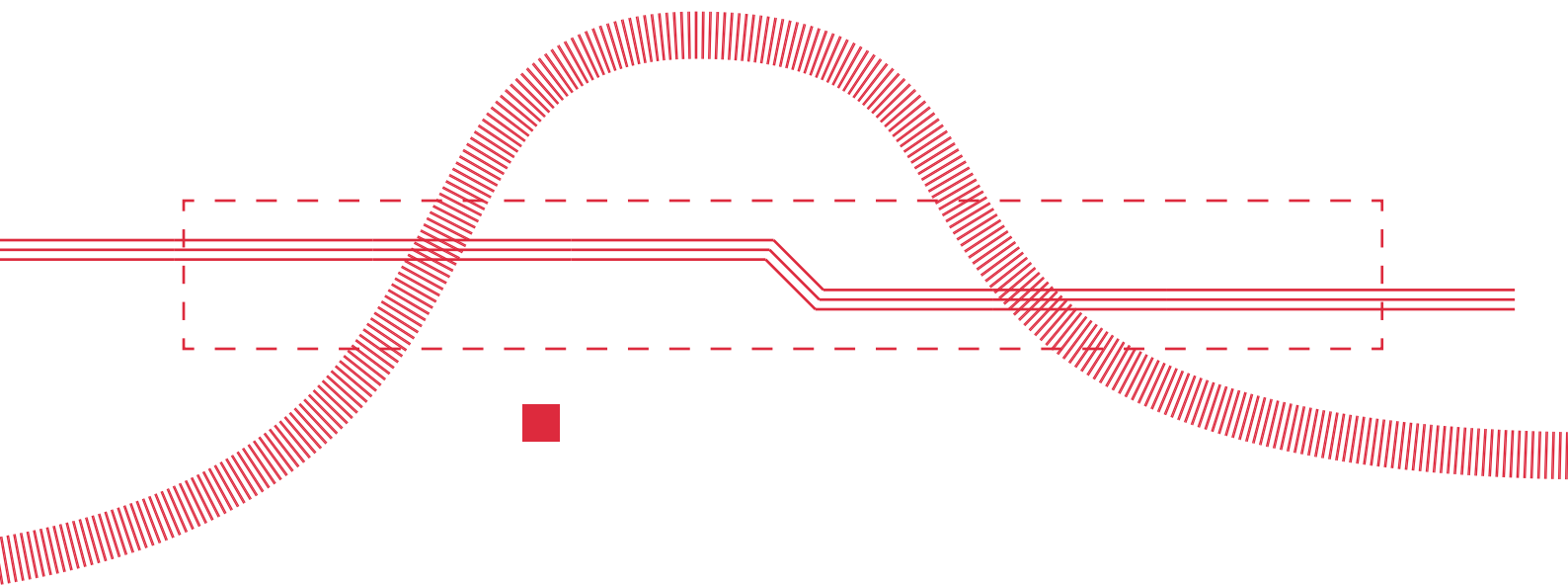




Roadmap for

Standardization & Certification



9 Roadmap for Standardization and Certification

9.1 Standardization

The International Organisation for Standardization (ISO) defines an international standard as a document containing practical information and best practice. It often describes an agreed way of doing something or a solution to a global problem [91]. Standardization or standardisation is the process of implementing and developing technical standards based on the consensus of different parties that include firms, users, interest groups, standards organisations, and governments [92].

Standards play a paramount role in the dispersion of knowledge and innovation and development. Or as expressed by relevant studies, ‘The processes for gaining this knowledge are at the heart of a standardization effort and the associated in- novation outcomes.’ ‘there is a contingency relationship between standardization, search, and innovation outcomes, where one size does not fit all.’ [92]

As stated by Mr. Peteris Zilgalvis, Head of Unit, Digital Innovation and Blockchain at DG CONNECT European Commission, ‘Standards are an essential part in achieving the goals of Green Transition and Digital Sovereignty’.¹⁶

The European Union has created and published a Rolling Plan for ICT Standardisation. This Rolling Plan ‘provides a unique bridge between EU policies and standardisation activities in the field of information and communication technologies (ICT). This allows for increased convergence of standardisation makers’ efforts towards achieving EU policy goals [92].’ Within this Rolling Plan, standardization actions have been identified also in the area of Cybersecurity. The actions and recommendations presented in this document take into account this Rolling Plan as well as various plans, frameworks, and actions proposed by other organisations such as IEEE, ISO, CEN/CENELEC or ENISA.

¹⁶ *You Tube*, accessed 24/11/2020

9.1.1 Challenges

From the certification and standardisation perspective, currently, the following challenges have been identified.

- **Challenge 1: A common (accepted) terminology and language:** As mentioned in the Scientific Opinion 02 of the High-Level Group of Scientific Advisors on Cybersecurity in the European Digital Single Market “Cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments, and the pace of technological change and innovation. In short, Cybersecurity is much more than a science.” In response to this fact, the European Commission has published a Proposal for a European Cybersecurity Taxonomy, to “align the Cybersecurity terminologies, definitions and domains into a coherent and comprehensive taxonomy to Facilitate the categorisation of EU Cybersecurity competencies.” ^[93] Until recently (and in some cases even today) a globally accepted and standardized definition of Cybersecurity and a clear identification of its domain of development and application had not been implemented. The Proposal for a European Cybersecurity Taxonomy provides a taxonomy and a set of definitions regarding the Cybersecurity domain so that (amongst others):
 - » All interested parties, all relevant initiatives, and activities can have a common point of reference and a common language.
 - » International Cybersecurity standards can have a common basis. To this last point, and to make sure that a strong basis exists to support the relevant standardization activities, this taxonomy should evolve from a static three-dimensional model to a full range dynamic network and to define and refine the definitions of other specific subdomains.
- This effort should be systematic, with an increased audience and stakeholder involvement so that it becomes a true tool and guide, that will keep the pace of the fast evolution of the digital world. Currently, this challenge is under investigation and development and related recommendations are anticipated to be included in further detail in subsequent Roadmap editions.
- **Challenge 2: Low awareness and utilization of Cybersecurity Standards:** ‘Standardization is one of the tools that can be applied to the continuous improvement of the organisation. Standardized work is one of the most powerful but least used lean tools.’ ^[94] Though important, ICT standardization and its methods remain a topic that is not easily accessible. It seems that this field is becoming increasingly limited to the expert

and remains mysterious to the non-expert. ^[95] During the last few years, initiatives have been undertaken to enhance, organise, fund, and coordinate ICT standardization. Although Cybersecurity originally belonged to the ICT domain, due to the increased complexity, variety and specialization, and consequences it has in daily life, society, and economy, dedicated effort should be given to the Cybersecurity Standardization aiming to the following:

- » Awareness and Education on Cybersecurity standardization. Through these actions, it would be possible to educate the general public and the various interested parties regarding the ongoing standardization activities and also create a new generation of professionals that would be willing to work within and contribute to Cybersecurity standardization
- » Funding for Cybersecurity standardization activities. Funding should be provided to facilitate the contribution to the Cybersecurity standardization activities.
- » Inclusiveness in Cybersecurity standardization activities. Initiatives should be implemented so that there is no bias or barrier to the contributing professionals (sex, origin, religion, physical abilities, background, etc.).
- » Open Standard Contributions to representatives from all types and sizes of organisations including micro, small and medium enterprises.
- » Support the adoption of Cybersecurity standards by making them affordable and by creating an alignment between legislative and regulatory actions and the relevant standards.

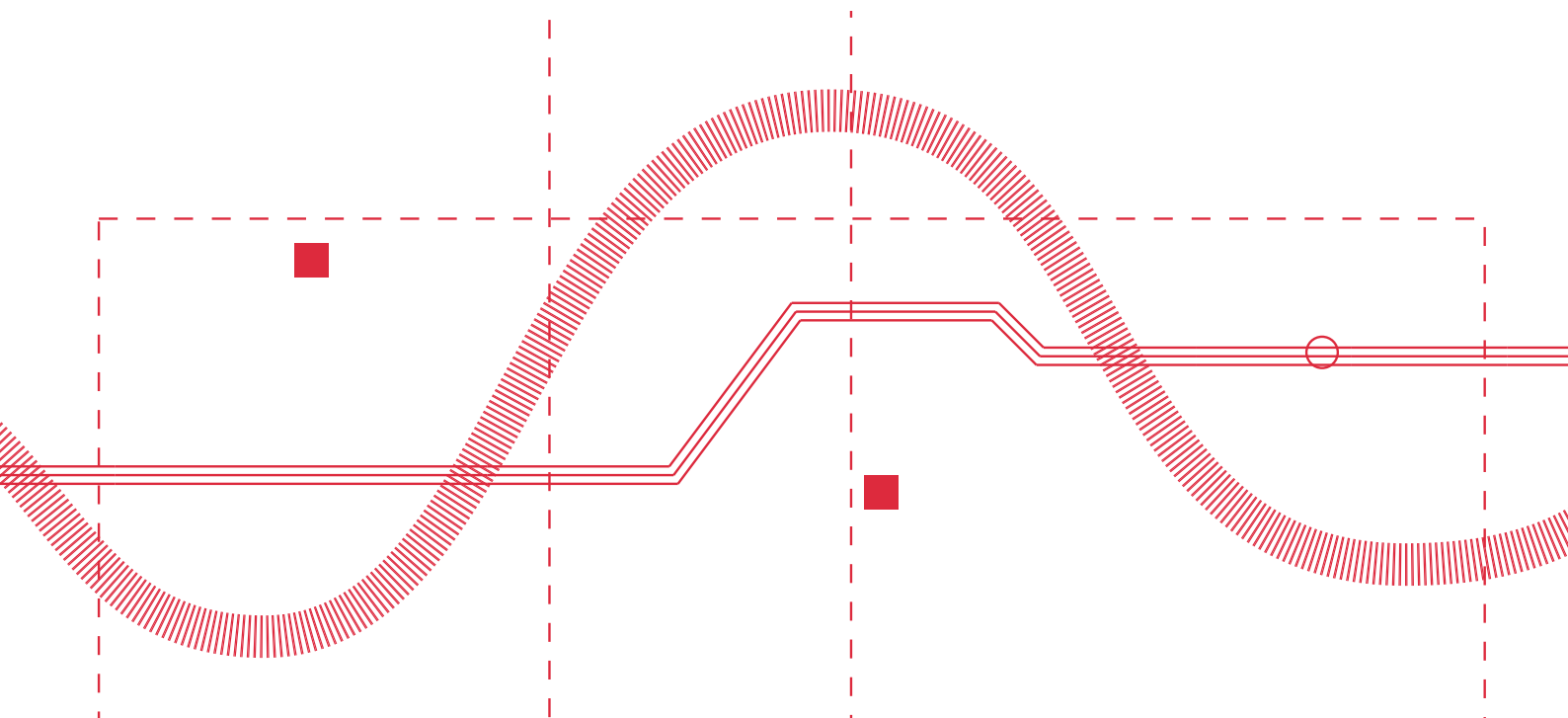
- **Challenge 3: A lot of work to be done.** As mentioned before the Cybersecurity domain is complex and has a high variety of domains and subdomains. This complexity is also inherited to and amplified in the standardization area. As shown by the proposal for a European Cybersecurity Taxonomy [93], each cybersecurity subject can to be structured on multiple dimensions, capturing not only the core and traditional research domains, but also impacted sectors and applications. A representation of the proposed three dimensions being:
 - » Research domains represent areas of knowledge related to different cybersecurity aspects. Given the multidisciplinary nature of cybersecurity, such domains are intended to cover different areas, including human, legal, ethical and technological aspects.
 - » Sectors are proposed to highlight the need for considering different cybersecurity requirements and chal-

- lenges (from a human, legal and ethical perspective) in scenarios, such as energy, transport or financial sector.
- » Technologies and Use Cases represent the technological enablers to enhance the development of the different sectors. They are related to cybersecurity domains covering technological aspects.
 - If this structure is also followed in standardization, this would mean that a subject relating to a specific combination of Research domains (e.g. Cryptology (Cryptography and Cryptanalysis)) and Technology and Use Cases (e.g. Hardware technology (RFID, chips, sensors, networking, etc.)) could need multiple standards (at least one per sector) (e.g. Health, Defense, Energy etc). There are a number of formal SDOs (Standard Developing Organizations) - a relevant list can be found at here - as part of the ICT Security Standards Roadmap project of ITU-T Study Group 17¹⁷. There are different types and levels of SDOs and at a given time more than one entity may decide to develop a standard covering a specific subject. This later also, adds to the complexity mentioned above and increases the need for coordination of the standardization efforts between the SDOs at all different levels. This coordination should allow for the efforts to be implemented once, implementation by the entity that has the greatest affinity to the subject and would provide the most valuable outcome multiple efforts to be carried out at the same time by the different entities and a later escalation and adoption by as many SDOs as possible to avoid market fragmentation.

- **Challenge 4: Keeping up with evolution:** Within the Threat Landscape of this document, the dimensions and evolution of Cybersecurity are presented. Moreover, the impact of the COVID-19 on the threats and the Cybersecurity domain is depicted. This information underlines the fact that Cybersecurity is a constantly evolving dynamic domain in need of constant overview, adaptation, and discovery. This dynamic nature of Cybersecurity should also be reflected in the standardization activities and outcomes. Considering that standards are a result of consensus and multiple party contribution (taking from one to five years to complete), a very real danger, especially for

¹⁷ This *ICT Security Standards Roadmap* is intended to support the security standardization work of the ITU by identifying existing published security standards, standards that are in development, and areas where a need for standards has been identified but where work has not yet been initiated. Although the focus is primarily on standards in the ITU-T space (i.e. security standards relating to telecommunication networks), the standards and work of other formal and informal regional and international standards development organizations (SDOs) are included in this Roadmap.

- the more technical standards, is for them to get deprecated, surpassed by current technology, and lose their value.
- Some related recommendations that should be taken into consideration are: For Cybersecurity standards to reach their goals of usefulness and adoption, the Cybersecurity standardization processes should be:
 - » Included in research activities as early as possible
 - » Realized in a 'leaner' way, allowing for at least initial versions of the standards to be available to a larger audience at an earlier time
 - » Coordinated and aligned every year. A Cybersecurity standardization plan should be established that will be regularly updated allowing for the changes in technology or situation to be adopted.
 - The Cybersecurity standardization plan should incorporate standardization efforts that would be implemented, in alignment with the strategic goals of the industry in the following areas:
 - » Compatibility/Interoperability
 - » Minimum Cybersecurity (Baseline)
 - » Informative
 - » Variety-reducing



Note: Types of standards needed within the Cybersecurity domain
 In the document *Understanding ICT Standardization: Principles and Practice* ^[95], the above types of standards are presented along with their economic effects. An adaptation of this information to the Cybersecurity domain provides the following definitions:

Compatibility/Interoperability Standards

A key role of standards is to ensure compatibility, which according to ISO 25010¹⁸ consists of two components: coexistence and interoperability. Coexistence means that an IT service/product shares a common environment as well as resources with other independent services/products without adverse side effects, whereas interoperability is the ability of components to work constructively with one another. In the ICT sector, compatibility/interface standards play a crucial role. Within the cybersecurity context, interoperability could be defined within the following two axes:

- The ability to have a selected security profile that is shared (communicated) between the various components of the system (e.g., a network)
- The sharing of Cybersecurity information, the ability to participate in threat-sharing communities or intelligence groups, and the analysis and evaluation of such solutions.

Elements of standardization belonging to this type could be:

- In relation to threat intelligence/threat information sharing
- Interoperability maturity model standard that will guide stakeholders towards the development of interoperable CTII sharing solutions, or the adaptation of their existing ones. Improving the interoperability of cybersecurity information sharing will facilitate more effective protection against cyber threats in the future.^[96]
- Threat data standard that will facilitate the exchange between different platforms, communities, organisations, and systems.
- DDoS clearing house / DDoS information exchange

In relation to IoT

- Secure communication standard for IoT. Achieving interoperability is vital for interconnecting multiple things together across different communication networks. It defeats the purpose to have billions of sensors, actuators, tiny and smart devices connected to the Internet if these devices cannot actually communicate with each other in a way or another. [97] To this we need to add that this communication should follow the basic Cybersecurity principles ensuring confidentiality and integrity as needed.

In relation to training/cyber ranges

- Cyber ranges scenarios standard to facilitate the sharing, re-using, and wider adoption of practical cyber range assisted education, training, and awareness.

¹⁸ ISO 25010

Minimum Cybersecurity (Baseline)

Minimum Cybersecurity standards refer to standards containing a set of minimum acceptable security level requirements. These standards when implemented for processes, products, services and organisation would aim in:

- Reducing the level of risk felt by byers of the service / product
- Increasing the transparency within the market
- Increasing awareness within the market
- Reducing the level of uncertainty for the implementor
- Establishing a minimum level of security per product / service / process /organisation type

The last few years, as shown also in the Legal and policy issues section of this document, a number of legislative and regulatory initiatives have been implemented (e.g., GDPR, NIS, eIDAS, EU CSA etc) that require Cybersecurity measures to be implemented. Although the requirement and aim are clearly stated and understood, their majority does not provide information or guidance regarding how to achieve them.

Moreover, existing popular ‘de facto’ information security standards like ISO 27001, has been designed to provide a risk-based framework for managing information security, without being able to provide specifics.

All the above lead to implementation uncertainty, zero transparency and an unknown status regarding security. Elements of standardization belonging to this type are:

- Baseline security standard (with minimum sets of controls) per industry
- Baseline security standard (with minimum sets of controls) for SMEs
- Baseline security standard (with minimum sets of controls) as part of the NIS directive implementation
- Security Maturity model standards that would allow for organisations to identify their security level, while also guiding them regarding possible actions for improvement.

Standards of this type would need to cover all the issues discussed within this document including: 5G, Quantum, IoT, AI, Remote control Systems, Virtual and Augmented reality, Remote working, Autonomous driving, Secure Coding, Security and Privacy by Design, Security and Privacy by Default, Blockchain, Distance learning, and Cloud Computing.

Also, standards of this type could also cover issues mentioned above within a specific sector: E-health, Maritime, Transportation, Railway, Telecommunications, Financial, Insurance, Healthcare, and Services.

Informative

Information and measurement standards contain codified knowledge and product descriptions. They constitute an important instrument for technology transfer, as they codify the work and experience of generations of experts in their specific fields, and support the dissemination of best practices. As such, they have a positive effect on the market by diffusing knowledge. [95] These standards would provide information regarding the various research domains and the technologies and use cases of cybersecurity. Within these standards, all interested parties would be able to retrieve knowledge regarding these areas, from the theoretical background, to the implementation techniques. Elements of standardization belonging to this type are:

- Standards describing Risk Management frameworks
- Standards describing the establishment of relevant Management Systems
- Standards containing information on security controls principles and implementations without predetermining specific software or hardware solutions (e.g. Virtualization or VPN)

Standards containing security assessment methods. Standards of this type would need to cover all the issues discussed within this document including: 5G, Quantum, IoT, AI, Remote control Systems, Virtual and Augmented reality, Remote working, Autonomous driving, Secure Coding, Security and Privacy by Design, Security and Privacy by Default, Blockchain, Distance learning, and Cloud Computing. Also, standards of this type could also cover issues mentioned above within a specific sector: E-health, Maritime, Transportation, Railway, Telecommunications, Financial, Insurance, Healthcare, and Services.

Variety reducing standards

Within the Cybersecurity domain, variety reducing standards would allow for the existence of components with specific security characteristics. These components could be physical, virtual or even human. Elements of standardization belonging to this type are:

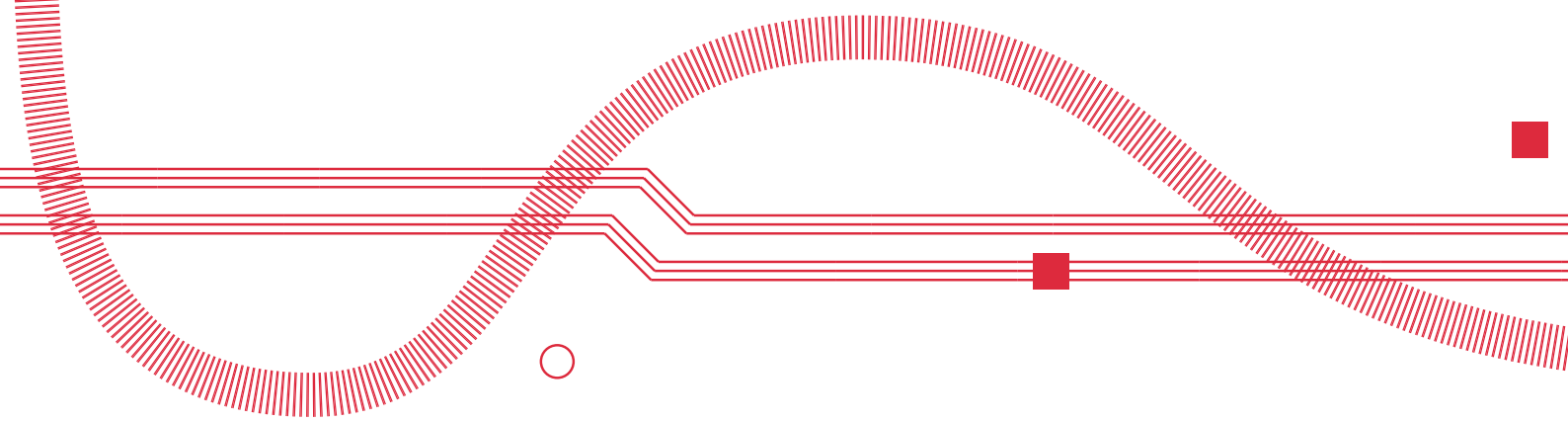
- Standards containing minimum competency definitions per Cybersecurity professional Role. This implementation would allow for equivalent systems of education, training and professional certification to be developed from different parties, in different parts of the European Union.
- Standards containing minimum characteristics for IoT devices allowing for a minimum level of security and communication.

9.1.2 Short-Term Aims

SA# Activity

- SA1. Development and evolution of a common (accepted) terminology and language
- SA2. Funding of Cybersecurity standardization activities.
- SA3. Inclusiveness in Cybersecurity standardization activities.
- SA4. Open Standard Contributions to representatives from all types and sizes of organizations including Micro, small and medium enterprises.
- SA5. Create a consolidated plan for European Cybersecurity Standardization and delegate responsibilities and authorities for standards development to a variety of organizations.
- SA6. Further strengthen the interlock between standardization and open source in the area of Cloud and establish and support bilateral actions for close collaboration of open source and standardization.
- SA7. Identify leading open source activities which complement standardization work and analyze to what extent they respond to EU requirements. Where useful establish dialogue, liaisons or partnerships with such open source projects.
- SA8. Include Cybersecurity standardization processes in research activities
- SA9. Support of standardization activities at different levels: H2020 R&D&I activities; support for internationalization of standardization, in particular for the DCAT-AP specifications developed in the ISA2 programme (see also action 2 under eGovernment chapter), and for specifications developed under the Future Internet public-private partnership, such as FIWARE NGSI-LD and FIWARE CKAN. Standardization can also be enhanced by using Core Vocabularies, as well as Core Public Service Application Profile implemented by the ISA2 program; new activities launched by the first implementations of the Digital Europe Programme and the legal framework progressively put in place following the Commission Communication on “A European strategy for data”.
- SA10. Implement a leaner and more open process of Cybersecurity Standardization
- SA11. Create a Secure communication standard for IoT
- SA12. Cyber range scenarios standards
- SA13. Minimum Cybersecurity standards for IoT (SDOs to provide standards that can be used for compliance for IoT products, systems, applications and processes)
- SA14. Minimum Cybersecurity standards for Cloud Computing. Identify needs for ICT standards and open source

- technologies to further improve the interoperability, data protection and portability of cloud services and continue or start respective development activities. This should also consider available open source technologies and their role for interoperability, data protection and management of multiple clouds.
- SA15. Promote the use of the ICT standards needed to further improve the interoperability, data protection and portability of cloud services as well as multi-cloud management.
 - SA16. Develop a European standard for cyber security compliance of products that is aligned with the current compliance framework of organizations based on the ISO 27000 Information Security Management Standards series and the GDPR regulation. Preferably the standard could be used to harmonize the requirements set out in the NIS directive.
 - SA17. SDOs to assess further gaps and develop standards on the safety and cybersecurity of IoT consumer products under the European Cybersecurity Act or sectorial legislation.
 - SA18. International acceptance and recognition of the globally applicable security standard for consumer IoT (TS 103 645). (This has further developed into EN 303 645 and published in June 2020.)
 - SA19. Minimum Cybersecurity standards for distance working
 - SA20. Cybersecurity Skills framework
 - SA21. Standards regarding auditing / assessment methodologies for cybersecurity products
 - SA22. Standards regarding end to end testing of systems and services
 - SA23. Security verification and security assessment/testing standards for new protocol/network specifications
 - SA24. Minimum Cybersecurity standards for 5G. (the European Commission has identified 5G networks as a strategic asset therefore requiring high cybersecurity standards and preserving lawful investigation capabilities. Commission Recommendation of 26 March 2019 on Cybersecurity of 5G networks and 10 8983/19 6 May 2019, Law enforcement and judicial aspects related to 5G, EU counter Terrorism coordinator. Especially for the later, Lawful interception and lawful disclosure related standards should be created that ensure proper provisions for enabling legal interception mechanisms in the context of 5G networks by encouraging and coordinating law enforcement involvement in 5G standardization related committees (e.g. ETSI TC LI, 3GPP SA3-LI) and promoting a European approach based on its legal system.)
 - SA25. SDOs to develop standards for critical infrastructure protection and thus in support of and responding to the requirements laid down in the NIS Directive.

- 
- SA26. SDOs to assess existing standards required to support the European Cyber-security Certification Framework to ensure that standards are available for providing the core of any certification activity. In particular, SDOs are encouraged to work on standards related to the specification and assessment of security properties in ICT products and services as well as those related to security in processes related to the design, development, delivery and maintenance of an ICT product or service
 - SA27. SDOs to investigate the availability of standards as regards to the security and incident notification requirements for digital service providers as defined in the NIS Directive and in support of possible other pieces of EU law.
 - SA28. SDOs to develop a “guided” version of ISO/IEC 270xx series (information security management systems including specific activity domains) specifically addressed to SMEs, possibly coordinating with ISO/IEC JTC1 SC27/WG1 to extend the existing guidance laid out in ISO/IEC 27003. This guidance should be 100% compatible with ISO/IEC 270xx and help SMEs to practically apply it, including in scarce resource and competence scenarios
 - SA29. SDOs to assess gaps and develop standards on cybersecurity of consumer products in support of possible certification schemes completed under the European Cybersecurity Act and in support of possible other pieces of EU law.
 - SA30. SDOs to develop secure coding standards for secure application development: EU-wide attention to standardization of privacy statements and terms & conditions as far as possible, given the existing state of mandatory acceptance of diverse, ambiguous and far-reaching online privacy conditions, taking into account the GDPR and the emergence of the IoT, where (embedded) devices process the device owner’s personal data and possible different device users’ personal data, creating additional challenges to transparency and informed consent.
 - SA31. International cooperation: European SDOs need to coordinate and establish a regular dialogue and cooperation with international level with relevant associations (IEEE, ACM etc.) and standardization bodies (ISO, NIST etc.) in the field of ICT professionalism and digital competence.

9.1.3 Mid-Term Aims

SA#	Activity
SA32.	Awareness and Education on Cybersecurity standardization.
SA33.	Support the adoption of Cybersecurity standards by making them affordable and by creating alignment between legislative/regulatory actions and the relevant standards.
SA34.	Implement Threat intelligence / threat information sharing related standards
SA35.	Minimum Cybersecurity standards for SMEs
SA36.	Further Cybersecurity standards for Critical infrastructure
SA37.	Minimum Cybersecurity standards for Remote control Systems
SA38.	SDOs to address data protection and privacy requirements (privacy by design) in ongoing standardization activities concerning location accuracy.
SA39.	Informational Standards for Security and Privacy by Design
SA40.	Data protection by design' (GDPR, Article 25) in eHealth products and services
SA41.	Informational Standards for Security and Privacy by Default
SA42.	Standards for Cybersecurity Education
SA43.	Minimum security standards for cybersecurity products (in relation to the CSA)
SA44.	Minimum baseline security and privacy requirements for the Aerospace Sector - with contextual risk- and impact-based measures added where appropriate - for easy and consistent implementation
SA45.	SDOs to consider cybersecurity and related aspects of artificial intelligence, to identify gaps and develop the necessary standards on safety, privacy and security of artificial intelligence, to protect against malicious artificial intelligence and to use artificial intelligence to protect against cyber-attacks
SA46.	SDOs to continue their efforts on "ethics" and trust of AI including transparency/explainable AI, privacy etc.
SA47.	Standardization potential around digital learning: SDO to investigate digital learning courses and resources, content repositories and exchange mechanisms with a focus on data privacy metadata, learning design and structure, technical and semantic interoperability supported by agreed protocols, exchange formats and vocabularies. Interoperability should include context-

aware, adaptable and mobile/ambient e-learning systems and also cross-domain aspects. This may include the learning trajectory or learning route including, e.g. the didactic approach, aimed learning & learner's profiles and the availability of additional tools that support digital learning. End users (learners and educators) should also be involved in the design, testing and development of digital learning solutions.

- SA48. The standardization community should continue analyzing possible standardization gaps and reflect on best way to fill them. Activities may focus on governance and interoperability, organizational frameworks and methodologies, processes and products evaluation schemes, Blockchain and distributed ledger guidelines, smart technologies, objects, distributed computing devices and data services. Regularly update the white paper on the EU perspective on blockchain/ DLT standardization.
- SA49. SDOs should work on interoperability standards for security and for linking communication protocols in order to provide end-to-end security for complex manufacturing systems including the span of virtual actors (from devices and sensors to enterprise systems). Standards should consider risk management approaches as well as European regulation and regulatory requirements.



9.1.4 Long-Term Aims

SA# Activity

- SA50. Minimum Cybersecurity standards for Quantum
- SA51. Standards for other areas: AI, Virtual and Augmented reality, Autonomous driving, Blockchain
- SA52. Standards for principle-based, risk- and impact based, human-centric continuous assurance for the security of critical infrastructures.
- SA53. SDOs to investigate security aspects of cooperative, connected and Automated Mobility (CCAM) and intelligent transportation systems.
- SA54. Development of harmonized standards in the area of additive manufacturing. Currently, there are no harmonized standards under the Machinery Directive for Additive Manufacturing (AM) equipment. The availability

of these standards could facilitate the manufacturer conformity assessment process. The European Commission should discuss together with SDOs and AM equipment manufacturers the possible need for harmonized standards in this area.

- SA55. Guidelines and collaborative work among key actors (associations, alliances, SDOs, etc.) for the definition of Water Big Data standardization frameworks, which contributes to implementing smart water best practices and an interoperability framework for smart water services. Special emphasis is made on key aspects of a big data platform such as integration, analytics, visualization, development, workload optimization, security and governance.



9.2 Certification

Certification is the third-party attestation related to products, processes, systems or persons. Whereas attestation, is issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated. Certification can apply to a product, process, system, person or body. Depending on the subject of certification, different international standards provide the related best practices (e.g., ISO 17021, ISO 17024 or ISO 17025).

The Cybersecurity Act (hereinafter CSA) entered into force in June 2019 with a view to bring together the current Cybersecurity certification activities and policies across the Member States. The CSA follows an array of legal instruments that compose the legal framework of the Digital Single Market while benefiting from the framework on standardisation, laid out by means of Regulation (EU) 1025/20123, and provisions on conformity assessment, laid out in Regulation (EC) 765/20084. The CSA is a multi-layered regulation that on the one hand addresses the updated ENISA mandate and, on the other, lays out the EU Cybersecurity certification framework. ENISA is tasked with a new competence, namely to prepare candidate Cybersecurity certification schemes. Thematic application areas likely to be affected by the Cybersecurity certification provisions of the CSA may include specific ICT products (e.g., semiconductors), services (e.g., cloud services) and processes (e.g., information security related methods).

The mission of ENISA in the area of the EU Cybersecurity certification framework is outlined as follows: ‘To proactively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes

in line with the Cybersecurity Act, and additional services and tasks. To the above-mentioned vision and scope of Cybersecurity of the CSA, the certification of Cybersecurity skills and organisations should be added.

The meaning of cybersecurity certification per element is:

- **For products**
 - » that products have been tested based on approved and appropriate methods
 - » that products fulfil specific cybersecurity requirements
 - » that products are achieving a specific level of assurance (e.g., basic, substantial and/or high)
 - » that the cybersecurity risk of using a specific product is of the equivalent value (e.g., basic, substantial and/or high)
- **For services**
 - » o that services have been designed and are operated according to specific Cybersecurity requirements
 - » o that services are achieving a specific level of assurance (e.g., basic, substantial and/or high)
 - » o that the Cybersecurity risk of using a specific service is of the equivalent value (e.g., basic, substantial and/or high)
 - » o that the services have been audited based on approved and appropriate methods
- **For processes**
 - » that processes have been designed and are operated according to specific Cybersecurity requirements
 - » that processes are achieving a specific level of assurance (e.g., basic, substantial and/or high)
 - » that the Cybersecurity risk of operating a specific process is of the equivalent value (e.g., basic, substantial and/or high)
 - » that the processes have been audited based on approved and appropriate methods
- **For skills**
 - » that specific Cybersecurity competence requirements have been identified per relevant Role
 - » that the skills have been assessed based on approved and appropriate methods
 - » that the competence of thus assessed individual is appropriate to the specific Role
- **For organisations**
 - » that the organisation has designed and implements a system for the management of its Cybersecurity posture based on specific Cybersecurity requirements that the organisation is achieving a specific level of assurance (e.g., basic, substantial and/or high) through this implementation that the Cybersecurity risk for this organisation

is of the equivalent value (e.g., basic, substantial and/or high) that the organisation has been audited based on approved and appropriate methods

When considering Cybersecurity certification, the following key benefits are identified:

- Certification enhances the ability of consumers and European Member States governments to acquire more cybersecure ICT products, services and processes.
- Certification provides a relative transparency regarding the level of assurance of the product, service or process being acquired.
- Certification allows organisations or governments to select the level of risk they will be exposed to by selecting the product / process / service of the respective level of assurance
- Certification allows for better comparison between different vendors
- Certification allows for circulation of products / services from a multitude of providers

The key challenges for Cybersecurity certification are market fragmentation and uncertainty with regard to the assurance provided by existing arrangements and schemes.

To minimize these risks, ENISA is envisioned to play the leading role in the certification ecosystem and coordinate the relevant activities.

As stated in the CSA, (Article 47) ‘The Commission shall publish a Union rolling work programme for European Cybersecurity certification (the Union rolling work programme) that shall identify strategic priorities for future European Cybersecurity certification schemes. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European Cybersecurity certification scheme [98]! The first version of the Union rolling work programme for European Cybersecurity certification was expected to be published on the 28th of June 2020 but has been delayed. [It is expected to be published within 2020]. At the same time the first two Cybersecurity certification initiatives has started under ENISA’s coordination. There are:

- The EUCC scheme (Common Criteria based European candidate Cybersecurity certification scheme) and it looks into the certification of ICT products Cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045. [99]
- V1.1.1 is the latest version of the scheme that has been updated based on the comments received through the public consultation and from the ECCG. ENISA also published the report

- presenting the outcome of the public consultation on the first draft of the cybersecurity certification candidate EUCC scheme.
- EUCS - Cloud Services Scheme. Acting on a prominent Commission initiative, dubbed CSP-CERT, representatives of both the private and the public sectors have already reached consensus and put forward a proposal for a certification scheme for the Cloud. The Commission request to ENISA concerning a Cybersecurity certification scheme for Cloud services has been grounded on the Regulation for the free flow of non- personal data. Other relevant aspects concerning the Cybersecurity of non- personal as well as personal data flows are likely to also come under the scope. [100]. At this point the public consultation for the scheme has been concluded and on Jan 11th, 2021 the EU Agency for Cybersecurity held a webinar presentation of the draft EUCS scheme.
 - Furthermore, the following ad-hoc Working Groups have been created or are in the process of being created, indicating efforts to be implemented in these areas within the next few years: Ad-Hoc Working Group on Awareness Raising; Ad Hoc Working Group on EU Cybersecurity Market; Ad-Hoc Working Group on Security Operation Centres (SOCs); Ad-Hoc Working Group on Enterprise Security; Ad-Hoc Working Group on Cyber Threat Landscapes; Ad-Hoc Working Group on Artificial Intelligence Cybersecurity

9.2.1 Challenges

Certification is a maturity action and as such several steps including development and standardization have to be completed before it is realized.

ENISA as key role

As mentioned above, ENISA is playing a key role in the design, implementation, approval and monitoring of the Cybersecurity schemes under the CSA. This by itself is a huge undertaking creating a bottleneck to the development process. At the same time, there is an increasing need from the market for guidance and support regarding Cybersecurity certification. As time goes by, more schemes will be created that will have a specific audience and recognition, leading to a market fragmentation and devaluation of certification. It is important especially for the circulation of products and services within the European Union that each country/vendor does not create a dedicated certification scheme, leading companies targeting multiple markets to have to comply many times to different or partially overlapping or even conflicting requirements. To address this challenge, the task of creating an acceptable set of requirements and relevant certification schemes should be spread to

the different stakeholders, allowing for fast and concurrent development in multiple areas

Cybersecurity Re: Privacy

Privacy has been a rising concern globally and in particular within the European Union after the activation of the GDPR. Putting it in simple terms, to make sure that personal information is protected also against threats to the confidentiality, integrity and availability of this information need to be implemented. Part of these measures are measures that would be implemented also from a Cybersecurity point of view. This apparent connection between these two terms, indicates that possible solutions of the one domain should take into consideration the other domain also. In Article 42 of the GDPR, relevant certification schemes are introduced which will be voluntary, transparent and approved by the relevant competent authorities (for National ones) and the European Data Protection Board (for European wide certification schemes). It would be useful, since such schemes have not been completed yet, to have an integration with the applicable Cybersecurity ones, so that more transparency and simplicity exists in the market.

The areas where Cybersecurity certification is needed are mentioned below (as a summary) and they are split based on the implementation timeline in the following section:

- Network devices,
- Storage devices,
- 5G,
- e-health devices,
- Services under the NIS,
- Secure Coding,
- Security by design,
- Security by default,
- IoT,
- AI,
- Wearable devices,
- Robots,
- Hosting services,
- Teleconference,
- Remote working,
- Distance learning,
- Computer games,
- Elections,
- Shared Lab infrastructure,
- Blockchain,
- Proximity applications and devices,
- Bitcoin,
- Autonomous transportation, and
- Quantum.

9.2.2 Short-Term Aims

CA#	Activity
CA1	Spread the creation of requirements and relevant certification schemes to the different stakeholders, allowing for fast and concurrent development in multiple areas, based on a concrete certification plan
CA2	Create an accepted methodology for testing cybersecurity products and a central certification framework
CA3	Create a European Accreditation framework for the testing and certification of cybersecurity products, processes and systems
CA4	Create a European Accreditation framework for the testing and certification of the privacy of products, processes and systems
CA5	Certification of Product Security Incident Response Team (PSIRT) program for vendors to help their customers in addressing the security of their products in a prompt and efficient way
CA6	Cybersecurity certification scheme for IoT (based on SOG-IS and CC)
CA7	Cybersecurity certification scheme for Network devices (based on SOG-IS and CC)
CA8	Cybersecurity certification scheme for Cloud services
CA9	5G
CA10	Services under NIS (2)
CA11	Cybersecurity Skills Certification Framework (including a model method for practical skills assessment)
CA12	Cybersecurity certification scheme - Industrial components (IACS)
CA13	Adoption and further development of the security standard EN 303 645 for "Cyber Security for Consumer Internet of Things". Implementation of a certification scheme under the Cybersecurity Act, and of the accompanying test specification and implementation guide as well as cyber security requirements for various types of devices.
CA14	Implementation of a certification scheme (cybersecurity on consumers products) under the European Cybersecurity Act and in support of possible other pieces of EU law.
CA15	Privacy by Design Certification scheme (would have to fulfil a set of requirements defined through appropriate EU standards)
CA16	Digitization of EU Industry Certification Scheme (Digitizing implies processing of data which includes personal data within the definition of the GDPR. That means, in addition to technical measures to ensure the security of the data, additional technical and social measures are needed to protect the privacy of personal data.)

CA17 Support and further develop the European Cyber-security Certification Framework to ensure that standards are available for providing the core of any certification activity.

9.2.3 Mid-Term Aims

CA#	Activity
-----	----------

CA18	Computer games
CA19	Teleconference
CA20	Distance learning
CA21	Wearable devices
CA22	Hosting services
CA23	Security by design
CA24	Security by default
CA25	e-health devices
CA26	Storage devices
CA27	Cybersecurity capabilities in aviation certification procedures as well as an upgrade to the certification procedures in this area as well.
CA28	Cybersecurity certification scheme for remote working

9.2.4 Long-Term Aims

CA29	Shared Lab infrastructure
CA30	Bitcoin
CA31	Autonomous transportation
CA32	Quantum
CA33	Blockchain
CA34	Elections
CA35	Robots
CA36	AI
CA37	Secure Coding
CA38	Services under the NIS

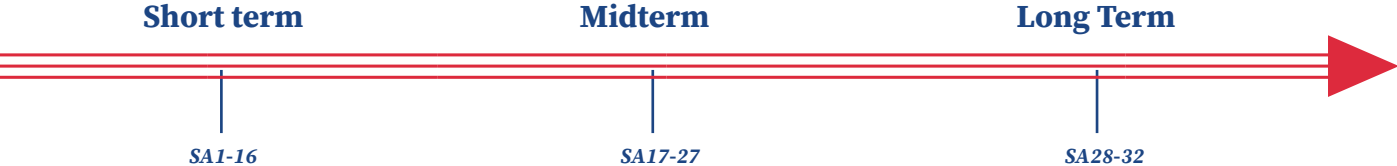
9.2.5 The Effect of COVID-19 on Standardization and Certification

As with all other aspects of life, standardization and certification has been influenced by the COVID-19 pandemic crisis. The rise of teleworking, distance learning and the genesis of proximity tracing systems has led to a shift in standardization towards these areas. Already, standards are being developed for the secure implementation of such systems and certification schemes should follow that would allow the consumer, organisations and governments to be able to gain a needed transparency to their cybersecurity posture.

9.3 Roadmap for Certification and Standardization

The visualized current roadmap for certification and standardization is shown in Figure 17.

(a) Standardization



(b) Certification

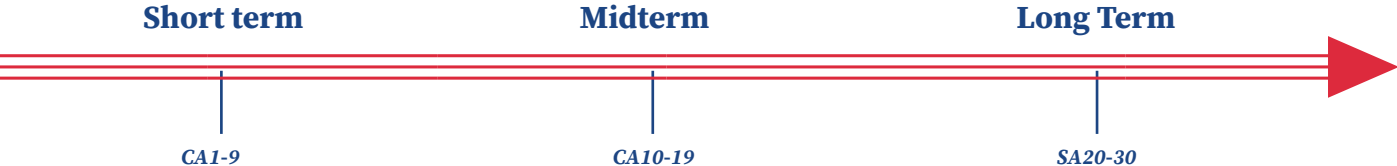
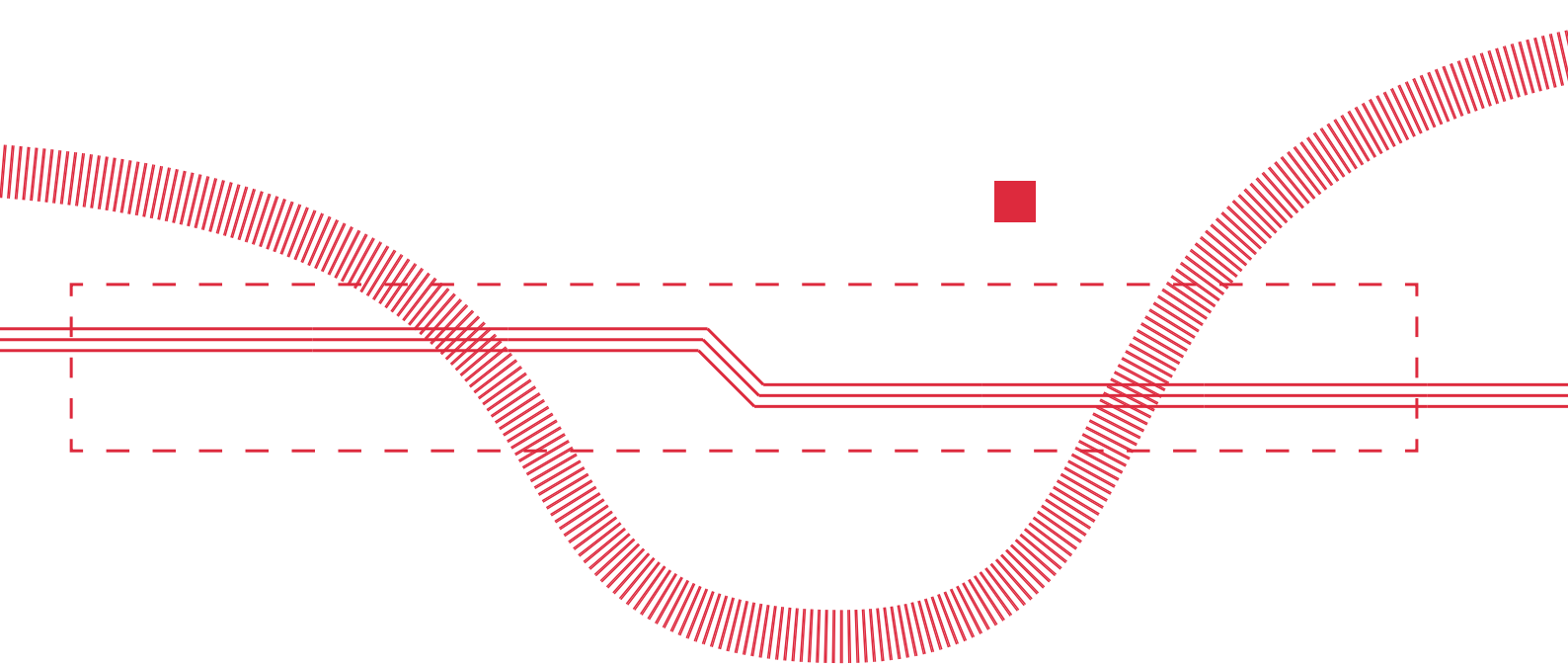


Figure 17: Overview from a Certification & Standardization perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines



9.4 Taking Stock: SOTA & the CONCORDIA Leadership

Over the 3 years of the project lifetime, we have developed under tasks T5.3 different activities related to standardization which could support the implementation of some of the Recommendations proposed above. Specifically, more information about the current and planned contribution of the CONCORDIA project is shortly provided below linked to the relevant recommendation: Activities already implemented or in progress

- **SA1: Development and evolution of a common (accepted) terminology and language:** The CONCORDIA partners have participated in the European Cybersecurity Atlas, a digital knowledge management platform to map and categorize cybersecurity competencies across Europe and stimulate collaboration between specialists. One of the main features of the European Cybersecurity Atlas is an EU cybersecurity taxonomy that aligns cybersecurity definitions and terminologies for a common understanding. Moreover, CONCORDIA participated in the review of taxonomies provided by other entities (e.g. JRC).
- **SA4: Open Standard Contributions to representatives from all types and sizes of organizations including Micro, small and medium enterprises:** Various CONCORDIA partners are participating in a number of standardization activities. Moreover, a specialized group has been formed within the CONCORDIA observer group for the subjects of Standardization and Certification. This group consists of external (to the project) organizations specializing in the fields of Standardization and Certification (Standardization Organizations, Certification Bodies, relevant unions or representatives). This group has been only recently formed with the aim of creating a direct bridge between these organizations and the CONCORDIA partners.

The vision is for the relationship to work in two directions (One direction is for the group members to provide inputs regarding their needs and the CONCORDIA partners to evaluate and possible help implement. The opposite direction has the CONCORDIA partners to present their progress, outcomes and achievements in order for the group members to evaluate them regarding their Standardization and Certification potential).

- **SA6: Include Cybersecurity standardization processes in research activities:** The CONCORDIA project has included considerations regarding Standardization by design. Half of Task 5.3. is dedicated to Standardization. The activities within this task have produced a list of standards that would prove interesting to the partners of the CONCORDIA project and a list of all the standardization activities the various partners are participating. Surveys and discussions are implemented on standardization potential within the project. The CONCORDIA project was selected and participated in a comprehensive on-line survey to collect and understand the experiences and views of beneficiaries on the role of standardization in valorising R&I results, launched by the European Commission (Directorate General for Research and Innovation). The survey was part of the implementation of the Communication on "A new ERA for Research and Innovation" the European Commission is developing Guiding Principles for knowledge valorisation. A set of codes of practice have been proposed in order to implement these Guiding Principles. One of these codes of practice will be a Code of Practice for researchers on standardization. This code will be co-created with relevant stakeholders to ensure its usefulness, relevance and create ownership. Further activities on standardization are planned also for the remainder of the project life, including the evaluation and lessons learned from the Standardization strategy adopted by the CONCORDIA project.
- **SA9: Cyber range scenarios standards:** The CONCORDIA project, has implemented a KYPO cyber range. Content is easy to be created, edited, and shared with the KYPO Cyber Range Platform thanks to standard tools like Ansible and Packer. Data are stored in open human-readable and serializable file formats like JSON and YAML. Import and export of training definitions can be done with just in few clicks. Furthermore, all data can be versioned and stored in a Git repository. The CONCORDIA project supports and participates through a number of partners in the European funded project REWIRE. The REWIRE project will built upon the existing outcomes of the CONCORDIA project and will further provide an ability for scenario packaging in order to enable standardized scenario building and exchange.

Planned Activities:

- **SA11: Minimum Cybersecurity standards for Cloud Computing:** The CONCORDIA project participated through a number of partners in the consultation of the draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services). It is within the plans of the CONCORDIA project to further participate in the evaluation of the new European Cybersecurity Certification Scheme for Cloud Services via internal processes, with the participation of the relevant Observer sub-group.
- **SA19: Implement Threat intelligence/threat information sharing related standards:** Several CONCORDIA partners are actively contributing to and coordinating cybersecurity standardization efforts in relation to threat intelligence. In fact, pieces of this work are utilized in Work Package 3 of Concordia. These efforts are within OASIS and include OpenC2, CACAO, TAC and CTI. The CONCORDIA project is investigating further activities on this subject.
- **SA27: Minimum baseline security and privacy requirements for the Aerospace Sector – with contextual risk- and impact-based measures added where appropriate – for easy and consistent implementation:** CONCORDIA has a pilot that is within the Aerospace Sector. The relevant US report by the US Government Accountability Office on cybersecurity rulemaking (particularly testing) to the FAA has been reviewed by the relevant project partners and relevant developments are being monitored through their participation in relevant standardization activities. (It should be noted that this effort could be of relevance for Europe as well, as EASA and FAA accept each other's rulemaking and generally apply very similar standards.)
- **CONCORDIA contribution to the Certification roadmap:** Over the 3 years of the project lifetime, we have developed under tasks T5.3 different activities related to certification which could support the implementation of some of the Recommendations proposed above. Specifically, more information about the current and planned contribution of the CONCORDIA project is shortly provided below linked to the relevant recommendation:

Activities already implemented or in progress

- **CA1: Spread the creation of requirements and relevant certification schemes to the different stakeholders, allowing for fast and concurrent development in multiple areas, based on a concrete certification plan.** A specialized group has been formed within the CONCORDIA observer group for the subjects of Standardization and Certification. This group consists of

external (to the project) organizations specializing in the fields of Standardization and Certification (Standardization Organizations, Certification Bodies, relevant unions or representatives). This group has been only recently formed with the aim of creating a direct bridge between these organizations and the CONCORDIA partners. The vision is for the relationship to work in two directions (One direction the group members to provide inputs regarding their needs and the CONCORDIA partners to evaluate and possibly help implement, Opposite direction the CONCORDIA partners to present their progress, outcomes and achievements in order for the group members to evaluate them regarding their Standardization and Certification potential).

- **CA2: Create an accepted methodology for testing cybersecurity products and a central certification framework.** CONCORDIA has already created a draft Cybersecurity Skills Certification Framework as part of the efforts within WP3. The framework is being piloted through a course and the relevant certification scheme for skills (Cybersecurity Consultant course – C3 by CONCORDIA certification scheme). At the same time, in collaboration with the CyberSec4Europe pilot, an effort has started to implement a certification scheme for Cybersecurity MOOCs, increasing the scope of the framework to products. Through the participation in the European funded project REWIRE, the results of the CONCORDIA project will be further utilized in order to create four more related certification schemes.
- **CA31 - Cybersecurity Skills Certification Framework (including a model method for practical skills assessment).** CONCORDIA has already created a draft Cybersecurity Skills Certification Framework as part of the efforts within WP3. The framework is being piloted through a course and the relevant certification scheme for skills (Cybersecurity Consultant course – C³ by CONCORDIA certification scheme). The first iteration of the pilot for the C³ by CONCORDIA certification scheme has been implemented in June 2021 and a second one is being planned for the autumn of 2021, after the relevant improvements and corrections are implemented. Through the participation in the European funded project REWIRE, the results of the CONCORDIA project will be further utilized in order to create four more related certification schemes.

Planned activities

- **CA6 - Cybersecurity certification scheme for IoT (based on SOG-IS and CC) & CA7 –Cybersecurity certification scheme for Network devices (based on SOG-IS and CC).** The CONCORDIA project participated through a number of partners in the consultation of the draft version of the related candidate European Certification scheme. Recently, the European Union Agency

for Cybersecurity has formally transmitted to the European Commission the first candidate cybersecurity certification scheme on Common Criteria. It is within the plans of the CONCORDIA project to further participate in the evaluation of the new scheme via internal processes, with the participation of the relevant Observer sub- group.

- **CA8 - Cybersecurity certification scheme for Cloud services. The CONCORDIA project participated through a number of partners in the consultation of the draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services).** It is within the plans of the CONCORDIA project to further participate in the evaluation of the new European Cybersecurity Certification Scheme for Cloud Services via internal processes, with the participation of the relevant Observer sub-group.
- **CA29 - Services under the NIS (2).** CONCORDIA has published paper describing the basic concepts of a “Cybersecurity Maturity Assessment Framework” (CMAF) to standardize the evaluation of the cybersecurity posture and to facilitate cybersecurity assessment/audits of critical infrastructures and organizations, according to different maturity levels (D4.2/6.3). It is further planned for a maturity assessment framework to be further improved in light of the new NIS (2) proposal, in cooperation with the Greek NCA (partner of the CONCORDIA group) and the National Cybersecurity Competence Centres and Agencies Stakeholders Group (NSG).
- **CA19 - Cybersecurity capabilities in aviation certification procedures as well as an upgrade to the certification procedures in this area as well.** CONCORDIA has a pilot that is within the Aerospace Sector. The relevant US report by the US Government Accountability Office on cybersecurity rulemaking (particularly testing) to the FAA has been reviewed by the relevant project partners and relevant developments are being monitored through their participation in relevant standardization activities. (It should be noted that this effort could be of relevance for Europe as well, as EASA and FAA accept each other’s rulemaking and generally apply very similar standards.)

Please note, that this is a part of the CONCORDIA Roadmap. If you are interested in the whole document, you can download it **here**.

- [91] Z. Xie, J. Hall, I.P. McCarthy, M. Skitmore, and L. Shen. 'Standardization Efforts: The Relationship Between Knowledge Dimensions, Search Processes and Innovation Outcomes'. *Technovation*, 48-49:69–78, (February-March 2016).
- [92] Nai Fovino, R. Neisse, J.L. Hernandot-Ramos, N. Polemi, G.-L. Ruzzante, M. Figwer, and A. Lazari. A Proposal for a European Cybersecurity Taxonomy. Technical Report JRC118089, European Commission, Brussels, Belgium, (2019). Accessed Dec. 18, 2020.
- [93] M. Mlkva, V. Prajova, B. Yakimovich, A. Korshunov, and I. Tyurin. Standardization - One of the Tools of Continuous Improvement. In *International Conference on Manufacturing Engineering and Materials*, volume 149, pages 329–332, Novy Smokovec, Slovakia (June 2016). *Procedia Engineering*.
- [94] N. Abdelkafi. Understanding ICT Standardization: Principles and Practice. Number 3748247427. ETSI, Sophia Antipolis, Frankreich. (May 2019).
- [95] K. Rantos, A. spyros, A. Papanikolaous, A. Kritsa, C. Illoudis, and V. Katos. 'Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem'. *Computers*, 9(1):1–17, (February 2020).
- [96] M. Elkhodr, S. Shahrestani, and H. Cheung. 'The Internet of Things: New Interoperability, Management and Security Challenges'. *ArXiv*, abs/1604.04824 (2016)
- [97] European Union Law. **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1**. (April 2019). Accessed Dec. 18, 2020.
- [98] European Union Agency for Cybersecurity (ENISA). **Cybersecurity Certification: EUCC Candidate Scheme**. (July 2020). Accessed Dec. 18, 2020.
- [99] European Union Agency for Cybersecurity (ENISA). **After cloud cybersecurity certification: launching the ENISA ad hoc Working Group on Cloud Services**. (March 6, 2020). Accessed Dec. 18, 2020.