its own sourcing and would invest in other scaleups, reaching a total number of around 50 scaleup.
Co-funding options:	• Seed-funded by regional authorities and the EC, supported by established industry players (including VC and family offices) • Strong synergies with DIHs, inter-clusters cooperation and Regional policies (S3 and EIC-Acceleration program) • Providing paid-for services to start-up investors and industry
Timeline (2025/2027/beyond)	2025

Platforms for market support to SMEs

Digital Europe Programme – DEP.3.B	
Specific Priority	**Platforms for market support to SMEs**
Description of the challenges **Why is it important?**	The European cybersecurity SMEs ecosystem suffers a number of structural weaknesses which are relevant for the current proposal: • Highly diversified cybersecurity SME industry serving mostly local markets • Missing/low visibility outside core/home markets • Majority of SMEs are too small to cope with long and costly cross-border sales cycle • Thus, they lack critical mass to market entry or growth in the internal market as well as accessing markets outside Europe • Specialization: Inability of many small SMEs to participate on tenders which cover larger parts of the cybersecurity value chain • Asymmetries between supply and demand (e.g. between SMEs with innovative/disruptive technologies and large-sized customers)
BASELINE	
What is the situation?	Marketing label available at national level (e.g. Label France Cybersecurity < https://www.francecybersecurity.fr>, IT Security made in Germany <https://www.german-brand-award.com/preistraeger/galerie/detail/14081-it-security-made-in-germany.html>)
Effort until now	Operating model developed by ECSO WG4 based on the discussion with national and local trade associations from 14 European countries. Registry already tested in the context of the Cyber Valley Pilot < http://tools.bdi.fr/annu_craft/cybersecurity.html> Action funded by DG REGIO in cooperation with 5 regions. The same taxonomy is currently used to map three additional regional ecosystems. That way, the ECSO mapping aims to be recognised as the first pan-European and transparent approach to market analysis.
DESIRED SCENARIO	
What more should be done? What gaps to	The SME Hub is intended as a market support and networking tool for European Cyber SMEs. It shall help SMEs to create **more market**

be filled? For what reason? **How can it be done?**	**transparency and facilitate local SMEs to market their solution at European level.** The Hub consists of three main functionalities aiming to give more visibility to European SMEs: • **The Registry: a** publicly accessible platform where SMEs can register their company and define the services or products, they offer in a predefined market segmentation structure which is based on the ECSO Taxonomy. Accordingly, this platform can be searched by interested companies who require services or products, based on type, quality and delivery capability of the registered SMEs. The provided market segmentation and categorisation can also be used to build consortia of different SMEs over larger parts of the value chain, e.g. when required for a project or large RfP. This platform will facilitate the creation of consortia and the visibility of SMEs to investors and business partners. • The **"Cybersecurity Made in EU" label**. The label is a **private marketing tool** fostering the claim of quality and security of European companies and NOT a certification. The label would target companies and NOT Products / Services, is based on self-declaration and NOT technical audit, is aimed mainly at SMEs but NOT excluding large companies. The operational model is based on a multiscale approach NOT competing with existing (similar) national label but rather aiming for synergetic co-existence with existing national/regional initiatives. The criteria are: a) The company is a registered entity located in Europe with headquarters are in Europe (if part of a group, then group headquarters in Europe) b) European ownership: company provides reasonable assurance that there is no majority ownership/control from outside Europe (declaring ownership structure / majority stakes) c) The company's has cybersecurity >50% of cybersecurity R&D activities located in EU and >50% of staff (FTE) d) The company offers trustworthy cybersecurity (ICT) products / solutions: The company declares to comply with the basic requirements defined by the ENISA Essential Security requirements for ICT including No-spy declaration: No offered product or solution contains backdoors (non-declared functionality) e) The company declare to be GDPR compliant • **The Quadrant.** The Hub shall give the possibility to serve as a market differentiator between SMEs based on their broadness of service, quality and capability to deliver. This shall be achieved by deriving various "European Cyber Quadrants" for the different market sectors, where cyber SMEs will be ranked according to clear and unambiguous criteria regarding quality and capabilities. The platform shall be open to all European Cyber SMEs, neutral and unbiased. It shall be provided via a web platform which is easily accessible by potential customers.
Expected benefit/impact	To be the leading market platform for European Cyber companies, forming an ecosystem where demand meets supply, funding, resources and know-how.

What can be achieved?	To foster and promote European Cyber companies, technologies and services in order to strengthen the cyber foundation of Europe
Timeline (2025/2027/beyond)	2025

International cooperation and investments

Digital Europe Programme – DEP.3.C	
Specific Priority	**International cooperation and investments**
Description of the challenges **Why is it important?**	Cybercrimes and misdemeanours have a global impact and require next to local cybersecurity actions also a global approach. Identifying challenges, approaches, innovations and potential ways of collaborations provide valuable insights in new initiatives and support for existing ones. Due to similar structural market challenges, both the European Union and other strategic partners (like Japan, South Korea, US, India, South Africa, Ukraine, Brazil and Canada) recognise the growing need for a closer cooperation on cybersecurity. There is interest, but scarce financial resources to foster these international relations from the private partners as the impact is usually on a long term. Financial and resources support should be provided to foster these relations. For example, Japan and South Korea have relatively small cybersecurity market, which is dominated by big international corporations, which pose challenges to the development of the local cybersecurity products and services (e.g. digital autonomy). There is a lack of visibility of the European companies in third countries and vice versa, but investors from both sides expressed their interest to scout market opportunities in the two regions Other international private and semi-private initiatives that exist, or that are expanding such as the CTA, GCA, Global EPIC, OWASP, EICAR, APWG, … seek stable European partnerships to help sharing expertise and experiences.
BASELINE	
What is the situation?	EU-JAPAN Economic Partnership Agreement (EUJEPA) came into force on 1 February 2019, creating new strategic cooperation and business opportunities in cybersecurity field. Existing global scale initiatives lack a European-wide collaboration and try to interact with the European institutions, or with initiatives in the member states. However, there is still a need to identify common vision, needs and challenges between other cybersecurity ecosystems, as well as business approaches to cybersecurity offerings and the needs of the vertical sectors. Other EU-Third country partnerships (like Ukraine, Canada)
Effort until now	• Strategic Partnership Agreement (SPA) between the European Union and Canada, EU-Japan, etc.

	• EEAS Technical seminars on transferring the best practices, including information on current threats and trends with third countries CERTs (e.g. Ukraine, South Korea) • Initial relations by WG chairs have led to the current interactions, but a more sustainable relation with the international partners should be envisaged with ECSO The first ECSO–EUNITY workshop, titled "Fostering EU-Japan dialogue in the field of cyber security and privacy" took place on 24 January 2019 in Brussels, Belgium. The workshop was designed to provide a forum for exchanging good practices and investigating new business opportunities in the field of cybersecurity and privacy between the European Union and Japan.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Given the similarities of ecosystems, emphasis would be placed on the mapping of the best technologies and services and private investors (corporate, VCs, banks) investing in cybersecurity. Resources should be made available to organize international exchanges, supported and funded by the local agencies to foster the international cooperation Activities should be organized on a bi-annual or quarterly basis, to ensure the continuity of the relations. This should be financed through the regions or on a European level. Understanding the geographic priorities of the foreign companies when going abroad: need for building a narrative to incentivise foreign companies to access the European market. Establishing a permanent forum (likely in the context of the EU-Japan Business Round Table), which allows a close EU-third country cooperation in the field of cybersecurity market in order to gather both companies and investors from third countries and European markets.
Expected benefit/impact **What can be achieved?**	Increased visibility and exposure of the European cybersecurity industry, its activities and development in other international markets, and vice versa. Direct take-up of technologies, setting up formal interregional or intercompany trade agreements, utilizing resources from a regional to a global level, lowering the level play field for all involved regions Increased business opportunities for the European companies to enter other markets, and vice versa.
Timeline (2025/2027/beyond)	2025

Support to competence building

Operational, interoperable and cognitive cyber ranges

Digital Europe Programme – DEP.4.A	
Specific Priority	**Operational, interoperable and cognitive cyber ranges**

Description of the challenges **Why is it important?**	Cyber ranges are rapidly raising up in importance within the security domain. The capability to support R&D, Training and test & certification configures cyber range as one of the key technological elements in the future cyber security landscape. Among the interesting features of modern cyber ranges is 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. Modern cyber ranges can also support physical appliances, resulting in "hybrid" environments even more flexible in their possible usage. Currently test ranges are based on fixed libraries of elements and networks that cannot be adapted to specialised or complex networks and don't represent exactly a "real" situation.
BASELINE	
What is the situation?	While the underlying technologies (private/public cloud, virtualisation platforms) are becoming mature, resulting on cyber range offers quite advanced, the market seems 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. Standardisation 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 standardisation of the scenario description metalanguages 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 training 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. 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 and test & certification (while potentially the EU Digital Single Market and the Certification Frameworks could benefit of cyber ranges as relevant test beds for security certifications). While technically feasible, the diffusion of sector specific cyber ranges seems still limited. Within the very last years the concept of 'federation' 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 standardise and organize the service offering of the single federated ranges), optimise the resources utilisation (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 both a military and a commercial 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 rationalise the output.
Effort until now	As previously stated, main efforts until now are related to the development and the implementation of the underlying necessary technologies, which can be considered mature for single range installations. Initial effort related to the maximisation 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.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	A platform able to give flexibility on content creation, including emulation of users, other attackers, latencies and wireless physics on a connected infrastructure. This platform should have also the possibility to emulate attack effects to understand blue team recovery capabilities for rapid response. These capabilities are important to support more real scenario that must include the entropy typical of a complex defensive/offensive situation, together with the possibility to measure the reaction capabilities of a blue team independently by the presence of a red team, imaging specific breaches. To realise this platform there is the need of actions on multiple levels. It should be available in a “plug n’ play” manner at an affordable price.
Expected benefit/impact **What can be achieved?**	Improve national security capabilities supplying a hands-on training capability on environments that cannot usually be available or tested, or situations where multiple behaviours related to users and machine to machine services compete on the same network Benefits related to the usage of cyber ranges are actually only barely perceived. The capability to leverage multisector training, test & certification activities, at a fraction of cost and much increased agility with respect to any testbed based on physical assets or on old virtualisation approaches.
Timeline (2025/2027/beyond)	2025

Citizens and social good

Digital Europe Programme – DEP.4.B	
Specific Priority	**Citizens and social good**
Description of the challenges **Why is it important?**	Citizens need to learn how to live in the digital society the same way they learn to live in the real world. Big(ger) companies generally take care of this themselves, but that’s not possible for all organisations and people. Citizen in general, and especially children, must be trained in their digital competences as a preparation for the digital age.

	This learning must start at kindergarten level and it must be adapted to the different learning periods in a person's life. In addition to citizens, attention must also be given to SME's as they are too small to deploy cybersecurity staff. SME's might also falsely assume that they're not a target of attacks. A last aspect here would the prevention of attacks altogether. The aspect of human element of security must be improved, for both defence or management purposes.
BASELINE	
What is the situation?	Efforts are mainly devoted to training scenarios for cybersecurity professionals and enterprises, but not so much oriented to the general public that need to know some basic hygienic cybersecurity means to apply not only in their private life but also in their professional one. Specifically, we see a number of target groups: • Citizens at large • Pupils at primary school • SME's as they are too small to employ dedicated cybersecurity staff Recent publications confirm the urgent need to educate people in the cybersecurity field as an evident demand for educated cybersecurity staff is increasing. Educated staff is a fundamental pillar for the key principles of cybersecurity. Stakeholders as well as educational institutions focus on educating young people up to universities and in higher education, in the spirit of their rapid preparation for the labour market. In this way, the gap caused by the rapid onset of digitalisation is just filling up, but the problem is not solved systematically. It is important to realise that we need to train young and old citizens on cybersecurity aspects. Pupils at primary school are not aware of the risks associated with using the Internet and an increasing number of them are becoming dependent on digital technologies as they spend more than 5 hours daily on them. A large number of children use the Internet for "chatting". They are not aware of the danger of communicating with an unknown person, they do not secure their own sensitive data and are not sufficiently prepared to face negative hate speech, extremism, radicalism, hoax, fake news, etc. Finally, most SMEs do not have a strategy or a budget in order to start working on their own cybersecurity. In the end, they also face cyber risks.
Effort until now	As regards the education of children, efforts vary across EU Member States and each Member State tackles education within its own capabilities. A European framework is a minimum requirement that every Member State can extend to its needs. The employer's goal is to have a competent and educated worker, which are currently lacking on the labour market, as soon as possible. There are some initiatives from Europol or the private sector on this. For instance, banks are offering support towards their business customers, but this nevertheless remains insufficient.
DESIRED SCENARIO	

What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Improve the knowledge and capabilities of citizens in general and more specifically of children. In addition to this, include SME's. Understand the evolutions of the social engineering threat landscape and prepare workable penetration testing scenarios/tools (simulated phishing is only one tiny element). Consider humans+IT as a unique attacked entity, promote cross-competences collaborations (e.g. behavioural design & security or links with cognitive sciences and usability designers). The use of simulation, games and virtual/augmented reality, adapted to each learning period, can help to better understand what the risks of living in the digital world are and how to behave in it. Invest in practical trainings, information tools, maybe legal obligation for SMEs to have a cybersecurity strategy. Simple actions and low-cost investments can protect an organisation against cyber events. Most of the time, managers do not take cybersecurity into account because they do not know how to do it. Nevertheless, the cybersecurity strategy of a company is under the responsibility of the management, not the IT department. Teachers are the ones who are in daily contact with pupils and can influence their behaviour. Therefore, the level of a teacher's quality and the need to ensure the development of their digital skills and competences are important in the education system in order to fully exploit the digital curriculum and thus motivate students to use it actively and acquire digital skills properly. In addition, we need to mainly: • Define and incorporate competences for the digital age and digital skills. Support specialising young people's skills in digital technologies for Internet of Things, data science, artificial intelligence, robotics, programming, algorithmic thinking, for further study of science, technology, technology and mathematics, but also for other areas of economics, economy and public administrations with regard to their digital transformation; • Introduce an innovative cybersecurity education system in primary schools; Focus on the competences and digital skills of young people leading to greater security on the Internet and use of digital technologies.
Expected benefit/impact **What can be achieved?**	More cybersecure aware citizens at all ages. Lower the cybercrime impact on SMEs in Europe and the financial impact and human impact if the company has to stop its activity due to a cyber event. Synergies with other human-related sciences (e.g. cognitive sciences, psychology etc.) Despite our efforts, education does not bring immediate results and investments are not valued as an immediate financial gain. The young generation is our future, which depends on their readiness. Future technologies bring along the challenges of a more digital and cyber world.

Timeline (2025/2027/beyond)	2025

Jobs and professional skills

Digital Europe Programme – DEP.4.C	
Specific Priority	**Jobs and professional skills**
Description of the challenges **Why is it important?**	There is no clear overview of the needed skills and competences for cybersecurity which hinders the filling of open positions in the field and hiring of people with the correct skills and competences. There is a workforce shortage and special effort is needed to attract women. There are currently many skills and competence frameworks (NICE, eCF, ISO27000, c-controls, etc) but there is a need for an aggregated European model that is based on dynamic skills and competence building. Related to this, we see fragmented practices of the cybersecurity education and professional training within European Member States. This has implications for the job market. There is currently no European solution or portal which provides a one stop shop for job profiling or job opportunities for a baseline understanding of the job market. This would provide enhanced support to HR and bring more experts to the market. We need to understand the demand for cybersecurity job opportunities and the motivations for involvement in cybersecurity as a domain (for women and girls in particular). To achieve that, we should have multiple programmes geared towards identifying cybersecurity related job and competence opportunities as well as career paths. HR departments require stronger support as well so a dedicated European competence portal is needed and should involve HR directly to provide an understanding of the HR market (how it works through recruitment, in house training etc.). Last but not least, in order to attract more people into the field, more cyber technology competitions should be organised. There is an interest to run competitions in Europe in several technological areas of excellence in cyber, including crypto, side channels attacks, automated bug finding. This would improve cybersecurity within Europe.
BASELINE	
What is the situation?	Recent state-of-the-art publications confirm the urgent need the grow the cybersecurity workforce in Europe. It is evident that the demand for cybersecurity professionals is increasing and that a shortage of cybersecurity professionals remains. The current higher education institutes are struggling to meet the working-life demand for cybersecurity professional education and training programmes. Current frameworks are built around categorisation and labelling which are too static to adapt to the dynamic and fast-paced nature of the cybersecurity field. There are competitions, e.g. for crypto, often won by Europeans but then the standardisation bodies benefitting those are mainly US-based.

Effort until now	There are fragmented efforts within European Member States and across the globe to fill the cybersecurity workforce gap. The situation leads to three-fold phenomena. Firstly, it is becoming more difficult to attract candidates to fill open cybersecurity positions due to a lack of qualified people. Secondly, the challenges relevant to the evaluation and assessment of candidates' required qualification for the open positions. Lastly, ever-increasing cybersecurity domains bring unforeseen and diverse ongoing challenges that can be met only by cybersecurity education and professional training. Ongoing cybersecurity professional certification framework approaches: • EU: eCF • US: NICE • Global: ISC2, ISO27000, c-controls specialty certifications • Some national projects but EU funding is needed to scale up Related to job profiling, we mainly see global or US-based efforts, example CyberSeek: https://www.cyberseek.org/pathway.html Some effort has been done in H2020; more should be devoted in DEP, especially for crypto.
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason? **How can it be done?**	Funding is needed to support projects (efforts are already ongoing, i.e. https://lll.digital/) that perform an aggregation of existing frameworks and controls, pool resources together and develop a European-wide assessment model with a number of skills and sub-skills. Such a model could support graduates and professionals to: 1. Assess their competences 2. Compare their career target and current activity needs 3. Develop their life-long learning plan 4. Periodically review and update their plan There is a need to do an inventory of all the education we have in Europe (formal and informal) and create an agenda of cybersecurity activities and repository of available resources (education, trainings, certifications) that can be used by individuals to build their "skills DNA". This is a personalised and agile approach to competence and career building that does not yet exist for cybersecurity, despite it being a domain which demands it. Developing an effective and efficient European professional cybersecurity workforce education and training programme that addresses three key challenges and questions: • *How can we fill the skills-gap needed for the cybersecurity workforce?* • *How can graduates possess the skills and competencies demanded by future employers?* • *How can cybersecurity professionals meet the ever-increasing unforeseen challenges of cybersecurity?* It is evident that cybersecurity workforce development efforts are fragmented across Europe, and it needs a systematic cybersecurity education and professional training approach to meet the workforce demand.

	Related to this is job profiling, i.e.: • *What is the role of an applied intelligence expert?* • *Or of a developer who works on security by design baselines?* A competence (job) portal could provide a clear categorisation which would allow candidates and recruiters alike to understand the real competences needed for a particular job/profile. Going further, a specialised Women4Cyber portal could be based on a correlation of role models (provided by W4C) and professional profiles (provided by ECSO's EHR4CYBER Task Force) that are to be standardised based on the ongoing work by related initiatives (i.e. EC Pilot projects) and legislations & regulations such as NIS and the Cybersecurity Act. A structure could also be created to set up, run, evaluate and exploit the results of competitions and propose actions based on those.
Expected benefit/impact **What can be achieved?**	• Harmonisation of job profiling (based on existing frameworks). • Clear and usable taxonomy of competences. • Support to HR departments, ensuring the right people are recruited for the right jobs. If successful, it can easily be scaled up and become a reference point not only for candidates & employers but also for universities to help them map their curricula according to the real and up-to-date needs of the market. There would be a social impact for women and young girls to choose cybersecurity as a programme and career. Increase the capability to test technological solutions, to evaluate and run competitions in order to improve the standardisation and certification efforts. Improve the image of the cybersecurity industry within Europe and globally, linked to the principles of the EU. The outcome and dissemination of the results would bring direct benefits towards harmonising European cybersecurity education and professional training in Member States, thus helping to fill the cybersecurity skills gap coherently across Europe.
Timeline (2025/2027/beyond)	2025

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