Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.20:

Policy Recommendations 2

Document Identification	
Due date	31 January 2022
Submission date	31 January 2022
Revision	4.0

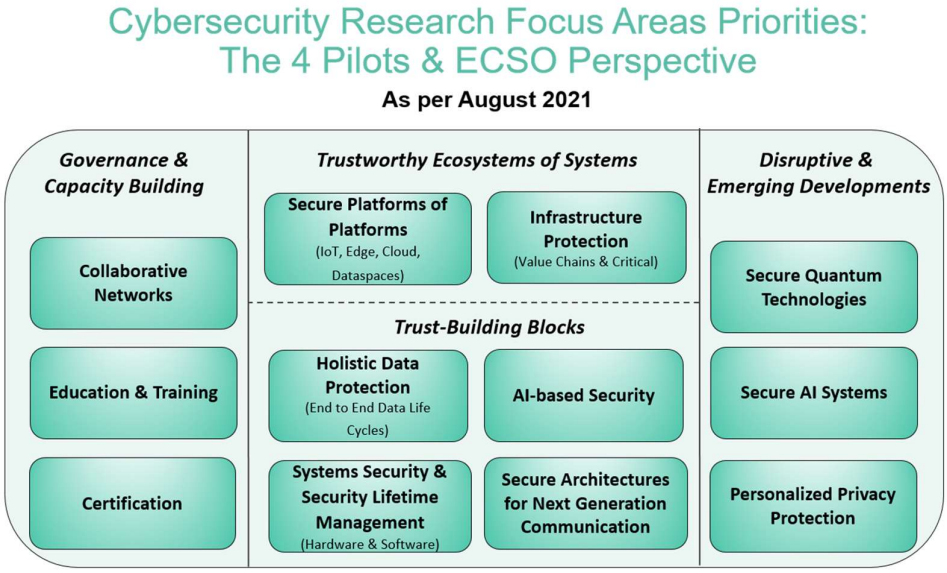
Related WP	WP9	Dissemination Level	Public
Lead Participant	FORTH	Lead Author	Evangelos Markatos
Contributing Beneficiaries	ARCH, ATOS CONCEPT, GUF, KUL, NEC, NTNU, UCY, UM, UMU, UPRC, POLITO, TDL, TLEX, VTT	Related Deliverables	D2.2, D2.3, D3.10, D3.11, D3.12, D4.4, D5.2, D5.3, D5.4, D6.3, D6.4, D7.1, D7.2, D7.3, D8.2, D9.1 - D9.14, D10.2

Abstract:
This deliverable is the second in a sequence of three reports that select policy recommendations of the CyberSec4Europe project and present them in a way that can be easily understood and used by interested parties, and especially by policymakers. The policy recommendations cover a wide variety of areas ranging from education to research and target a wide variety of stakeholders including the European Commission, European agencies, European organisations and policymakers in EU Member States.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

CyberSec4Europe plays a very active role in helping policymakers formulate the policies that will shape the future of the cybersecurity of the EU and its Member States. To provide effective policy recommendations, CyberSec4Europe follows a two-pronged approach.
In a *reactive* approach Cyber4SecEurope members accept invitations to provide recommendations in several forums, including workshops, concertation meetings, EU-level organisations, etc. Such organisations include ECSO (the European Cyber Security Organisation), JRC (the EU Joint Research Centre), and ENISA (the EU Agency for Cybersecurity). One of the most notable policy recommendations includes the list of research priorities in the area of cybersecurity which was delivered by CyberSec4Europe (in collaboration with the other three pilots and ECSO) to the JRC and was picked up later by ENISA. These priorities are:



In a *proactive* approach the Cyber4SecEurope members acknowledge that much of the work already performed in the project may essentially create contributions that are practically policy recommendations. In this deliverable we collect these contributions, phrase them as policy recommendations and provide evidence that underlines their importance.

Some of the policy recommendations that stand out include:

- **Recommendation 1: <u>Ensure the active engagement of the European cybersecurity communities in the implementation of EU Regulation 2021/887</u>**
    - The overall recommendation here is to go beyond the structure outlined in the regulation and to facilitate better visibility and communication between the wide range of local communities nationally and supranationally; and to ensure that the governance model of the NCCs encourages and facilitates the functioning and participation of local communities.
    - The participation of the community in the decision about the members of the Advisory Group as well as guidelines for the involvement of the Advisory Group

in decisions of the Governing Board, for example in its rules of procedure, are strongly recommended.
    - This recommendation opposes a one-size-fits-all approach and proposes that CHECK (Community Hub of Expertise in Cybersecurity Knowledge) initiators establish both topic-specific and sector-specific CHECKs, as well as regional CHECKs, provided that basic requirements for the establishment of a CHECK are met.
    - This recommendation proposes that the process for creating CHECKs should be uniform at the European level.
- **Recommendation 2: Create a harmonisation strategy for GDPR compliance among Member States**
    - It is recommended that the relevant stakeholders continue to address their national authorities, raising concerns related to the need for the further harmonisation of the GDPR across Member States and seeking clarification whenever possible
    - The project-oriented guidelines for GDPR Compliant User Experience need to be continuously updated in order to adequately reflect the constantly evolving data protection regulatory field.
- **Recommendation 3: Encourage adoption of security and privacy by design**
    - The adoption of security and privacy solutions from the perspective of usability must be approached as a multi-dimensional problem, where different dimensions have to be addressed and funding should be made available for the development of the relevant tools
- **Recommendation 4: Encourage "blue sky" research in cybersecurity**
    - A good architecture of European funding may consist of blue-sky individual projects under the ERC, plus a large number of collaborative EIC Pathfinder projects in strategic areas – that could also network the results stemming from the ERC – complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

Document information

Contributors

Name	CyberSec4Europe Consortium Member
Elias Athanasopoulos	UCY
Panagiotis Bountakas	UPRC
Daniele Canavese	POLITO
Sunil Chaudhary	NTNU
Christos Douligeris	UPRC
Vasileios Gkioulos	NTNU
David Goodman	TDL
Hans Graux	TLEX
Elma Kalogeraki	UPRC
Anni Karinsalo	VTT
Bostjan Kezman	UM
Evangelos Markatos	FORTH
Mark Miller	CONCEPT
Dirk Müllmann	GUF
Aljiosa Pasic	ATOS
Davy Peuveneers	KUL
Renáta Radócz	ARCH
Alessandro Sforin	NEC
Antonio Skarmeta	UMU
Christina von Wintzingerode	GUF

Reviewers

Name	CyberSec4Europe Consortium Member
David Goodman	TDL
Stephan Krenn	AIT
Jozef Vyskoc	VAF
Afonso Ferreira	UPS-IRIT

History

Version	Date	Authors	Comment
0.01	2021-10-29	Evangelos Markatos and all partners	1st Draft
1	2021-12-01	All partners	2nd Draft
2	2021-12-16	David Goodman	1st Complete Draft
3	2021-12-21	All partners	Draft to be sent to reviewers
3.1	2022-01-14	All partners	Draft for second round of reviews
4	2022-01-20	All partners	Final version for submission

Table of Contents

List of Acronyms

A	ABC	Attribute-Based Credentials
	AIS	Automatic Identification System
	API	Application Programming Interface
	APS	Autonomous Passenger Ship
	APT	Advanced Persistent Threat
C	CHECK	Community Hub of Expertise in Cybersecurity Knowledge
	CS4E	CyberSec4Europe
D	DARPA	Defense Advanced Research Projects Agency
	EC	European Commission
E	ECSO	European Cyber Security Organisation
	ECT	Emergency Control Team
	eIDAS	electronic IDentification, Authentication and trust Services
	ENISA	European Union Agency for Cybersecurity
	ERC	European Research Council
	EU	European Union
F	FET	Future and Emerging Technologies
G	GDPR	General Data Protection Regulation
	GPS	Global Positioning System
	ICT	Information and Communication Technologies
	IDM	Identity Management
M	MAPE	Monitor Analyse Plan Execute
	MS	Member States
N	NCC	National Coordination Centre
R	RCC	Remote Control Centre
S	SME	Small and Medium-sized Enterprise
T	TEE	Trusted Execution Environment
U	UCD	User-Centred Design

1 Introduction

This is the second deliverable of Task 9.6: Policy Recommendations. According to the Description of Action, the task identifies and prioritises[1] policy recommendations based on the results of the conclusions and roadmaps associated with the demonstration activities, to define a sustainable path for the technologies developed in CyberSec4Europe.
Indeed, several of the project deliverables have produced solid scientific and technical results that can be used to guide future policy recommendations. Capitalising on these results, the project can have an impact not only technically, but also in the field of policy.

To pave the road towards effective policy recommendations, the project is following a two-pronged approach:

- A **proactive** approach. The CyberSec4Europe members collect possible policy contributions created by the various technical activities of the project and present them in a form that can be used by policymakers.
- A **reactive** approach. The CyberSec4Europe members decided to accept (to the extent possible) requests for contributions to policy documents at either the EU or Member State level.

This deliverable describes the outcomes of these two approaches.
Section 2 describes the proactive approach and lists the main deliverables of the project. Section 3 summarises some of the policy recommendations. Section 4 describes the reactive approach and provides pointers to our contributions. Finally, Annex I provides more policy-related information extracted from the deliverables of the project for future use and reference.

[1] Prioritisation is at two levels. First, we collect all possible policy-related recommendations of the Deliverables and list them in Annex I. Then, we select some of these recommendations we expend them, we provide more information and we list them as subsections in section 3.

2 The proactive approach

The project has already produced and will continue to produce high-quality deliverables that may include technical contributions that can be used as policy recommendations. In this task, we collect these technical contributions into knowledge that can be communicated to policymakers.
To collect such policy recommendations, we started from the project deliverables that had been submitted at the time this work started. From those deliverables we excluded those that did not have any policy-making potential (such as those from WP1: Project Management). The final set of deliverables studied was[2]:

- Deliverable D2.2: Internal Validation of Governance Structure
- Deliverable D2.3: Governance Structure v2.0
- Deliverable D3.10: Cybersecurity Outlook 1
- Deliverable D3.11: Definition of Privacy by Design and Privacy Preserving Enablers
- Deliverable D3.12: Common Framework Handbook 2
- Deliverable D4.4: Research and Development Roadmap 2
- Deliverable D5.2: Specification and Set-up Demonstration case Phase 1
- Deliverable D5.3: Validation of Demonstration Case Phase 1
- Deliverable D5.4: Requirements Analysis of Demonstration Cases Phase 2
- Deliverable D6.3: Design of Education and Professional Framework
- Deliverable D6.4: Flagship 1
- Deliverable D7.1: Report on Existing Cyber Ranges, Requirements
- Deliverable D7.2: Virtual Lab For Open Source Tools Education and Research
- Deliverable D7.3: Evaluation Report On Integration Demonstration
- Deliverable D8.2: Project Standards Matrix (together with the Standards Matrix)
- Deliverable D8.3: Cybersecurity Standardization Engagement Plan 2
- Deliverable D9.1: Website and Social Media Accounts
- Deliverable D9.2: Dissemination Material: Brochures, Posters
- Deliverable D9.3: Dissemination and Awareness Plan
- Deliverable D9.4: Website and Social Media Accounts
- Deliverable D9.5: Report on the Outreach and Dissemination Activities
- Deliverable D9.6: SME Cybersecurity Awareness Program 1
- Deliverable D9.7: CyberSec4Europe Summer Schools 1
- Deliverable D9.8: Policy Recommendations
- Deliverable D9.9: Website and Social Media Accounts 3
- Deliverable D9.10: Report On The Outreach and Dissemination Activities 2
- Deliverable D9.11: SME Cybersecurity Awareness Program 2
- Deliverable D9.12: Supply Chain Security Recommendations
- Deliverable D9.13: Awareness Effectiveness Study

[2] All deliverables can be downloaded from https://cybersec4europe.eu/publications/deliverables/

- Deliverable D9.14: Exploitation Strategy Report 1
- Deliverable D10.2: Clustering Results & SU-ICT-03 Project Concertation Conference Year 2

For all the deliverables, we contacted the editor (or co-editor) asking for possible policy recommendations that might come out of the deliverable. In particular, we asked the following targeted questions:

- Do you think that your deliverable can be used by policymakers? Possibly for future calls for proposals? For the Horizon Europe programme? For the Digital Europe programme? For future versions of NIS? of the GDPR? of the ePrivacy regulation? etc.
- If yes, what findings in your deliverable would be most relevant to the policymakers? Can you summarise them in no more than one paragraph per finding?
- Suppose that you had the opportunity to talk to a member of the European Parliament for five minutes. What would you like them to know about your deliverable?

The responses are included in this deliverable in Annex I.

3 Policy Recommendations

In this section we list the policy recommendations derived from the various project activities and deliverables, as well as possible next steps. For each recommendation we adopt the following structure:

- One-sentence-long title of the recommendation
- Background: explain the setting
- One or more individual recommendations that come out of the main "high-level" recommendation
- More details: documents where more details can be found
- Target audience: who is the target audience for this recommendation

3.1 Ensure the active engagement of the European cybersecurity communities in the implementation of EU Regulation 2021/887

3.1.1 Background

The call for proposals to establish and operate a pilot for a Cybersecurity Competence Network[3] envisaged new governance models to address:

> *… an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities.*

Specifically in relation to governance, the call expected work to include:

> *… the assessment of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry. Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people) and will be implemented, tested and validated in the demonstration cases (see below) involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure.*
>
> *Projects will demonstrate the effectiveness of their selected governance structure by providing collaborative solutions to enhance cybersecurity capacities of the network and develop cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).*

On 20 May 2021, EU Regulation 2021/887[4] for the setting up of a European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and a network of National Coordination Centres (NCCs) was formally adopted. It contains ideas for the governance design, yet it still leaves a lot of options open. One of the goals of CyberSec4Europe has been to design the governance structure for a European network that will address today's main cybersecurity challenges. The role and the structure of the wider cybersecurity competence community, which was left open for interpretation in the regulation, will be crucial for mastering those cybersecurity challenges due to its potential impact on research, development and dissemination activities.
Based on stakeholder feedback, legal requirements and best practices, the project designed such a governance model: a bottom-up approach to address stakeholder demands to further European cybersecurity research and development based on the concept of CHECKs[5]. Since then, additional governance structures have been analysed and the implementation process of CHECKs in Toulouse and the region of Murcia have delivered some first insights on the challenges, further stakeholder

[3] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887

[5] CHECK: Community Hub of Expertise in Cybersecurity Knowledge. See also D2.1 Governance Structure

requirements and possible approaches on the hub governance design. Using these additional findings, the governance structure with a focus on the CHECKs concept has been developed further.
On the evening of. 18 November 2021, CyberSec4Europe hosted a roundtable discussion[6] featuring Miguel Gonzalez-Sancho, head of Unit H1, DG CONNECT and Interim Executive Director of the ECCC as well as representatives from seven European cybersecurity communities[7]. Each Member State has its own set of cybersecurity-related priorities or agenda relevant to the specific strengths of its key sectors, many of which have a common set of challenges. Of particular interest is the degree of connectedness of the communities with each other, both at national and supranational levels, which plays into expectations relating to the governance and decision-making processes of the NNCCs and their relationship with the new ECCC. What emerged from the roundtable was a common desire for increased skills training and better transitioning and communication between research and industry for cybersecurity solutions and services – both capacity and community building. It was also apparent that the communities' landscape was somewhat fragmentary, both nationally and cross-border, requiring better networking as a key component.

3.1.2 Recommendation (1)

The regulation was designed to address many of the challenges raised by the communities. This framework and the NCCs in particular have a remit to accommodate the wide diversity of experience and expertise across the wider European cybersecurity community and, through a common agenda, ensure that all voices can be heard. The role of the EC is to facilitate this collaboration. **The overall recommendation here is to go beyond the structure outlined in the regulation and to facilitate better visibility and communication between the wide range of local communities nationally and supranationally; and to ensure that the governance model of the NCCs encourages and facilitates the functioning and participation of local communities.**

3.1.3 Recommendation (2)

The recently introduced Strategic Advisory Group of the ECCC highlights the importance of the communities' influence on political decisions. **The participation of the community in the decision about the members of the Advisory Group as well as guidelines for the involvement of the Advisory Group in decisions of the Governing Board, for example in its rules of procedure, are strongly recommended.** In order to relieve the Governing Board in particular, an Executive Board should be introduced into the structure of the ECCC, to which the processing and preparation of time-intensive tasks can be assigned. The governance structure of ENISA can serve as a model for the distribution of tasks and the relationship between the actors. In the context of the NCCs, it should be noted that the regulation of their cooperation, organisation and work is, to a large extent, the task of national legislators. Nevertheless, basic issues of information exchange and cooperation should be addressed and regulated from a European level by the regulation in order to be able to create a unified structure and a pan-European perspective on the work of the NCCs to be performed.

---

6 Community Perspectives On The Future of Cybersecurity in Europe
7 Germany, Greece, Ireland, Italy, The Netherlands, Norway, Spain

The following two recommendations address issues and improvements to the CHECK concept which is CyberSec4Europe's recommended building block for the implementation of the regulation to achieve the desiderata stated above.

3.1.4 Recommendation (3)

CyberSec4Europe's monitoring of two pilot CHECKs to date is leading to further refinements of the concept and optimisation of their design. **The recommendation opposes a one-size-fits-all approach and proposes that CHECK initiators establish both topic-specific and sector-specific CHECKs, as well as regional CHECKs, provided that basic requirements for the establishment of a CHECK are met.** In this way, the different starting conditions in the Member States, but also in the different regions of Europe, can be taken into account and at the same time as the creation of a Europe-wide network for the involvement of the wider cybersecurity community.

3.1.5 Recommendation (4)

The process for creating CHECKs should be uniform at the European level. While the initiative to create a CHECK can come from a coalition of private actors or from governmental or semi-governmental bodies suggesting it to private parties, the act of designating an initiative as a CHECK should be done either by the ECCC or a NCC. By verifying the existence of the necessary conditions for the establishment of a CHECK, the quality of the work of the CHECKs and the qualification of the actors gathered in them will be ensured.

3.1.6 More details

For more details see the relevant deliverables:

- D2.3: Governance Structure v2.0

3.1.7 Target audience

- European Commission DG CONNECT
- ENISA
- European Cybersecurity Competence Centre

3.2 Create a harmonisation strategy for GDPR compliance among Member States

3.2.1 Background

The rapid emergence in the digitalisation of our everyday lives has not only dramatically increased the volume of data collection but accelerated the flow of information. As this data could be used for malicious purposes, the EU has agreed to develop one single regulation for strengthening the rights of data subjects and to create a single European digital market. Although the GDPR is directly binding and applicable across all Member States, it provides a certain level of flexibility: Member States can choose the form and method they implement the GDPR in their national legislation whether by adopting new legislation or by supplementing existing ones.

The GDPR sets forth requirements that continuously challenge businesses to implement the necessary measures for compliance, with substantial fines for those who fail to comply. Nevertheless, these requirements are often vague and subject to interpretation. Additionally, several other frameworks must be consulted or considered, including ISO/IEC frameworks, European Data Protection Board (EDPB) guidelines or recommendations from relevant national authorities, to ensure the correct implementation of measures. As an example, article 32[8] of the GDPR requires data controllers and processors to implement "*appropriate technical and organizational measures*" but it does not define these measures. Data controllers and processors must then consult the guidance of national supervisory authorities for further clarification and may seek to follow an international standard on the topic (e.g., ISO/IEC 27701:2019 on privacy information management[9]). Furthermore, personal data protection regulations, directives and privacy requirements are ever evolving, and need constant monitoring to ensure the highest level of compliance, further enforcing market fragmentation.

As mentioned in Deliverable D3.6 [10], the requirements of the GDPR require substantial effort from both data controllers and processors for effective and proper implementation. The combined framework and guidelines generated throughout D3.6 seek to enable data controllers and processors to pursue compliance in a structured manner, following a clear roadmap. For these guidelines to be useful, substantial work is required to continuously update it following any new recommendation/legislative evolution to maximise its sustainable use. Furthermore, it is expected that data controllers and processors will face certain barriers, (e.g., in relation to cross-border compliance within the EU such as due to the differences in the minimum age of consent in the various Member States) which have yet to be solved.

Based on the above identified causes for regulatory segmentation on the market, the following sections introduce recommendations for effective management of the issue both on a consortium and Europe-wide level.

[8] https://gdpr-info.eu/art-32-gdpr/

[9] https://www.iso.org/standard/71670.html

[10] https://cybersec4europe.eu/wp-content/uploads/2021/02/D3.6-Guidelines-for-GDPR-compliant-user-experience-Revision-2.0.pdf

3.2.2 Recommendation (1)

In order to create a harmonised strategy for GDPR compliance among Member States and to allow data controllers and processors to successfully implement the required safeguards for ensuring the proper protection of data subjects' rights, **it is recommended that the relevant stakeholders continue to address their national authorities, raising concerns related to the need for the further harmonisation of the GDPR across Member States and seeking clarification whenever possible**. One such way towards harmonisation would be the joint work of the European national data protection authorities (DPAs) in providing practical guidelines that further support the uniform enforcement and implementation of the GDPR in a non-discriminatory manner. Here, the EDPB could play a crucial role in ensuring that national frameworks, guidance, criteria, and recommendations are aligned, without conflicts. This action would ensure the development of a comprehensive European approach and the development of common understandings between the DPAs and, more broadly, the Member States. Nevertheless, the EC recognises[11] that the GDPR still requires additional work to be most effectively implemented within the EU.

3.2.3 Recommendation (2)

From a practical point of view, a complete GDPR harmonisation strategy would require not only substantial efforts but also significant time and resources. The GDPR mentions over 70 times the term 'certification' as a potential solution to enable the demonstration of compliance across European boundaries. The EDPB has published its guidelines[12] on a common certification mechanism resulting in the European Data Protection Seal. Therefore, **it is recommended to have GDPR certifications in place as described in Articles 42-43 of the GDPR**. **The recognition of general GDPR certification schemes across Europe could bridge the harmonisation gap and enable not only global organisations but even SMEs to certify their data processing in a cost-efficient manner, further enhancing the trust of data subjects.** As a statement of conformity, a GDPR certification makes the processing activities more transparent and comprehensible for the data subjects by guarantying that their data is being handled with an appropriate level of security and implementing data protection by-design and by-default principles. Furthermore, a certification that attests to such accountability improves B2B relations and market access, instigates trust in international data transfers, and its aggregation helps meet GDPR due diligence requirements when contracting third parties.

3.2.4 Recommendation (3)

As mentioned in the previous paragraphs**, the project-oriented guidelines for GDPR Compliant User Experience need to be continuously updated in order to adequately reflect the constantly evolving data protection regulatory field.** The deliverable aims at serving as a "roadmap" for data controllers and processors to either execute data protection impact assessment or ensure GDPR compliance. Even though the sole adherence to the guidelines cannot resolve the market segmentation attributed to the distinct complementary Member State requirements, they can serve as a unified minimum standard for compliance.

[11] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163

[12] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en

3.2.5 More details

For more details see the relevant deliverables:

- Deliverable D3.6: Guidelines for GDPR Compliant User Experience

3.2.6 Target audience

- European Commission DG CONNECT
- ENISA
- European Cybersecurity Competence Centre
- EU Parliament
- European Data Protection Board

3.3 Encourage adoption of security and privacy by design

3.3.1 Background

Privacy is currently being provided as a software add-on where users must configure it themselves, which is unreasonable. Researchers and industry must work together to devise products that make privacy and security features transparent, preventing citizens from having to worry about them while being confident that their data is adequately protected by design.

The idea of privacy and security by design recognises the importance of incorporating privacy and security principles within the design, operating and management processes of organisational systems, to attain a frame of integral protection regarding data protection and security. It also promotes the adoption of the foundational principles of privacy by design as defined by Ann Cavoukian[13] and incorporated in ENISA's "Privacy and Data Protection by Design – from policy to engineering" report[14]. In a similar spirit, the "Resolution on Privacy by Design"[15] invited data protection authorities "to actively work on and promote the inclusion of privacy by design in policies and legislation on data protection within their respective States".

This is a priority. Today's top digital services are all coming from US companies storing, in several cases, European users' data on US servers. Needless to say, this data is subject to US law, not EU law. Therefore, it would be an additional guarantee (and an encouraging sign) for EU citizenry to have some good, well-designed solutions coming from "home", not from the other side of the world.

We underline the necessity of security and privacy by-design in solutions, considering that both are complementary, through the following principles and guidelines:

- The processing or transmission of privacy-sensitive data must be compliant with the protection of data regulations.
- The GDPR introduced the obligations to report security incidents for Trust Service Providers. The assessment criteria and the set of information to be provided are defined in the ENISA Guidance on Incident reporting[16] for eIDAS.

3.3.2 Recommendation

The adoption of security and privacy solutions from the perspective of usability must be approached as a multi-dimensional problem, where different dimensions have to be addressed. The recommendation is that funding be made available for the development of tools:

- for end-users that enable security and privacy by design to simplify access, update or deletion of data, with a special focus on the management of access policies,
- for guidance and learning for users and professionals; and
- used by professionals to analyse whether solutions are secure and private by design and how they can be improved in those respects.

[13] https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
[14] "Privacy and Data Protection by Design – from policy to engineering". ENISA. January 12, 2015
[15] https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf
[16] https://www.enisa.europa.eu/publications/technical-guideline-for-incident-reporting

3.3.3 More details

For more details see the relevant deliverables:

- Deliverable D5.2: Specification and Set-up Demonstration case Phase 1
- Deliverable D5.3: Validation of Demonstration Case Phase 1
- Deliverable D5.4: Requirements Analysis of Demonstration Cases Phase 2
- Deliverable 3.16: Security Requirements and Risks Conceptualization (no published version yet)

3.3.4 Target audience

- European Commission DG CONNECT
- ENISA
- European Cybersecurity Competence Centre
- EU Parliament
- European Data Protection Board
- National agencies and bodies in charge of directives and control of privacy and data protection

3.4 Encourage "blue sky" research in cybersecurity

3.4.1 Background

Research is guided by funding opportunities, often provided by large institutions. The EU provides research funding for several different scientific disciplines, and these funds are distributed through structured calls that provide very well-defined lists of requirements for the proposed research. In contrast to these structured calls, the EU used to provide a track, called FET (Future and Emerging) Open[17], which was entirely open. That is, researchers may come with their own scientific problems, that do not adhere to any call requirement, and request funding. The idea was to promote highly sophisticated, blue-sky research, the impact of which may be very significant in the upcoming years.

During a recent panel, *The Future of Cybersecurity*[18], there was a discussion on how to approach future directions in research around cybersecurity. Apparently, advances in cybersecurity progress happen fast and cover, year by year, many entirely different new domains. Traditionally, we had the common types of security applied on systems and networks, but now we have AI, the IoT, blockchains, new network designs, such as 5G, etc.

This is evident if we try to assess what has changed in the last five years in cybersecurity. We can all see cybersecurity incidents in the daily news, we can see the consequences of the lack of cybersecurity in so many applications, from every-day commuting and traveling abroad to our health systems and to emerging technologies, such as self-driving vehicles. Therefore, with the pace with which more security-critical applications are entering our everyday life, it is useful to invest in more blue-sky research for cybersecurity, that will address our cybersecurity needs of the future. The discussion on how to approach the requirements of funding research for cybersecurity, which advances too fast, had the following recommendations.

3.4.2 Recommendation (1)

Create an "EIC PathFinder" for Cybersecurity: It is possible to form a collaboration between EIC Pathfinder or a similar research line and the research community to support "blue sky" research in the future challenges of cybersecurity.

3.4.3 Recommendation (2)

Restructure Funding: A good architecture of European funding may consist of blue-sky individual projects under the ERC, plus a large number of collaborative EIC Pathfinder in strategic areas of cybersecurity – that could also network the results stemming from the ERC – complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

[17] https://ec.europa.eu/programmes/horizon2020/en/node/791

[18] https://cybersec4europe.eu/wp-content/uploads/2020/03/D10.1-Clustering-results-and-SU-ICT-03-project-CONCERTATION-conference-year-1.pdf page 42

Essentially, by refocusing existing EU funding schemes, like the EIC Pathfinder and the ERC, we can accelerate the production of practical research in cybersecurity that can address our needs for the future.

3.4.4 More details

For more details see the relevant deliverables:

- Deliverable D10.1: Clustering Results & SU-ICT-03 Project Concertation Conference Year 1

3.4.5 Target audience

- European Commission DG CONNECT
- ENISA
- European Cybersecurity Competence Centre
- EU Parliament

3.5 Support the development of new solutions for securing autonomous maritime vessels

3.5.1 Background

Maritime transport is an important driving force of the EU economy. In particular, maritime transport engages operators that utilize critical infrastructures related to inland, sea and coastal passenger and freight water transport, port facilities and vessel traffic services, which have been characterised according to the NIS Directive and the NIS 2 proposal, as "Operators of Essential Services". Considering the high impact of maritime transport on the EU economy, it is highly important to invest in the protection of critical EU maritime infrastructures to maintain their security and thereby ensure the sector's preparedness and resilience.
From another point of view, the lockdown measures in various Member States due to the Covid outbreak, the growing impact of the Omicron and Delta variants, has increased the trend towards teleworking in maritime transport. Regardless of the difficult pandemic situation, the show must go on: commercial vessel operations must continue with the shipment of passengers and goods, while a lot of on-ship inspections and maintenance must be done remotely.
The effort of increased digitalisation in maritime transportation within the last couple of years, points to autonomous and semi-autonomous ships as the maritime transport means of the near future, where autonomous ships are seaborne vessels that transport freight over navigable waters with or without limited human interaction. The communication architecture of the autonomous passenger ship (APS) enables communication in its operational context through a heterogeneous group of different technologies. It enables the APS to perform ship-to-shore communication with a remote-control centre (RCC) to carry remote navigation and control functions. In addition, it enables ship-to-ship communication to support safe navigation functions and emergency communication to carry out emergency navigation and control functions by an emergency control team (ECT).

However, the large deployment of emerging technologies on such systems (i.e. IoT-enabled maritime navigational systems, collision avoidance systems, cargo management systems and infotainment systems) increases the cybersecurity threat landscape in maritime transport (e.g. code injection, tampering and modification, GPS spoofing, AIS spoofing, signal jamming, communication link eavesdropping and disruption, APT attacks such as ransomware attacks), because these technologies are not yet fully secure for use in the maritime environment.

In view of guiding maritime transport operators to invest on policies that could increase their defense to these emerging threats applying on sectoral infrastructures, such as autonomous and semi-autonomous vessels, the following recommendations are provided aiming to:

- improve the security of their communications (i.e., vessel-to-port, port-to vessel, vessel-to-vessel)
- increase their preparedness and resilience by adopting security solutions and utilizing techniques which promote the early identification and assessment of cyber threats and risks that can be found particularly on maritime critical infrastructures.

The proposed policy recommendations are derived from specific evidence that came from the various technical activities conducted during the current project as a means to address prominent maritime security challenges.

3.5.2 Recommendation (1)

- **Improve secure maritime communications**:
  - Strong and efficient encryption to ensure safeguarding of data amid maritime communications (e.g. encrypt AIS messages in satellite communication)
  - Highly secure and efficient communication protocols for the protection of control and monitoring channels can be utilised in autonomous/semi-autonomous ships and submarines.
  - Satellite connectivity for data management.
  - Improve global navigation satellite system (GNSS) security, by encouraging the application of GNSS signal authentication to verify the authenticity of the information and corresponding source and the adoption of cryptographic spoofing defense techniques.
  - Physical protection measures where unmanned equipment is in use.

3.5.3 Recommendation (2)

- **Focus on the early identification and assessment of cyber risks and threats appearing in such architectures**:
  - Use methodologies from the tactical to the strategic level to maximize the effectiveness of assessment for decision making.
  - Development of innovative decision support systems for maritime security, involving different communities; integrating of decision support tools in operational environments (i.e., in legacy systems); research efforts in artificial intelligence applicable to security decision support systems.
  - Apply war game methodologies supported by tools to test threat scenarios and conflict situations that apply specifically to maritime transport systems in order to support the decision-making process and handle potential cybersecurity events that reside in autonomous and semi-autonomous vessels.
  - Utilise adaptive and dynamic threat modelling and risk assessment methodologies specifically tailored to the needs of the maritime transport sector.

3.5.4 More details

For more details see the relevant deliverables:

- Deliverable D4.4: Research and Development Roadmap 2

3.5.5 Target audience

- European Commission DG CONNECT
- ENISA
- European Cybersecurity Competence Centre

4 The Reactive Approach

Between M18 and M26, CyberSec4Europe researchers received several invitations to contribute[19] to various policy-related activities. Some of these are included below.

4.1 Cyberwatching.eu Roadmap

The project contributed to the roadmap[20] prepared by cyberwatching.eu:


Home » D4.7 EU Cybersecurity & Privacy Final Roadmap

D4.7 EU CYBERSECURITY & PRIVACY FINAL ROADMAP

This deliverable summarises and shares the key points of the significant deliverables with the cyberwatching.eu project, especially those that are relevant for the roadmap. As such, this deliverable is thus the culmination of the project work for cyberwatching.eu and can be used as a building block for further efforts after the project is complete.

Attachment:

D4.7_EU-Cybersecurity-&-Privacy-Final-Roadmap_v1.0Final.pdf

4.2 ECSO – The European Cyber Security Organisation

The project contributed to ECSO's policy document on the research priorities for Horizon Europe as follows. Indeed, the project proposed two major research priorities:

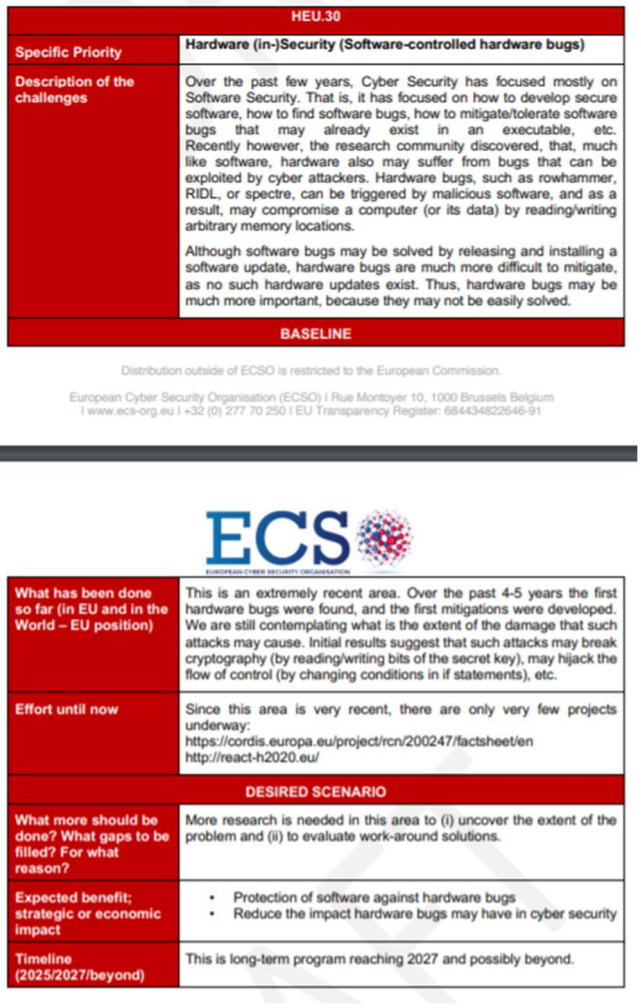
- Software-controlled hardware bugs

[19] Note that in some cases the participants were invited as representatives of the CyberSec4Europe project and in other cases they were invited in their personal capacity as experts in the area. This is because some events invite projects (such as the concertation events) whereas other events invite experts. Similarly, some bodies (such as ENISA's Advisory Group) invite people *ad personam* as experts – they do not invite organisations or projects. For the purposes of this document, we do not make any distinction.

[20] https://cyberwatching.eu/d47-eu-cybersecurity-privacy-final-roadmap

- This is a new family of exploits that uses software to trigger errors that may exist in hardware

- Software hardening
  - i.e. how to make software more robust against exploitations and attacks



HEU.30	
Specific Priority	**Hardware (in-)Security (Software-controlled hardware bugs)**
Description of the challenges	Over the past few years, Cyber Security has focused mostly on Software Security. That is, it has focused on how to develop secure software, how to find software bugs, how to mitigate/tolerate software bugs that may already exist in an executable, etc. Recently however, the research community discovered, that, much like software, hardware also may suffer from bugs that can be exploited by cyber attackers. Hardware bugs, such as rowhammer, RIDL, or spectre, can be triggered by malicious software, and as a result, may compromise a computer (or its data) by reading/writing arbitrary memory locations. Although software bugs may be solved by releasing and installing a software update, hardware bugs are much more difficult to mitigate, as no such hardware updates exist. Thus, hardware bugs may be much more important, because they may not be easily solved.
BASELINE	

ECS
EUROPEAN CYBER SECURITY ORGANISATION

What has been done so far (in EU and in the World – EU position)	This is an extremely recent area. Over the past 4-5 years the first hardware bugs were found, and the first mitigations were developed. We are still contemplating what is the extent of the damage that such attacks may cause. Initial results suggest that such attacks may break cryptography (by reading/writing bits of the secret key), may hijack the flow of control (by changing conditions in if statements), etc.
Effort until now	Since this area is very recent, there are only very few projects underway: https://cordis.europa.eu/project/rcn/200247/factsheet/en http://react-h2020.eu/
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason?	More research is needed in this area to (i) uncover the extent of the problem and (ii) to evaluate work-around solutions.
Expected benefit; strategic or economic impact	• Protection of software against hardware bugs • Reduce the impact hardware bugs may have in cyber security
Timeline (2025/2027/beyond)	This is long-term program reaching 2027 and possibly beyond.

HEU.05 Software Hardening

HEU.05	
Specific Priority	**Software Hardening**
Description of the challenges	Most of the recent cyberattacks usually depend on some kind of programming error (usually called "bug" in the colourful language of computers), which, when exploited, may give control of the execution to the attacker, compromising in this way the victim computer. Buffer overflows, heap overflows, dangling pointers, etc. have all been used in the past to hijack the program's execution and enable the attacker to gain control of the victim computer with no explicit user interaction. One might think that we can find these software bugs through an ordinary "debugging" process. Unfortunately, it is not easy to find these software bugs, since by definition, they are mistakes made inadvertently by computer programmers, and thus they are not known. One way to deal with these unknown bugs is to "harden" the executable so that when/if the bug is triggered it will not allow the attacker to compromise the computer. Hardening should not introduce significant performance overhead. The approach software hardening takes is the following: "We do not know what the bug is, but we can make sure than when/if it is triggered, it will not compromise the computer.
BASELINE	
What has been done so far (in EU and in the World – EU position)	This is a very recent area. Although the initial ideas may be traced back to the 80's, real work in the area has blossomed only in the past decade, after the realization that software security is much more difficult that what we originally thought.
Effort until now	Since this area is very recent, there are only very few projects underway: https://www.cybersec4europe.eu/ http://react-h2020.eu/
DESIRED SCENARIO	
What more should be done? What gaps to be filled? For what reason?	We need to do more research in order to understand the potential and cost of software hardening. In effect we need to see how we can move the software prototypes out of the lab and into the real market.
Expected benefit; strategic or economic impact	• Protection of software against unknown bugs with low performance overhead • Reduce the financial impact of zero-day attacks since zero days will not be able to compromise the victim computers

4.3 Center for European Policy Studies

4.3.1 Artificial Intelligence and Cybersecurity

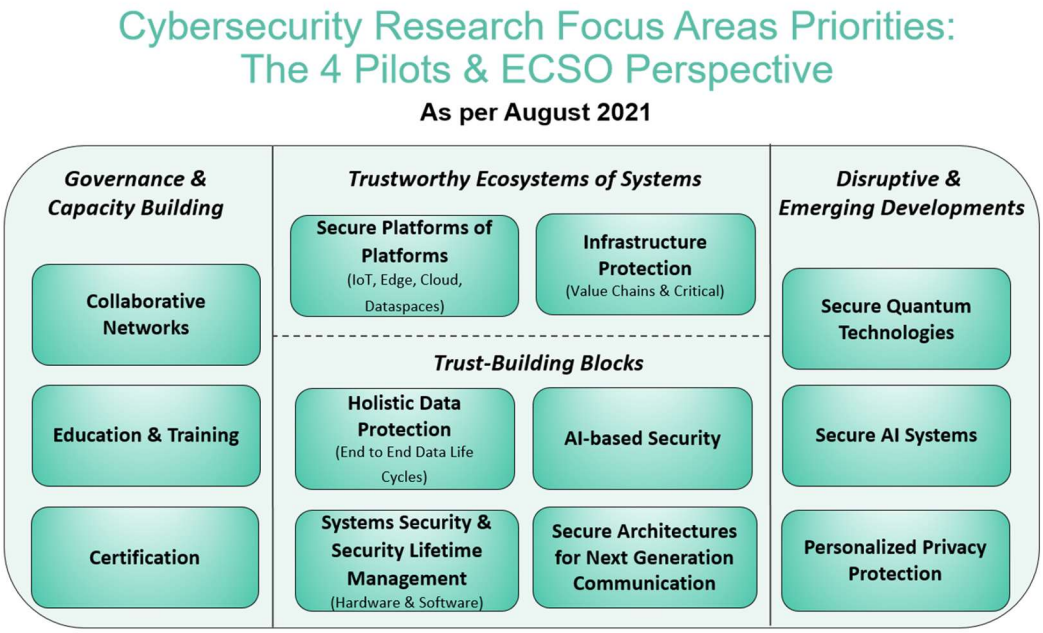
CS4E member Afonso Ferreira was the rapporteur of the report on "Artificial Intelligence and Cybersecurity - Technology, Governance and Policy Challenge"[21] published by CEPS, the Centre for European Policy Studies, a Think-Tank based in Brussels.
CEPS launched a Task Force on Artificial Intelligence and Cybersecurity[22] in the autumn of 2019, to consider the technical, ethical, market and governance challenges posed by the intersection of AI and cybersecurity. The resulting report contributes to EU efforts to establish a sound policy framework for AI, more specifically by:

- providing an overview of the current landscape of AI in terms of beneficial applications in the cybersecurity sector and the risks that stem from the likelihood of AI-enabled systems being subject to manipulation
- presenting the main ethical implications and policy issues related to the implementation of AI as they pertain to cybersecurity
- proposing constructive and concrete policy recommendations to ensure that the rollout of AI is secure, according to the objectives of the EU's digital strategy.

4.4 Roadmapping Focus Group

The four pilot projects along with ECSO have formed a working group (WG) on roadmapping. This WG has created a set of important research directions in the area of cybersecurity. These directions have been communicated to the JRC (Joint Research Centre) of the European Commission as well as to several other EU bodies. CyberSec4Europe has been a leading contributor to this WG and the research priorities.

[21] https://hal.archives-ouvertes.fr/hal-03417316/
[22] https://www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity-2/

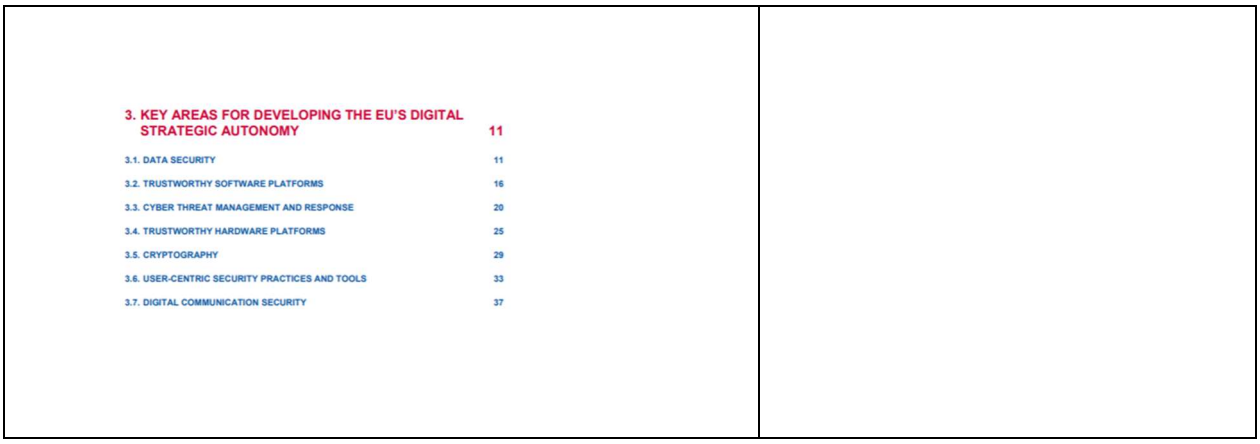


4.5 ENISA

4.5.1 Cybersecurity Research Directions for the EU's Digital Strategic Autonomy

In April 2021 ENISA published a deliverable outlining some of the important research directions that contribute to EU's Digital Strategic Autonomy[23]. CS4E member Evangelos Markatos (leader of CyberSec4Europe WP4) was a co-author of this document. Markatos, along with other CyberSec4Europe members (including Kai Rannenberg, Afonso Ferreira and Elias Athanasopoulos) contributed to this document.

[23] https://www.enisa.europa.eu/news/enisa-news/exploring-research-directions-in-cybersecurity



The report identified several important research areas:

1. Data security
2. Trustworthy software platforms
3. Cyber threat management and response
4. Trustworthy hardware platforms
5. Cryptography
6. User-centric security practices and tools, and
7. Digital communication security

4.5.2 The year in review

CS4E member Christos Douligeris contributed to this deliverable[24] with the **key findings** regarding the following security threats in 2020: (a) malware, (b) phishing, (c) spam, (d) insider threat, (e) physical manipulation/damage /theft/loss, (f) information leakage, (g) identity theft, (h) cryptojacking, (i) ransomware, and (j) cyber espionage.

4.5.3 Sectoral and thematic trend analysis

Douligeris also contributed[25] with data of **contextualised cyber threat intelligence (CTI)** for the aforementioned security threats (4.4.2(a) to 4.4.2(j)) in 2020 per sector. The report contains an additional thematic trend analysis, based on the incidents trend per sector.

4.5.4 Emerging trends

Douligeris contributed[26] **emerging trends** regarding the challenges and the attack vectors for the aforementioned security threats (4.4.2(a) to 4.4.2(j)), as reported in 2020.

[24] ENISA Threat Landscape - The year in review https://www.enisa.europa.eu/publications/year-in-review
[25] ENISA Threat Landscape 2020 - Sectoral/thematic threat analysis https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis
[26] ENISA Threat Landscape - Emerging trends https://www.enisa.europa.eu/publications/emerging-trends

4.5.5 Main Incidents in the EU and worldwide

Douligeris contributed[27] data regarding the **incidents timeline, most targeted sectors, important findings per threat, emerging and most active actors, and attack vectors** for the aforementioned security threats (4.4.2(a) to 4.4.2(j)), as reported in 2020.

4.5.6 List of top 15 threats

Douligeris contributed[28] a full report for the aforementioned security threats (4.4.2(a) to 4.4.2(j)) in 2020.

4.5.7 ENISA Threat Landscape 2021

Douligeris contributed[29] a full report regarding the **major findings, the incidents and trends, the recommendations, and the threats anatomy based on the MITRE ATT&CK knowledge base**, for the following security threats in the period April 2020 to mid-July 2021: (a) ransomware, (b) e-mail related threats, and (c) threats against data.

4.5.8 Security Framework for Trust Service Providers

CS4E member Hans Graux supported the drafting of this framework report for ENISA, specifically by providing guidance on the legal possibilities for imposing security obligations on trust service providers under Article 19 of the eIDAS regulation. This required an assessment of the lower degree of standardisation for non-qualified trust service providers under the regulation, so that the approach should be based on security best practices, rather than binding legal obligations. The report addressed general risk management, incident management, and recommended security measures.

4.5.9 Conformity assessment of qualified trust service providers

Graux also provided legal inputs to the report, which gives an overview of the conformity assessment framework for qualified trust service providers as defined in the eIDAS regulation. This process generally aims to confirm that the assessed service or service provider fulfils the legal requirements of the Regulation, including in terms of security. This report discusses the typical process flow and the methodology used to perform conformity assessments. For each phase of the assessment, guidance is provided to the affected service providers.

4.6 Other contributions

CS4E partner CYBER has been interacting with the Estonian government and the European Commission (Director General Roberto Viola) on the upcoming revision of the eIDAS regulation (The European Digital Identity Framework Proposal (EUid)[30], stressing the importance of technology neutrality while maintaining a high level of information security.

---

[27] ENISA Threat Landscape 2020 - Main Incidents https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

[28] ENISA Threat Landscape 2020 - List of top 15 threats https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

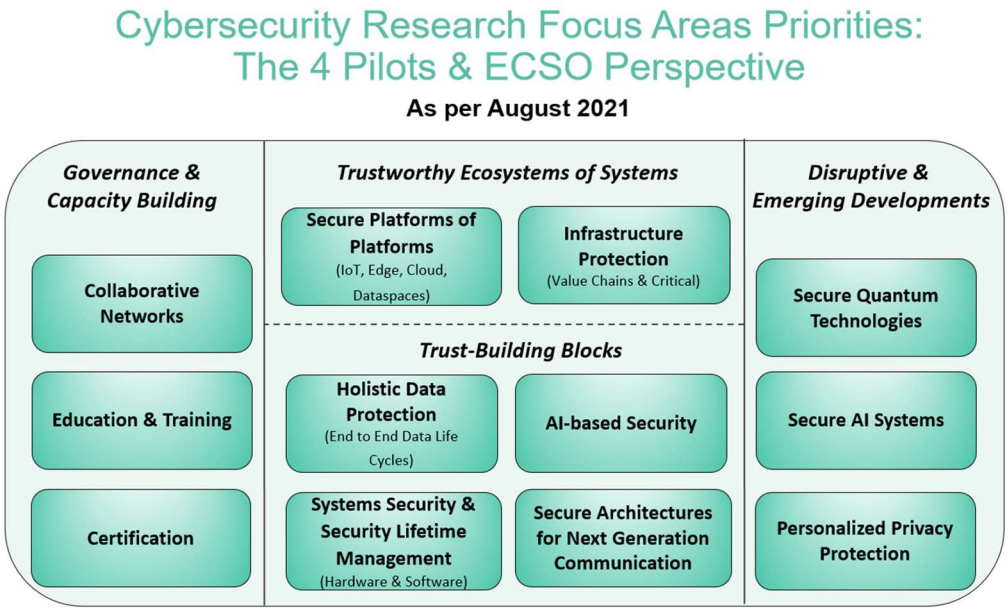
[29] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[30] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-eid/09-2021

5 Summary – Recommendations

5.1 Summary

CyberSec4Europe plays a very active role in helping policymakers formulate the policies that will shape the future of the EU and the Member States. To provide effective policy recommendations, CyberSec4Europe follows a two-pronged approach.
Following the first *reactive* approach CyberSec4Europe members receive and accept invitations to provide recommendations in several fora, including workshops, concertation meetings, EU-level organisations, etc. Such organisations include ECSO (the European Cyber Security Organisation), JRC (the Joint Research Centre), and ENISA (the EU Agency for Cybersecurity). One of the most notable policy recommendations includes the list of research priorities in the area of cybersecurity which was delivered by CyberSec4Europe (in collaboration with the other three pilots and ECSO) to JRC and was picked up later by ENISA. These priorities are:



5.2 Recommendations

Following the second *proactive* approach, the CyberSec4Europe members acknowledge that much of the work already performed in the project may essentially create contributions that are practically policy recommendations. In this deliverable we collect these contributions, phrase them as policy recommendations and provide evidence that underlines their importance.

Some of the policy recommendations that stand out include:

- **Recommendation 1: <u>Ensure the active engagement of the European cybersecurity communities in the implementation of EU Regulation 2021/887</u>**
    - The overall recommendation here is to go beyond the structure outlined in the regulation and to facilitate better visibility and communication between the wide

range of local communities nationally and supranationally; and to ensure that the governance model of the NCCs encourages and facilitates the functioning and participation of local communities.
    - The participation of the community in the decision about the members of the Advisory Group as well as guidelines for the involvement of the Advisory Group in decisions of the Governing Board, for example in its rules of procedure, are strongly recommended.
    - This recommendation opposes a one-size-fits-all approach and proposes that CHECK (Community Hub of Expertise in Cybersecurity Knowledge) initiators establish both topic-specific and sector-specific CHECKs, as well as regional CHECKs, provided that basic requirements for the establishment of a CHECK are met.
    - This recommendation proposes that the process for creating CHECKs should be uniform at the European level.
- **Recommendation 2: Create a harmonisation strategy for GDPR compliance among Member States**
    - It is recommended that the relevant stakeholders continue to address their national authorities, raising concerns related to the need for the further harmonisation of the GDPR across Member States and seeking clarification whenever possible
    - The project-oriented guidelines for GDPR Compliant User Experience need to be continuously updated in order to adequately reflect the constantly evolving data protection regulatory field.
- **Recommendation 3: Encourage adoption of security and privacy by design**
    - The adoption of security and privacy solutions from the perspective of usability must be approached as a multi-dimensional problem, where different dimensions have to be addressed and funding should be made available for the development of the relevant tools
- **Recommendation 4: Encourage "blue sky" research in cybersecurity**
    - A good architecture of European funding may consist of blue-sky individual projects under the ERC, plus a large number of collaborative EIC Pathfinder projects in strategic areas – that could also network the results stemming from the ERC – complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

5.3 Next Steps

The project has planned various activities through which these policy recommendations can be disseminated. These include traditional dissemination through the project's dissemination channels (such as website, social media, etc.), the upcoming CONVERGENCE event and various other topical events. Specifically, we are going to highlight a recommendations page on the project website, accessible directly from the home page.

5.4 Concluding Remarks

CyberSec4Europe, through a combination of proactive and reactive approaches, proposes policy recommendations that focus on (i) supporting research in the area of cybersecurity (ii) restructuring of the funding schemes, (iii) supporting the implementation of GDPR, and (iv) mobilizing of the

cybersecurity community in Europe. CyberSec4Europe policy-related work will continue to involve the relevant stakeholders both from within as well as from without. Being a cutting-edge research project, CyberSec4Europe is in a unique position to provide advice and recommendations in the area of research and help policy makers make the right decisions that can propel Europe in the lead of the world-wide cybersecurity ecosystem.

Annex I: Policy-related considerations (by Deliverable)

I.1 Deliverable D2.2: Internal Validation of Governance Structure

Various implications for how the governance model should look like have been extracted in the deliverable, for example combination between R&D with capability-building, policy interventions or funding activities (national and regional), and challenges such as insufficient collaboration between academia and industry or the lack of focused investment from the public and private sectors, have been highlighted. These could be link to Digital Europe program, as this program aims to support creation of national and regional cybersecurity "hubs".
In this deliverable we came to a conclusion that "one size does not fit all" and that it is important to differentiate at least two types of CHECK, namely one that is an economic actor in the cybersecurity landscape and must be sustained by a sound business model, and another that is part of the public administration and financed as a public good. We can also understand these two basic models as "top-down" and "bottom-up" models, but man other CHECK dimensions have been discussed (national versus regional, sector-specific versus technology specific etc). Governance issues related to the interaction between these "hubs" at national and EU level remains one of the challenges.
Alignment between EU, national and regional interests or research agendas should find place on a regular basis. Once active, EU Cybersecurity Competence Centre (ECCC) and the National Centres should interface with many forms of "community hubs", including recently activated European Digital Innovation Hubs (EDIHs), which follow model similar to CHECKs. Interfaces at different levels (sectorial such as financial sector, technology such as IoT cybersecurity, capacity building such as start-up support etc) would thus be necessary to achieve coordinated approach, to avoid any kind of duplication in structure and to limit overlaps.

I.2 Deliverable D2.3: Governance Structure v2.0

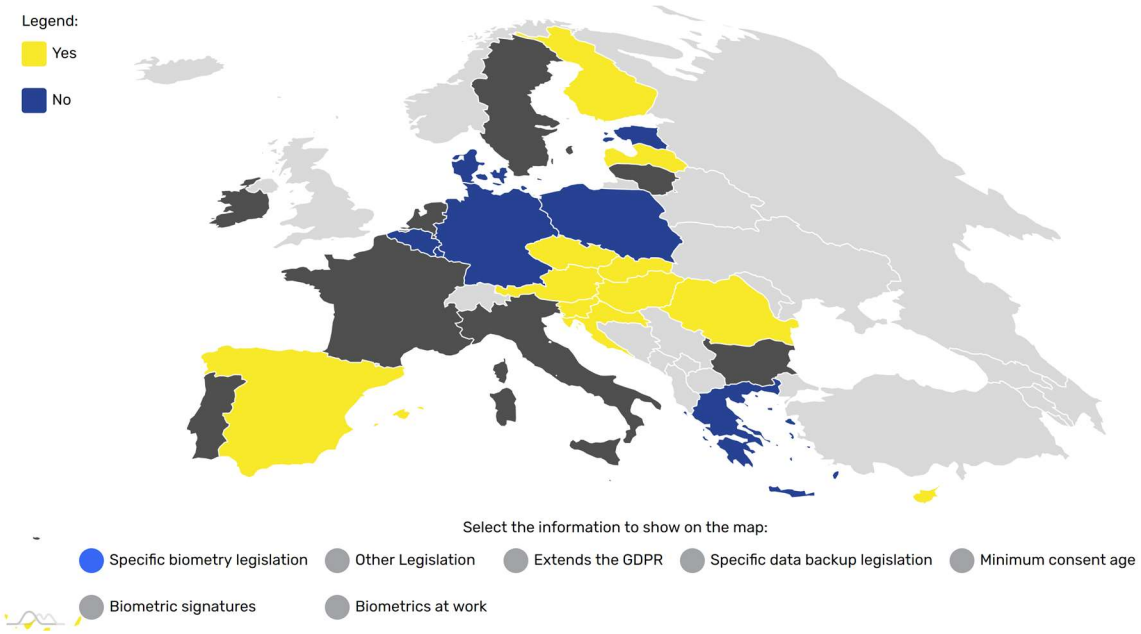
The findings in this deliverable (also in combination with the preliminary work done in D2.1) contain relevant legal assessments, evaluation of existing governance structure types and founded suggestions for ways to activate and organize the cyber community. These findings could be used either for future versions of the new Regulation (EU) 2021/887 (the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres) and for Member States (and especially their National Coordination Centres) to get in touch with and organize their stakeholders and local communities. In a greater context this is also relevant for the Horizon Europe Program and the Digital Europe Program.
The evaluation of existing governance structures (Chapter 2) identified certain strengths and weaknesses of governance types. The most promising structure design to avoid weaknesses in a network is a combination of top-down and bottom-up structures. This allows for the needed formal stability and at the same time does not suffocate stakeholder and community engagement, which is crucial to keep the cybersecurity network agile and up to date.
The idea to organize the community in CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge), which has initially been in introduced in D2.1 already, has been investigated deeper for D2.3 (Chapters 3 and 4). The interview campaign lead by the IRIT team suggests that the keys to the necessary stakeholder commitment lay in the possibility of active involvement, confidence in their collaboration partners and the existence of benefits from their contribution. This

observation is in line with the findings from the evaluation of existing governance structures and thus backs the conclusion to combine top-down and bottom-up elements. At the same time, the general concept of CHECKs is flexible enough to allow for different set-up types and can be adapted to the needs of the community e.g. in certain regions, for certain topics or sector related (Chapters 4., 5.2.1 and 5.2.4).
CHECKs are a necessary community driven bottom-up element besides the Competence Centre and the Network of National Coordination Centres and can provide significant added value. CHECKs forming a sub-network will encourage and accelerate the knowledge exchange between CHECKs, i.e. the Community, and thus also accelerate dissemination activities towards other stakeholders as well as National Coordination Centres and the Competence Centre (Chapters 5.2.1 - 5.2.5). CHECKs could also contribute to the European Cybersecurity Atlas (Chapter 5.2.7).
Reasonable funding options are crucial for the successful establishment of CHECKs (Chapter 5.2.6). On the long run CHECKs could generate the necessary means by taking on e.g. consultation, education or research assignments or could apply for EU, national or regional calls. However, the creation and implementation period of new CHECKs needs some attention in regards of stakeholders being most cautious on a return on their investment (human resources, time, money). Public funding during this period therefore seems of high importance to push the development of new CHECKs and overcome the set-up and trust-building phase.

Regulation (EU) 2021/887 has been created on the insight, that a wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union, but needs to be pooled, networked and used in a more efficient manner. Besides the Competence Centre and the National Coordination Centre the Regulation therefore also aims at the establishment of the Cybersecurity Competence Community. However, the Regulation necessarily stays abstract in this point and the Community cannot be established by legal order. Instead, you need to motivate possible members to form this Community and contribute to it voluntarily. Based on stakeholder viewpoints, the observation of different network governance approaches and also legal considerations our deliverable suggests the concept of CHECKs to create and organize a vivid and strong community. To summarize: the Cybersecurity Network of Regulation (EU) 2021/887 needs vivid participation of the Cybersecurity Community which can be created and organized by CHECKs.

I.3 Deliverable D3.6: Guidelines for GDPR Compliant User Experience

Lack of harmonization across the Member States is hindering cross-border markets. The consequences are market entry obstacles because different markets require different functions of products and services or even their disablement for compliance reasons. This is rising development costs and making some (smaller) markets unappealing. Simple examples are different GDPR ages for consent, various limitations for the use of biometrics.
We have created a map of with the visualization of heterogeneity. Use it as a baseline to foster future harmonization efforts. When planning the harmonization strategy, please consider that some issues could be solved using technology – a trusted, computer-readable registry of rules/requirements could solve simpler, but common and most prevalent issues of cross-border compliance efforts and alleviate EU enforced regulation concerns. Also, please consider adding more requirements in the regulation that are not only constraints but focused on specific permits, e.g. a specific requirement that some form/function of a product or service must be allowed in all Member States.



I.4 Deliverable D3.3: Research Challenges and Requirements to Manage Digital Evidence

The number of false positive threats needs to be reduced in order to address alarm fatigue with security professionals, thus creating the need to increase the quality of shared threat information and thus to apply more appropriate analysis techniques with lower error rates.
It is vital to reduce the time needed to detect threats, as new solutions are needed to collect and analyse collaborative threat information beyond the typical sharing of compromise indicators intended primarily for human operators.
Threat intelligence needs better contextualisation to be able to analyse data from different sources of information, using open source intelligence services and similar services to enrich the context of the data during analysis.
An open challenge is the availability of enabling technologies that can help increase trust between producers and consumers of threat information and platforms to overcome the reluctance to share sensitive information.

It is vital for effective joint threat intelligence to define new strategies, methodologies and formats for storing and interpreting the digital evidence to improve the efficiency and flexibility of the analysis.

There is a need for cyberthreat analysis and digital investigation techniques that protect the use of privacy-enhancing techniques, such as encryption, against the misuse of information and privacy breaches.

The challenge is to put in place mechanisms to adequately inform all the different cooperating entities in the threat intelligence ecosystem, defining the need for new solutions that are flexible

enough to facilitate the interpretation and understanding of the context by different experts and stakeholders.

An open issue for the successful adoption of AI in security applications is to enhance the robustness of machine learning and deep learning models to reduce the attack surface of security applications.

I.5 Deliverable D3.10: Cybersecurity Outlook 1

This deliverable can be used by policymakers as food for thought since it is a report on the latest advances of some emerging topics and ideas in the cyber-security field. Being aware of what are the cutting-edge technologies and the current research trends can be useful for defining policies that are both viable and practical using state-of-the-art software and hardware instead of relying solely on more traditional, and usually more limited, approaches. The deliverable can also be used for new call for proposals since the topics that we explored are promising to reshape the cyber-security field, thus they can easily become a core element in new projects proposed by the various EU calls.
Some recommendations may be:

- **Save logs and traffic for training machine-learning models**. Many companies are starting to integrate machine-learning techniques in their products for detecting a wide variety of threats. These techniques have proven their reliability and quick response time in detecting complex network attacks and new types of malwares that can be challenging to recognize with more traditional approaches. The downside of these technologies is that they can require a vast collection of data for their training phases. Thus, for the policy makers, it is important to stress in the best practices to keep the logs and entire traffic captures not only for historical and legal purposes, but also for eventually training machine-learning models.
- **Securely store logs and traffic to avoid poisoning attacks**. Logs of past events and traffic captures must be stored safely and their integrity must be correctly safeguarded, especially if this data can be potentially used later for training a set of machine-learning-based tools. Several data set poisoning attacks can be used to maliciously steer the classification abilities of several machine-learning models.
- **Plan replies to decrease automatic learning of AIs**. Artificial intelligence techniques are starting to become also powerful allies for attackers to produce large scale malicious activities in a (nearly) full automatic fashion, especially social engineering calls and phishing messages. To decrease the chance of success, the personnel should be aware that incoming calls, messages and interactions are not necessarily coming from human beings and that their answers can be used by a machine to retrain itself and become more accurate. As a result, replies, especially regarding potentially critical topics, should be adequately planned by the personnel and automatic answering tools should also be correctly designed and placed.
- **There is no standard regulating TEEs**. Trusted Execution Environments (TEE) are secure areas protected by the hardware itself. These technologies are a very promising approach to ensure a high (i.e. military) level of protection and many big players are actively working in this area (e.g. Intel, AMD and ARM). However, every vendor is

producing its proprietary solution and there is not yet a proper standard defining how a TEE should be implemented or its public interfaces. This is proving to be a barrier for creating an heterogeneous system of interconnected TEE using a multitude of different technologies and our deliverable can be a starting point for investigating the creation of a TEE standard.

- **Analyse and secure the entire SDN virtualization stack**. Cloud and virtualisation technologies are commonly used in deploying 5G infrastructures, however, several security risks and attacks have been frequently identified in various SDN implementations. Security of virtualised environments depends on a multitude of factors (the OSes, the hypervisors, the virtual machines themselves, etc.) that should all be considered to achieve more secure 5G networks.

Technology is continuously evolving and spreading its influence in our daily lives. New advances in secure hardware and artificial intelligence allow us to better protect our privacy and reacts to cyber-attacks faster than before. The investigations in our deliverables, however, has also proved that similar techniques can be used by attackers for a variety of malicious purposes (e.g. mounting attacks faster and doing massive social engineering campaigns). Of course, incentivising the adoption of state-of-the-art cyber-security technologies can help in reducing the effectiveness of several cyber-attacks. However, on the other hand, key personnel must be adequately trained to properly use these technologies and spot social engineering attacks.

I.6 Deliverables D5.2, D5.3, D5.4

EU efforts to ensure its citizens security and privacy are out of sync. Despite the EU efforts to boost its citizens' privacy via legislation (e.g., GDPR) and legal actions (e.g., heavily fining private companies with dubious practices), existing technologies are not good enough. For example, most of them avoid the obligation to be GDPR compliant by requiring users to consent to so called "Terms of Service" (often written in obscure legal language) in which users are asked to relinquish the ownership of their data. Few technologies are built with GDPR compliance – that is, privacy by design – in mind.

We need to establishing projects that promote privacy and security by design. Social media taught us that people do not understand privacy (in the cyber-world) at all. Currently, privacy is an add-on to software, and users have to configure it themselves, which is unreasonable. Researchers and industries must work together to come up with products that make privacy and security transparent. Citizens shouldn't worry about this or that setting; they should be assured that their data is protected adequately by the software, by design. This is a priority. If possible, a 100% European solution would be good. Today's top services are all coming from US companies storing users' data on US server. Needless to say, these data are subject to US law, not EU law. Therefore, it would be an additional guarantee (and an encouraging sign) for the EU citizenry to have some good, well-designed, solution coming from "home", not from the other side of the world.

I.7 Deliverable 6.3: Design of Educational and Professional Framework

The deliverable can be used by policy makers as

- a reference (such as for utilizing it in the security audit process related to professionals' education capabilities),

- visualization tool for any party (such as Cyber Security skill requirements posed to various job profiles),
- for the purpose of further use (such as adding to the existing evaluation results, or Cyber Security skill evaluation of a new work field or job profile), or
- for the purpose of further development work (such as enriching the framework itself with new skills, evaluation viewpoints etc.)

The most relevant parts of the deliverable are naturally the evaluation framework itself, and not just the results gained by it, but also the understanding of how many and variating are the Cyber Security skill capabilities needed in professions. Of course, this emphasizes, how important it is to invest in the quality education. The framework can be understood by as the means or tools to clarify the (perhaps complex) education needs of a Cyber Security professional, but can also be applied to a specific, non-technical field as well.
In order to accomplish and maintain the high level of Cyber Security education European-wise, we need tools to mobilize the education progress, as well as clarification about the context and factors around it. Our deliverable aims at understanding and visualizing the needs in the current environment. Our framework is a tool that can be expanded to serve different contexts of Cyber Security education of professionals. What is needed now is to maintain and strengthen the co-operation in this matter. Regarding co-operation with CyberSec4Europe and other projects in this context, we are active in the CCN education group, led by Felicia Cutas.

I.8 Deliverable D8.3: Cybersecurity Standardization Engagement Plan 2

Ensure that European Commission funding would continue to be set aside in order to enable the broadest participation of experts in cybersecurity standardization work. This should clearly be an objective within the funding structure of the Cybersecurity Competence Centre in Bucharest.

I.9 Deliverable D9.11: SME Cybersecurity Awareness Program 2

Small and Medium-Sized Enterprises (SMEs) represent a major part of the European economy. At the same, they are also the most vulnerable group to cybercrimes. Many past studies have shown that a large number of SMEs are not in a position to afford advanced and up-to-date security measures including cybersecurity awareness. Due to this, they either have to compromise with their security or depend on security technologies and services that are available mostly for free. In the latter option, however, their main difficulty is the availability of such security technologies and services that fulfill their needs and suit organizational culture. In the case of security awareness, we found out that a large number of organizations and projects both at regional (European) and national levels design, develop, and distribute awareness materials and resources for free. In contrast, SMEs complain about a lack of security awareness materials that meet their needs and suit organizational culture. We observed two major gaps in the existing research practices that upcoming programs should prioritize and include.

- Most security awareness materials and resources are not designed to meet the needs and organizational culture of SMEs. Considering the vast representation and contribution of SMEs to the European economy, the existing share they get in security and security

awareness research is inadequate. The upcoming programs are recommended to incorporate more security research specifically focusing on SMEs.

- With the existing dissemination methods or practices, projects and organizations producing security awareness materials and resources are capable of reaching largely to participating SMEs. When in fact, these security awareness materials and resources should have reached most (ideally all) applicable SMEs in the nation or region. We recommend the upcoming programs to include and also prioritize research on the dissemination/distribution channels (or technologies or paradigms) that would facilitate the producers of security awareness materials and resources (organizations and projects) to easily reach the most applicable SMEs. These channels at the same should also facilitate SMEs in finding security awareness materials and resources that best fit their needs and meet organizational culture.

I.10 Deliverable D9.12: Supply Chain Security Recommendations

Supply chain security comprises different security dimensions. With the advent and integration of new technologies, supply chain security is becoming more complex and expensive. It may not be an issue for large organisations to afford advanced and up-to-date security, but the supply chain also includes resource-constrained SMEs. Any compromise in the security of participating SMEs could jeopardise the whole supply chain and cause damage to other participants. But most existing security research works are focused on producing robust security solutions. We recommend the upcoming programmes not solely focus on supply chain security research but to produce economically viable security solutions that SMEs can afford and utilise.

I.11 Deliverable D10.1: Clustering Results & SU-ICT-03 Project Concertation Conference Year 1

The first Concertation Event of CyberSec4Europe entitled **Cybersecurity for Europe 2019**, which took place at the Hôtel de Région in Toulouse, from 13-15 November 2019 “. This first Concertation event– the first of three annual CyberSec4Europe consultation events - represented a unique opportunity to obtain a snapshot of the current state of play in policy, research, and innovation in European cybersecurity, while at the same time it provided an opportunity to listen to and meet high level political representatives discussing the challenges and opportunities in cybersecurity. The panels cover the following topics:

- Panel 1 – Cybersecurity Policy & Capacity Building
- Panel 2 – Recommendations for Cybersecurity Research & Innovation
- Panel 3 – European Cybersecurity Governance
- Panel 4 – Good practices in data sharing for incident handling
- Panel 5 – Who’s calling? Managing identities in the cyber world
- Panel 6 – The future of European Cybersecurity
- Panel 7 – The upcoming European Cybersecurity Competence Network: a conversation with the four pilots

- Panel 1: Cybersecurity Policy & Capacity Building

- **Cooperation**. Cooperation is key to succeed with policy challenges. It is crucial for member states to cooperate, as well as for the organizations and stakeholders at regional, national and European level. For that it is most important to have a common or at least a common strategy. If different strategies exist they should be coordinated. It is necessary that initiatives at the local level are visible. This is also their local responsibility. At the same time, they need to think big and consider how best practices on a local level can be transferred to national or EU level and what effect local best practices can have on larger ecosystems. Policy makers and managers at EU and national levels need to sense avidly the effect of their policy decisions.
- **An Interdisciplinary Approach with Diversity is a must.** It is essential to team up with people form academia, industry and policy to address the arising issues with people who have different expertise. To really understand all kind of threats, people from all different backgrounds are needed. This also includes gender diversity.
- **Enhancing European Competitiveness**. In Europe, the European civilizational values and the welfare of people are cherished. However, they cannot be taken for granted and need to be made sustainable. For this, it is is necessary to be competitive, i.e. in 5G, data management, artificial intelligence, etc. For this, the responsible sharing of data – while respecting the GDPR and privacy regulations in general– needs to be facilitated. To design and implement sharing of data in a responsible manner, help from cybersecurity experts is needed.
- **Attainable Certification for All.** As certification comes with costs, which might not be easy to cover for smaller players, such as SMEs, it is mandatory for its application needs to be well planned including financing models. Research can explore better solutions, however it is time for decisions, at least for trials for a limited time. This needs to include a spectrum of mechanisms from liability provisions to simple self-declaration by providers.
- **Important to be Working from the Design Stage**. In order to create solutions that are working for consumers and end users, it is important to consider perspective. Therefore it is useful to collaborate with designers, as designers know how to gather and incorporate end-user feedback throughout the whole development process.

- Panel 2: Recommendations for Cybersecurity Research & Innovation
  - **EU Regional ecosystems built into a European-scale ecosystem**. In Toulouse, home of Airbus, an ecosystem has been set-up in order to be independent. A hope / recommendation is that through the pilot hubs, the set-up of such an ecosystem is being built-up to address and contribute to an independent Europe.
  - **EU leadership in privacy-by-design.** USA has been very successful in its strategy for cysbersecurity. There is an opportunity for Europe to also be successful by respecting the privacy of the individual.
  - **Cybersecurity must be considered as an important component in all projects in all of the European funding programs.** Cybersecurity should be considered as part of every call, not just specific cybersecurity calls. All projects should have cybersecurity included and should be included within a vertical. European funding programs (such as H2020, DEP and other funding programmes) must ensure that cybersecurity is a component of all projects, e.g. health, financial, transport, critical infrastructure, etc.

- **Investment in cybersecurity**. Investment in cybersecurity in Europe is crucial. Europe is far (by a factor of 10) from what countries like USA and China are investing in cybersecurity. Europe needs to invest more in cybersecurity. There is a need to identify the kind of investments and a need to define the real priorities. Maybe an approach is to build 10 smaller airbus-type models in different sectors, e.g. in AI. Second, we do need investment because we have today the issue of 5G security. We are discovering what could have been discovered before. In Europe, we have not recognized that it is now the time to invest in this sector, in AI, blockchain, quantum. We need to invest in research right up to reaching the market level.
- **Cybersecurity industrial policy is necessary.** If Europe wants to be serious in cybersecurity, it is not only about the investment. The dynamics, the driving force, and the appropriate objectives need to be created. There should be a specific program in Europe on envisaging how we can make sure that there are new companies that can emerge in Europe. Focussing on research is insufficient. Think about industrialization in this realm.
- **Cybersecurity education should be a priority.** To have an outside perspective from the R&I bubble is extremely important. The best of EU is in education. The threat of USA is there. We need to plan on how to address this.

- Panel 3: European Cybersecurity Governance
  - **Governance has to be context related.** To remain open-minded with respect to governance, as different governance templates will be needed for different contexts (e.g. health, financial, Member States, etc.), including membership and structuring mechanisms and procedures, not forgetting to involve unusual stakeholders, for example, civil society, NGO's, and open source communities.
  - **Effective infrastructures for connection and cooperation.** To establish effective infrastructures for connection and cooperation, including research groups, connections to the wider community, and the need to go beyond individual interests.
  - **Common vision and mission promoting European values via hubs communities.** To federate in the hubs communities with a common vision and mission that promote the European values. Furthermore, the hubs should remain open and engage with effective strategies to build trust with the involved communities.
  - **Concentrate on innovative offers for demand driven services and capacity building offerings.** To concentrate the innovation offer on services, use cases, and capability building, that are demand-driven and oriented to serve the citizens. In this respect the hubs should engage SMEs and find the champions which can grow.
- Panel 4: Good practices in data sharing for incident handling.
  - **Real time reactive data sharing solutions.** The impact of cybersecurity has immediate impact in the digital world hence it is important that we have real-time and reactive data sharing.
  - **New tools for support data sharing and privacy**. Data sharing shows vulnerabilities and that is why it is important to have tools for cross-border sharing with privacy support.
  - **Machine learning tools to improve data management**. The increase in the size of shared data and transferred data, need to be made more manageable. Using machine-

learning, it is possible to find out which threats are more important and the order of sharing.
    - **Prevention based on resilience of the systems and predictive intelligence.** There is a need to work on automatic and diverse reactions to strengthen our defence before the attack happens. Work is needed on new domains like civil aviation for prevention by increasing the resilience in civil aviation and related stakeholders. Prevention needs to be covered in the entire system, including Air operation centers.
    - **Advanced analytics tools and for threat intelligence.** Research is needed in providing an adaptative security loop to cyber threats and new attack vectors. Solutions need to be timely, automated and able to adapt dynamically, and more tools to support increased processing and analysis in machine-readable format.
- Panel 5: Who's calling? Managing identities in the cyber world
    - **Creation of an "identity ecosystem".** A complex ecosystem needs to be created forcing at the same time the creation of an "identity ecosystem". As part of the identity ecosystem, it is necessary to consider the level of cooperation between partners (risk management into IdM processes), the interactions and performance of operations (for example, in the Supply Chain scenario), and certification updates.
    - **Provision of certification of attributes.** This might help users to build trust on the mechanisms used.
    - **Provision of Privacy default settings.** This might include the provision of a dynamic consent form that the users can update according to their needs and the different privacy requirements of the applications.
    - **Use of auditing mechanisms.** This could help to ensure the appropriate use of identities by companies.
    - **Transparency.** It is essential that it is transparent to the users the Identity Management mechanisms that are being used in each specific stage.
- Panel 6: The future of European Cybersecurity
    - **Open source solutions.** Open- source solutions can potentially lead to better cybersecurity approaches.
    - **Fund larger projects.** Short-term projects (two to three years long) do not provide the sustainability needed to start from research and go all the way to the market. Projects longer than five years, possibly in the form of "Grand Challenges", such as the ones set by the CERN model, can completely transform the projects and their results
    - **Create a FET Open for Cyber Security**. It was also suggested that we should look at FET Open and be collaborative with ERC, where excellent research is performed but the market is missing. The best ideas should flourish. The DARPA model provides a good example of ideas moving to market and project ending if they do not perform in a short time period.
    - **Restructure Funding.** A good architecture of European funding would therefore consist of blue-sky individual projects under ERC, plus a large number of collaborative FET Open projects in strategic areas – that could also network the results stemming from ERC –, complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

- **Move from "National" to "European"**. There is a need for EU solidarity (the EU budget should take into account the digital market along with the welfare of its citizens). We should move from the national security approaches to a pan European security approach.
- **Improve communication.** Possibly, also we need better communication: the research community needs a better way to communicate their ideas to decision makers, including the European Commission, the European Parliament, and the European Council.

- Panel 7: The upcoming European Cybersecurity Competence Network: a conversation with the four pilots.
  - **Increasing Stakeholder Participation At Future Events.** A concerted effort has to be made, not only by the CyberSec4Europe organisers but the other pilots and the wider stakeholder community as well, to ensure that future events better fulfil expectations.
  - **Meeting Expectations On Collaboration.** The four pilots are consistently and constantly being made aware of the importance of both creating real synergies on project work and also being seen to collaborating in areas where there is obvious overlap. It should be a target for early 2020 for the coordinators to demonstrate concrete collaborative initiatives, perhaps through the proposed focus groups.
  - **Pooling Presentation Material and Representation.** Whilst it has been important during the first 12 months of the four pilots to have representatives from each participate at stakeholder events in Brussels and elsewhere, it is time-consuming and expensive. The four pilots' communications group working closely with the coordinators should come up with a series of presentations that a single appropriate representative from any of the four pilots is able to present. The presentation should contain an overview section ('chapeau') pertaining to all four pilots in addition to brief individual sections for each pilot.
  - **Addressing Strategic Autonomy.** One of the ever-present conundra is, despite the wealth of talent and experience, the lack of strategic autonomy for cybersecurity in European industry. There is a degree of urgency for the pilots individually and collectively to provide recommendations to the stakeholder community.
  - **Minding The Gaps.** Despite the broad range of technical and business issues covered by the pilots, there are many broad areas not covered as demonstrated by the taxonomy mappings. There are even more areas that require attention that need to be identified with recommendations as to how they should be addressed.

I.12 Deliverable D10.2: Clustering Results & SU-ICT-03 Project Concertation Conference Year 2

- Create an ecosystem that fosters innovation through SMEs and start-ups: Provide investment capital to support young people, start-ups and SMEs in the European ecosystem.
- Protect the European know-how from foreign companies and states: Create possibilities, incentives for young people in Europe so as to retain European skills and services.
- European products and innovations as key to the future: For a lot of services and devices, no European alternatives that are in line with the European values exist as yet. The consumer is the king maker, deciding which product will be successful. Build European

databases and train European algorithms with European data instead of financing foreign products with our data.

- The role of decentralization: The Competence Centre can only work with teamwork, cooperation and trust to build a sound European digital ecosystem.
- Stick to European values: Encourage young people to build solutions and products that are in line with European values so that the consumer in the end has the ability to choose.
- Learn from the Covid pandemic experience: Be prepared so that Europe in the future can respond adequately and together in an emergency crisis.
- Use the knowledge base of the pilots to form a foundation for the Centre: Look after smaller and more vulnerable actors like citizens and SMEs, as they are key for a strong Europe as a whole. Make sure that they and the NGOs that represent them, are represented on the boards that make decisions for the Centre.