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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.8

Policy Recommendation Report I[1]

Document Identification	
Due date	31 July 2020
Submission date	31 July 2020
Revision	1.0

Related WP	WP9	Dissemination Level	Public
Lead Participant	FORTH	Lead Author	Evangelos Markatos
Contributing Beneficiaries	TDL, ARCH, UCY, NTNU, UMU	Related Deliverables	D2.1, D3.1, D3.3, D3.4, D3.5, D3.7, D3.9, D4.2, D4.3, D5.1, D6.2, D10.1

1 This is the first deliverable of a series of three "Policy Recommendations" deliverables. The next two are envisioned to be delivered in M36 and M42 respectively.

Abstract:
This deliverable (Policy Recommendation Report I) is the first in a sequence of three deliverables 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 even policy makers in 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 EU and the Member States. To provide effective policy recommendations, CyberSec4Europe follows a two-pronged approach. In the first *reactive* approach, Cyber4Europe partners 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), ENISA (the EU Agency for Cybersecurity), the European Data Protection Supervisor, etc. In the second *proactive* approach, the partners 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:

- EU to support novel privacy-preserving technologies including data sharing for COVID-19
- EU university curricula to provide more attention to certain cybersecurity topics including security-by-design and privacy-by-design
- EU to adopt integrated models for legal compliance and sanction avoidance
- EU to coordinate Member States on achieving cybersecurity sovereignty
- EU to continue to invest in novel solutions for cybersecurity threats
- EU to take leadership in the research and development of blockchain applications
- EU to consider secure 5G as a crucial enabler
- EU to adopt a common eIDAS-based trust framework for Member State digital identity trust schemes
- EU financial services institutions to adopt a privacy-preserving approach to sharing KYC data and IBAN information among banks and other financial institutions

Document information

Contributors

Name	Partner
Pasquale Annicchino	ARCH
Elias Athanasopoulos	UCY
Sunil Chaudhary	NTNU
Vasileios Gkioulos	NTNU
David Goodman	TDL
Evangelos Markatos	FORTH
Antonio Skarmeta	UMU

Reviewers

Name	Partner
David Goodman	TDL
Stephan Krenn	AIT
Jozef Vyskoc	VAF

History

Version	Date	Authors	Comment
0.01	2020-05-29	Evangelos Markatos	1st Draft
0.1	2020-06-13	Evangelos Markatos	Version to be sent to PC at D-45
0.2	2020-06-25	Evangelos Markatos	Version to be sent to the reviewers for first round of reviews

0.3	2020-07-14	Evangelos Markatos	Version to be sent to the reviewers for second round of reviews
0.4	2020-07-20	Evangelos Markatos	Version to be sent to the PC and the WP leader
0.5	2020-07-22	David Goodman	Feedback from WP leader
1.0	2020-07-29	Evangelos Markatos	Version to be submitted

Table of Contents

List of Figures

List of Acronyms

A	**ABC**	Attribute-Based Credentials
	API	Application Programming Interface
C	**CHECK**	Community Hub of Expertise in Cybersecurity Knowledge
D	**DARPA**	Defense Advanced Research Projects Agency
E	**EBA**	European Banking Association
	ECB	European Central Bank
	ECSO	European Cyber Security Organisation
	eIDAS	electronic IDentification, Authentication and trust Services
	ENISA	European Union Agency for Cybersecurity
	EOS	European Organisation for Security
	EPC	European Payments Council
	ERC	European Research Council
	EU	European Union
F	**FET**	Future and Emerging Technologies
G	**GDPR**	General Data Protection Regulation
I	**IBAN**	International Bank Account Number
	ICT	Information and Communication Technologies
	IDM	Identity Management
K	**KYC**	Know Your Customer

M	**MAPE**	Monitor Analyse Plan Execute
	MSs	Member States
N	**NNCC**	Network of National Competence Centres
O	**OBSIDIAN**	Open Banking Sensitive Data Sharing Network
P	**PSD2**	Payment Services Directive 2
S	**SMEs**	Small and Medium-sized Enterprises
T	**TEE**	Trusted Execution Environment
U	**UCD**	User-Centred Design

1 Introduction

This is the first deliverable of Task 9.6: Policy Recommendations. According to the Description Of Action, the task *identifies and prioritises 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 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.

EU MEMBER STATES MUST COORDINATE TO ACHIEVE CYBERSECURITY INDEPENDENCE FROM NON-EU COUNTRIES

Deliverable D2.1

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

- The **proactive** approach. The partners 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.
- The **reactive** approach. The partners 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 and their contributions to various policies. Section 3 summarises some of the most distinct policy recommendations. Section 4 describes the reactive approach and provides pointers to our contributions. Finally, Annex I provides more policy-related information.

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 bite-sized chunks that can be communicated to policymakers when needed.

To collect these policy recommendations, we selected a set of project deliverables to study. The deliverables chosen were those that had been delivered at the time this work started. From those deliverables we excluded any ones that did not have any policy-making potential (such as those from WP1: Project Management). The final set deliverables studied were:

- Deliverable D2.1: Governance Structure[2]
- Deliverable D3.1: Common Framework Handbook #1[3]
- Deliverable D3.2: Cross Sectoral Cybersecurity Building Blocks[4]
- Deliverable D3.3: Research Challenges and Requirements to Manage Digital Evidence[5]
- Deliverable D3.4: Analysis of Key Research Challenges for Adaptive Security[6]
- Deliverable D3.5: Usable Security & Privacy Methods and Recommendations[7]
- Deliverable D3.6: Guidelines for GDPR Compliant User Experience [8]
- Deliverable D3.7: Usability Requirements Validation[9]
- Deliverable D3.8: Framework and Toolset for Conformity[10]
- Deliverable D3.9: Research Challenges and Requirements for Secure Software Development[11]
- Deliverable D4.1: Requirements Analysis from Vertical Stakeholders[12]
- Deliverable D4.2: Legal Framework[13]
- Deliverable D4.3: Research and Development Roadmap[14]

2 https://cybersec4europe.eu/wp-content/uploads/2020/02/D2.1-Governance-Structure-final-Submitted.pdf
3 https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf
4 https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.2-Cross_sectoral_cybersecurity-building-blocks-v2.0.pdf
5 https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.3-Research-challenges-and-requirements-to-manage-digital-evidence-Submitted.pdf
6 https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.4-Analysis-of-key-research-challenges-for-adaptive-security_Submitted.pdf
7 https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.5-Usable-security-privacy-methods-and-recommendations-Submitted.pdf
8 https://cybersec4europe.eu/wp-content/uploads/2020/02/D3.6-Guidelines-for-GDPR-compliant-user-experience-Submitted.pdf
9 https://cybersec4europe.eu/wp-content/uploads/2020/03/D3.7_Usability_requirements_validation_Submitted.pdf
10 https://cybersec4europe.eu/wp-content/uploads/2020/03/D3.8-Framework-and-Toolset-for-Conformity-v1.0-Submitted.pdf
11 https://cybersec4europe.eu/wp-content/uploads/2020/04/D3.9-Research-challenges-and-requirements-for-secure-software-development-v1.0-Submitted.pdf
12 https://cybersec4europe.eu/wp-content/uploads/2020/06/D4.1-Requirements-Analysis-from-Vertical-Stakeholders-WithAnnex-v14.0.pdf
13 https://cybersec4europe.eu/wp-content/uploads/2020/02/D4.2-Legal-Framework-Submitted.pdf
14 https://cybersec4europe.eu/wp-content/uploads/2020/02/D4.3.Research-and-Development-Roadmap-1-Submitted.pdf

- Deliverable D5.1: Requirements Analysis of Demonstration Cases[15]
- Deliverable D6.1: Case Pilot for WP2 Governance[16]
- Deliverable D6.2: Education and Training Review[17]
- Deliverable D8.1: Cybersecurity Standardization Plan[18]
- Deliverable D10.1: Clustering Results and SU-ICT-03 Project Concertation Conference Year 1[19]

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 versions of Call for Proposals? For the Horizon Europe Program? For the Digital Europe Program? 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?*

We received several responses, which are included in this deliverable in Annex I. There is wide variation in both the format and the length of the coverage of policy recommendations in each considered response. This is because some deliverables are more suitable for policy recommendations and already contain text that can be easily formulated in an appropriate way. For example, D2.1 and D4.3 were very close to the world of policy. Similarly, D10.1, which reports on the concertation meeting with policymakers, provided a wealth of policy recommendations. In contrast, other deliverables were more focused, more technical and somewhat distant from the policy world. For example, WP3 deliverables (i.e. deliverables D3.1 to D3.9 as mentioned above) are more focused on technologies and tools. Still, however, most of the studied deliverables were able to produce one policy recommendation.

15 https://cybersec4europe.eu/wp-content/uploads/2020/06/D5.1-Requirements-Analysis-of-Demonstration-Cases-Phase-1-v3.0.pdf
16 https://cybersec4europe.eu/wp-content/uploads/2020/06/D6.1-Case-Pilot-for-WP2-Governance-V4-.pdf
17 https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf
18 https://cybersec4europe.eu/wp-content/uploads/2019/11/CS4E-Deliverable-D8.1_v2.1_2019_08_05_final.pdf
19 https://cybersec4europe.eu/wp-content/uploads/2020/03/D10.1-Clustering-results-and-SU-ICT-03-project-CONCERTATION-conference-year-1.pdf

3 Policy Recommendations

In this section we list the main policy recommendations derived from the various project activities and deliverables, as well as possible next steps.

3.1 EU to support novel privacy-preserving technologies including data sharing for COVID-19

Europe has traditionally been a leader in the area of data protection and privacy. For example, the General Data Protection Regulation (GDPR) has demonstrated this leadership by completely changing the legal landscape of data collection, data processing and data protection; significantly, it has been used as the basis for similar regulations in other jurisdictions. The regulation reflects the values held dear by European citizens – values that govern their everyday lives and shape their future.

Building on top of these values and the strong legal foundation, now, more than ever, we need to support novel technologies in the area of privacy. Indeed, the COVID-19 outbreak shows that we need to find a way to share location data in order to identify people who have come in contact with COVID-19 cases and help them to stay healthy. At the same time, it was clearly expressed that such sharing of location data must be carried out in a privacy-preserving way; otherwise, we run the danger of creating a surveillance society, an ever-present panopticon that would monitor the whereabouts of all citizens at all times – a virtual jail that would allow virtual "guards" to monitor European citizens as they come and go. The goal would be noble: to protect citizens' health; the means could end up being a little better than digital slavery.

Privacy-preserving COVID-19 contact tracing seems like a contradiction: we want to know whether people have contacted other people with COVID-19 but we do not want anyone to know who contacted whom. This sounds like an impossible trade-off, an unsolvable problem. Fortunately, such problems do have solutions – even better, numerous European research activities are addressing them. Having realised the impact that data sharing can have during a pandemic, we believe that we should support scientific endeavours in this challenging field. To be more specific we need to support:

- **Privacy-preserving data sharing** could be used for medical/health purposes, such as COVID-19 contact tracing. Such sharing may also be needed in other fields, including scientific processing, research, secondary processing, epidemiology, etc.
- **Privacy-by-design technological approaches**. Do not let privacy be an afterthought. It should be included in the production process from the first design phases on. Such emphasis on privacy should also be taken seriously even in times of emergency, when privacy can easily fall prey to fear or demagogy.
- **Privacy-enhancing technologies**. Help European citizens protect their privacy when online. When people are online they leave digital "crumbs" that can be used to follow citizens all over the Internet. Like it or not, citizens frequently have no other choice: they need to provide their IP address in order to communicate, have to accept a cookie if they want to receive decent service from the web server, and have to be subjected to device fingerprinting if they want to access an

online service, etc. Privacy-enhancing technologies can help users protect their IP address, protect their devices, protect their identity.

For more detailed insights:

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

Target audience:

- European Commission (DG CNECT)
- ENISA

3.2 EU university curricula to provide more attention to certain cybersecurity topics including security-by-design and privacy-by-design

Certain cybersecurity topics have not attracted the attention they deserve in university curricula. Some of these cyber topics will have broad applicability in the near future.

Security-by-Design and Privacy-by-Design

Security-by-design seeks to minimise the flaws in a system that could compromise its security. This is possible only by integrating security into the entire developmental lifecycle of a system, including specification, design, testing and deployment. This knowledge topic is becoming more relevant with rapidly evolving fields, such as autonomous vehicles and the Internet of Things (IoT). For example, using only the current security model, where safety and security vulnerabilities are addressed (or fixed or patched) when they are found, one cannot produce an autonomous vehicle that is certain to be as safe and secure as possible from the start.

Privacy-by-design or *privacy-as-default* means "data protection through technology design", and this is only possible when privacy is considered and integrated into the technology when it is created. This has become more relevant in the context of big data analytics, where privacy has become a serious concern due to the extensive collection and processing of personal information.

Therefore, it is of the utmost importance to teach students this knowledge and provide them with these skills, so that future systems will be less vulnerable to security attacks than at present and are able to fulfil privacy obligations.

System Retirement

The development of public IT systems is often based on calls for tender and contracts offered for a limited time period only, in which case there is a major security risk when data is migrated from an old system, with its own security enforcement mechanisms, to a new system with different mechanisms. Therefore, universities should prepare students with the knowledge and skills to avoid or mitigate such incompatibilities between two different systems.

Security Operations and Personal Security

Organisational security topics, such as operational and personal security, are also inadequately covered by university curricula. These topics relate to the overall security posture of an organisation. For example, *operational security* involves the detection and analysis of cybersecurity incidents using a combination of technology solutions and a strong set of processes to generate an appropriate response. Similarly, *personal security* helps employees to become accustomed to good security practices and raise their security awareness. Therefore, IT graduates, who may need to take up these kind of responsibilities, should not be left with inadequate knowledge and skills to carry out their tasks.

For more detailed insights:

- Deliverable D6.2: Education and Training Review

Target audience:

- European Commission (DG CNECT)
- ENISA

3.3 EU to adopt integrated models for legal compliance and sanction avoidance

There is a need for a better harmonised interaction between the different obligations imposed by the existing EU directives and regulations in the field of data protection, privacy and cybersecurity. Considering that various obligations (e.g. notifications) are similar, they could be better harmonised through integrated models for legal compliance and the avoidance of sanctions.

The European cybersecurity legal environment is characterised by a multiplicity of legislations, such as those defined in the GDPR[20], PSD2[21], the eIDAS regulation[22] and the NIS directive[23]. All these pieces of legislations entail the adoption of specific technical and organisational solutions with the aim of fostering cybersecurity in the European Union and making the EU a unique environment for the development of data protection and cybersecurity-oriented technologies and practices.

A significant part of the analysis carried out in the context of the research for D4.2 was driven by defining the common security and data protection building blocks that characterise the EU regulatory framework on data and (cyber)security. In this light, two of the main outcomes of the task, as regards the legal and regulatory requirements, are:

- An overview of the potential overlap among the existing legal obligations in the field of cybersecurity (e.g. notifications, certifications)
- The outline of a general, comprehensive and cross-cutting map of legal obligations and procedures related to cybersecurity.

The results of this analysis show how the GDPR provides a general framework, setting out the key principles for the use of data, also in terms of data security. In this sense, these general principles – such as data minimisation, storage limitation and data confidentiality – shape the entire regulatory framework and are further applied in detail by sector-specific legal instruments (PSD2, the eIDAS regulation and the NIS directive). These different legal instruments define the common core of the EU approach, which is based on five main pillars:

- **Risk-based approach**: technological development must be based on an operational and security risk-management framework, including adequate technical measures
- **By-design approach:** secure technologies by design and by default must be provided
- **Reporting obligations:** specific procedures for reporting must be adopted
- **Resilience:** mandatory response and recovery plans must be developed
- **Certification schemes:** *ad hoc* certification schemes have been provided for by law

Based on the above, all the provisions laid down in the legal instruments under examination require, explicitly or implicitly, the development of specific technologies for cybersecurity and data security. The framework provided by these different legal sources is not to be understood as a patchwork, but as a coordinated harmonious model, in which similar technologies are required by different regulations to address issues related to the common core of these legal instruments.

20 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EL
21 https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
22 https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014
23 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

This uniformity demonstrates the coherence that guides the whole approach adopted by EU legislators in the field of data protection and cybersecurity, and undoubtedly provides a clear and unique framework for the development of a roadmap for the implementation of the NNCCs. Taking into consideration the analysis undertaken in D4.2, we can repeat the need for better harmonised interaction between the different obligations imposed by the existing EU directives, and regulation in the field of data and security. Considering that various obligations are similar, they could be better harmonised through integrated models for legal compliance and avoidance of sanctions. This could be particularly relevant in light of the forthcoming EU initiatives connected to the EU data strategy.

For more detailed insights:

- Deliverable D4.2: Legal Framework

Target audience:

- European Commission (DG CNECT)
- ENISA

3.4 EU to coordinate Member States on achieving cybersecurity sovereignty

Deliverable D2.1 outlines a study of more than 80 stakeholders via a survey, interviews, and workshops. When these experts were asked about what the European Union should achieve as an *overall goal* in cybersecurity, *coordination* was identified as the most important goal, together with *independence* from non-EU countries with regard to technology and the protection of citizens, businesses and state actors.

CYBERSECURITY NEEDS A NEW GENERATION OF EXPERTS TRAINED THROUGH AN INTERDISCIPLINARY APPROACH MASTERING THE SECURITY OF SYSTEMS AND UNDERSTANDING HOW CYBERSECURITY AFFECTS THE BUSINESS

Concerning the *desired changes* to improve the situation, the respondents considered transparency of cybersecurity decisions, trustworthiness, and resilience as challenges. Authority supervisors and industry managers outlined *the need for knowledge and education* to be *constantly updated to meet the dynamic changes in cybersecurity*.

In particular, this need was highlighted by the European Data Protection Supervisor, along with other respondents: cybersecurity needs a new generation of experts, trained through an interdisciplinary approach, mastering the security of systems and understanding how cybersecurity affects business. In other words, professional skills and education were considered key. A CISO from big pharma, along with a number of other respondents, highlighted R&D funding and supporting SMEs.

Some participants raised the issue of making sure that the *EU taxpayer money in cybersecurity research* through open calls *does not benefit US companies* through their EU subsidiaries, as pointed out by an ENISA senior manager. In general, according to some authoritative board members, university professors and hacktivists, the goal is to achieve *cyber sovereignty, independence and control*, clearly expressing preference for *the broader focus*.

For more detailed insights:

- Deliverable D2.1: Governance Structure

Target audience:

- European Commission (DG CNECT)
- ENISA

3.5 EU to continue to invest in novel solutions for cybersecurity threats

With the integration of new computing paradigms, such as 5G, IoT, big data, artificial intelligence, etc., the interconnected ICT systems increase the attack surface of critical infrastructures. They have therefore become a prized target for malicious adversaries and cyber criminals who aim to disrupt services to extract sensitive data, or to abuse their victims' machines and networks in order to perform other malicious activities. Indeed, the accelerating wave of sophisticated attacks and advanced persistent threats is a growing security and privacy concern for both consumers and businesses.

To enhance the detection and prevention of cyber threats, organisations collaborate to define defensive actions against complex attack vectors by sharing information and knowledge about threats, sightings, indicators of compromise and mitigation strategies. In consequence, interoperability across different security expert systems becomes a necessity. Threat intelligence platforms have therefore become a critical security component within enterprises to deal with the increasing volume and sophistication of cyberattacks. These systems are not used as extensively as they could be, partly because people lack confidence in their reliability. An organisation will not share relevant and confidential information if it is not assured of a secure and trustworthy environment, risk protection measures and standards. Some of the research areas that need attention include:

- **Modern intrusion detection systems for sophisticated and unseen attacks.** Cyber threat detection solutions need to become more intelligent in order to automate detection and response in an effective manner.
- **Secure access control in heterogeneous systems.** Here the focus is on systems that (i) can react quickly to adverse events (such as cyberattacks), and (ii) can help European citizens deal with cybersecurity threats in the new ICT interconnected infrastructures. This will require a trade-off between a deep analysis of what is happening and a fast analysis to produce a quick reaction.
- **Scaling trusted execution environments (TEE**). TEEs allow private computations to run in untrusted environments. As such, they represent a promising solution to the problem of cloud-based data processing in scenarios where data to be processed must be kept hidden from the host. Novel TEEs should be able to maintain the expected properties of security and privacy, while at the same time offering enhanced flexibility so that they may be used in different scenarios, from standalone client machines to massive cloud deployments.
- **Standardisation of software hardening techniques.** Software hardening is considered ambitious, since:
  (a) despite the many available defences in place, software is still exploitable
  (b) generic software can be fairly diverse, which makes a global hardening solution unsuitable
  (c) security defences impose severe overheads
  (d) security defences can alter the functionality of the software
  (e) legacy software may be hard to analyse or change.
- **Standardisation of software strengthening by design.** For instance, by identifying and eliminating memory errors before deploying software, or by writing all code using a safe programming language. Such solutions can be applied during the early stages of the software lifecycle.

For more detailed insights:

- Deliverable D3.1: Common Framework Handbook #1
- Deliverable D3.3: Research Challenges and Requirements to Manage Digital Evidence
- Deliverable D3.4: Analysis of Key Research Challenges for Adaptive Security
- Deliverable D3.5: Usable Security & Privacy Methods and Recommendations
- Deliverable D3.7: Usability Requirements Validation

- Deliverable D3.9: Research Challenges and Requirements for Secure Software Development

Target audience:

- European Commission (DG CNECT)
- ENISA

3.6 EU to take leadership in the research and development of blockchain applications

Europe has traditionally worked on blockchain-based technologies that are primarily designed to provide credibility and validate transactions, including, for example, cryptocurrencies such as bitcoin. In addition to cryptocurrencies, blockchain can also be applied to several other areas where immutable secure logs are needed: education, healthcare, insurance, etc.

Take, for example, supply chains that are complex systems that move products or services from suppliers to customers. Supply chain processes unfold over a multitude of stages and geographical locations, making it very hard to trace events and investigate incidents, or to track the ownership of goods and inventory at each step. Furthermore, transactions between the companies involved usually require the manual transfer of paper records (orders, invoices, etc.), a costly bureaucratic process that is subject to human errors, losses, damages, thefts and frauds. This inherent complexity only leads to economic losses, inefficiencies and delays that will upset both a company's health and its customers' satisfaction. Customers have no reliable way to verify and validate the value of the goods that they purchase, because of a lack of transparency and prices that do not reflect the true costs of production. In some extreme cases, there might be serious legal consequences. In a hard to manage supply chain, it is difficult to detect illicit activities such as counterfeiting or forced labour in factories. Blockchain can help with most of the mentioned problems by providing a secure and distributed way to record information that cannot be altered. This accurate record of information can be used to resolve many future disputes and false claims. Some potential research areas related to blockchain include:

- **Novel solutions:** That is, solutions for industrial challenges that combine scalable secure and practical consensus layers, smart contract security and efficient privacy-preserving blockchain protocols.
- **Blockchain compliance with EU regulation.** Blockchain provides a secure immutable log. This means that once data is written in the blockchain ledger it cannot be removed. Unfortunately, this immutability of the blockchain's ledger may not be compatible with the GDPR, unless more research is carried out in this area that will preserve the benefits of blockchain while also being compliant with the GDPR.

For more detailed insights:

- Deliverable D3.1: Common Framework Handbook #1
- Deliverable D3.3: Research Challenges and Requirements to Manage Digital Evidence
- Deliverable D3.4: Analysis of Key Research Challenges for Adaptive Security
- Deliverable D3.5: Usable Security & Privacy Methods and Recommendations
- Deliverable D3.7: Usability Requirements Validation
- Deliverable D3.9: Research Challenges and Requirements for Secure Software Development

Target audience:

- European Commission (DG CNECT)
- ENISA

3.7 EU to consider secure 5G as a crucial enabler

The development of 5G technologies is widely considered to be one of the main enablers of future digital services. The EC has launched ambitious initiatives to support cooperation among stakeholders in different Member States for the development of 5G-enabled services. These initiatives include the 5G Action Plan,[24] which represents a strategic effort to align roadmaps and priorities for coordinated 5G deployment across the EU. The 5G Infrastructure Public Private Partnership (5GPPP)[25] is a joint initiative between the EC and EU industry (including telecommunications operators, SMEs and research institutes) to foster a common vision about 5G developments in the EU. Indeed, the development of 5G is widely considered as crucial to ensure the strategic autonomy of the EU.

In this context, previous initiatives consider cybersecurity as a critical aspect for the deployment of 5G in the EU. It is expected that 5G technologies will play a key role in the Digital Single Market, with a strong impact in several vertical sectors, such as energy, transport or health services. Furthermore, 5G will enable a more interconnected world, where vulnerabilities of 5G systems in a single Member State could affect the EU as a whole. Therefore, there is a need to promote collaboration and cooperation among countries to support coordinated and secure 5G deployment. To address such aspects, the EC launched a recommendation in 2019 to propose a set of concrete actions for ensuring the cybersecurity of 5G networks,[26] including the development of national risk assessment strategies for 5G infrastructures. The main goal is to leverage national efforts to develop a coordinated EU risk assessment, in order to create a common toolbox of best risk management measures. As part of these efforts, the "EU coordinated risk assessment of the cybersecurity of 5G networks" report[27] identifies the main threats, threat actors, sensitive assets, vulnerabilities and associated risks of 5G networks. This report was used together with a recent ENISA report on 5G threats[28] to create the initial version of the mentioned toolbox.

To ensure the development of secure 5G deployments, cybersecurity certification is essential to promote a transparent and trustworthy ecosystem of 5G devices and systems. The Cybersecurity Act[29] came into force in 2019 to create a cybersecurity certification framework for any ICT product, service or process. It complements the existing GDPR and NIS Directive to strengthen cybersecurity in the EU. Indeed, the Cybersecurity Act is expected to play a key role in the development of 5G technologies. As described in the already mentioned recommendation, "Cybersecurity of 5G networks", the realisation of such a framework is an essential tool to promote consistent levels of security and the creation of certification schemes adapted to 5G-related equipment. Furthermore, the abovementioned toolbox identifies the EU certification for 5G network components, customer equipment and/or suppliers' processes as one of the main technical measures to strengthen the security of 5G networks. In this regard, a common understanding of the threats, assets, attacks and risks of 5G systems is essential to creating a certification scheme that could help recognise the security level of a certain 5G system across all the Member States. To this end, the outcomes of existing initiatives, such as the creation of an EU risk assessment strategy, could help reach such a harmonised view. Based on such initiatives, some recommendations to foster the development of secure 5G systems from the certification perspective are:

24 https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan
25 https://5g-ppp.eu/
26 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks
27 https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6049
28 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
29 https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

- **Identification of a common set of cybersecurity requirements** that can be tested and certified for 5G systems. These requirements should be based on standardised approaches and can leverage the results of existing initiatives (e.g. the toolbox mentioned above).
- **Definition of common assessment and testing procedures for the cybersecurity certification of 5G systems**, considering the different assurance levels described in the Cybersecurity Act
- **Analysis of the potential risks associated with the deployment of 5G systems** certified under conformity self-assessment procedures (Article 53 of the Cybersecurity Act)
- **Fostering the creation of a cybersecurity certification scheme** to promote mutual recognition of 5G systems across Member States by considering a specified common set of requirements. This initiative can be considered in the scope of the Union rolling work programme, which is intended to identify strategic priorities for future European cybersecurity certification schemes.[30]
- **To promote collaboration and cooperation among Member States** for the creation of a common platform to share cybersecurity information associated with 5G systems throughout their lifecycle. This "living" platform could include information about new software/hardware vulnerabilities, relationships among several certification schemes, or the cybersecurity certificates of any 5G system.

For more detailed insights:

- Deliverable D3.1: Common Framework Handbook #1
- Deliverable D3.3: Research Challenges and Requirements to Manage Digital Evidence
- Deliverable D3.4: Analysis of Key Research Challenges for Adaptive Security
- Deliverable D3.5: Usable Security & Privacy Methods and Recommendations
- Deliverable D3.7: Usability Requirements Validation
- Deliverable D3.9: Research Challenges and Requirements for Secure Software Development

Target audience:

- European Commission (DG CNECT)
- ENISA

[30] https://ec.europa.eu/digital-single-market/en/european-cybersecurity-certification-group

3.8 EU to adopt a common eIDAS-based trust framework for Member State digital identity trust schemes

On the back of the eIDAS regulation entering into force on 29 September 2018,[31] it became mandatory for Member States to enable cross-border recognition of eIDs, allowing citizens and businesses to share their identity data when necessary.

According to Commissioner Mariya Gabriel at the time[32]:

> *To increase citizens' trust, public authorities are not the only ones to play an active role. It is important that also the private sector benefits from eIDAS' full potential, as this legislation holds the power to create a market for authentication, authorisation and attributed services worth more than 2.13 billion EUR by 2022.*

At present, Member States are working individually to create their own digital identity ecosystems: most are developing systems based on public-private cooperation and interoperability, but in the majority of cases there is still some way to go. *What is missing is an EU-level initiative to synchronise these efforts by individual Member States for the benefit of national and cross-border governmental and business transactions.*

Several of the key areas in the work of CyberSec4Europe for which this development would be of benefit are:

- **Interoperable eKYC (electronic Know Your Customer):** At present, adoption in this area is limited, with different standards and approaches being proposed and piloted in the EU and elsewhere. For banks and other financial institutions, the benefits are an increase in reliability, transparency and efficiency in the online onboarding of new customers, a win-win for both customers and banks, who generally have to rely on paper-based documents to complete identity verification. While this is a desired outcome across the financial community, it would also benefit the legal and accountancy professions, and others.
- **Higher education certificate exchange**: Privacy-preserving identity credentials are required to ensure the secure and trustworthy exchange of these documents between organisations, including educational institutions, universities, state agencies and private sector organisations, so that graduates can easily, and in a verifiable way, share their certificates and prove their expertise.
- **Medical data exchange:** In order to securely manage the exchange of patient data between healthcare institutions, such as hospitals, general practitioners and pharmacies, especially cross-border, having a privacy-preserving digital identity trust framework would be of considerable benefit.
- **Smart city citizen engagement:** Emerging business and government models involving citizens and other city stakeholders, primarily the municipalities, can only be fully enabled by the secure and privacy-preserving exchange of user data: being able to easily and securely identify all citizens of – and visitors to – a smart city will eventually become a burning business problem.

31 https://ec.europa.eu/digital-single-market/en/news/electronic-identification-and-trust-services-eidas-clear-benefits-smes

32 https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market

Even if not apparent before, one of the impacts of the COVID-19 lockdown has been the recognition that many societal and business processes – including track-and-trace app development – are stalled without the availability of easily verifiable digital identity credentials.

Although there are numerous national and EC-funded projects and initiatives, it is our belief that a greater concerted effort should be made to build an identity ecosystem that works across all sectors and across borders. A first step would be to get the backing and support of Member States and key verticals.

For more detailed insights:

- D4.1: Requirements Analysis from Vertical Stakeholders
- D4.3: Research and Development Roadmap
- D5.1: Requirements Analysis of Demonstration Cases
- D5.2: Specification and Set-up Demonstration case Phase 1

Target audience:

- European Commission (DG CNECT, DG SANTE, DG ECFIN)
- European Banking Association

3.9 EU financial services institutions to adopt a privacy-preserving approach to sharing KYC data and IBAN information among banks and other financial institutions

Cyber threats in the financial sector have been increasing since the functionality introduced with PSD2 and the growth in consumer banking

(1) Threats are increasingly professional and repeatable, and continue to succeed, particularly by leveraging human weaknesses pitted against the high skills and large resources of the attackers, who are able to move from one bank to another without significant effort and without being tracked.

(2) The evolution of consumer banking towards ever more real-time transactions limits the ability of banking players to react effectively in the event of proven fraud.

(3) Banking information system architectures have been deeply remodelled with a focus on APIs as critical business components, fuelled by the preferential use of mobile devices to consume banking services and accelerated by PSD2. The reliance of a banking information system on APIs creates organisational and methodological impacts that go beyond pure software development and introduce new security issues.

These new issues require a complete transformation in the provision of banking services; and in particular the co-creation and co-design of an open approach to security that will federate the whole banking ecosystem, to make it globally aware and informed of any fraud attack in real time.

Two of the key areas in the work of CyberSec4Europe on Open Banking for which a privacy-preserving approach to data sharing would be of benefit are:

- **Sharing KYC data** among banks and other financial institutions. At present, activity in this area is limited to small scale projects and pilots, whereas what is required are large-scale, cross-border pilots. As a consequence of the increase in efficiency in the online onboarding of new customers, sharing KYC between banks, nationally and cross-border, would provide a massive boost to preventing cyber attacks by malicious actors using false or falsified documentation to get illegal access to banking systems.
- **Sharing IBAN information** among banks, in conjunction with sharing KYC data, would prevent fraudsters making similar fraud attacks using the same IBAN at one bank after another.

Providing Europe-wide support for the OBSIDIAN (Open Banking Sensitive Data Sharing Network) network that CyberSec4Europe is developing and promoting for Europe would help cut down on one of the major sources of bank-related fraud.

For more detailed insights:

- D4.1: Requirements Analysis from Vertical Stakeholders
- D4.3: Research and Development Roadmap
- D5.1: Requirements Analysis of Demonstration Cases
- D5.2: Specification and Set-up Demonstration case Phase 1

Target audience:

- European Banking Association (EBA)
- European Central Bank (ECB)
- European Payments Council (EPC)

3.10 Communication – 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.), concertation events, and topical events, such as an Open Banking event anticipated for early 2021.

4 The Reactive Approach

During the first eighteen months of the project, CyberSec4Europe received several invitations to contribute[33] to various policy-related activities. Some of these are included below.

4.1 ECSO – The European Cyber Security Organisation

In June 2019, the European Cyber Security Organisation (ECSO) delivered several strategic research priorities to the European Commission for future policy recommendations[34]. The partners of the project played a leading role in defining and writing most of the text for several of the priorities:

- Certification schemes for data protection
- Disintermediated and user-centric, privacy-respecting identity and access control ecosystem
- Holistic security orchestration in heterogeneous systems and networks
- Security certification formal format
- Hardware (in)security (software-controlled hardware bugs)
- 5G and IoT convergence
- Software hardening

[33] 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.

[34] The document is not publicly available. However, we have included some screen dumps of this document in Figure 2.

HEU.06	
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
Timeline (2025/2027/beyond)	2027
Keywords	*<Hardware / Software / Process> <Design / Development / Assessment>* *<Technological / Economical / Impact>*

Figure 1: Contribution of CyberSec4Europe partners to ECSO's research priorities document. CyberSec4Europe proposes that research should be funded in the area of software hardening.

HEU.27	
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	
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.
Keywords	*<Hardware / Software / Process> <Design / Development / Assessment>* *<Technological / Economical / Impact>*

Figure 2: Contribution of CyberSec4Europe partners to ECSO's research priorities document. CyberSec4Europe proposes that research should be funded in the area of software-controlled hardware bugs.

4.2 ENISA Research Prioritisation

ENISA is preparing a document on research prioritisation to achieve European Digital Sovereignty.[35] The goal of the document is to identify the areas of cybersecurity where the EU should focus its cybersecurity research activities.

The experts on this project have contributed to several aspects of this document, including participation in:

- the questionnaire
- the research prioritisation
- the preparation of the text

4.3 First CyberSecurity Project Workshop

The first CyberSecurity Project Workshop[36] was held on 29 November 2019. In a joint presentation with the SPARTA project (represented by Claudia Eckert), CyberSec4Europe (represented by Fabio Massacci) proposed a general overview of the challenges faced by the whole chain of operating system, middleware and hardware as requested by the EC. Digitisation is built upon a hardware and software continuum. Non-EU manufacturers dominate the global hardware and OS market. This creates a strong dependency for the EU as there is no warranty that European software could not be shut down via an activated kill switch nor that backdoor information leakages might not happen. Non-EU hyperscale platforms (AWS, Azure, Google) dominate the cloud market which are another source of dependencies in terms of lock-in, loss of control over data and possibly even leakage of business secrets. Such dependencies impact European stakeholders across the board: enterprises, governments, citizens.

The presenters argued for the following combination of integrated measures:

- Develop **trusted hardware** based on open source hardware, trusted designs (code review, IP verification) and trusted manufacturing and packaging (split manufacturing)
- Develop **trusted platforms based on open source software**, Isolated container (trusted execution of applications), Attestation (remotely check security status of OS at any time)
- Develop **trusted CI/CD** (continuous integration – continuous deployment) chain by a continuously updated artefact test toolchains based on open source software.
- Develop and run a reference **trusted data sharing infrastructures** leveraging on the above Trusted connector, service brokers, and App Stores.

These measures would allow to protect the whole lifecycle of any hardware/software component including its long-term updates and evolution and ensure the trustworthiness of the hardware/software platform over its lifecycle irrespective of where it is made. In this respect we could leverage previous and upcoming work: International Data Space (IDS), GAIA-X, etc.

Products could then be tested for security in the EU for a trusted open source chain of "assurance": either it originates from a trustworthy supply chain or it meets its secure baseline. Eventually one could envisage an open software suite available to SMEs for final customer integration.

35 At the time of writing the document has not been published. That is why we do not have a link to it.
36 https://www.ffg.at/sites/default/files/downloads/CCCNworkshop.pdf

4.4 Other contributions

CyberSec4Europe partners have been invited to contribute to several workshops and meetings organised by the European Commission and other European organisations, including ECSO, ENISA, EOS, et al. The partners contributed to the final documents produced. More information about these meetings can be found in deliverable D10.1.[37]

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

5 Summary – Recommendations

CyberSec4Europe aspires to help policymakers formulate the policies that will shape the future of the EU and the Member States. Towards this goal, CyberSec4Europe provides policy recommendation using a two-pronged approach. In the first *reactive* approach, Cyber4Europe partners receive and accept invitations to provide recommendations in several fora, including workshops, concertation meetings, EU-level organisations, including ECSO, ENISA, the European Data Protection Supervisor, et al. In the second *proactive* approach, the partners suggest that much of the work already performed in the project may essentially create contributions that are practically policy recommendations. In this deliverable we collected these contributions, phrased them as policy recommendations and provided evidence that underlines their importance.

Some of the policy recommendations that identified include:

- EU to support novel privacy-preserving technologies including data sharing for COVID-19
- EU university curricula to provide more attention to certain cybersecurity topics including security-by-design and privacy-by-design
- EU to adopt integrated models for legal compliance and sanction avoidance
- EU to coordinate Member States on achieving cybersecurity sovereignty
- EU to continue to invest in novel solutions for cybersecurity threats
- EU to take leadership in the research and development of blockchain applications
- EU to consider secure 5G as a crucial enabler
- EU to adopt a common eIDAS-based trust framework for Member State digital identity trust schemes
- EU financial services institutions to adopt a privacy-preserving approach to sharing KYC data and IBAN information among banks and other financial institutions

Annex I: Policy-related Considerations (by Deliverable)

I.1 Deliverable D2.1: Governance Structure 1

D2.1 processed various inputs from stakeholders and academic research. Based on these, we have extracted various implications for how the governance model for cybersecurity in the EU should address the following four core problems:

- Stakeholders express widespread support for the objectives of cyber sovereignty, independence, and control at the EU level, combining this with a view that the focus of the network of national competence centres (NNCCs) should be broader than only stimulating research and development, and should also include capability-building and policy interventions.
- In terms of governance structures, there was support for a combination of a hierarchical and a network model, as well as for a governance structure that is open to a diverse set of actors, initiatives and collaborations.
- The insufficient collaboration between academia and industry in the EU is a systemic problem that is apparent in the leading cybersecurity research venues where innovative work is published. The new governance structure, therefore, cannot just be a platform, but has also to address the lack of focused investment if the EU wants to better capitalise on the synergies from joint R&D by academia and industry.
- By examining different types of governance structure, we have identified a number of elements that could provide valuable lessons for the governance design of the NNCC. For example, the synergy between formal and informal, top-down and bottom-up structures can be achieved by integrating informal structures, thus leading to a more efficient stakeholder engagement throughout all levels of society. As another example, transparency is a key element for facilitating trust in an organisation.

Based on these findings, CyberSec4Europe is developing a draft governance model for the NNCC. CyberSec4Europe's overall approach is to explore a community-driven approach for the governance model, to complement – and slightly modify – the EU Regulation Proposal 2018/0328[38] within the legal requirements. At the core of our model are community-level cybersecurity hubs that should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area. Notably, they should be able to shorten the chain between decision-making and existing needs on the ground. Accordingly, the governance model needs accompanying mechanisms to increase funding and investment, including at the EU level. In addition to making the bottom-up approach work with the EU proposal, we put forward the introduction of a community-based stakeholder council, as a substructure for the central competence centre, along with a modification of the existing governance structure for the proposed NNCC under the regulation proposal. Our recommendation focuses on the involvement of civil society through the stakeholder council to build and strengthen its cybersecurity capabilities, as well as facilitate transparency and promote trust.

In short, D2.1 proposes a network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), which will provide an auspicious environment for community-level research, innovation, and capacity-building in cybersecurity. By connecting to the NNCC, while staying close to the operational environment and cybersecurity professionals, the CHECKS will be well positioned to leverage regional and

38 https://eur-lex.europa.eu/procedure/EN/2018_328

industry-related practices and expertise. As a part of its ongoing activities, CyberSec4Europe will evaluate the internal governance of the suggested institutions, such as the competence centre and CHECKs.

I.2 Deliverable D3.1: Common Framework Handbook 1

D3.1 made recommendations for research priorities that were included in the ECSO research priorities (see section 4.1):

- Certification schemes for data protection
- Disintermediated and user-centric, privacy-respecting identity and access control ecosystem
- Holistic security orchestration in heterogeneous systems and networks
- Security certification formal format
- Hardware (in)security (software-controlled hardware bugs)
- 5G and IoT convergence
- Software hardening

I.3 Deliverable D3.3: Research challenges and requirements to manage digital evidence

Some of the key findings that can be used by policymakers include the following:

- Lack of trust in the way threat intelligence information is handled by receiving parties is a key factor in making organisations reluctant to share information
- The application of security techniques – such as end-to-end encryption, onion routing, etc. – makes it harder to harvest threat intelligence from monitoring data and event logs.
- The AI capabilities of contemporary threat intelligence platforms enable new kinds of attacks that allow adversaries to learn how to evade detection or may leak sensitive information and thus require strong protection to avoid privacy concerns or loss of reputation of the reporting entity.

I.4 Deliverable D3.4: Analysis of key research challenges for adaptive security

We recommend that future research should focus on:

a) considering the cyber and physical spaces where modern systems operate during monitoring and execution of security controls;
b) integrating multiple security objectives during decision-making;
c) considering the stakeholders during design and development of the activities of the adaptive security MAPE loop;
d) provision of perpetual security assurances that can be regenerated after adaptation;
e) reducing security uncertainties.

It is also important to think about “adaptive security/privacy policies” to create policies that are more robust, resilient to change over time and make explicit provision for learning. A promising idea could be related to taking into account the principle of “design for change” and the adaptive security decision-making process in the way security and privacy policies are defined.

I.5 Deliverable D3.5: Usable security & privacy methods and recommendations

To reach more usable security and privacy enhancing systems, D3.5 provided a short list of recommendations. Some of these are general and some are directed towards specific use cases, such as user authentication.

- Authenticated encryption should be used in the application layer or during network layer communications whenever possible. The use of authenticated encryption protects both the integrity of the communications and the privacy of the content. There are many tools available to achieve this, and they can be applied in a vast majority of use cases that involve communication over a network. When this is done right, and when user needs, user knowledge and user work are carefully identified at design time, the impact to end users is minimal
- Early user involvement should be a priority for new security and privacy features. User centred design approaches advocate the involvement of end users in the early stages of the development process (e.g. via brainstorming sessions and work analysis).
- User modelling and/or user tests should be conducted for new security and privacy features. Although collecting information on users is not a straightforward task, as both automated and other approaches have their shortcomings, it is important to test and/or model users in all new security and privacy features. User research methods should thus be used throughout the design, development and assessment of security mechanisms.
- Users need to be provided with authentication methods that are both secure and privacy-friendly, as user authentication is the security measure that in many cases is the most visible to users. This may be accomplished in many ways, but at the moment convenience and user experience seem to be pushing towards the use of biometrics. It should be possible to conduct user authentication in a user-friendly way while meeting security objectives and respecting users' privacy.

CYBERSECURITY IS NOT JUST ABOUT PROTECTING COMPUTERS: IT IS ABOUT PROTECTING DATA: PEOPLE'S DATA

Deliverable D4.3

I.6 Deliverable D3.7: Usability requirements validation

- Usability and security or privacy requirements need to be reconciled and considered as two facets of the same objective, rather than being viewed as mutually exclusive, as is often the case.
- Validating usability is neither simple nor cheap, so care needs to be taken to include elements of user modelling and/or user testing in the early stages of the design of new security and privacy features.

I.7 Deliverable D4.2: Legal Framework

There is a need for a better harmonised interaction between the different obligations imposed by recent EU directives and regulations. Considering that various obligations (e.g. notifications) are similar, they could be better harmonised through integrated models for legal compliance and sanction avoidance.

I.8 Deliverable D4.3: Research and Development Roadmap 1

- "**Data Security and Privacy**" The most popular research area by far was data security and privacy. This presents simply and clearly the goal of cybersecurity, which is not about protecting computers but protecting data – people's data. This radical shift in mentality from *big iron* infrastructures to *soft data* represents a whole new way of approaching cybersecurity.
- "**Know your enemy**" Support research to understand cyber attackers. Traditional roadmaps to cybersecurity research start with a list of vulnerabilities, a list of important system properties, or even a list of research areas that should probably be explored. D4.3 follows a different direction, asking very simple and obvious questions: "Who is the attacker? What does the attacker want?"

Only after having fully understood the potential attackers is one able to reasonably protect a system against them.

I.9 Deliverable D5.1 Requirements Analysis of Demonstration Cases Phase 1

Integration of vertical sectors with IT technologies. Surprisingly enough, the deliverables revealed that, despite today's technological advancements, key industrial sectors are still relying upon outdated technologies, often inadequate against modern attackers. In some cases, important operations (e.g. dispute resolution in supply chains) are still carried out via tedious, error-prone, bureaucratic processes.

Blockchain. This relatively new technology is at the forefront of the modernisation of the industry sectors. Three out of seven project's verticals– open banking, supply chain security assurance, and medical data exchange – plan to use it as a core part of their solution to bring about security by design, reliability, scalability, and traceability of transactions.

User data protection technologies are still lacking. Today's cybersecurity techniques are inadequate to counter modern attacks. In particular, privacy-preserving identity management and privacy-preserving data handling techniques are in high demand. The number of data breaches and data (mis)management scandals in recent years corroborate their importance. They are, in one way or another, at the core of all seven demonstrators that need to handle sensitive data, from storing for traceability and transparency reasons, to trading as a part of their services.

Lack of interoperability in today's cybersecurity technologies. Today's cybersecurity solutions solve a single problem well – a good strategy, because it reduces the attack surface. However, they often do not work well in concert with other technologies as building blocks of broader solutions. This is what CyberSec4Europe's demonstrators are trying to achieve.

T5.1: Open Banking – Adoption of an agreement from the competent authorities to allow the exchange of sensitive fraud-related information between banks

Threats are increasingly professional and repeatable and continue to succeed, particularly leveraging human weaknesses pitted against the high skills and large resources of the attackers, who are able to move from one bank to another without significant effort and without being tracked.

The evolution of consumer banking towards ever more real-time transactions limits the ability of banking players to react effectively in the event of proven fraud.

Banking information system architectures have been deeply remodelled with a focus on APIs as critical business components, fuelled by the preferential use of mobile devices to consume banking services and accelerated by PSD2. This reliance on the APIs of a banking information system creates organisational and methodological impacts that go beyond pure software development and introduce new security issues.

These new issues require a complete transformation in the provision of banking services, and in particular the co-creation and co-design of an open approach to security by federating the whole banking ecosystem, to make it globally aware and informed of any fraud attack in real time.

T5.2: Supply Chain – Policies for supply chain security assurance

Existing recommendations and standards already define procedures and best practices that focus on aspects such as the integration of traditional security procedures, how to perform risk analyses to make decisions and create contingency plans, and the management of interactions between suppliers and providers. However, as the number and impact of attacks that specifically target supply chains is on the rise, and the previous recommendations and standards do not capture the full complexity of this ecosystem, it is necessary to consider (i) the actors, services, and assets that comprise the current supply chain ecosystem, (ii) their interactions, (iii) the most important threats that such ecosystems face, and, finally, (iv) what security solutions need to be considered.

T5.3: Identity Management – A way to manage strong authentication keys for end users

The need to construct identity management (IDM) in a strong privacy-preserving and easy-to-use approach leads to several recommendations. The core challenge is to develop IDM solutions that satisfy all the following requirements at the same time:

- strong privacy protection & authentication
- no single point of failure or trust
- usability, i.e. choice to be privacy-preserving and should be easy to use.

Most technologies that already exist satisfy only two out of the three requirements above. For instance, current privacy-preserving IDM solutions developed by the research community, such as Idemix, provide strong privacy, but are too complex, not easy to use, as they require different user actions to obtain and handle credentials, which users will not be able to understand and manage easily.

Another core requirement is to simplify privacy-preserving IDM solutions by avoiding trying to fit all features into the same system. In particular, existing IDM solutions in practice lack strong, end-to-end authentication, which should be the main goal. Examples of good trade-off solutions are Cloudflare, Privacy Pass or ABC (attribute-based credentials) for Cloud (i.e. the approach taken by the CREDENTIAL project), where an intermediary in the Cloud runs everything on behalf of the user with good-enough privacy guarantees.

The concrete problem of looking for more distributed privacy-preserving systems, for instance where trust is distributed in a single sign-on, is to find a way to **manage strong authentication keys for end users.**

T5.7: Smart Cities – Addressing data management challenges in 5G smart cities

The key challenge for cities will be managing the data complexity that will come with 5G, particularly in the context of the vast number of devices, and points of data provision and data processing. Specifically, the impact on data management needs to consider the impact on how data are processed and stored. Data will need to be processed, transferred and stored instantly: speed, data consistency and reliability will be the triptych of critical requirements.

Data management solutions can be implemented across a range of data infrastructure and cloud-based solutions, including on-premise cloud, hybrid cloud and off-premise cloud platforms. These solutions offer the advantage of dense processing of information (such as batch data) and the ability to efficiently apply advanced analytics and deep learning techniques. Alternatively, fog (or edge) computing solutions are beginning to impact the market, addressing the need for low latency and near real-time processing, storage and analytics in cases where edge management of IoT data is critical to the application. 5G's ability to support data collection and distributed processing through edge computing might assist certain aspects of data analytics and digitisation. Depending on the type of data being transmitted and the need for computation, information may also need to be exchanged with a backend server for processing (such as aggregation with other information and summarisation). The possibilities of big data and deep learning processing this huge amount of data, and more importantly the creation of secondary applications for detected patterns of behaviour, mobility, usage of services, etc., represent an important challenge to address from a data governance perspective, within cities and on behalf of citizens that use their infrastructures.

Edge technologies make it feel as though every device is a supercomputer. Digital processes become lightning fast. Critical data are processed on the edge of the network, right on the device. Secondary systems and less urgent data are sent to the cloud and processed there. With SDN (software-defined networks), more flexibility will be available to define rules on where and how data are processed to optimise application

performance and the user experience, but at the same time new challenges will appear regarding how data will be shared and by whom, and the need to define different levels of security and privacy management over the whole data-flow process. Sharing data may lead to security breaches, data losses and, in extreme instances, high-impact cyberattacks. As data sharing grows and new technologies drive a more interconnected infrastructure ecosystem, the range of potential threats reported will expand.

5G will soon promote the rapid proliferation of the IoT, connecting billions of devices to billions of people. 5G's strong and robust data transport capacity – 1000 times faster than 4G – will produce enormous amounts of information, where location, identity and personal data leakage will become the new security challenges. As more 5G antennae and base stations are placed in high population density areas, location privacy protection of IoT and end-users is expected. By implementing privacy protocols within the very architecture of 5G networks, the actors in 5G deployments can collectively take a proactive approach towards privacy protection, and assure users their identity, location and personal data are in safe hands.

I.10 Deliverable D6.2: Education and Training Review

The survey of European universities (described in D6.2[39]) shows a number of cybersecurity skills that are currently not being considered in MSc programmes to the extent they should be. The areas of organisational security, societal security and component security and, most significantly, the skills related to component procurement and system retirement are clearly the least covered, according to our survey. This is quite worrying, because the development of public IT systems is often based on calls for tender and contracts offered for a limited time period only, in which case there is a major security risk when data are transferred and transformed from the old system and its security enforcement mechanisms to the new system and its different security enforcement mechanisms.

Our survey also shows that the topics most covered focus on well-understood communication vulnerabilities and how to mitigate them using cryptographically secure communication protocols, whereas topics central to achieving security-by-design and privacy-by-design are not considered to a sufficient extent. It is likely to be in these areas that students will acquire key skills to ensure that future IT systems are less vulnerable to security attacks than present-day systems.

In sum, the apparent lack of focus on topics related to system procurement, retirement, security- and privacy-by-design is critical, as the use of legacy and third-party software and systems, possibly produced outside the EU, and their dismantlement and replacement, pose challenges to security and privacy that require specialised training and skills. We believe that those skills should be promoted to enrich cybersecurity education programmes.

I.11 Deliverable D10.1: Clustering results and SU-ICT-03 project CONCERTATION conference

Cooperation is key to succeeding with policy challenges. Cooperation between Member States is crucial, as well as between organisations and stakeholders at the regional, national and European levels. It is most important at least to have a common strategy, but if different strategies exist, they should be coordinated. Initiatives at the local level should be visible and subject to local responsibility. At the same time, policy makers need to think big and consider how best practices at a local level can be transferred to a national or EU level, and what effect local best practices can have on larger ecosystems

39 https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf

Enhancing European competitiveness. In Europe, civilised values and people's welfare are cherished. However, they cannot be taken for granted and need to be made sustainable. For this, it is necessary to be competitive, e.g. in 5G, data management, artificial intelligence, etc., and the responsible sharing of data needs to be facilitated, while respecting the GDPR and privacy regulations in general. Help from cybersecurity experts is needed to design and implement the sharing of data in a responsible manner.

Attainable certification for all. As certification comes with costs, which smaller players, such as SMEs, might find it hard to cover, it is essential that the application of certification, including financing models, should be well planned. Research can provide better solutions: however, it is time for decisions, at least as regards trials for a limited time. This process should include a spectrum of mechanisms, from liability provisions to simple self-declaration by providers.

Cybersecurity must be considered an important component in all projects in European funding programmes. Cybersecurity should be considered as part of every call, not just specific cybersecurity calls. Almost all R&D projects that have some IT dimension should take cybersecurity into account. European funding programmes (such as H2020, DEP and others) should ensure that cybersecurity is a component of all projects, e.g. health, financial, transport, critical infrastructure, etc.

Cybersecurity education should be a priority. To have a perspective from outside the research and innovation bubble is extremely important

Common vision and mission promoting European values via hub communities. Hub communities should federate with a common vision and mission that promote European values. Furthermore, hubs should remain open and engage with effective strategies to build trust with the communities involved.

Real-time reactive data sharing solutions. Cybersecurity has an immediate impact in the digital world; hence, it is important that we have real-time and reactive data sharing.

New tools to support data sharing while preserving privacy. It is important to have tools that enable cross-border sharing of data without compromising privacy. Although methods and tools already exist (including differential privacy[40] and k-anonymity[41]), new challenges need to be addressed, such as those presented by COVID-19.

Machine learning tools to improve data management. The increase in size of shared data and transferred data needs to be made more manageable. Using machine learning, it is possible to find out which threats are more important and the order of sharing.

Provision of privacy default settings. This might include the provision of a dynamic consent form that users can update according to their needs and the different application privacy requirements.

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 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 projects and their results.

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

40 https://link.springer.com/chapter/10.1007%2F11681878_14
41 https://epic.org/privacy/reidentification/Sweeney_Article.pdf

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 national security approaches to a pan-European security approach.

Improve communication. We may also need better communication: the research community needs a better way to communicate its ideas to decision makers, including the European Commission, the European Parliament, and the European Council.

Addressing strategic autonomy. An ever-present conundrum is the lack of strategic autonomy for cybersecurity in European industry, despite the wealth of talent and experience.