cyberwatching.eu
The European watch
on cybersecurity & privacy

D4.4 EU Cybersecurity & Privacy Interim Roadmap

Author(s)	CPT
Status	Final
Version	v1.0
Date	14/05/2019

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Abstract:

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP – D4.4	
Deliverable lead	CPT
Related work package	WP4
Author(s)	Mark Miller, Victoria Menezes Miller
Contributor(s)	Trust-IT, ICTL, UOXF, AON, DSME
Due date	28/02/2019
Actual submission date	14/05/2019
Reviewed by	ICTL and UXOF
Start date of Project	01/05/2017
Duration	48 months

Revision history

Version	Date	Authors	Notes
v.01	26.03.2018	M. Miller	
v.02	12.12.2018	M. Miller/ V. Menezes Miller	
v.03	04.01.2019	M. Miller/ V. Menezes Miller	Revised structure following Review Meeting
v.04	15.01.2019	M. Miller/ V. Menezes Miller	
v.05	22.01.2019	N. Ferguson	Revised structure
v.06	06.02.2019	Mark Miller/ V. Menezes Miller	Compilation of contributionns from partners AEI (Sections 8.5, 9.2, 11.4.2); Digital SME (Chapters 5, 6.2, 6.3, 7.2, 9.2, 11.3.4), TRUST-IT (Chapter 2), UXOF (Chapter 3)
v.07	13.02.2019	A. Botsi / L. Senatore	Contribution ICT-Legal (Chapter 4, Section 9.1, 10.1.2, 11.2.2, 11.3.1, 11.4.1.)
v.08	01.03.2019	S. Garbin	Contribution AON (Section 5.2, Section 8.4)
v.09	03.2019	N. Ferguson, N. Zazzeri	Revision
v.10	03.2019	N. Ferguson, N. Zazzeri	Revision
v.11	03.2019	J. Favarro, N. Ferguson, N. Zazzeri	Revision
v.13	18.04.2019	N. Ferguson, N. Zazzeri	Re-structure
v.14	30.04.2019	M. Miller/ V. Menezes Miller	Revision, overall re-structure, Roadmap (Chapter 4)
v.15	02.05.2019	P. Balboni / A. Botsi / L. Senatore	Revision/Review
v.18	6 May 2019	M Drescher	Review
v.19	6 May 2019	M. Miller/ V. Menezes Miller	Revised to include reviewers' comments
v.Final	14 May 2019	N. Ferguson	Final version

Executive Summary

During the latest Cyberwatching.eu project review meeting, the reviewers requested that it would be important to have a deliverable which discusses the overall project and how all of the pieces and parts fit together and how the project functions as a whole. In order to address this request, the consortium agreed to change the content of this specific deliverable (D4.4) to focus on this requirement. As a result, the primary purpose of this document is thus an Executive Summary of the project with all of the interconnections and orientations and results explained in a clear format.

First, in order to explain how the whole Cyberwatching.eu project fits together, the following diagram shows the main elements and orientation toward project results with significant impact.

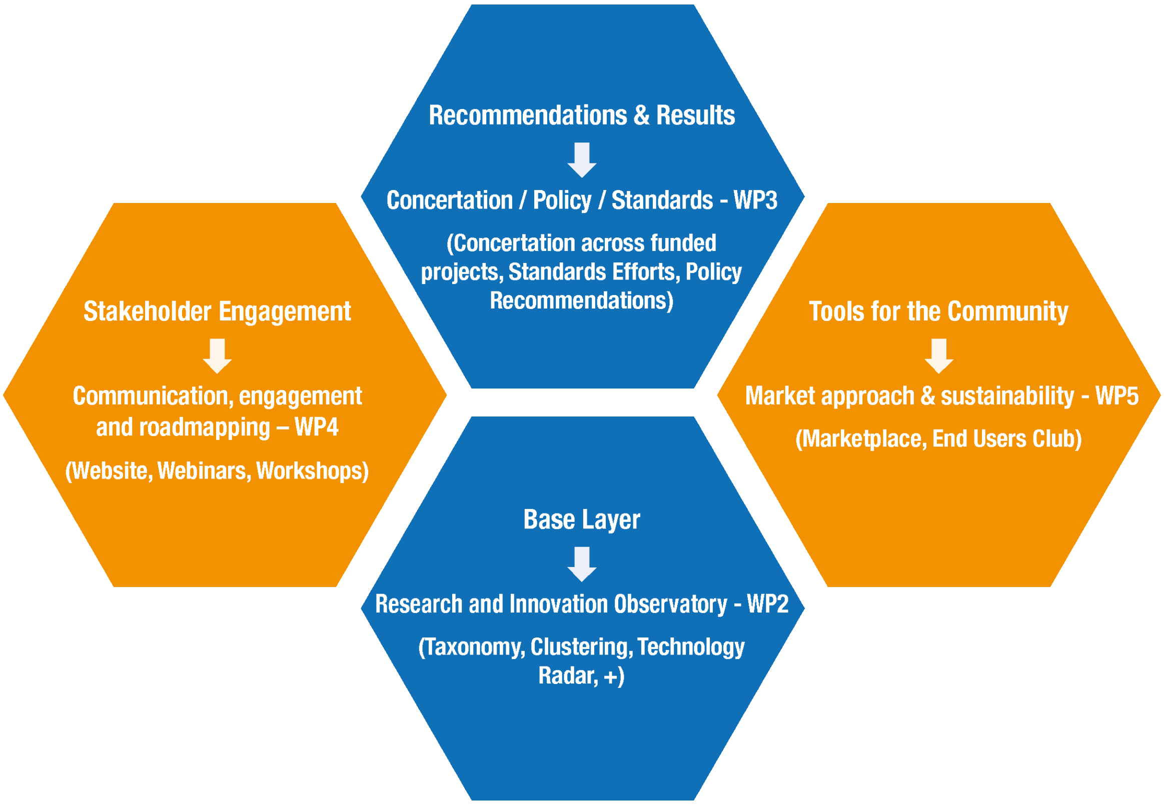

Recommendations & Results
Concertation / Policy / Standards - WP3
(Concertation across funded projects, Standards Efforts, Policy Recommendations)
Stakeholder Engagement
Communication, engagement and roadmapping – WP4
(Website, Webinars, Workshops)
Tools for the Community
Market approach & sustainability - WP5
(Marketplace, End Users Club)
Base Layer
Research and Innovation Observatory - WP2
(Taxonomy, Clustering, Technology Radar, +)

Figure 1: cyberwatching.eu project impact

A number of key components have been developed at the base layer with the idea being that the project results will be actionable recommendations and tools to enable the better functioning of the market for cybersecurity solutions in Europe. With benchmarking and best practices identification and sharing, Cyberwatching.eu is also enabling fast learning and competitive functionality as well.

However, in addition to the "project overview and summary" as requested by the reviewers, in order to prepare for the later final Roadmap deliverable (due in the final project work period) and to provide some early important touchpoints and elements, we have also included a section here within the title and theme of the original intent of the document. This Roadmap section herein by no means represents all of the work done in preparation for the original theme, but rather is included as a way to look forward toward the final Roadmap approach. As such, quite a significant number of already existing “Roadmaps” were researched and studied in this process and therefore certain themes start to be apparent. It is relevant to note that these themes are also consistent with the recommendations and orientation found within our D3.4 deliverable as well.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Section 1 - Introduction

Investment in cybersecurity is crucial as trust and awareness are the foundation for a functioning and trustworthy Digital Single Market. The EU has adopted wide-range of cybersecurity measures, including the first EU-wide cybersecurity legislation (NIS Directive).

€1 billion has been invested in cyber security and privacy under the EU's Horizon 2014-2020 research programme which also focusses on the smooth implementation of key regulations such as the GDPR and Cybersecurity act. The cyberwatching.eu project aims to provide an observatory and mapping of EU projects in this area and provide a channel for recommendations from partners of R&I projects to the EC on key policy topics. With so much funding for cybersecurity and privacy, it is also important to see a return on investment with R&I results impacting on target end-users. Cyberwatching.eu also targets end-users and in particular SMEs who make up a large percentage of the 60,000 strong EU cybersecurity and privacy market. The objective being to facilitate projects and potential validation or uptake of results.

With this in mind, this document will provide an overview of the project at this point in time (M24), how all of the pieces fit together and how the project is functioning as a whole. As such, the primary purpose of this document is an Executive Summary of the project with all of the interconnections and orientations and results explained in a clear format. The document also provides a first version and the key elements of one of the project's key outputs: a cybersecurity and privacy roadmap. The final version of the roadmap will be published in January 2021.

The work in this deliverable is, therefore, given in two main parts.

1) Chapter 2 addresses the reviewers request and to provide an overall view of cyberwatching.eu and how the pieces fit together;

2) Chapter 3 addresses Objective 8 of cyberwatching.eu, i.e., to "Deliver two versions of an "EU Cybersecurity & privacy Roadmap" to chart calls to actions and recommendations". This chapter given an indication of the key areas which we will focus on in the next two years. Some emerging areas presenting challenges related to CS&P have been presented and will be further elaborated in the second version of the Roadmap (M48). is the first version of the Roadmap (M22) which will be revised in the Second version of the Roadmap (M48).

2 Cyberwatching.eu – The Big Picture

With a plethora of cybersecurity and privacy (**CS&P**) research and innovation actions, there is a strong need for more coordination and synergy-enhancing supporting actions to help decision makers at different levels and in different organizations make sense of the cybersecurity service landscape, be aware of existing best practices, and understand which services would best help them secure their organizations. In the first 18 months of its 48-month lifetime, cyberwatching.eu laid some key building blocks for creating an active and engaged community.

Analysing the EU cybersecurity RIA landscape. Cyberwatching.eu acknowledges the need for a comprehensive and organic view of all of the Research & Innovation (**R&I**) activities carried out in the EU and Associated Countries to face the growing and rapidly evolving CS&P challenges. For this reason, we are delivering an "observatory watch" to avoid dispersion of efforts and investments, and build on synergies to further encourage excellence. Cyberwatching.eu will sustain the pace of innovation & growth in the global economy in the face of determined cyber-attacks that require dramatic change now and even yesterday. R&I projects are key to the ecosystem and our CS&P observatory includes overviews of over 300 EC & nationally-funded CS&P projects. Using a two-layered CS&P **Taxonomy** (Section 2.1.1), we have mapped 134 EC-funded projects to our **Technology Radar** (Section 2.1.2). The radar visualizes projects according to the taxonomy and project lifetime maturity. Policy makers and potential exploiters of all types can find an illustrative overview of the current technological climate and near-term future for the CS&P sectors. Complementary to this, six clusters of projects have been identified based on **Principal Components Analysis** (Section 2.1.1). The next step will be to ignite collaboration and exploit synergies among the projects.

Monitoring the regulatory, policy, and certification landscape. Cyberwatching.eu takes into account all aspects of the CS&P ecosystem including governance, risk management, standards and certification as outlined in our white paper (D3.3). The white paper provides a comprehensive snapshot of the current EU and international landscape, leveraging input from key players such as ECSO, ENISA and the R&I community. The landscape is broad, fragmented and fast-moving by nature. The **General Data Protection Regulation** (Section 2.2.1) came into force at the dawn of the cyberwatching.eu project and we are uniquely positioned to track its early take-up and identify key issues in its implementation. The **NIS Directive** (Section 2.2.2) is also in its early stages and cyberwatching.eu expertise is helping to navigate the issues confronted as the Member States implement its requirements.

Transferring results from the RIA projects to European SMEs. Focusing on Unit H1 projects, the first Concertation meeting and Service catalogue (49 projects) (April 2018) show how R&I is responding to the needs of the ecosystem. It recognises the lack of mutual recognition and harmonization of standards and highlights the cost issues for **Small to Medium Enterprises**. CS&P is essential for a successful Digital Single Market and also for European SMEs. R&I can have a key role and by publishing a methodology for assessing project **Market Readiness Levels** (Section 2.1.3) we will enable projects to quantify their current state in order to improve their readiness levels with the aim of creating a self-assessment tool.

Creating a sustainable European CS&P community of SMEs. A growing community of 1,200+ has been built within the cyberwatching.eu website the central hub hosting all assets. Active engagement has been established through events, webinars, questionnaires, social media and collaborations with projects and EU clusters. These have fed into our deliverables. The cyberwatching.eu SME validation and end-user club provides a bridge for projects to SMEs and the opportunity for uptake and collaboration. By inviting finished projects with results and SMEs to publish their results in our marketplace we are providing a new platform for potential exploitation of opportunities. Creating a set of sustainable project assets is a real goal. We have identified 21 exploitable project assets and a business plan based upon analysis of the current market and stakeholder needs.

2.1 Mapping, engaging & clustering the EU R&I community

With research projects situated upstream of any innovation entering their respective market, publicly funded projects function as an early indicator of activities and opportunities downstream, similar to earthquake seismographs or tsunami buoys deployed as indicators for civil disaster prevention programmes. However, with approximately 150 projects funded by the Commission alone over the years, and about as many projects funded on the national level, it requires considerable effort to stay abreast of developments and progress among all of those projects.

Cyberwatching.eu offers a way to keep oversight of the European R&I landscape for its readers and followers to absorb, greatly reducing the overall and repetitive effort spent in doing so. We offer a two-pronged approach:

- A **taxonomy**, coupled with powerful clustering techniques for determining synergies among EU R&I projects;
- A **Technology Radar**, providing a complementary, intuitive dashboard of the R&I landscape coupled with indicators of market readiness.

2.1.1 Taxonomy

In the cybersecurity and privacy arena, many different taxonomies are in use, aligned with many different goals and outcomes. As we deal with Research and Innovation projects, an appropriate taxonomy is necessary to allow structuring the R&I community in an agreed fashion. The University of Oxford, hosting one of the UK's academic centres of excellence in cybersecurity research, contributed the taxonomy that it had developed to internally describe the vast swathes of activity ongoing both at a purely institutional level and also in collaboration with others.

In brief, the taxonomy features two levels of detail allowing drilling down into closer inspection of projects as and when needed (see Table 1 below).

Level 1: Category	Level 2: Cluster
Foundational technical methods & risk management for trustworthy systems in cybersecurity & privacy	Operational Risk and Analytics
	Verification and Assurance
Applications and user-oriented services to support cybersecurity and privacy	Secure Systems and Technology
	Identity, Behaviour, Ethics and Privacy
	National and international security and governance

Level 1: Category	Level 2: Cluster
Policy, governance, ethics, trust, and usability, human aspects of cybersecurity & privacy	Human Aspects of Cybersecurity

Table 1: The Cyberwatching R&I taxonomy for cybersecurity & privacy (from D2.1)

This taxonomy and its associated semantics serve to connect and expose projects to each other, creating synergies as well as offering outputs of finished projects that may still be relevant for exploitation by still active projects. (Qualitatively speaking, output and efficiency of projects increase in an exponential fashion[1] rather than linearly with increased project collaboration.)

Clustering of projects is achieved through the following sequence of events:

1. Categorising projects per taxonomy level 1
Using the R&I taxonomy outlined above, projects are first *categorised* according to level 1 of the taxonomy. Sometimes a project fits more than one category, in which case a mechanism is employed for ranking the focus of the projects.

2. Clustering projects per taxonomy level 2
Next, projects are *clustered* on taxonomy level 2. Assignment of level 2 terms is only permitted within the constraints and scope of the previous level 1 categorisation. Once again, if more than one clustering term applies to a project, a ranking mechanism is used to characterize the focus of the project as precisely as possible.

3. Statistical analysis of level 2 clustering assessment
The results of step 2 above then undergo a standard *principal component analysis* (PCA), allowing the formation of clusters of projects that have sufficient overlap and commonalities that there should be the basis for collaboration to emerge (details available in project deliverable D2.1).

4. Reaching out to the projects to form clusters
Once actual project clusters are identified in step 3, outreach to the active projects commences to form the clusters on a practical and operational level. Parts of this outreach focus on common events, practical technical collaboration opportunities, technology exchange, and deep dive events hosted by cyberwatching.eu.

5. Operational conduct of clusters
Clusters are envisioned to be very lightweight, with little to no governance and no formal legal structure. Rather, the focus is on close and productive collaboration between the participating projects.

As time progresses, newly funded R&I projects will feed into the clustering process, resulting either in their incorporation into existing clusters or possibly the formation of entirely new clusters, depending on the research topics addressed by the projects.

[1] For obvious reasons, the exponent to that function is subsumed to be larger than 1.0.

At the time of writing, the first three steps have been completed, with step 4 (outreach to projects) having just started. Over the coming year we expect step 4 and 5 to complete for the first iteration of this process.

2.1.2 Technology Radar

The Cyberwatching Technology Radar was first published in deliverable D2.2 “Cyberwatching Technology Radar” in autumn 2018. It is based on the well-known Technology Radar developed by ThoughtWorks as an intuitive dashboard for technological development in the general IT landscape. While sharing the same value and message as the original, the Cyberwatching Technology Radar has been specifically customized to suit the purposes of cyberwatching.eu. For example, the numbers of “sectors” has been adjusted to accommodate the taxonomy, and the number of “ring” areas has been adjusted to reflect the typical lifecycle of IT software and services. Finally, rather than relying on expert judgement for placing items on the radar, as originally practiced (and profitably marketed) by ThoughtWorks, cyberwatching.eu has developed a systematic, repeatable methodology – which is, however, designed to evolve over time as experience is gathered in the project.

2.1.3 Assessing & incorporating project readiness into the Technology radar

Currently, the Technology Radar uses one source of information: it assigns EC funded projects according to *project age* – a reasonably accurate source of information, since EC funded projects are under continuous scrutiny. While this delivers a good first approximation of a Technology Radar, it was never meant as the *only* way of populating it with projects. Future versions of the Technology Radar will incorporate at least one more source of information to determine the exact location of a project within its rings: **project readiness**.

EU projects always set out with a number of goals to achieve, outputs to produce, and envisioned impact on the wider landscape generated by it. Our project readiness assessment captures this on scales reflecting progress on a technology maturity oriented scale (the well-known Technology Readiness Level technique) and a similar scale of maturity capturing the readiness of supporting operations and activities to bring the technology to market and into production: the **Market Readiness Levels**, invented and formulated by Frank Bennett in 2016[2].

The outcome of the readiness assessment is used in two ways: to influence the next iteration of the Technology Radar, and to populate the online marketplace of outputs and services offered by the assessed projects.

2.1.4 How it all fits together to create an engaged R&I community

Building upon the work carried out in the research area, Cyberwatching.eu has developed close collaborations with R&I projects in order to ignite synergies and active collaboration between them.

In particular, key assets of cyberwatching.eu such as the Observatory, the Service Offer Catalogue, as well as the structure of first edition of the Concertation Meeting have been designed and populated reflecting the Taxonomy but also taking into account the Taxonomy validation from the projects themselves.

[2] Published under CC BY-SA-NC

The Taxonomy has also fed into the creation of meaningful clusters of projects based on shared commonalities which aims at overcoming the typical “working in siloes” mentality of R&I and build the ground for more collaborative synergies.

In addition, the Taxonomy also served as a basis to refine the Market and Technology Readiness Level framework, which supports projects in maturing their innovative ideas advising on how to develop a business case starting with the end user problem being addressed, advice on packaging the ‘big idea’ and enabling the cross pollination of ideas for business models between projects as a source of valuable feedback. The assessment of the projects will be the basis of the population of the cyberwatching.eu Marketplace with actual CS&P products coming from R&I projects.

Furthermore, cyberwatching.eu is continuously keeping a direct engagement with projects both through one on one exchanges and through online activities, which are basically reflected on the cyberwatching.eu website and social media channels, serving as a direct support for communication and dissemination activities.

Finally, cyberwatching.eu is working on upgrading its website into a real collaborative hub for the projects, building upon not only the Taxonomy, but also specific needs and preferences. Besides each project being able to autonomously upload and publish relevant information about the initiative’s status, progress, events, resources such as demos, products and solutions, each project will be also able to have direct communication capabilities between different projects and stakeholder groups (i.e. Service/product providers and potential customers), while being automatically notified and updated on similar R&I events, initiatives and latest progress. The version of the website including the collaborative hub for projects will be published in June 2019.

2.2 The Evolving Legislation Landscape

The regulatory framework is increasing yearly, not only in quantity but also in complexity, creating sophisticated approaches to protect personal data, network security and information systems and to achieve a high level of cybersecurity, cyber resilience and to promote trust.

In 2018, two new European legislation were implemented within the European Union: the General Data Protection Regulation (GDPR), which is applicable since 25 May 2018; and the Directive on the Security of Network and Information Systems (NIS Directive), which entered into force in August 2016, requiring Member States to transpose the Directive into their national laws by 9 May 2018 and, further identify operators of essential services by November 2018. As a result of these new legislations, it has become a necessity for the market to have a clear understanding and awareness of the expected changes, mechanisms, or tools in order to implement these requirements, and best practices as a result of the priorities of these new laws.

Meanwhile, the near future may expect the revision of another important legislation. The European Commission has proposed a text for a new ePrivacy Regulation (which will update the previous ePrivacy Regulation of 2009), and the European Data Protection Supervisor (Mr. Giovanni Buttarelli) published an article[3] asking for the urgent revision of the confidentiality of electronic communications through the ePrivacy Regulation.

[3] Article by Giovanni Buttarelli “The urgent case for a new ePrivacy law” - https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

In 2017, the Cybersecurity Act was proposed as part of a set of measures to address cyber attacks and to build cyber resilience. The Cybersecurity Act aims to reinforce the role of ENISA as a center of expertise and advice for cybersecurity, as well as introduce an EU cybersecurity framework. On March 12, 2019, the EU Parliament approved the proposal for the Cybersecurity Act.

Certainly, such active evolvement of the law can help regulate the CS&P market more adequately than before, and it is clear that in the near future further transformations of the legal system will take place (such as case law or amendments to ensure consistency and less legal uncertainty). These developments will make the current and future work of cyberwatching.eu very important, as it can play a role in helping the legislation be communicated in a straightforward manner in the different fields that it applies to, thereby actively contributing to the CS&P Roadmap.

2.2.1 The General Data Protection Regulation

In 2018, which can be summarized as the year of implementation of the GDPR, we saw the emergence of a strict risk-based approach in the sphere of cybersecurity and information security. This is reflected both at the European but also at the national levels which will have to follow the European harmonized approach.

2.2.1.1 The GDPR and national landscapes

It is important to note that the GDPR leaves some leeway for the European Member States (hereinafter referred to as Member States) in specific areas, to establish further guarantees for their national legislation.[4] This inevitably creates a more complex harmonization process where the controllers and processors also have to check their accountability with reference to the EU and to the national legislation. As expected by legal professionals, the national implementations of the GDPR will further help in defining the specifications of all derogations that the GDPR allows for. At the same time, these local derogations demand a lot of caution from smaller enterprises that may be established, offering goods or services, or monitoring behaviour of data subjects in more than one European Member State; since they do not only need to comply with the GDPR but also with each applicable national law. As a consequence, companies could be in a position where resources are limited, and the legislation has quickly evolved so as to make data protection a serious duty for any company that stores or processes personal data, even occasionally.

On the other hand, national data protection authorities have been more active in providing organizations with guidance on how to cope with the requirements and obligations that have arisen from both the EU and national laws.[5] The data protection authorities and the European Data Protection Board help transform the legal complex documents into more comprehensive and practical tools.[6]

Cyberwatching.eu will help raise awareness of national legislations that can differentiate from the harmonized law by providing recommendations to SMEs which specifically mention where a derogation of a Member State is possible or not. However, even though the GDPR provided an updated legal framework to protect personal data, the challenge comes up when one considers what the practical implementation of this

[4] Such derogations can be found in the following Articles of the General Data Protection Regulation: Art. 6(2), Art.8, Art. 9, Art. 35 (10), Art. 86 (2) and (3), Art. 87, Art.88, Art. 89(2) and (3).
[5] For example, the Information Commissioner Office's Guide to the GDPR, or the *Commission Nationale de l'Informatique et des Libertés'* Guide for Processors.
[6] The *Commission Nationale de l'Informatique et des Libertés* has also produced a software to conduct a Privacy Impact Assessment that can be freely used by any organisations.

framework is. The GDPR allows for approved certification mechanisms as a way to demonstrate the compliance with the data protection rules[7]; however, until such certification mechanisms get approved according to the GDPR[8], the data protection matters still cannot be easily integrated with the cyber security solutions available in the market. This means that currently there seems to be a gap between the legislation and its application when it comes to techniques of ensuring and demonstrating compliance through certifications. Furthermore, there seems to be a gap in applying the GDPR in more complex processing operations that may be involved in, for example, Internet of Things and Artificial Intelligence. See Sections 3.3.1 and 3.3.3 for a discussion of the impact that these new technologies may have on the implementation of the GDPR.

2.2.1.2 The GDPR international landscape

To complicate matters further, the reach of the GDPR extends outside the borders of the European Union. It is fundamental to mention that the amount and complexity of international legislation on data protection can vary enormously – any country may have new, old or no laws relating to this field. In consideration of the possible disparity that may exist internationally, the GDPR has created a requirement where in order for transfers of personal data to take place outside the European Union, there must be appropriate safeguards for the protection of personal data. One of the possible ways to assess an adequate level of protection in a country outside the EU is to check whether there has been an adequacy decision published by the European Commission, which will allow controllers and processors to transfer legally.[9]

Furthermore, another crucial element that enlarges the impact of the GDPR on an international level is its extraterritorial scope. More precisely, the GDPR is applicable to all legal entities who:

- process personal data (e.g., name, surname, e-mail address, phone number, location, IP address) in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether or not the processing takes place in the European Union;
- offer goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union.
- monitor the behaviour of data subjects as far as their behaviour takes place within the European Union.

Hence, this means that the GDPR applies also to organizations that do not have an establishment in the European Union. This international scope has generated further challenges, such as, when it comes to jurisdictional matters regarding online services of technological companies violating the applicable law. An example of this uncertainty is the 50 million euros administrative fine issued by the French Data Protection Authority to Google, which used the reasoning that since at the moment of investigation Google Ireland Limited was not the controller of Google's processing activities, it allows for the Commission Nationale de l'Informatique et des Libertés

[7] According to Article 24(3) of the GDPR: "Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller".

[8] The mechanism of approval of certifications is described in Articles 42 and 43 of the GDPR.

[9] An updated list of the countries that have received an adequacy decision by the European Commission can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

(CNIL) to also issue a fine instead of having a scenario where the Irish Data Protection Authority is considered to be the "lead supervisory authority".[10]

2.2.1.3 How cyberwatching.eu helps to navigate the GDPR

Cyberwatching.eu makes an impact by acting as the facilitator between the SMEs, R&I and the complex legislation. The work of cyberwatching.eu can serve both as a source of expert knowledge, which can be used as guidance by projects which have only conducted minimum efforts in digesting the GDPR, but also as a check-list, which can serve as a swift assessment of compliance with the GDPR for the more advanced stakeholders who have already started their efforts in implementing a framework.

In mid-2019, Cyberwatching.eu will deliver a recommendation (D3.4) which combines the legislation, the best practices available, and guidelines or opinions of the European Data Protection Supervisor. A part of this document will also be converted into an online tool (The GDPR Temperature Tool) in order to facilitate distribution and usage to all stakeholder communities. In addition, cyberwatching.eu will promote many of the services emerging from R&I projects that are working in this field – all for the purpose of offering a robust package of recommendations that fit every stakeholders' needs. Clear explanations of the vital obligations included in the GDPR can only be given out by the experts that apply these best standards on a day-to-day basis, making the Cyberwatching.eu partners the most appropriate means of creating this impact. Several tools have been and continue to be developed. They are meant to complement one another, with the final goal resulting in self-assessment tools with handy self-explanatory legal practical recommendations.

The next step is the online promotion among the stakeholders by all means possible in order to get the tool in action. The 2019 Concertation Meeting, 4 June, Brussels, will also offer valuable opportunities for R&I exposure and participation in discussions on the challenges of the CS&P ecosystem. Specifically, we will touch upon the concerns raised by the Internet of Things and Artificial Intelligence –with particular attention to the GDPR (see Sections 3.3.1 and 3.3.3).

2.2.2 The NIS Directive and its challenges

A challenge that applies to all stakeholders is to understand the overlap between legislations and consistently apply it throughout the Union. While the GDPR focuses on the rights of the data subjects and the obligations of relevant actors in processing activities, the NIS Directive concerns the national critical infrastructure of Member States and focuses on the main economic sectors.

The first challenge of the NIS Directive is that this is the first complete effort of the European Union to harmonise the cyber-security of critical infrastructure by increasing the common level of security in all Member States – therefore it is expected that a large effort from all Member States will be required on the individual national level.[11]

As a result of the above, another challenge arises, since coordination between Member States is vital in order for Member States to be compliant with the NIS Directive. This will require not only cooperation nationally between the single point of

[10] "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC" 21 January 2019; https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc; last accessed on 15/02/2019.

[11] By way of example, an identification of operations of essential services (Art. 5(1) NIS Directive), a national strategy on security of network and information systems (Art. 7 NIS Directive), as well as a designation of a National competent authority (Art. 9 NIS Directive) is expected by all Member States.

contact of each Member State and the Computer security incident response teams (CSIRTs) but also among Member States' governments and enforcement agencies. The cooperation is expected on many levels: firstly, between the CSIRTs, which will create a CSIRTs network to effectively exchange information and support one another, but also between national competent authorities that need to assess the compliance of operations of essential services.

Lastly, the legal instrument utilised by the European Union legislators - a Directive, means that even though it is a legally binding act, it requires each Member State to implement the set of objectives and further specifications in its national legislation. Unavoidably, this represents a further level of difficulty in the harmonisation of a high common level of security of network and information systems across the European Union.

Due to the GDPR and the NIS Directive, and soon the Cybersecurity Act, the European Union is undergoing a major reform in terms of the protection of personal data of consumers, but inevitably, increasing the complexity of conducting business and providing online services to customers. These latest legislative initiatives have transformed the risk management (of network and information security) into tangible and actionable elements. The risk-based approach, which is the fact that an organization must first assess the risks present in the processing operations it conducts – and subsequently implement appropriate security measures, is a novel achievement.

2.2.3 EU Cybersecurity Act

After the entry into force of the NIS Directive, the European institutions continued their legislative efforts on the security of networks and information systems through the European Commission's priority to present to the European legislators a comprehensive package of measures to strengthen cyber security in the European Union. One of the most important measures consists of a proposal for a Regulation which aims to create a European framework for the certification of cyber security of ICT products and digital services, as well as to strengthen the role of the European Agency for Network and Information Security ("ENISA"): the so-called Cybersecurity Act.[12]

The Cybersecurity Act can be divided into two parts: in the first part, the role and mandate of ENISA are specified, whilst, in the second part, a European system of certification of the cybersecurity of devices connected to the Internet and other digital products and services is introduced[12]. Since this is a regulation, once adopted and entered into force, the Cybersecurity Act will be immediately applicable in all Member States, as was the case for the GDPR.

Specifically, a first key point of the Cybersecurity Act concerns the strengthening of the role and mandate of ENISA, because currently ENISA has a temporary and limited mandate that will expire in 2020. Until today, the role of ENISA has been mainly to assist in technical terms both Member States and the European institutions in the development of policies on the security of networks and information systems; therefore, strengthening their capacity to prevent, detect and react to cyber accidents. With the new mandate that will be introduced by the Cybersecurity Act, the operational

[12] "Briefing EU Legislation in Progress – ENISA and a new cybersecurity act" - http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

management of cyber incidents will be an exclusive competence of the Member States. The Cybersecurity Act intends to reinforce the role of ENISA by guaranteeing it a permanent mandate and allowing it to carry out not only technical consultancy activities, as it has been up to now, but also perform tasks that are partly operational. In this way ENISA will be able to provide concrete support to Member States, European institutions and businesses in key sectors, including the implementation of the NIS Directive. ENISA will also have a leading role in the management and support of the certification system introduced by the Cybersecurity Act.

More precisely, the Cybersecurity Act introduces an EU wide ICT security certification system for digital products and services. This specific objective will attempt to solve the problem of the numerous existing certification schemes in some Member States but not recognized in other Member States. The Cybersecurity Act will provide an overall framework with a set of rules that will govern the European ICT certification schemes for specific categories of products and services – to ensure that those future certification schemes will be validly recognized in all Member States of Europe.

Under this mandate, ENISA could perform functions to support the internal market and cover a cybersecurity 'market observatory' to analyze the trends of the cybersecurity market and then reflect that in the EU policy development in the ICT standardization. ENISA would also be involved in the EU Cybersecurity Blueprint, in order to coordinate responses to large-scale cross-border cybersecurity incidents and crises at the EU level.[13] This blueprint will be applicable only to cybersecurity incidents with extensive effects on two or more Member States and with political significance on the EU political level.

The Commission's second draft, after having consulted several Committees (such as the Internal Market and Consumer Protection, Budgets and Civil liberties committees, and the Industry committee) enhances the initial mandate that the first draft created – by making some cybersecurity framework schemes for ICT products, services and processes mandatory.[13] Additionally, the second draft requests that the certification schemes not only include ICT products and services but also processes, which covers a wider scope of application.

On March 12, 2019, the EU Parliament approved the proposal for the Cybersecurity Act. The next step is for the Council to approve the proposal before it can be published in the Official Journal of the European Union. The Cybersecurity Act would enter into force on the 20th day after its publication.

2.2.4 Cyberwatching.eu and evolving European Legislation

The cyberwatching.eu "GDPR Temperature Tool" (under development) will be a valuable tool for SMEs as it will raise awareness on what is needed to be GDPR compliant, also in consideration of the risk-based approach introduced in this legislation. The questionnaire has been drafted with both the practical and theoretical aspects of data protection in mind and will allow SMEs, who are inevitably likely to have less resources for compliance, to be granted with an approximate understanding of their potential exposure to GDPR sanctions.

[13] "Briefing EU Legislation in Progress – ENISA and a new cybersecurity act"; http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

2.2.5 Cybersecurity standards and certification

Within Working Group ESCO WG1[14], the Challenges Of The Industry (COTI) is an internal document which lists some 290 inputs or issues highlighted by individual members of the ECSO WG as challenges encountered in addressing cybersecurity standards and certification. Given that the COTI is not public, the specifics contained therein cannot be shared here. Nevertheless, cyberwatching.eu experts have detailed knowledge of the COTI, and as such the concerns of the industry, the research community, the public sector and the user community are inherently addressed in our work. At the same time, ENISA is taking a leading role in certification. This framework is currently being elaborated.

In our deliverable D3.3 "White Paper on Gap Analysis", gaps in the NIS standards were identified, pointing to a need for new standards. Cyberwatching.eu has recommended the elaboration of a common research agenda across the EU Member States (MS), whereby through the vehicle of the European Research Council (ERC) (available to all MS scientists) it would be sensible to open specific calls for projects in the area of cybersecurity with clear aims and requirements on developing in areas of relevance to standards in cybersecurity. This call should be preceded by a large publicity campaign. It would not be possible to get the Member States themselves to use internal funding in a coherent manner, so centralized funding (such as the ERC) focusing on academic research would be a more cost-effective mechanism. The push should also continue for EC-sponsored research to be fully open-access not only in the final publication but also in the protocols, software, and data used within the supported projects.

A real challenge in the realm of standards is the length of time taken to develop, adopt, and disseminate a standard. In addition, with the number of languages within the European Union, the time to translate into national languages adds to the amount of precious time before actual implementation can take place. Another challenge is the pace of emerging technologies and the standards which could be related or need to be developed (see Section **Error! Reference source not found.** and Section 3.2.3).

2.2.6 Cyberwatching.eu and emerging technologies

In Section 3.3, the challenges of some key emerging technologies such as the Internet of Things (IoT), Next Generation Virtualized Infrastructure and Artificial Intelligence (AI) are presented. Cyberwatching.eu's technological observatory, with its mapping, clustering, and Technology Radar mechanisms described in Section 2.1, provides a powerful tool for identifying gaps and synergies in the coverage of research in key areas of emerging technological challenges, such as those discussed earlier. As new problems are discovered with promising technologies (such as Blockchain, which also has serious GDPR-related data-retention issues), the cyberwatching.eu tools can quickly verify adequate research coverage and assist the EU in issuing new calls for research and innovation actions to fill the coverage gaps.

2.3 SMEs and market challenges

SMEs make up 99,8% of European enterprises, yet they are ill-prepared for cyber attacks. Although the average performance in terms of awareness and preparedness is low, SMEs in northern Europe perform marginally better than those in southern Europe.

[14] ECSO WG1 - https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management

European SMEs are increasingly dependent on their information systems and networks to provide services to customers and meet their business objectives. The use of new technologies introduces several information security and privacy risks. Addressing these risks plays a significant role in business success and development nowadays, as growing security threats may cause various direct and indirect issues, potentially even disrupting business continuity[15]. Potential impacts of cyber threats include: business interruption; sensitive data loss; loss of customers; brand damage and loss of reputation due to decreasing consumers' trust.

In addition, the cybersecurity threats facing SMEs not only come from cyber-attacks (the most visible impact) but also from poorly designed, configured and used infrastructure, systems and interfaces. SMEs often do not have related processes, tools and staff in place to implement cybersecurity in their organisation. The main challenges that SMEs are facing could be summarised as following:

1. **Lack of awareness**. 69% of European companies have either no or only basic understanding of their exposure to cyber risks[16].
2. **Lack of resources.** Most perceive cybersecurity as expensive and lack the necessary resources to adopt adequate security measures. In proportion to their size and income, the investments can be as much as double compared to investments of larger organizations[15].
3. **Not only lack of skills and expertise, but also lack of training.** More than 35% of all unfilled vacancies in ICT sector are those of cybersecurity specialists[17]. There is also a shortage of cyber experts in academia and civil society for educational and training activities. And retaining cybersecurity experts in Europe is another big challenge.
4. **Low uptake of cybersecurity insurance**. Premiums for SMEs are often high and often may not cover some of the prevalent risks, such as losing IP or market share. SMEs therefore may consider cybersecurity investments as inefficient – i.e. costing more than reducing risk[18].
5. **Under-reporting of cyber incidents.** Cyber-risks could be handled much easier if early warnings would reach companies on time. However, given the financial repercussions and reputational damage, companies can be reluctant to share information on the number of attacks and the extent of losses incurred, especially companies whose business models are based on trust and privacy[19].
6. **Lack of trust.** This is the main inhibitor of cross-sector and cross-border collaboration for SMEs. Intense competition and mistrust of rivals often prevents information exchange and cooperation among different stakeholders. Because of their particular vulnerability, SMEs tend to show a high mis-trust.
7. **Cybersecurity market fragmentation**. The supply of ICT security products and services on the European market is rather fragmented[20]. As a result, even those SMEs that might be willing to adopt cybersecure solutions might need to

[15] ENISA Publication « Information Security and Privacy for SMEs » (2015) - https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport -

[16] Marsh, "Continental European Cyber Risk Survey: 2016 Report," October 2016, 7 - https://www.marsh.com/cy/en/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html

[17] IDC – Worldwide Skills survey (2017).

[18] Study prepared for the European Economic and Social Committee – "Cyberseurity - Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks" - https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

[19] Tackling cybersecurity threat information sharing challenges - https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html

[20] European Commission (2015), Cybersecurity industry

undergo different certification processes to sell their products and services in several Member States.

2.3.1 Engagement through SME WGs and associations

In particular, an important way to engage key stakeholders on the consumer side – namely, SMEs, is the cyberwatching.eu collaboration with ECSO WG 4 *Support to SMEs, coordination with countries and regions (ECSO WG 4). ECSO WG 4* is particularly important for cyberwatching.eu consortium due to its outreach to the SME community (mostly, to the providers of cyber security solutions). Therefore, cyberwatching.eu participated in WG4 e-meetings, face-to-face events, and the platform has also been promoted through internal communication channels of the WG4. Further promotion of the Marketplace to ECSO members, and engagement of the members, is planned to be intensified through the life-span of the project (during the WG meetings, through members' mailing lists, by disseminating printed material in ECSO events, etc).

In addition, SME stakeholders have also been engaged through DIGITAL SME's membership which covers more than 2000 SMEs in Europe. The members are regularly informed about the project's outputs and are invited to join the Marketplace and SME end-user club (via e-mails, during the Board meetings and common events).

Furthermore, cyberwatching.eu is also involving other actors, such as clusters active in the ICT sector. Therefore, the consortium has analysed potentially interested European clusters and has grouped them into categories, and tried to personally contact them by phone or by e-mail, explaining the project and its benefits. Collaboration has been deepened via clusters' participation in cyberwatching.eu webinars and events (such as the Annual Event, concertation meetings, etc.).

2.3.2 Fostering European innovation and bridging the gap between R&I and market

Through its market-facing activities, cyberwatching.eu is actively engaging both on the research and the market side to develop a unique space in which these two worlds can both meet their needs to address the emerging challenges and opportunities of the European CS&P landscape.

Cyberwatching.eu is dedicating several assets to this mission, namely the Marketplace, the SME Club, both available through the website, and events such as SME workshops, webinars and its Annual workshop.

2.3.2.1 Marketplace

With needs of SMEs identified and the various R&I initiatives mapped on the cyberwatching.eu technology and market radar, the cyberwatching.eu online marketplace is designed to provide a platform for new and innovative services. These can be provided by R&I projects (or their partners) and/or SMEs innovating in this space.

The SMEs' perspective

The Marketplace can be used by an SME in two ways: 1) as a platform to display its own products, developed by the company's internal research and innovation activities, or 2) as a platform to find and purchase from other producers pre-commercial cybersecurity solutions that can later be integrated into their own products or services. SMEs are able to communicate directly through the Marketplace with other providers in order to ask questions or request a quotation. They can become part of a broader community and benefit also from awareness raising activities such as workshops, monthly webinars and free guidance through the cyberwatching.eu website.

The R&I perspective

The Marketplace can be used by R&I projects to upload their services and solutions, whether they are in prototype/demo phase or in a more ready to market phase, and to promote them in a pool of SMEs looking for accessible CS&P solutions. Furthermore, cyberwatching.eu is supporting R&I projects in assessing and improving their market readiness so that they are able to package their results in a way that is understandable and usable by consumers, and their assessment through the Market Readiness Level activity will be the basis of the population of the cyberwatching.eu Marketplace.

2.3.2.2 SME Club

The club has been developed with the main goal to engage SME as early validators and test selected R&I results or activities. SMEs registered in the club have a direct channel of communication with those R&I projects that have uploaded their services and solutions in a prototype/demo phase or that request some sort of SME validation such as surveys on SME needs and challenges, or feedback gathering.

2.3.2.3 Events

SMEs and R&I projects can also benefit from other activities such as workshops, monthly webinars and free guidance through the cyberwatching.eu website. Topics already addressed by cyberwatching.eu webinars[21] and events reflect many of the challenges that SMEs face while following a standardised inclusive format always including R&I projects, SMEs & CS&P Clusters representatives as speakers to ignite practical dialogue and concrete synergies.

2.3.2.4 Other resources

The new version of the cyberwatching.eu website and marketplace in June 2019, cyberwatching.eu will offer SMEs access to free CS&P guides & advice from consortium such as risk assessment guides for example to help organizations assess their own risk profile and new services such as legal guides and the GDPR temperature Tool.

[21] Free Webinars from cyberwatching.eu – Archives at https://www.cyberwatching.eu/webinar

3 CS&P Roadmap

Although the request from the reviewers at the previous review meeting was to transform this deliverable into an overview and summary of how the project fits together with further explanation of the “helicopter view”, we have also begun significant research with respect to the original intent of this deliverable in addressing a Cyber Security and Privacy Roadmap. Extensive work has been undertaken already in many key relevant areas and as such we have begun to research the existing and important elements that have been previously identified and studied. In essence, we aim to understand the focal points and to consolidate our approach so that we do not “reinvent the wheel”. This Section 3 of the deliverable is thus a first “snapshot” of some significant existing inputs into our thought process and therefore gives some “pointers” toward aspects that will form parts of our full Roadmap deliverable due at the end of the project. By no means is this to be considered a complete and comprehensive initial study, but we have attempted to cover the most important components in our first touch on this.

3.1 Researched strategies, frameworks and roadmaps

Much progress has been made in the cybersecurity and privacy legislative field with the implementation of the GDPR, the NIS Directive and with the dawn of the Cybersecurity Act. These major legislative changes are clearly influencing the cybersecurity landscape positively.

In preparing the CS&P roadmap, several previous roadmaps related to cybersecurity and/or strategies or frameworks to implement a cyber secure environment have been examined in order to identify the common threads, the challenges and timeframe. A few of these documents are mentioned hereafter with the key points highlighted, as follows:

3.1.1 European Cyber Security Organisation (ECSO) – Strategic Agenda

In its publication “ECSO Strategic Research and Innnovation Agenda (2017)[22]“, ECSO identified 7 key priority areas:

Taken from ECSO Strategic Research and Innovation Agenda (2017)[22]

“**Ecosystem for Education, training, market growth and SME support**

- Cyber range and simulation
- Education and training
- Certification and standardization
- Dedicated support to SMEs

Demonstrations for the society, economy, industry and vital services

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

[22] ECSO Strategic and Innovation Agenda (WG6, 2017) - http://ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

Collaborative intelligence to manage cyber threats and risks

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

Remove trust barriers for data-driven applications and services

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

Maintain a secure and trusted infrastructure in the long-term

- ICT infrastructure protection
- Quantum resistant crypto

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

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

From security components to security services

- Advanced Security Services"

3.1.2 National Institute of Standards and Technology (NIST) - Framework

On April 25, 2019, NIST (USA) published an updated version of its Framework[23].

The high-priority "Areas for Development, Alignment, and Collaboration" as taken from NIST frameworkError! Bookmark not defined. are:

"5.1. Confidence Mechanisms
5.2. Cyber-Attack Lifecycle
5.3. Cybersecurity Workforce
5.4. Cyber Supply Chain Risk Management
5.5. Governance and Enterprise Risk Management
5.6. Identity and Access Management
5.7. Internet of Things
5.8. Measuring Cybersecurity
5.9. Privacy Engineering
5.10. Referencing Techniques
5.11 Secure Software Development

[23] NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1
https://www.nist.gov/sites/default/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf

NIST has identified and targeted several focus areas for continued coordination and collaboration of cybersecurity guidelines and principles:

4.1. Federal Agency Cybersecurity Alignment;
4.2. International Aspects, Impacts, and Alignment; and
4.3. Small Business Awareness and Resources."

3.1.3 Project CAMINO – Roadmap (Research Agenda)

The Comprehensive Approach to cyber roadMap coordination and development (CAMINO)[24] was a 24 month project funded under EUFP7. In 2016, CAMINO prepared a "Comprehensive roadmap (research agenda) for fight against cybercrime and cyber terrorism"[25] in 2016 with short-term, medium-term and long-term actions until 2025 and which focused on the following areas:

Summary from CAMINO Roadmap[25]:

TECHNICAL DIMENSION

- Strengthening emerging tools - big data analysis and cloud security/forensics", with the following objectives:
  - Evolution from monitoring systems to problem aware systems
  - Processing the data under realistic workload conditions (real-time or near real-time)
  - Addressing cyber security of Big Data infrastructure
  - Investments in event correlation capabilities
- Security assurance - establishing metrics and framework for cyber security testing, with the following objectives:
  - Assurance at different stages of product development process
  - Definition and communication of quality of protection level to product consumers
  - Development of representative security metrics
  - Robust and flexible access control for dynamic and distributed environment
  - Trust management in a distributed environment
  - Establishing information and data sharing between different organisations
  - Building open testbeds for cyber security testing
- Improving preparedness - security engineering and testing capabilities, with the following objectives:
  - Promotion of responsible knowledge
  - Modelling and simulation tools development
  - Increasing the number demonstrations and cyber exercises
  - Standards and protocols definition

[24] CAMINO Project - http://www.fp7-camino.eu/
[25] CAMINO Roadmap - http://www.fp7-camino.eu/

- Countering cybercrime - botnets, Advanced Persistent Threats and cybercrimes affecting mobile devices and social networks, with the following objectives:
    - Development of new ways to counter new, robust botnets
    - Focus on detection and countering of malware, ransomware and botnets
    - Investing in large-scale testing capabilities
    - Development of new paradigms for fighting against malware targeting mobile and small/micro devices (IoT)

HUMAN DIMENSION

- Development of training tools and raising cyber security awareness, with the following objectives:
    - Ensuring critical assessments keep pace with technological advances
    - Appropriate degree of risk awareness
    - Implementation of user's education, training and awareness
    - Incident management
    - Development of awareness tools

- Promoting use of Privacy Enhancing Technologies, with the following objectives:
    - Data minimisation
    - Anonymisation/ pseudonymisation
    - Encryption management

- Appropriate use and re-use of data, with the following objectives:
    - Ensuring appropriate safeguards are in place to enable LEA access to big data analytics
    - Enabling users to have control over data pertaining to them, and its use
    - Management of user expectations of control/privacy of their data
    - Monetisation of personal data within the users control

ORGANISATIONAL DIMENSION

- Adapting organisations to the cross-border nature of the Internet and cybercrime
    - Homogenisation of legislation
    - Cooperation frameworks between law enforcement agencies
    - Cooperation between CERTs
    - Cross-country monitoring
    - Incentive-based cooperation for information sharing vs. mandatory ones
    - Cross-border agile countermeasures selection and reaction
    - Interoperable forensic tools and best practices

- Introducing cyber security as a society culture need
    - User awareness of their own responsibility for cyber security
    - Optimal exploitation of new technologies without introducing socially unacceptable risk
    - Support for users in conducting positive behaviour change in relation to the adoption of good security habits
    - User friendly and with added value cyber security
    - Certification

- Promoting EU institutional support to generic challenges and obstacles at the SME level
    - Establishing a channel of communication between SMEs and EU institutions
    - EU certification programme
    - Development of a communication platform

- Promoting EU cyber insurance market development
    - Cyber insurance as a tool for improving security
    - Cyber risk assessment procedures suitable for different types of insureds
    - EU cyber security certification
    - Support for organisations in exchanging the information on incidents
    - Encouraging re-insurance of cyber risks
    - Preparing LEA and courts for cyber insurance cases

REGULATORY DIMENSION

- Investigatory powers in intra-jurisdictional and trans-border cases
    - Reducing the gap between the average efficacy of investigations in “real-world” enquiries and cyber-enquiries by adequate investigatory powers
    - Finding an effective, fundamental rights-compliant framework for the future of data exchange between national and EU law enforcement authorities
    - Improving the efficacy of the investigatory powers beyond the EU borders (cybercrime and money laundering)

- Civil and criminal courts forensics, admissibility and evidential standards
    - Homogeneity and European consensus of the admissible forensic analysis process for digital evidence
    - Adaption and updating the current legislation to the cyber and digital scenario
    - Coordination of the future evolution of citizens’ rights protection with the adoption of new evidential standards
    - Digital forensics training and certification schemes

- Electronic identity and trust services for data protection across borders
    - Agreement on levels of authentication
    - Alignment of public/private eIDAS levels within EU
    - International management of interoperability

3.1.4 SecUnity Project – Roadmap on Cybersecurity Research

SecUnity is a project funded by the German Federal Ministry for Education and Research (BMBF) to intensify IT security research in Germany and Europe. On

February 5, 2019, SecUnity published its cybersecurity research Roadmap[26] which presents the key challenges and course of action.

Taken from SecUnity – Roadmap on Cybersecurity Research[26]:

A. Key Challenges
1. Securing Cryptographic Systems against Emerging Attacks
2. Trustworthy Platforms
3. Secure Lifecycle despite of Less Trustworthy Components
4. Quantifying Security
5. IT Security and Data Protection for Machine Learning
6. Big Data Privacy

B. Interdisciplinary Challenges
1. Measurable, Risk-adequate Security in Law .
2. Holistic Human-centred Security and Privacy Research
3. Digital Business Models for a Fair Economy and Society

C. Technologies and Applications 35
1. Safeguarding Key Services of the Internet
2. Security of Blockchain Technology
3. Accountability and Transparency for Information Quality
4. User-centric Privacy Tools
5. Remotely Un-hackable PC
6. IT Security for Autonomous Driving

3.1.5 ENISA Publication – "Looking into the Crystal Ball" - emerging technologies

In January 2018, ENISA in collaboration with experts from academia and industry published "Looking into the Crystal Ball – a report on emerging technologies and security challenges"[27].

From ENISA's publicationError! Bookmark not defined.:
This report provides insight into the current top technological challenges (non-exhaustive) and lists them[27] as:

- "The Internet of Things
- Autonomous systems
- Next generation virtualized infrastructures (including SDN and 5G)
- Upcoming societal challenges
- Virtual and augmented reality
- The Internet of Bio-Nano Things
- AI and robotics"

Taking into account the above, ENISA listsError! Bookmark not defined. the most important emerging-security related areas as:

- "Elaboration on certification
- Coordination of actions in cyber space
- Development of trustworthiness
- Coverage of complete lifecycle

[26] SecUnity project Roadmap https://it-security-map.eu/en/home/

[27] Taken from ENISA publication "Looking into the Crystal Ball – a report on emerging technologies and security challenges"

- The future of cryptography
- Future Identification Technologies
- Use of Artificial Intelligence (AI) and Machine learning in cyber security
- Increasing end-user involvement"

3.2 Key areas in the CS&P Roadmap

Some common threads which appear in our research are:

- Trust: Confidence in what you use (products, solutions, services)
- People: awareness, training, expertise in the field of cybersecurity
- Certification: standards (European and International), emerging technologies
- Cross-border business and requirements
- SMEs: lack of resources and support tools

At this phase of the cyberwatching.eu project, the following key areas emerge in the CS&P roadmap as areas where focus should be placed:

- Cyber security by design
- Training – Education – Raising awareness
- Standarization and privacy
- International Dialogue
- Building trust - Establishment of an EU certification scheme
- Emerging Technologies

3.2.1 CS&P by design

After a number of high-profile security breaches over the last decade, the cybersecurity community has understood that security cannot be easily "added on" after a product has been deployed in the market – and it is particularly difficult and expensive to repair products and systems after a security breach. This has led to the development of a "By-Design" movement, which strives to build security and privacy into products and systems from the very beginning.

3.2.1.1 Security by design

Security-by-design is an approach to constructing systems with secure characteristics "built in". This involves a number of principles that have been proven effective over the years.

An example of such a principle is "No Security Through Obscurity". This means that the security of a design should not depend on being a secret. The design should be open for all to see, so that its security can be verified openly and any flaws can be detected quickly by many eyes.

Other such principles include the "principle of least privilege", whereby each authorised user should have the minimum permissions to do what must be done.

Together with other principles such as "defence in depth", these constitute a body of knowledge about secure systems design that is now quite mature and ready to disseminate to system builders throughout Europe. That is part of the mission of cyberwatching.eu.

3.2.1.2 Privacy by Design

The older concept of privacy by design, which is widely spoken of in the field of information security, has been consolidated as an obligation in EU General Data Protection Regulation, more in particular in Art. 25 GDPR. Furthermore, the latest Opinion of European Data Protection Supervisor Working Party (now the European Data Protection Board), “the Preliminary Opinion on Privacy by design”, with the aim of providing guidance on the measures that need to be taken by companies in order to ensure that they follow an approach of “privacy by design”.[28] The GDPR’s definition of the privacy by design is the general obligation to implement appropriate technical and organizational measures to show that you have considered and integrated the principles of data protection into your processing activities.[29]

According to the Opinion, data protection by design consists of four dimensions, specifically:

1. each personal data processing supported, in whole or in part, by IT systems should be the outcome of a design project, in which the safeguards to be implemented should be analyzed and considered at the whole project’s lifecycle;
2. since the GDPR does not specify mandatory security measures, a risk-management approach should be adopted in order to select and implement the actual measures needed for effective protection. In this respect, each organization is responsible to choose from the available safeguards, those to be implemented, and balancing the cost of the measures (the “state of the art”) against the identified risks for the rights and freedoms of individuals. In any case, cost considerations can never lead to insufficient protection measures implemented for individuals;
3. the identified measures must be appropriate and effective. This requirement has to be tested against the purpose of these measures, which is to implement the data protection principles set forth by the GDPR (e.g., the transparency principle, data subject’s rights, and data minimization);
4. the identified safeguards must be integrated into the processing itself, as opposed to being “external” safeguards (such as privacy notices).

In other words, data protection by design requires that the protection of individuals’ fundamental rights and freedoms becomes one of the main aims of an organization, rather than an afterthought or a minor issue. Data protection should be incorporated in the governance and management structure, along with a comprehensive and coherent allocation of roles and responsibilities in this respect.

3.2.2 Training / Education / Awareness

Cybersecurity is increasingly necessary in our environment and the process of technology transfer in the field of cybersecurity must be accelerated to other strategic sectors, particularly at the industry and public administration levels.

[28] Opinion 5/2018 Preliminary Opinion on privacy by design, 31 May 2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

[29]“Data protection by design and by default”, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/; last accessed on 15/02/2019.

In order to improve the capacities of industries it is necessary to integrate cybersecurity in their production processes, bringing cybersecurity technologies and services closer to companies, especially SMEs, which do not have specialized training and which are at greater risk of being attacked.

Cybersecurity specialists are among the most sought-after professionals in the technology sector. However, at present, the training offer is limited and regulated training is general in the field of ICT.

The lack of cybersecurity subjects in the educational system (university or technical college) is left for later postgraduate training programs, as a specialty.

During educational processes, more importance is given to other issues such as web programming, system administration, app development, design, telecommunications, etc.

3.2.2.1 EU Cybersecurity Network and Competence Center

A positive move forward as part of the EU cybersecurity strategy, the European Commission proposed the creation as a next step of a new European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres.

The mission of the proposal to establish a European Cybersecurity Network and a Competence Centre is to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. The Competence Centre will facilitate and help coordinate the work of the Network and nurture the Cybersecurity Competence Community, driving the cybersecurity technological agenda and facilitating common access to the expertise of national centres.

For the Network of National Coordination Centres, each Member State will nominate one National Coordination Centre. They will function as a contact point at the national level for the Competence Community and the Competence Centre. There are more than 660 cybersecurity expertise centres from all Member States.

The positive aspects of the creation of this Center are:

1. Increase the competitiveness of the EU's cybersecurity industry and turn cybersecurity into a competitive advantage of other European industries.
2. The initiative will help to create an inter-connected, Europe-wide cybersecurity industrial and research ecosystem.
3. It should encourage better cooperation between relevant stakeholders to make the best use of existing cybersecurity resources and expertise spread across Europe.
4. It will allow relevant research and industrial communities as well as public authorities to gain access to key capacities such as testing and experimentation facilities, which are often beyond the reach of individual Member States due to insufficient financial and human resources.
5. The proposal will contribute to closing the skills gap and to avoiding a brain drain by ensuring access of the best talents to large-scale European cybersecurity research and innovation projects and therefore providing interesting professional challenges.

6. The Centre will be involved in coordinating the funding streams from the Digital Europe and Horizon Europe programmes and it would be advisable to extend the synergies to other EU financial instruments.

Some interesting recommendations from the European Economic and Social Committee (EESC) are:

1. The future Network and the Centre should build as far as possible on the Member States' expertise and cyber skills, and that competences should not all be concentrated in the new Centre.
2. It is also important to ensure that the activities of the future Network and the Centre do not overlap with existing cooperation mechanisms and bodies.
3. Extend the partnership to include the industry, on the basis of firm commitments on the scientific and investment fronts, and by including it in future in the Governing Board.
4. The national centres should be co-funded by the EU, at least when it comes to their administrative costs, thereby facilitating harmonisation in terms of administration and expertise, so as to reduce the gap between European countries.
5. The importance of human capital: in cooperation with universities, research centres and higher education institutes, the Competence Centre can promote initiatives aimed at educating and training people to a standard of excellence, including through dedicated third-level and secondary-school courses. In the same vein, it is essential to provide for specific support for start-ups and SMEs.

In summary, awareness and concrete actions towards increasing the cybersecurity workforce in Europe is taking place summed up as follows:

- Continuous support for awareness raising activities in cybersecurity and privacy in R&I projects through cyberwatching.eu, as well as through Digital Innovation Hubs, competence centers and other EU-funded initiatives;
- Use of the infrastructure of competence centers and innovation hubs to provide access to training and use of cybersecurity products/facilities for SME staff;
- Support and promotion of existing cybersecurity communities in Europe (cyberwatching.eu, ECSO, etc.) with the aim to help them expand and grow.
- Cybersecurity month activities every October.

3.2.3 Standardization and privacy

The Commission has issued two standardisation requests to the EU standardization bodies in relation to privacy:

- mandate M/289[30] in support of the European Directive on the protection of individuals with regard to the processing of personal data, published in 1999 and
- mandate on M/530[31] in support of the implementation of privacy and personal data protection management in the design and development and in the production and service provision processes of security technologies.

[30] EU Commission M/289 - http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=167"

[31] EU Commission M/530 mandate - http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548

The three recognized EU standardization bodies are: CEN, CENELEC and ETSI.

As explained in Section 2.2, the legislative framework is a foundation for building upon CS&P, more particularly, the EU cybersecurity certification framework under the Cybersecurity Act. In ENISA publication "Guidance and Gaps Analysis for European standardisation – Privacy standards in the information security context" (December 2018),[32] an indication of the standards which may play a role in the area of privacy in each of the relevant instruments[33] is provided as given in Table 2 below. Unless standards are specified in the legislation or technical legislation, application of those standards is on a voluntary basis:

EU LEGISLATIVE INSTRUMENTS/PROPOSALS	ARTICLE NR.	TOPIC
Network and Information Security Directive[34]	Recital 66 Article 14 Article 16 Article 19 Annex I	- Harmonised standards for high level of security of network and information systems at Union level. - Standards for security requirements and incident notification - Standardised practices for CSIRTs for incident and risk-handling procedures, incident, risk and information classification schemes.
General Data Protection Regulation (GDPR)[35]	Article 12 Article 21 Article 32 Article 33 Article 34 Article 35 Article 40 Article 43	- Standardised Icons - Technical specifications to exercise the right to object - Data security, data breach notification - Data Protection Impact Assessment (DPIA) - Codes of Conduct - Technical standards for data protection certification
Proposal for a Regulation on Privacy and Electronic Communications[36]	Article 8	- Standardised icons for informing users about the collection of information.
Proposal for a Cybersecurity Act[37]	Recital 34 Recital 47 Recital 49 Article 8 Article 46	- Standards for risk management and for measurable security of electronic products, systems, networks and services.

[32] ENISA Publication "Guidance and Gaps Analysis for European Standardisation" https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

[33] As indicated in ENISA publication 2Guidance and Gaps Analysis for European Standardisation", the instruments mentioned are provided by means of example and an indepth analysis is not provided

[34] Network and Information Security Directive - https://publications.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en

[35] General Data Protection Regulation - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

[36] Proposal for a Regulation on Privacy and Electronic Communications - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[37] Proposal for a Cybersecurity Act - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

EU LEGISLATIVE INSTRUMENTS/PROPOSALS	ARTICLE NR.	TOPIC
	Article 47	- Technical standards on cyber security requirements - interoperability standards - Standards for risk management and the security of ICT products and services - Standards for security requirements for operators of essential services and digital service providers

Table 2: EU Legislative Instruments and references to standards and technical specifications overview taken from ENISA Publication[32]

General privacy standards in the field of Information Technology is within the Scope of ISO/IEC JTC 1/SC 27 IT. In ENISA publication, "Guidance and Gaps Analysis for European standardisation – Privacy standards in the information security context"[44], information about specific standards relevant to privacy at the international level, i.e. ISO/IEC, is provided and summarized in ANNEX B – PRIVACY STANDARDS ECOSYSTEM. Many of the ISO/IEC standards have recently been revised, are in draft form or are soon to be published as given in the afore-mentioned ENISA publication[33].

The EU landscape of standards related to privacy is clearly evolving rapidly and already has an impact on the CS&P roadmap making Europe a leader in cybersecurity and privacy. How assessment and compliance of CS&P fit within the expected EU cybersecurity framework will unfold within the near future.

3.2.4 International Dialogue

On the global landscape, Europe has taken a lead in the field of data privacy in particular with the implementation of the GDPR in 2018. However, data protection and privacy using solutions, goods and services across borders is challenging and many issues arise within a dispersed global supply chain. As indicated in cyberwatching.eu deliverable D3.3, an international dialogue should open in order for Europe to benefit from best practices, lessons learned and evolving frameworks:

Recommendation from cyberwatching.eu deliverable D3.3:

"A FOURTH RECOMMENDATION - **International Cooperation** was identified as an area to be looked upon for opportunities to benchmark best practices and standards that may already exist as a way to not "reinvent the wheel", however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. From the results of ongoing projects in US and JP, several common areas of interest for collaboration emerged."

The EU Horizon 2020 AEGIS project (Accelerating EU-US Dialogue in Cyberwatching and Privacy) issued a report in June 2018 entitled "Report on Cybersecurity and privacy R&I Priorities for EU-US cooperation. AEGIS Project"[38]). Conclusions in this report were derived from a survey carried out by AEGIS among ICT and cybersecurity researchers from academia and the industry, decision makers, government institutions

[38] AEGIS report "Report on Cybersecurity and privacy R&I Priorities for EU-US cooperation" - http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Report-on-Cybersecurity-and-Privacy-RI-Priorities-for-EU-US-cooperation.pdf

and associations in EU and the US. AEGIS further identified the following themes[38] as areas of common interest for EU-US collaboration in the CS&P R&I:

> Excerpt from "Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation. AEGIS project."[38]
>
> - The "Top 4 cybersecurity research priorities for EU-US collaboration are Data Security and Privacy, Trust and Privacy, Fight Against Cybercrime and Cybersecurity Education. Among these research domains of common interest for transatlantic collaboration, it is not surprising that **Data security and privacy is seen by more than 80% of the survey respondents as the top research priority in both the US and the EU,** given the policy changes in data security and privacy over the past few years. In fact, the EU implemented what are considered to be the world´s toughest data protection and privacy regulations, the Directive on the Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR), in May 2018.
> - "The Internet of Things is seen as the top priority"
> - "Health and Financial Services are overwhelmingly considered the most important sectors to be protected"
> - "The cybersecurity and privacy community views the different policies and legislation in the EU and the US as a barrier for collaboration. It´s important to note that although the EU and the US share cybersecurity objectives in policy areas such as public-private information sharing and the creation of international or harmonized cybersecurity standards and policies, collaboration between both regions has not always been easy[39]. One example of this is the recent implementation in the EU of the NIS Directive and the GDPR, laws that do not have a US equivalent and which caused some US websites to block access to European visitors because they could not comply with the requisites in time[40]. It´s therefore a logical conclusion that an uneven policy and legislation landscape between both regions can lead to R&I difficulties."
> - "The lack of coordination between funding programs in the US and Europe is also considered an important barrier for R&I collaboration"

In the Trump Administration, the National Cyber Strategy (September 2018)[41] mentions in its IV Pillar, the following:

> Taken from USA National Cyber Strategy (September 2018)[42]
> "**IV. Pillar – Advance American Influence**
> Promote an Open, Interoperable, Reliable, and Secure Internet
>
> Protect and Promote Internet Freedom
> Work with Like-Minded Countries, Industry, Academia, and Civil Society
> Promote a Multi-Stakeholder Model of Internet Governance
> Promote Interoperable and Reliable Communications Infrastructure and Internet Connectivity

[39] AEGIS D.1.3 - White Paper on Cybersecurity Policies. Common Ground for EU-US Collaboration, (2018, May 31)

[40] Hern, A., & Belam, M. (2018, May 25). LA Times among US-based news sites blocking EU users due to GDPR. Retrieved from https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times

[41] USA National Cyber Strategy https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[42] USA National Cyber Strategy - https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

> Promote and Maintain Markets for United States Ingenuity Worldwide
>
> Build International Cyber Capacity
>
> Enhance Cyber Capacity Building Efforts”

Given the IV. Pillar objective above, an opportunity to collaborate with USA on common areas of interest could be beneficial for both so as to learn from best practices, lessons learned and evolving frameworks and not reinvent or duplicate the wheel.

Overall, there is a need to develop privacy and security-centric mechanisms and drive efforts with a broader view of assessing adoption of international standards and their alignment with the European legal framework and market needs.

> Recommendation from ENISA publication “Guidance and Gaps Analysis for European standardisation – Privacy standards in the information security context“ (December 2018),[43]
>
> **“EU policy makers and European Standards Organisations should promote the development of European input to privacy and cybersecurity standards. While leadership is needed, to drive standardization efforts in this area, the stakeholders’ need to be provided with guidance might be met with private initiatives from beyond the EU. In addition, the aforementioned stakeholders should also establish a mechanism to assess the viability of adopting international standards with European (legal) requirements and filter international efforts to match EU levels.**
>
> ESOs should develop dependable privacy and security-centric mechanisms and associated pools of experts to support them, for the purpose of assessing the adoption of international standards and their alignment with European legal requirements and market needs. The existence of stable mechanisms and experts pools would guarantee consistency in the long-term and ensure avoidance of overlap of standards. Furthermore, such practice would identify potential overlap even among European standards developed by CEN and CENELEC on the one hand, and ETSI on the other.
>
> In the absence of EU initiatives and leadership in this area there is a growing risk of de facto standardisation of practices via market consolidation as innovative EU-based service providers may gradually be consolidated in non-EU-led groups of companies.”

3.2.5 Building trust - Establishment of an EU certification scheme

Trust is built upon secure products, solutions and services. For assurance of the security of products, solutions and services, a certification framework is necessary which aligns itself with the standards and legislative requirements. In this complex area of European standards and international standards in a cyberspace without borders, the situation is even more complex, in particular, validating or assessing privacy conformance is not always straightforward. With the forthcoming

[43] ENISA Publication “Guidance and Gaps Analysis for European Standardisation” https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

Cybersecurity Act[44] and the role of ENISA, an EU certification framework will be proposed and much coordinated guidance will be necessary.

In the context of certification of cloud services, the Digital Single Market cloud stakeholder community group was created. Following a first meeting in 2017, two cloud stakeholder Working Groups were formed to carry out work in the following areas:

- The Switching and Porting between Cloud Service Providers with two sub-working groups which will develop codes of conduct, work started in 2018: one for Infrastructure-as-a-Service (IaaS) cloud services and the other for Software-as-a-Service (SaaS) cloud services. Platform-as-a-Service (PaaS) may be considered at a later stage.
- the European Cloud Service Provider Certification Working Group (CSP CERT) with the objective to explore the possibility of developing a European Cloud Certification Scheme in the context of the Cybersecurity Act and to provide a recommendation to ENISA. CSP CERT expects to finalize this work (which commenced in 2017) and provide recommendations to ENISA by mid-June 2019 at its road show event in Amsterdam (yet to be announced). These recommendations will be considered by ENISA for further integration into their work on the larger cyber security certification schemes.

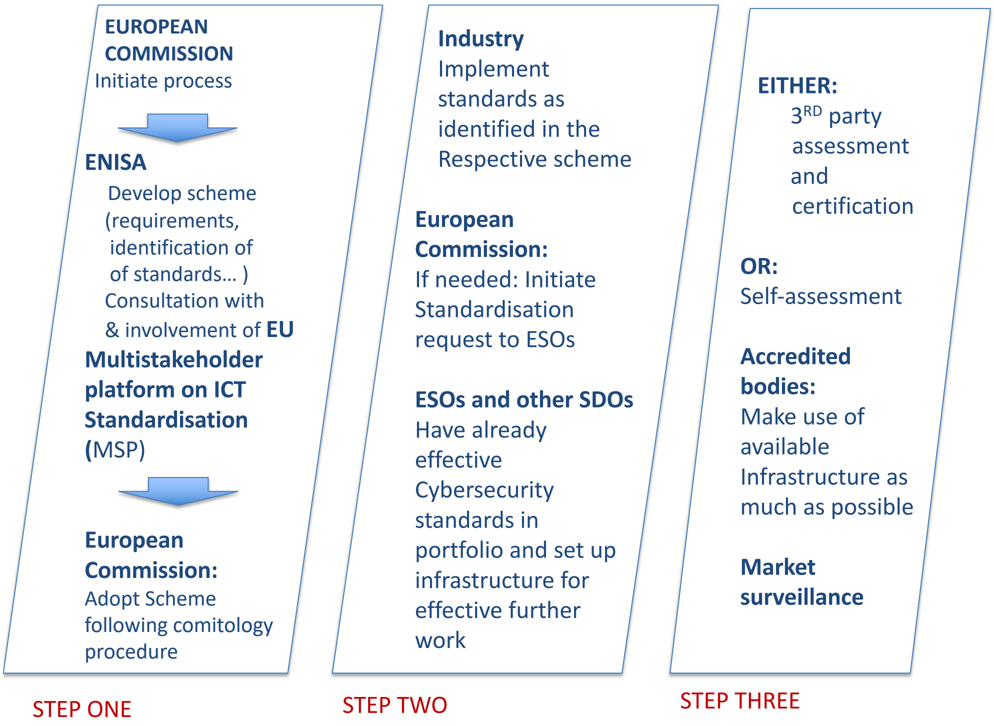
An overall envisaged process for a European certification framework is given in a three-step process in Figure 2 (source: OpenForum Europe 2018) and a further updated proposed process, subject to approval, is given in Figure 3 (source: Presentation of Gonzalez at ECSO Meeting on 27 February 2019)[45].

An overall envisaged process for a European certification framework is given in a three-step process in Figure 2 (source: OpenForum Europe 2018) and a further updated proposed process, subject to approval, is given in Figure 3 (source: Presentation of Gonzalez at ECSO Meeting on 27 February 2019)[46].

[44] "Briefing EU Legislation in Progress – ENISA and a new cybersecurity act"; http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf

[45] Presentation by Gonzalez at ECSO Meeting on February 27, 2019 - https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Gonzalez.pdf

[46] Presentation by Gonzalez at ECSO Meeting on February 27, 2019 - https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Gonzalez.pdf



EUROPEAN COMMISSION
Initiate process

ENISA
Develop scheme (requirements, identification of of standards…)
Consultation with & involvement of **EU Multistakeholder platform on ICT Standardisation** (MSP)

European Commission:
Adopt Scheme following comitology procedure

Industry
Implement standards as identified in the Respective scheme

European Commission:
If needed: Initiate Standardisation request to ESOs

ESOs and other SDOs
Have already effective Cybersecurity standards in portfolio and set up infrastructure for effective further work

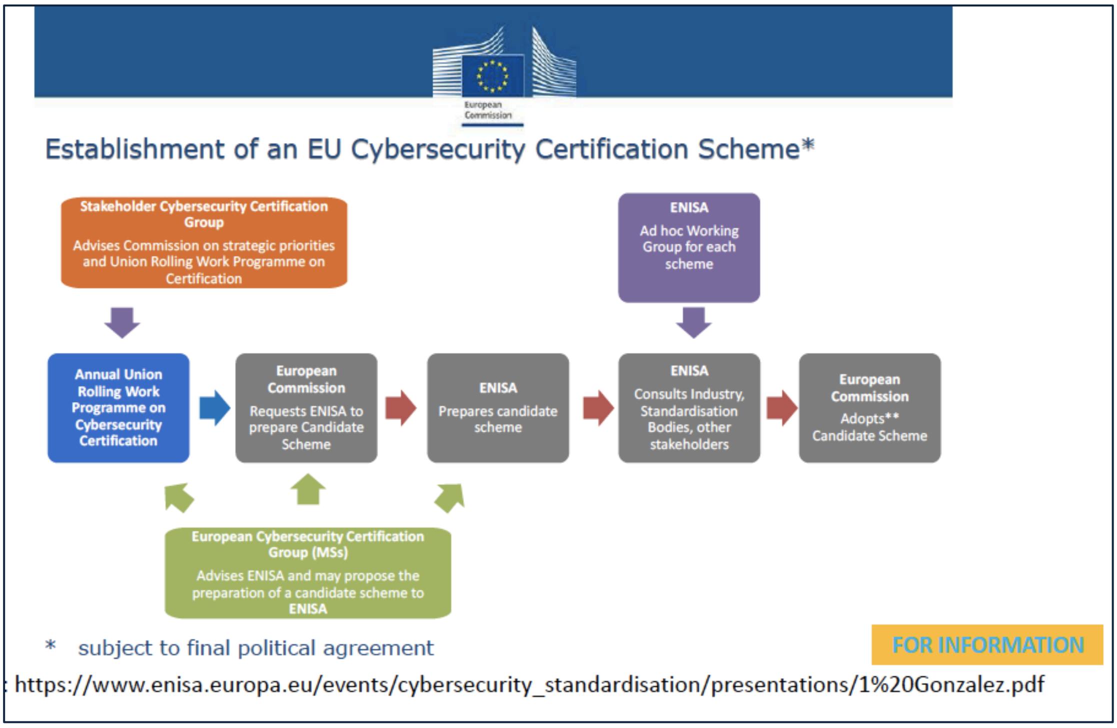
EITHER:
3RD party assessment and certification

OR:
Self-assessment

Accredited bodies:
Make use of available Infrastructure as much as possible

Market surveillance

Figure 2: From Certification Scheme to Certification (Source: OpenForum Europe 2018)



Establishment of an EU Cybersecurity Certification Scheme*

Stakeholder Cybersecurity Certification Group
Advises Commission on strategic priorities and Union Rolling Work Programme on Certification

ENISA
Ad hoc Working Group for each scheme

Annual Union Rolling Work Programme on Cybersecurity Certification

European Commission
Requests ENISA to prepare Candidate Scheme

ENISA
Prepares candidate scheme

ENISA
Consults Industry, Standardisation Bodies, other stakeholders

European Commission
Adopts** Candidate Scheme

European Cybersecurity Certification Group (MSs)
Advises ENISA and may propose the preparation of a candidate scheme to ENISA

* subject to final political agreement

FOR INFORMATION

: https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Gonzalez.pdf

Figure 3: Slide from presentation of Gonzalez at ECSO Meeting on 27 February 2019 [46]

3.3 Key challenges in Emerging Technologies

In the cybersecurity and privacy roadmap, one of the biggest challenges is the pace of emerging technologies and innovation. There are constantly new ways of performing functions in life which impact the end user in a multitude of ways, in particular, in the area of privacy and data protection.

Several of these emerging technologies, as indicated in ENISA's Publication "Looking into the Crystal Ball", have been singled out as particularly urgent to address, both in the realm of privacy and in security. We discuss some of them in more detail in the next sections.

3.3.1 Internet of Things

The Internet of Things promises to make our lives better in myriad ways, from smart refrigerators that know when the milk needs to be replaced to home assistants who can turn on the lights and stereo music player. But the challenges both to security and privacy are enormous, rightfully placing the IoT in one of the very top priorities for urgent action.

What if the milk in that smart refrigerator is kosher? This is private information about your religion, which could unknowingly be released if the refrigerator is compromised by a hacker – or knowingly compromised if the refrigerator sells that information to a grocery vendor for targeted advertisements to you. The same considerations apply to that smart home assistant, which can collect arbitrary amounts of data about your personal habits and preferences, selling them to appropriate advertisers. Your smart TV can spy on you[47] for a number of reasons, ranging from advertising to national security. Even worse, many IoT devices are *cyber-physical systems*, which control real, physical processes – like a self-driving car or a heart pacemaker. If compromised, they can therefore pose not just a danger to privacy, but also a clear and present danger to life and limb.

The enormous challenge posed by the IoT has multiple facets. One problem raised many times by security expert Bruce Schneier[48] is that IoT devices are often inexpensive consumer products that manufacturers have no incentive to make secure, or to fix when vulnerabilities are discovered. Regulatory innovation will be necessary to ensure that even the manufacturers of IoT devices can be held accountable to a reasonable degree for the security and privacy in their products. Another problem is the sheer variety of IoT devices, making it extremely difficult to converge on a consistent set of standards to govern their construction and their interaction. The international IoT community will need to collaborate purposefully and effectively in order to establish a sound basis for secure IoT technology.

In the meantime, the UK has taken an intermediate step of issuing a Code of Practice for consumer IoT security, which provides guidelines and best practices[49] for doing the best that is possible with today's IoT technology.

3.3.2 Next Generation Virtualized Infrastructures

Virtualized infrastructure is becoming an essential part of the next generation of information technology services. What started out as a simple form of providing a

[47] Sapna Maheshwari (NY Times) - How Smart TVs in Millions of U.S. Homes Track More than What's On Tonight - https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html

[48] Bruce Schneier's article "New IoT Security Regulations - https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html

[49] UK.gov guidance "Secure by Design" https://www.gov.uk/government/collections/secure-by-design

different operating system environment (e.g. an old operating system) on a desktop computer has become a core feature of modern business models such as “X as a Service”. Cloud computing centres offer virtualized environments to individual customers. 5G wireless networks offer customized Service Level Agreements that involve “network slicing” of software defined network features.

But virtualized infrastructures bring heavy challenges with them. There are various approaches to ensuring security of virtualized environments (e.g. agent-based, light agent, etc.), but the stakes are high. As security experts Kapersky have noted[50], virtual infrastructure effectively doubles the cost of a security breach. For large companies, the average cost of a security breach is more than $800K, lending a clear sense of urgency to the problem.

3.3.3 Artificial Intelligence

Artificial intelligence, to a great degree through the enormous recent advances in Machine Learning, promises to become an important element in information systems in the future, ensuring not increased responsiveness and personalization for customers, but also enhanced return on investments for the vendors. However, the promise of AI is balanced by great dangers posed both to security and privacy.

In the area of privacy, the advent of the GDPR in particular has created considerable difficulties for AI technologies to surmount. Machine learning uses algorithms that use training data to progressively improve, in order to recognize patterns (for example, user book-buying habits). Eventually they evolve beyond even their creators’ abilities to explain how they operate.

This is nearly antithetical to the requirements of the GDPR: whereby the GDPR requires minimization of data, machine learning collects enormous amounts of Big Data that may or may not be relevant; automated decisions must be explainable – but machine learning algorithms become opaque very quickly; and it is very hard to get rid of Big Data, or to know whether and which data has been eliminated.

The alignment of AI with the GDPR and other privacy-related directives will be a major challenge in the future. But privacy is not the only challenge confronting artificial intelligence. It is gradually becoming clear that it is uncomfortably easy to “trick” a machine learning algorithm into learning the wrong things. Tricking a machine learning algorithm into thinking a panda is a vulture may be amusing, but it becomes much less amusing when an automobile’s machine vision system is tricked into thinking that another car is just a bird or a leaf. In other words, not just the machine learning algorithms but the training data itself becomes a significant target of attack by malicious operators. Even rule-based AI systems could be seriously compromised if the set of rules is hacked and replaced by other rules by a malicious intruder, with totally unpredictable results. In summary, also security will be one of the major challenges facing AI in the future.

3.3.4 KEY AREAS CONCLUSIONS

These key areas are by no means representing a comprehensive identification of all of the issues that are important for our CS&P Roadmap, but really represent the core of the first roadmaps, strategies and frameworks studied – as with our previous

[50] Kapersky Lab “”IT Security Risks Special Report Series” - https://media.kaspersky.com/en/business-security/enterprise/it_risks_survey_report_virtualization.pdf

deliverable D3.4 this comparison study is the first of its kind and this will be the core of our final Roadmap deliverable at the end of the project.

4 CONCLUSIONS

The Cyberwatching.eu project encompasses a significant opportunity to look at a snapshot of the broadest set of cybersecurity projects Europe-wide and even globally to a certain extent. The project is built upon the most solid of foundations, using existing work as the base, focusing upon clustering and concertation, developing practical and useful tools for the community. Furthermore, the road mapping in this early deliverable is looking at existing and previous roadmap exercises identifying key elements requiring more study and efforts within the final roadmap deliverable due at the end of the project. In essence, we have not only addressed the request of the reviewers from our last project review to provide a “project overview and summary” deliverable, but we have also done the initial analysis in preparing the eventual roadmap, which will be provided at the end of the project.

5 REFERENCES

Articles:

Giovanni Buttarelli "The urgent case for a new ePrivacy law" - https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en

"The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC" 21 January 2019; https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

Marsh, "Continental European Cyber Risk Survey: 2016 Report," October 2016, 7 - https://www.marsh.com/cy/en/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html

IDC – Worldwide Skills survey (2017)

Study prepared for the European Economic and Social Committee – "Cyberseurity - Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks" - https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

Tackling cybersecurity threat information sharing challenges - https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html

Opinion 5/2018 Preliminary Opinion on privacy by design, 31 May 2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf.

Data protection by design and by default", https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/; last accessed on 15/02/2019.

Hern, A., & Belam, M. (2018, May 25). LA Times among US-based news sites blocking EU users due to GDPR. Retrieved from https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times

Sapna Maheshwari (NY Times) - How Smart TVs in Millions of U.S. Homes Track More than What's On Tonight - https://www.nytimes.com/2018/07/05/business/media/tv-viewer-tracking.html

Bruce Schneier's article "New IoT Security Regulations - https://www.schneier.com/blog/archives/2018/11/new_iot_securit.html

UK.gov guidance "Secure by Design" https://www.gov.uk/government/collections/secure-by-design

Kapersky Lab ""IT Security Risks Special Report Series" - https://media.kaspersky.com/en/business-security/enterprise/it_risks_survey_report_virtualization.pdf

Cloud Services Working Group

- CSP CERT - https://cspcerteurope.blogspot.com/

ECSO

- ECSO Strategic and Innovation Agenda (WG6, 2017) - http://ecs-org.eu/documents/publications/59e615c9dd8f1.pdf
- ECSO WG1 - https://ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management

EU Commission

- EU Commission M/289 - http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=167#
- EU Commission M/530 mandate - http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548
- European Commission (2015), Cybersecurity industry

EU Legislation

- General Data Protection Regulation - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

  - Information Commissioner Office's Guide to the GDPR, or the *Commission Nationale de l'Informatique et des Libertés'* Guide for Processors.
  - The *Commission Nationale de l'Informatique et des Libertés* has also produced a software to conduct a Privacy Impact Assessment that can be freely used by any organisations.
  - According to Article 24(3) of the GDPR: "Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller".

- Network and Information Security Directive - https://publications.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en
- Proposal for a Regulation on Privacy and Electronic Communications - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010
- Proposal for a Cybersecurity Act - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

EU Projects:

- AEGIS report "Report on Cybersecurity and privacy R&I Priorities for EU-US cooperation" - http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Report-on-Cybersecurity-and-Privacy-RI-Priorities-for-EU-US-cooperation.pdf
- AEGIS D.1.3 - White Paper on Cybersecurity Policies. Common Ground for EU-US Collaboration, (2018, May 31)
- CAMINO Project - http://www.fp7-camino.eu/
- CAMINO Roadmap - http://www.fp7-camino.eu/
- Cyberwatching.eu - Free Webinars from cyberwatching.eu – Archives at https://www.cyberwatching.eu/webinar
- SecUnity project Roadmap - https://it-security-map.eu/en/home/

ENISA:

- ENISA Publication « Information Security and Privacy for SMEs » (2015) - https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
- ENISA Publication "Looking into the Crystal Ball – a report on emerging technologies and security challenges"
- ENISA Publication "Guidance and Gaps Analysis for European Standardisation" https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation
- ENISA Briefing EU Legislation in Progress – ENISA and a new cybersecurity act - http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf
- Presentation by Gonzalez at ECSO Meeting on February 27, 2019 - https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/1%20Gonzalez.pdf

ESOs and Committees, ISO/IEC

- CEN-CENELEC – https://www.cencenelec.eu/Pages/default.aspx
- CEN - https://www.cen.eu/Pages/default.aspx
- CENELEC - https://www.cenelec.eu/
- ETSI - https://www.etsi.org/about
- ISO - https://www.iso.org/
- ISO/IEC JTC1/SC 27- https://www.iso.org/committee/45306.html
- CEN/CENELEC JTC13 - https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B
- CEN/CENELEC JTC13 list of imported ISO/IEC JTC1 SC27 standards https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5
- ETSI web site – status on response to EC mandate 530 https://portal.etsi.org/webapp/WorkProgram/TUBEReport.asp?titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qFREQUENCIES_BOOLEAN=OR&qMandate_List=%27M%2F530%27&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY&optDisplay=10
- Copolco Committee - https://www.iso.org/committee/55000.html

USA

- NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 https://www.nist.gov/sites/default/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf
- USA National Cyber Strategy - https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

6 ANNEX A - GLOSSARY

Term	Explanation
AI	Artificial Intelligence
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CNIL	Commission Nationale de l’Informatique et des Libertés (CNIL)
CS&P	Cybersecurity and Privacy
DSP	Digital Service Providers
ECSO	European Cyber Security Organisation
ERC	European Research Council
ESOs	European Standardisation Organisations
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
IA	Innovation Action
IaaS	Infrastructure-as-a-Service
IEC	International Electrotechnical Committee
IoT	Internet of Things
ISO	International Organization for Standardisation
MTRL	Market and Technology Readiness Level
NISD	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
PaaS	Platform-as-a-Service
PCA	Principal Component Analysis
RA	Research Action
RIA	Research & Innovation Action
SaaS	Software-as-a-Service

7 ANNEX B – PRIVACY STANDARDS ECOSYSTEM

This Annex contains a summary of standards in the information security and privacy field, first from a European level and second, an international level. The information is summarized from ENISA publication "Guidance and Gaps Analysis for European standardisation – Privacy standards in the information security context" (December 2018).[51]

7.1 EUROPEAN STANDARDS

Specific committees from the three recognized SDOs bodies (CEN, CENELEC and ETSI) which address matters related to privacy and standards are summarized below:

7.1.1 CEN/CENELEC JWG8

CEN/CENELEC created in 2015 the JWG8 Committee to respond to M/530 mandate and proposed to the Technical Committee to prepare the following deliverables:

- WI 001- Data protection by design and by default (type of deliverable: EN)
- WI 002- Video surveillance (CEN/ TR)
- WI 003- Biometric for access control including face recognition (CEN/TR)

Within its scope, JWG8 proposed to recognize ISO/IEC 29134 (privacy impact assessment Methodology) as a European standard.

7.1.2 CEN/CENELEC JTC13

This is a Technical Committee created in 2017[52] to handle privacy in a more generic basis data protection and privacy by design and by default. This Committee has been tasked with importing relevant ISO/IEC JTC1 SC27 standards, the updated status of which is available on the ISO website[53].

7.1.3 ETSI Technical Committee Cyber (TC Cyber)

This committee was created in 2014, and designated by the Board of ETSI to act as coordinator of the work to fulfil the EC mandate M530. TC Cyber identified several privacy topics as a priority domain to be tackled by ETSI. To respond to the EC mandate M530, ETSI prepared the following deliverables:

- DTR/CYBER-0010, TR 103 370, Practical introductory guide to privacy
- DTS/CYBER-0013, TS 103 485, Mechanisms for privacy assurance and verification
- DTS/CYBER-0014, TS 103 486, Identity management and naming schema protection mechanisms

[51] ENISA Publication "Guidance and Gaps Analysis for European Standardisation" https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

[52] CEN/CENELEC JTC13 - https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2307986&cs=1E7D8757573B5975ED287A29293A34D6B

[53] CEN/CENELEC JTC13 list of imported ISO/IEC JTC1 SC27 standards https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5

- DTS/CYBER-0020, TS 103 458, Application of Attribute Based Encryption (ABE) for data protection on smart devices, cloud and mobile services

The updated status of deliverables in response to M530 mandate is available on the ETSI web site.[54] There are several other standards which are related to more generic cybersecurity and management themes and which may relate also to privacy but they are not detailed herein.

7.2 INTERNATIONAL STANDARDS

In the field of IT, the general standards of privacy lies within the scope of ISO/IEC JTC 1/SC 27 IT Security Techniques (SC 27)[55]. Within SC 27, standards of relevance to the field of privacy have been developed within ISO/IEC JTC 1SC 27/WG 5 - the Working Group on Identity Management, Privacy and Biometrics.

The Copolco committee (ISO's Committee on consumer policy) has initiated a new project committee (PC 317) on "Consumer protection: privacy by design for consumer goods and services"[56]

The following is a summary (non-exhaustive) of relevant privacy standards, largely summarized from ENISA Publication "Guidance and Gaps Analysis for European standardisation – Privacy standards in the information security context" (December 2018)"[51] and the information on the ISO website[57]

REFERENCE	TITLE	STATUS AT 04/2019
Privacy framework :		
ISO/IEC 29100: 2011	Privacy Framework https://www.iso.org/standard/45123.html	Last reviewed in 2017
Corrigenda/ Amendment	ISO/IEC 29100:2011/Amd 1:2018 https://www.iso.org/standard/73722.html)	Published 06/2018
ISO/IEC 29190:2015	Privacy capability assessment model https://www.iso.org/standard/45269.html	Published 08/2015
ISO/IEC 29151:2017	Code of practice for personally identifiable information protection https://www.iso.org/standard/62726.html	Published 08/2017

[54] ETSI web site – status on response to EC mandate 530 https://portal.etsi.org/webapp/WorkProgram/TUBEReport.asp?titleType=all&qSORT=HIGHVERSION&qETSI_ALL=&SearchPage=TRUE&qINCLUDE_SUB_TB=True&qINCLUDE_MOVED_ON=&qSTOP_FLG=N&qKEYWORD_BOOLEAN=OR&qCLUSTER_BOOLEAN=OR&qFREQUENCIES_BOOLEAN=OR&qMandate_List=%27M%2F530%27&qSTOPPING_OUTDATED=&butExpertSearch=Search&includeNonActiveTB=FALSE&includeSubProjectCode=FALSE&qREPORT_TYPE=SUMMARY&optDisplay=10

[55] ISO/IEC JTC1/SC 27. SC 27 is a subcommittee of the Joint Technical Committee 1 (JTC 1) of ISO and IEC, scoped to address Information Technology.
https://www.iso.org/committee/45306.html

[56] Copolco Committee - https://www.iso.org/committee/55000.html

[57] ISO website – https://iso.org

REFERENCE	TITLE	STATUS AT 04/2019
ISO/IEC 27552	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines	Under development at “DIS” stage (draft international standard)
ISO/IEC 29134:2017	Guidelines for privacy impact assessment https://www.iso.org/standard/62289.html	Published 06/2017
Identity Management related standards:		
ISO/IEC 24760-1 (Previously ISO/IEC 24760-1:2011)	A framework for identity management. Part 1: Terminology and Concepts https://www.iso.org/standard/77582.html	Under development at « FDIS » stage (final draft international standard)
ISO/IEC 29115 (Previously ISO/IEC 29115:2013)	Entity Authentication Assurance Framework https://www.iso.org/standard/73909.html	Under development at « WD » stage (working draft)
ISO/IEC 29146	A framework for access management https://www.iso.org/standard/45169.html	Published 06/2016
Technical implementation of privacy:		
ISO/IEC 29101:2018 (Previously ISO/IEC 29101:2013)	Privacy architecture framework https://www.iso.org/standard/75293.html	Published 11/2018
ISO/IEC 27550	Privacy engineering https://www.iso.org/standard/72024.html	Under development
Sector-specific privacy standards:		
ISO/IEC 27018:2019 (Previously ISO/IEC 27018:2014)	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors https://www.iso.org/standard/76559.html	Published 01/2019
ISO/IEC 27570	Privacy guidelines for smart cities https://www.iso.org/standard/71678.html	Under development at « WD” stage (working draft)
ISO/IEC 17030	Guidelines for security and privacy in Internet of Things (IoT) https://www.iso.org/standard/44373.html	Under development at « WD » stage (working draft)
ISO/IEC 29184	Online privacy notices and consent https://www.iso.org/standard/70331.html	Under development at CD stage (committee draft)

REFERENCE	TITLE	STATUS AT 04/2019
Security evaluation standards with privacy relevance		
ISO/IEC 5408-1 (Previously ISO/IEC 15408-1:2009)	Evaluation criteria for IT security https://www.iso.org/standard/72891.html	Under development at « CD » stage (committee draft)
ISO/IEC 18045 (Previously ISO/IEC 18045:2005 Now under review ISO/IEC 18045:2008)	Methodology for IT security evaluation https://www.iso.org/standard/72889.html	Under development at « CD » stage (committee draft)
ISO/IEC TC 19608:2018	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408	Published 10/2018
Standards on the implementation of security techniques with privacy relevance (some examples)		
ISO/IEC 18033-1 (Previously ISO/IEC 18033-1:2015)	Encryption algorithms https://www.iso.org/standard/76156.html	Under development at « WD » stage (working draft)
ISO/IEC 18370-1:2016	Blind digital signatures https://www.iso.org/standard/62288.html	Published 11/2016
ISO/IEC 20008-2:2013	Anonymous digital signatures https://www.iso.org/standard/56916.html	Corrected version 12/2017
ISO/IEC 20009-4:2017	Anonymous entity authentication https://www.iso.org/standard/64288.html	Published 08/2017
ISO/IEC 29191:2012	Requirements for partially anonymous partially unlinkable authentication https://www.iso.org/standard/45270.html	Reviewed and confirmed in 2018
ISO/IEC 20889:2018	Privacy enhancing data de-identification terminology and classification of techniques https://www.iso.org/standard/69373.html	Published 11/2018
ISO/IEC WD 27551	Requirements for attribute-based unlinkable entity authentication https://www.iso.org/standard/72018.html	Under development at « WD » stage (working draft)
Generic information security management standards (broad application area but which may be relevant to privacy in a wider context)		
ISO/IEC 27000	Information security management systems - Overview and Vocabulary	

REFERENCE	TITLE	STATUS AT 04/2019
ISO/IEC 27001	Information security management systems – Requirements	
ISO/IEC 27005	Information security risk management	
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems	
ISO/IEC 27007	Information security management systems - auditor guidelines	
ISO/IEC 27008	Guidelines for the assessment of information security controls	
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements	
ISO/IEC 27013	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	
ISO/IEC 27014	Governance of information security	
Examples of sector-specific information security management standards		
ISO/IEC 27002	Code of practice for information security controls	
ISO/IEC 17030	Guidelines for security and privacy in Internet of Things (IoT)	
ISO/IEC 27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services	