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

Project start: 1 February 2019
Project duration: 47 months

Cyber Security for Europe

D9.28:

Policy Recommendations 3

Document Identification	
Due date	31 December 2022
Submission date	23 December 2022
Revision	1.0

Related WP	WP9	Dissemination Level	Public
Lead Participant	FORTH	Lead Author	Evangelos Markatos
Contributing Beneficiaries	CYBER, NTNU, TIMLEX, TDL, UM, TUD, UPRC, UCY	Related Deliverables	D9.8, D9.20

Abstract:
This deliverable is the third in a sequence of three reports that select policy recommendations from 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 awareness to research and target a wide variety of stakeholders including the European Commission, European agencies, European organisations and policymakers in EU Member States. In this final deliverable we present the recommendation reports as "**policy briefs**": two-page-long documents that present the problem and the proposed solution in a way that is quick and easy to grasp.

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

Over the past four years, the partners of the CyberSec4Europe project have been doing research and development in the area of cybersecurity. The experience that they gained can be used not only in technical contributions for cybersecurity technologies but also in policy interventions. Towards this direction they have collected their policy recommendations in this deliverable. To disseminate them in a fast and easy way they have formatted the recommendations into two-page-long "policy briefs". Each policy brief deals with one issue: it presents the problem, the findings, and lists 2-3 policy interventions that can be used to address the problem. The policy briefs prepared are:

- Develop new funding instruments to support blue-sky research in the area of cybersecurity
- Support the design and development of new password-less authentication methods
- Institutionalize the Cybersecurity Competence Community
- Support projects working towards exploring the role of Privacy Enhancing Technologies (PETs) in reducing risk and advancing European data protection policy to promote the use of advanced PETs
- Encourage cybersecurity research projects targeting sector-specific SMEs, as well as with efficient and actionable plans to attract relevant SMEs
- Encourage the European Data Protection Supervisor to issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDIW in Article 6a (2) of the eIDAS2 Proposal.
- Fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks

In addition to the above the partners have made contributions to several European and Member States organizations and institutions including ECSO, ENISA, JRC, DG JUST, the European Parliament, and others.

Document information

Contributors

Name	CyberSec4Europe Consortium Member
Elias Athanasopoulos	UCY
Dan Bogdanov	CYBER
Panagiotis Bountakas	UPRC
Sunil Chaudhary	NTNU
Andreas Dionysiou	UCY
Vasileios Gkioulos	NTNU
David Goodman	TDL
Hans Graux	TIMELEX
Natalia Kadenko	TUD
Liina Kamm	CYBER
Evangelos Markatos	FORTH
Antonio Skarmeta	UM
Christos Xenakis	UPRC

Reviewers

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

History

Version	Date	Authors	Comment
1.0	2022-11-20	Evangelos Markatos and all partners	1st Draft
1.01	2022-11-29	Evangelos Markatos and all partners	2nd Draft
1.1	2022-12-20	Evangelos Markatos and all partners	3rd Draft (after internal review)
1.11	2022-12-23	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Acronyms

E	**EIC**	European Innovation Council
	ENISA	European Network and Information Security Agency
	ERC	European Research Council
F	**FET**	Future and Emerging Technologies
I	**ICT**	Information and Communication Technologies
	IoT	The Internet of Things
M	**ML**	Machine Learning
P	**PETs**	Privacy Enhancing Technologies
S	**SME**	Small Medium Enterprise
T	**TRL**	Technology Readiness Level
	TTC	Technology Trade Council

1 Introduction

This is the third 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 create **two-page-long policy briefs,** each one of which focuses on a single issue. They present the problem and the recommendations in a quick and simple way that is easy to grasp.
- 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.

[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 Policy Briefs

To make our policy recommendations easier to distribute we have formatted them into 2-page-long policy briefs. All policy briefs follow the same format:

- Policy Recommendation Title
- Context and Findings
- The problem
- The scene
- The implications
- Policy recommendations
- References
- Contact

In this deliverable we include the following policy briefs:

- Promote Blue-sky Research

Password-less Authentication

- Data Protection by Design
- Community Engagement
- SMEs
- European Digital Identity Wallet
- Vulnerability attribution

2.1 Promote Blue-sky Research

This policy brief deals with the need to support basic research in cybersecurity – what we call "blue-sky research". The main recommendations of this brief are:

- **Develop new funding instruments to support blue-sky research in the area of cybersecurity.** Currently very few, if any, instruments exist to support blue-sky research in cybersecurity. We need a new FET-like or EIC Pathfinder-like programme completely dedicated to cybersecurity. Such programmes would support the entire range of cybersecurity projects ranging from hardware security all the way to application security. One might think that such instruments already exist (such as the European Research Council or Marie Skłodowska-Curie Actions) and that they are enough to cover cybersecurity along with the rest of the disciplines that they cover. However, the existing instruments provide only a small fraction to funding cybersecurity research. We need to step up on this, as cybersecurity is one of the very few areas of research that touches almost all aspects of life: from the mundane, such as the coffee maker not working, to the important, such as cars crashing because of faulty software, all the way to national security, such as an electricity grid going down during a time of crisis because of an advanced persistent threat that was maliciously planted by a third-party supplier.
- **Support cybersecurity research projects with very low TRLs.** Existing funding instruments should support cybersecurity projects with a very low TRL. Indeed, current

funding instruments request a medium to high TRL of 4 or 5 which is equivalent to technology implemented and validated in a relevant environment. This deprives all low TRL inventions from the opportunity to receive funding. Without support for very low TRLs, it's unlikely that new algorithms will be created or new systems developed from scratch. And without new algorithms and new systems, we would not be able to pave the way to real ground-breaking innovation. Fundamental low TRL new ideas will not be funded by the EU and without funding they are less likely to be created, at least on European soil. They will more likely be invented (and possibly patented) in non-EU countries and imported back to Europe perpetuating the endless loop. Europe keeps importing its cybersecurity because Europe does not fund low TRL research that will develop the required technology.

- **Provide funding for cybersecurity research projects that last more than five years.** Most existing calls for proposals provide funding for projects that are relatively short: two to three years long. This is shorter than the time it takes for a PhD to complete. Indeed, a PhD often takes five to six years at leading universities, although it can be even seven to eight years in most US universities2. A typical EU-funded project lasts for half or even a third of the duration of a PhD. Such short-lived projects just do not have the time necessary to catalyse the creation of fundamentally new inventions that start from a very low TRL. Some European countries, such as the Netherlands, have already realised this problem and have started funding projects that last five or even six years.

Cyber Security for Europe —

Policy Recommendation

Support blue-sky research in cybersecurity

Context and Findings

Europe's digital sovereignty may be at risk from imported cybersecurity technologies developed in non-EU countries.

Most **EU-funded research projects in cybersecurity have a duration that is too short** to allow the development of fundamentally new innovative solutions.

Most **calls for proposals in the area of cybersecurity ask for projects with a technology readiness level (TRL)** that is far too high for basic research minimising the opportunity to deliver fundamentally new breakthroughs.

European researchers in cybersecurity have demonstrated that their new ideas can have an impact worldwide.

EU funding instruments should **support European cybersecurity researchers at the very earliest stages** of idea development.

The Problem

Although Europe invests significant amounts of funding in cybersecurity research, most of the funds are for **short-term medium/high-TRL projects** which have practically no time to explore fundamentally new and promising technologies. Unfortunately, without the proper environment to create new developments and to nurture them to fruition, **Europe is forced to import its cybersecurity technologies from overseas.** Such a practice not only increases Europe's reliance on imported technology but may also significantly undermine its long-term digital sovereignty.

The Scene

Ground-breaking ideas that could significantly change the world for the better usually need a lot of time to develop and reach maturity. In addition, such ideas also need space: a nurturing environment in which to grow, flourish and find their place in the sun. We should be willing to take high risks to create such environments to give them a chance to ultimately reap high rewards. Highly innovative ideas and technologies need a lot of time between their gestation and the time they achieve a noticeable market share. For example, the mobile phone took 29 years to reach 20% market penetration; LED lights took 24 years; the Internet took more than 25 years, ATM cards took 25 years, etc[1]. These are inventions that most people in the developed world use every day and almost no-one can properly function without. And, still, it took those amazing and desperately useful inventions almost three decades to get out of their nurturing environment and achieve a decent percentage of market share.

The Implications

As the old proverb goes: **"great things just take time"**. Time, indeed, is what most new cybersecurity ideas are deprived of in the current European Commission funding scheme. Indeed, over the past few years research funding in the area of cybersecurity follows a completely different approach with respect to time: it favours short-term projects with immediate market application, high TRLs and rapid market exploitation. This approach effectively deprives cybersecurity ideas from the nurturing environments they need to grow and thrive in: these environments are dwindling, market-ready solutions do not leave enough space for new ideas to grow and new inventions just cannot reach maturity quickly enough.

We are afraid that such a short-term approach to cybersecurity is just not the proper environment for fundamental ideas which need an opportunity to grow and eventually a chance to change the world. We are afraid that, without such a nurturing network for new ideas, Europe will be forced to just import its cybersecurity technology from abroad – a practice which will have dire implications for Europe's long term digital sovereignty.

TRL	Definition
1	Basic principles observed
2	Technology concept formulated
3	Experimental proof of concept
5	Technology validated in relevant environment (industrially relevant environment in case of key enabling technologies)
9	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies or in space)

Policy Recommendations

If EU-supported cybersecurity funding initiatives do not change, we will probably end up with an environment that is hostile to the development and fruition of new inventions. This will probably have an adverse impact on the European cybersecurity ecosystem, the development and fruition of novel inventions and eventually on European digital sovereignty. To reverse this trend, we have three policy recommendations:

1) **Develop new funding instruments to support blue-sky research in the area of cybersecurity**
Currently very few, if any, instruments exist to support blue-sky research in cybersecurity. We need a new FET-like or ERC-like programmes completely dedicated to cybersecurity. Such programmes would support the entire range of cybersecurity projects ranging from hardware security all the way to application security. One might think that such instruments already exist (such as ERC or Marie Skłodowska-Curie Actions) and that they are enough to cover cybersecurity along with the rest of the disciplines that they cover. However, the existing instruments provide only a small fraction of funding to cybersecurity. We need to step up on this, as cybersecurity is one of the very few areas of research that touches almost all aspects of life: from the mundane ones, such as the coffee maker not working, to important one, such as cars crashing because of faulty software, all the way to national-security-related ones, such as the electricity grid going down during a time of crisis because of an advanced persistent threat that was maliciously planted in there by a third-party supplier.

2) **Support cybersecurity research projects with very low TRLs**
Existing funding instruments should fund cybersecurity projects with a very low TRL. Indeed, current funding instruments request a mid- to high- TRL of 4 or 5 which is equivalent to technology implemented and validated in a relevant environment. This deprives all low-TRL inventions from the opportunity to receive funding. Without support for very low TRLs, it's unlikely that new algorithms will be created or new systems developed from scratch. And without new algorithms and new systems we would not be able to pave the way to real ground-breaking innovation. One might think that funding for new algorithms and new systems as well as their testing and validation falls outside the scope of EU support, which is a valid point. But it does not solve the problem. It just takes us back to square one. Fundamental low-TRL new ideas will not be funded by the EU and without funding they are less likely to be created, at least on European soil. They will be more likely to be invented (and possibly patented) in non-EU countries and imported back to Europe perpetuating the endless loop. Europe keeps importing its cybersecurity technology because Europe does not fund low-TRL research that will develop this technology

3) **Provide funding for cybersecurity research projects that last more than five years**
Most existing calls for proposals provide funding for projects that are relatively short: two to three years long. This is shorter that the time it takes for a PhD to complete. Indeed, a PhD often takes five to six years at leading universities although even seven to eight years in most US universities[2]. A typical EU-funded project lasts for half or even a third of the duration of a PhD. Such short-lived projects just do not have the time necessary to catalyse the creation of fundamentally new inventions that start from a very low TRL. Several European countries have already realised this problem and have started funding projects that last five or even six years.

References

1 Hanna, R., Gross, R., Speirs, J., Heptonstall, P., & Gambhir, A. (2015). Innovation timelines from invention to maturity: A rapid review of the evidence on the time taken for new technologies to reach widespread commercialisation. UKERC Technology and Policy Assessment, December.

2 Betsy Bizot. Time to degree in computing, https://cra.org/crn/2014/04/time_to_degree_in_computing/

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Evangelos Markatos markatos@ics.forth.gr | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors and the Commission is not responsible for any use that may be made of the information it contains.

2.2 Password-less Authentication

This brief deals with the difficulties of using several passwords and proposes the use and deployment of password-less authentication. The main recommendations of this brief are:

- **Support the design and development of new password-less authentication methods**. Over the next few years, the progress in computer systems is anticipated to change the current scene in computer science by solving complex problems in very little time (e.g., password guessing, breaking cryptographic keys). This will have an immediate negative effect on the existing, mostly password-based authentication methods, since the problems they already have, such as brute-force attacks and lack of user-friendliness, will have increased due to the enhanced processing power and user experience. Thus, the EU should support research into password-less authentication in order to design and develop methods that are able to cope with the expected advances in computer science (e.g., quantum computers). This goal could not be accomplished without supporting research for alternative password-less authentication solutions: for example, attribute-based and device-based authentication.
- **Provide funding for research on user-machine-IoT authentication**. IoT is a relatively new paradigm that has changed our everyday lives. However, authentication among different entities has not been adequately covered by existing funding schemes leaving a gap in the emerging autonomous and distributed networking ecosystem that is comprised of users, machines and IoT devices. The EU should offer new funding schemes to researchers to design and develop innovative and flexible authentication schemes and protocols, that will satisfy novel concepts (e.g., secure IoT device authentication in a smart home), such as zero-knowledge proof and zero trust that are promising and have not been thoroughly exploited yet.

Cyber Security for Europe

Policy Recommendation

Support research in the password-less authentication

Context and Findings

A strong password is not enough to guarantee security and, even though it can be safely stored (e.g., as a hash value), it can be subject to various attacks that target the user (e.g., through social engineering) or the system (e.g., password leakage). On average, EU citizens handle **hundreds of passwords** which may lead them either to select easily guessed passwords or password reuse that seriously affects security.

Weak and obsolete authentication methods may compromise individual accounts and put at risk via privilege escalation whole European organisations and critical infrastructures. Most of the existing **password-less authentication** solutions are password managers trying to address password overload and password typing problems. Nevertheless, they **still employ passwords**.

Therefore, the EU should request from Member States and other stakeholders to develop and implement **secure, true password-less authentication solutions such as FIDO**, which have been designed and implemented to counteract password attacks, while they ensure user-friendliness and high interoperability following the latest standards.

Nevertheless, the existing solutions cannot cope with the newly emerging **autonomous and distributed networking ecosystem**, which encompasses users, machines and IoT devices. Thus, **innovative** and **flexible authentication methods** and **protocols** are required that also satisfy the concept of **zero-knowledge proof** and **zero trust**.

The Problem

Although authentication (i.e., the procedure of verifying the identity of a person or a device) is one of the pillars of cybersecurity, most authentication systems today are still based on outdated approaches including the use of passwords. Indeed, password-based authentication solutions are subjected to various attacks, such as phishing, guessing and password file leaks, all of which enable attackers to impersonate their victims. According to Verizon's Data Breach Investigations Report, more than 67% of the data breaches in 2020 were caused by password vulnerabilities[1].

As people use an increasing number of passwords – several hundred passwords per user in some cases – they find it difficult to remember them all, and thus tend to reuse the same weak passwords[2].

Multi-factor authentication (MFA) solutions (such as USB tokens, one-time codes, SMS etc) overcome some of the weaknesses caused by passwords. However, it has been proven that MFA can also be vulnerable to several attacks including theft, bypassing, phishing, etc. Password-less authentication solutions, such as biometrics and USB tokens, have been proposed over the years to replace traditional password-based authentication, which indeed address some of its drawbacks (e.g., password stealing and cracking). Nevertheless, these solutions have not managed to prevail due to several issues, such as applicability, security concerns and lack of knowledge[3].

Currently, the majority of password-less authentication deployments mainly act as password managers, which retain many of the weaknesses of passwords.

The Scene

Over recent years, a new approach to authentication has emerged: password-less authentication. In this approach, users prove their identity by convincing the server that they know a secret without ever revealing it. One such approach is FIDO 2 – a password-less authentication and web standard[4]. Nevertheless, the research that has been conducted in the password-less authentication domain is in its infancy because previous and current work has mostly focused on user-to-device authentication with one-time passcodes. Indeed, there are several issues that are yet to be studied including the complexity and applicability of password-less as well as device-to-device authentication. Finally, further research is needed to establish a common framework that will facilitate the evaluation and validation process of new password-less authentication methods.

Despite its importance, EU research funding has not managed to offer the appropriate technologies and solutions for authentication, which will satisfy all the different networking environments, since only a limited number of research projects focus on advancing authentication. Nowadays, with an autonomous and distributed networking ecosystem, the authentication process involves different entities, (i.e., users, machines, IoT devices, etc), in which each one has different requirements and capabilities.

The Implications

The authentication process is an essential part of ICT and has an immediate application to every sector that appears in the Joint Research Council's taxonomy "A Proposal for a European Cybersecurity Taxonomy"[5]. Thus, the implementation of obsolete or weak authentication solutions in critical sectors, such as energy, health, government, transportation, supply chain, etc., might lead to catastrophic consequences for Europe.

New robust authentication solutions should be studied and introduced to cope with the attack surfaces, due to the evolution of the networking ecosystem and the increase in computing power. Otherwise, Europe will be compelled to import secure password-less authentication solutions from overseas, risking its digital sovereignty.

cybersec4europe.eu

How does password-less authentication work?

During the authentication process, a client (say, Alice) tries to convince a server (such as her bank) about her identity. Once Alice manages to prove her identity, the bank logs Alice in and gives her access to her bank account(s). In password-based systems, authentication proceeds as follows:

(i) There is a registration phase where Alice gives a secret (e.g., the password)to the bank which stores it in a password database; the secret should not be revealed to anyone else.
(ii) When Alice wants to log in, she provides the bank with her password; if itmatches the password stored in the database, Alice is granted access.

Password-less systems work in a similar way: they have a secret, they have a registration phase and they require Alice to prove that she knows the secret.

There is, however, one major difference: the bank will never receive a copy of the secret, not even at registration. Since the secret is not stored in the bank and is not transmitted over the network, it is not subject to traditional attacks such as phishing and password database leaks. However, the obvious challenge now is: *"How is Alice going to prove to the bank that she knows the secret when the bank does not even have a copy of this secret?"*.

Although this sounds very difficult (if not impossible), it can be easily solved with public key cryptography: Alice generates two keys:

(i) her private key (the secret) which is stored in a secure space and never revealed (not even to the bank); and
(ii) her public key which is given tothe bank.

The two keys are complementary: what is encrypted with the one can be decrypted with the other.

To verify Alice's identity, the bank proceeds as follows:

(i) it chooses a long random number – say, X (a different one each time) and sends it to Alice
(ii) Alice encrypts X with her private key and sends the result (say, Y) back to her bank;
(iii) the bank decrypts Y with Alice's public key; if the result is X, Alice is granted access.

Policy Recommendations

In the era of ubiquitous access to myriad applications and services that can be granted via different devices and networks, a password, no matter how strong, is not enough to preserve security as it can be subject to theft and phishing. Although EU generously funds the area of cybersecurity, the relevant calls for proposals do not explicitly ask for innovative, user-friendly and secure authentication solutions. This results in the recycling of obsolete password-based authentication techniques.

In this setting, the cybersecurity strategy of EU should focus on stimulating research into password-less authentication to address questions such as exploring ways to enhance the security of device-to-device authentication, to increase the applicability of password-less authentication methods and to evaluate and validate password-less authentication solutions.

In addition, it would be worth investigating whether there are any password-less authentication methods that have not been studied.

1) **Support the design and development of new password-less authentication methods**
Over the next few years, the progress in computer systems is anticipated to change the current scene in computer science by solving complex problems in very little time (e.g., password guessing, breaking cryptographic keys). This will have an immediate negative effect on the existing, mostly password-based authentication methods, since the problems they already have, such as brute-force attacks and lack of user-friendliness, will have increased due to the enhanced processing power and user experience. Thus, the EU should support research into password-less authentication in order to design and develop methods that are able to cope with the expected advances in computer science (e.g., quantum computers). This goal could not be accomplished without supporting research for alternative password-less authentication solutions: for example, attribute-based and device-based authentication.

2) **Provide funding for research on user-machine-IoT authentication**
IoT is a relatively new paradigm that has changed our everyday lives. However, authentication among different entities has not been adequately covered by existing funding schemes leaving a gap in the emerging autonomous and distributed networking ecosystem that is comprised of users, machines and IoT devices. The EU should offer new funding schemes to researchers to design and develop innovative and flexible authentication schemes and protocols, that will satisfy novel concepts (e.g., secure IoT device authentication in a smart home), such as zero-knowledge proof and zerotrust that are promising and have not been thoroughly exploited yet.

References

1 Verizon, 2020 Data Breach Investigations Report, https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report
2 Papadamou, K., Zannettou, S., Chifor, B., Teican, S., Gugulea, G., Caponi, A., ... & Sirivianos, M. (2019). Killing the password and preserving privacy with device-centric and attribute-based authentication. IEEE Transactions on Information Forensics and Security, 15, 2183-2193.
3 Angelogianni, A., Politis, I., & Xenakis, C. (2021). How many FIDO protocols are needed? Surveying the design, security and market perspectives. arXiv preprint arXiv:2107.00577.
4 W3C, 2019, W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins, https://www.w3.org/2019/03/pressrelease-webauthn-rec.html
5 Nai, F., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G. L., Figwer, M. and Lazari, A., A Proposal for a European Taxonomy, JRC118089, Publications Office of the European Union, Luxembourg, 2019.

Contact

This brief was produced by members ofthe CyberSec4Europe consortium.
Contact person: Professor Christos Xenakis xenakis@unipi.gr

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.

cybersec4europe.eu

2.3 Data Protection by Design

This policy brief focuses on privacy enhancing technologies (PETs). The main recommendations of this brief are:

- **Support projects working towards exploring the role of PETs in reducing risk and advancing European data protection policy to promote the use of advanced PETs.** There is a great need to push the boundaries of knowledge on what can be achieved with technologically enforced data protection. We need risk-analysis methodologies that help us understand the risks and benefits of using different PETs. If we can categorize PETs by the level of re-identification avoidance provided (feasibility of re-identification), we can have a better estimate on what is the current state of the art and which technologies and which settings can be considered strong enough to protect sensitive and special categories of personal data. Future Horizon Europe and Digital Europe calls working on data and security technologies of data should be encouraged to provide a re-identification risk-analysis based on re-usable methodology. Different risk-analysis methods work for different technologies, so multiple methodologies will need to emerge and reach a higher level of maturity. Re-use and extension of these methodologies should be encouraged to reach a higher maturity of re-identification risk-analysis that leads to an increased uptake of PETs.
- **Initiate a PET lighthouse project programme**. PETs have been used in a few European-scale systems, e.g. many of the exposure notification apps deployed to inhibit the spread of COVID-19. However, there are many areas where no successful blueprints for deploying PETs in Europe have been established, even though there is a great need. We need a program that encourages projects that:
    - provide reusable technical and legal blueprints for a certain area or use case,
    - deploy PETs in production for public sector and public-private collaborations and
    - achieve a high technical readiness level (TRL 7-8).

  The pilots should be aligned with the European Data Spaces initiative and other relevant programs. We believe that there is an opportunity to reuse the same collaboration that Europe has used for cybersecurity and blockchain innovations – a PET observatory, PET competence co-located with cybersecurity competence centres etc.

- **Launch selected PET lighthouse projects with the United States of America.** A few funding and collaboration instruments exist for EU-US research collaborations. At the same time, developing technical controls to support secure data collaborations with US research partners or to securely use US cloud infrastructures could have a high impact on enabling collaborations. Thus, we recommend having three separate EU-US project calls in Horizon Europe in collaboration with partners like the US National Science Foundation and the National Institute of Health to design and launch privacy technology pilots between European and US data owners, technology providers and regulatory experts. The three projects should be in the domains of healthcare, financial crime prevention and cyber defence. We note that the healthcare project could support both the European Commission's Conquering Cancer and the US White House Cancer Moonshot missions. This program could also collaborate with the EU-US Technology and Trade Council (TTC).

Cyber Security for Europe

Policy Recommendation

Set up a data protection by design and by default technology programme

Context and Findings

Digital services and cloud markets are global and highly competitive, encouraging the transfer of European personal and business data both within and beyond Europe.

Not all non-EU territories provide an adequate level of cybersecurity or data protection to EU citizens' data, as has been demonstrated with high-level court cases[2 3].

With its data protection by design and by default principle, the GDPR **requires appropriate technical and operational measures to be implemented to counteract high risks** involved with the processing and sharing of sensitive data.

In their 2020 set of recommendations, the European Data Protection Board suggests that **cross-border data transfer use cases can be protected by privacy enhancing technologies (PETs)**[1].

The European Union has invested in privacy enhancing technologies in numerous framework programs, but there has been **no notable or significant adoption in Member States**.

The Problem

European personal and corporate data does not enjoy the same level of protection in all territories outside Europe. While adequacy agreements have been negotiated, they have not been found to be compliant with European law by the Court of Justice of the European Union. Well-known, high profile examples of non-compliance cases include Schrems I[2] and Schrems II[3] but there are many more. New agreements are regularly negotiated and re-negotiated, but they may also be challenged in court, leading to a cycle where it is very complicated to develop business and research collaborations between EU Member States and many non-EU countries.

The Scene

PETs have been developed to reduce the need to process identifiable data in systems. While we are used associating privacy with personal data, the PET technologies can also be used to process business or government secrets. There has been notable investment into privacy technologies in the world. The European Commission has invested considerably developing PETs in recent Horizon 2020[4] projects as well as in earlier programs. In the United States, DARPA, IARPA[5], the National Science Foundation and the National Institute of Health have probably invested even more heavily in secure computing technologies alone. In the last five years, venture capitalists have also invested significantly in companies developing individual technologies like secure multi-party computation. The United Kingdom and United States have recently launched a set of prize challenges to unleash the potential of PETs to combat global societal challenges[6]. Singapore has launched a PET Sandbox to develop and pilot use-cases and to support businesses with PET projects[7]. While European legislation is rapidly developing to improve data protection and the data economy, technology adoption by Member States is lagging behind due to a lack of skills and lighthouse projects that could inspire new systems that use PETs to follow the data protection by design and by default principle in the GDPR.

The Implications

Europe is building new data-driven services using technologies and infrastructure from all around the world. Cloud service providers from other territories are offering competitively priced infrastructure and services that are becoming an integral part of our digital transformation. Many European websites are parts of global user tracking and advertising infrastructure that transfers data to other territories. Apps in our mobile phones are storing our identities and secrets, while also using technologies that monitor and share data. Europeans are losing control over that data together with the related identities and business models.

Similarly, our ability to collaborate in global research is reduced, as personal data collaboration with non-European researchers is hindered by the lack of tools supporting privacy-preserving research. This is a most pressing concern in health sciences, where developments in not only genomics and personalised medicine but also pandemic response require collaboration at the widest level with the freedom to share high volumes of sensitive data with confidence.

cybersec4europe.eu

Policy Recommendations

We have three policy recommendations to support the adoption and implementation of European regulations and policies surrounding the data economy, the Digital Single Market and international trade agreements.

1) **Support projects working towards exploring the role of PETs in reducing risk and advancing European data protection policy to promote the use of advanced PETs**
There is a great need to push the boundaries of knowledge on what can be achieved with technologically enforced data protection. We need risk analysis methodologies that help us understand the risks and benefits of using different PETs. If we can categorize PETs by the level of re-identification avoidance provided (feasibility of re-identification), we can have a better estimate on what is the current state of the art and which technologies and which settings can be considered strong enough to protect sensitive and special categories of personal data.

   Future Horizon Europe and Digital Europe calls working on data and security technologies of data should be encouraged to provide a re-identification risk analysis based on re-usable methodology. Different risk analysis methods work for different technologies, so multiple methodologies will need to emerge and reach a higher level of maturity. Re-use and extension of these methodologies should be encouraged to reach a higher maturity of re-identification risk analysis that leads to an increased uptake of PETs.

2) **Initiate a PET lighthouse project programme**
PETs have been used in a few European-scale systems, e.g. many of the exposure notification apps deployed to inhibit the spread of COVID-19. However, there are many areas where no successful blueprints for deploying PETs in Europe have been established, even though there is a great need.

   We need a program that encourages projects that:
   a) provide reusable technical and legal blueprints for a certain area or use case,
   b) deploy PETs in production for public sector and public-private collaborations and
   c) achieve a high technical readiness level (TRL 7-8).

   The pilots should be aligned with the European Data Spaces initiative and other relevant programs. We believe that there is an opportunity to reuse the same collaboration that Europe has used for cybersecurity and blockchain innovations – a PET observatory, PET competence co-located with cybersecurity competence centres etc.

3) **Launch selected PET lighthouse projects with the United States of America**
As there are only a few funding and collaboration instruments that exist for joint EU-US research activities, developing technical controls to support secure data-related work with US research partners or to securely use US cloud infrastructures could have a high impact on enabling formal collaboration initiatives. Thus, we recommend having three separate EU-US project calls in Horizon Europe in collaboration with partners like the US National Science Foundation and the National Institute of Health to design and launch privacy technology pilots between European and US data owners, technology providers and regulatory experts. The three project calls should be in the domains of healthcare, financial crime prevention and cyber defence. We note that the healthcare project call could support both the European Commission's Conquering Cancer[8] and the US White House Cancer Moonshot[9] missions. This initiative could also collaborate with the EU-US Technology and Trade Council (TTC).

References

1 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. European Data Protection Board. Adopted on 10 November 2020. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

2 Schrems I, 6 October 2015: https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-362%252F14&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&lg=&page=1&cid=797704

3 Schrems II, 16 July 2020: https://curia.europa.eu/juris/liste.jsf?num=C-311/18

4 For example, UaESMC, PRACTICE, SafeDEED, SODA, CyberSec, SafeCloud and many others.

5 Intelligence Advanced Research Projects Activity

6 US-UK Privacy Enhancing Technology challenge: https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/

7 Singapore PET Sandbox: https://www.imda.gov.sg/How-We-Can-Help/Data-Innovation/Privacy-Enhancing-Technologies-Sandbox

8 European Commission Cancer Mission: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/eu-mission-cancer_en

9 White House Cancer Moonshot: https://www.whitehouse.gov/cancermoonshot/

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Dan Bogdanov dan@cybernetica.ee | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors and the Commission is not responsible for any use that may be made of the information it contains.

2.4 Community Engagement

This policy brief deals with the recommendations on how to organize the Cyber Security Community. The main recommendations are:

- **Institutionalize the Cybersecurity Competence Community.** It is key that the National Coordination Centres have a systematic approach to registering communities and hubs. With the Regulation providing no guidelines on how possible members, that are not already well networked and informed, should learn about the possibility of application and registration, it is important to develop mechanisms to do so. The benefits and added value for possible members to get acknowledged as members of the Community through the application and registration procedure should be made clear.
- **Use CHECKs to organise the Community, in order to address the existing challenges, while providing flexibility.** We offer the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation, and capacity building in cybersecurity. This concept answers concrete stakeholder demands and is based on requirements, empirical best practices, and stakeholder feedback. The existing diversity in the Member States and their connection to the NCCs and to the Community can be integrated through CHECKs (thus resulting in complementary approaches for addressing the same mission).
- **Dedicate funds to capitalize on the existing community connections and networks**. The H2020 pilot projects (CyberSec4Europe, ECHO, Sparta and Concordia) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups also represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focusses, maturity stages, and objectives. Therefore, dedicated funds should be provided, e.g. under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

Cyber Security for Europe

Policy Recommendation

Facilitate cybersecurity collaboration by creating flexible and accessible community engagement mechanisms

Context and Findings

Europe's cybersecurity potential is not being fully realized due to the existing fragmentation of the cybersecurity landscape and inefficient cooperation and collaboration.

One of the ways to overcome the existing fragmentation is by **promoting the already existing and functioning structures**, especially at the national level, while actively pursuing the aim of a pan-European community through networking.

The concept of **CHECKS** ('Community Hubs of Expertise in Cybersecurity Knowledge') as a grassroots bottom-up approach was developed by CyberSec4Europe in the course of the past years as a way to provide additional involvement channels and complement the bodies and organisations set up by EU legislation, namely the European Cybersecurity Industrial, Technology and Research Competence Centre, the National Coordination Centres and their network, and the Cybersecurity Competence Community.

These community-level **cybersecurity hubs should enable collaboration** between industry and academia, bring market security innovations, and help build capabilities in the area by shortening the chain between decision-making and existing needs on the ground.

The governance model would benefit from **targeted European cybersecurity funding mechanisms** in the next decade to build and maintain a pan-European cybersecurity community.

The Problem

The European Union has articulated the ambition to increase its sovereignty and become a global leader in the digital economy, guided by both by the need to protect democratic values and to develop the capabilities to be resilient when it comes to cybersecurity threats. The European Commission has accordingly identified four main challenges in the area of cybersecurity that need to be overcome in order to realize this ambition[1]:

- Lack of cooperation between Member States, industries, and academia, leading to fragmented efforts in research and development (R&D)
- Insufficient investment in cybersecurity
- Increased demand for skills, know-how, and facilities, while access thereto is limited
- Inconsistency of new policies and governance with the existing legal frameworks

Currently, despite the availability of a broad range of talent, cybersecurity cooperation in the EU suffers from the lack of dedicated institutions and structures that would facilitate collaboration, as well as from the underrepresentation of certain stakeholders that are important for a sustainable approach to R&D, such as privacy and ethics activists.

The Scene

In order to meet these challenges, the European Commission has set up a European Cybersecurity Industrial, Technology and Research Competence Centre, mandated the establishment of National Coordination Centres (NCCs) and their network, and created the notion of the Cybersecurity Competence Community[2].

CyberSec4Europe's Work Package 2 deliverables have assessed the best governance practices for the Community. They analysed governance proposals for the various levels of and diverse approaches to cybersecurity governance, tested them against the input required by the relevant stakeholders, and drew conclusions about the desired characteristics of a governance model that would be able to answer the identified challenges.

Through research and practice, CyberSec4Europe explored bottom-up governance approaches and came up with the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation and capacity-building in cybersecurity. The advantage of such hub structure is low participation threshold for underrepresented actors and the potential to accommodate different types of organisations in order to facilitate coordination.

The Implications

In combating fragmentation in the cybersecurity domain the existence and promotion of "communicating vessels" is of paramount importance. Knowledge should flow where it is needed – i.e., it should be transported between the countries and/or sectors to overcome "the cybersecurity divide" of maturity and funding.

This flow of information is important in order to realize the full potential of Europe's vibrant and dynamic cybersecurity community in achieving more engagement and involvement from the grassroots level of cybersecurity in Europe. At the same time, this communication will ensure broader participation from those who may not have the time, the resources or the opportunities to contribute as stakeholders, users, solutions providers, as well as from regulators and public sector agencies.

The Regulation[3] does not provide any organisational structure for the public-private and the inter-institutional collaborations between the Community members. It is therefore unlikely that the Community will achieve the aim of overcoming the fragmentation of EU cybersecurity stakeholders without additional collaboration mechanisms or dedicated funding.

Policy Recommendations

With no active institutional and funding efforts towards ensuring the cohesion of the European cybersecurity community, the rich existing potential of research, skills-building, and market applications is in danger of not getting exploited. The new structure based on the European Centre, the NCCs, and the Community pillars needs to include more tangible actions for nurturing and structuring the Community. A cohesive European cybersecurity ecosystem is essential to further develop and enhance the European innovation potential, as well as to ensure European digital sovereignty. Based on the findings of CyberSec4Europe's Work Package 2, we offer the following three main policy recommendations:

1) **Institutionalize the Cybersecurity Competence Community**
   It is key that the National Coordination Centres have a systematic approach to registering communities and hubs. With the Regulation providing no guidelines on how possible members, that are not already well networked and informed, should learn about the possibility of application and registration, it is important to develop mechanisms to do so. The benefits and added value for possible members to get acknowledged as members of the Community through the application and registration procedure should be made clear.

2) **Use CHECKs to organise the Community, in order to address the existing challenges, while providing flexibility**
   We offer the concept of a collaborative network of local cybersecurity hubs, 'Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)', which are envisioned as environments for community-level research, innovation, and capacity building in cybersecurity. This concept answers concrete stakeholder demands and is based on requirements, empirical best practices, and stakeholder feedback. The existing diversity in the Member States and their connection to the NCCs and to the Community can be integrated through CHECKs (thus resulting in complementary approaches for addressing the same mission).

3) **Dedicate funds to capitalize on the existing community connections and networks.**
   The H2020 pilot projects (CyberSec4Europe, ECHO, Sparta and Concordia) and their focus groups, as well as the European Cyber Security Organisation (ECSO) and its working groups also represent a rich connected community. The majority of relevant stakeholders are involved in the cybersecurity ecosystem through the four pilots and ECSO, forming an ecosystem with different focusses, maturity stages, and objectives. Therefore, dedicated funds should be provided, e.g. under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

References

[1] See D2.1 Governance Structure v1.0, https://cybersec4europe.eu/wp-content/uploads/2020/02/D2.1-Governance-Structure-final-Submitted.pdf

[2,3] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Natalia Kadenko n.i.kadenko@tudelft.nl | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors and the Commission is not responsible for any use that may be made of the information it contains.

2.5 SMEs

This policy brief deals with support for SMEs. The main recommendations are:

- **Encourage cybersecurity research projects targeting sector-specific SMEs, as well as with efficient and actionable plans to attract relevant SMEs.** Building cybersecurity solutions (e.g., cybersecurity technologies, guidelines, approaches, and standards) for SMEs require their satisfactory participation and consultation in the project to understand their requirements. This is of utmost significance for the project's outcomes and success. There are also industry-specific security needs. While certain threats are global in nature, many SMEs must fight against specialized threat actors. For example, healthcare must protect IT infrastructure, patient data, and smart medical devices, while retail & wholesale must secure the customer and payment card data. However, it appears that the majority of cybersecurity projects funded by the EU and its Members States are aimed at SMEs as a whole than at specific sectors. The same has been evident from the low usefulness and applicability of most project-produced cybersecurity solutions for SMEs that are funded by the EU and its Member States. This poor-quality results from projects can also be attributed to the enormous difficulties of attracting and engaging with SMEs, which most projects do not adequately consider and plan for. The two potential strategies to address the quality issue of cybersecurity solutions produced from projects are as follows:
    - It is well known and often has been acknowledged that the majority of SMEs lack adequate human and financial resources. Cybersecurity projects should therefore be well-publicised with the reassurance of clear and immediate benefits for the participating SMEs.
    - Cybersecurity research projects should target sector-specific SMEs and have efficient and actionable plans to attract a large number of participants or relevant SMEs
- **Encourage cybersecurity research projects with efficient and actionable plans for large-scale dissemination of their results to relevant SMEs.** The cybersecurity solutions developed by projects supported by the EU and its Member States should ideally reach and be adopted by all applicable SMEs to make the best use of the resources and efforts invested in them. Every relevant SME in the region is entitled to use and benefit from these project-produced cybersecurity resources. However, most EU and its Member States funded projects struggle to reach a few hundred, and in exceptional cases to a few thousand SMEs (this is insignificant given the number of SMEs in the millions) with the present dissemination methods or practices. Particularly, such projects to reach out to micro and small SMEs, who could greatly benefit from the project-produced cybersecurity solutions, as well as make their results accessible and attractive for them is a key challenge. These projects cannot continue to operate on the premise that relevant SMEs will find and utilise the cybersecurity solutions they have produced simply because these resources have been made available online on the websites. Therefore, cybersecurity research projects should have efficient and actionable plans for large-scale dissemination of their results, and such projects should receive high priority for funding.

Cyber Security for Europe

Policy Recommendation

Support research in SMEs cybersecurity

Context and Findings

SMEs are the backbone of the EU economy and are also among **the most vulnerable groups to cyberattacks and cybercrimes**. The COVID-19 pandemic, which accelerated existing trends in remote work and e-commerce, has made their cybersecurity condition even worse. Additionally, SMEs are **often resource-constrained and suffer many other challenges** that affect their cybersecurity posture.

SMEs might substantially benefit from affordable and free cybersecurity solutions developed through the EU and the Member States-funded research projects. However, **many of these cybersecurity solutions, unfortunately, fall short of their needs, while others do not reach the majority of relevant SMEs**.

Therefore, the EU funding instruments and the Member States should **prioritise and encourage cybersecurity projects targeting sector-specific SMEs, as well as those with efficient and actionable plans for attracting participants and disseminating findings**.

The Problem

Small and Medium-sized Enterprises (SMEs) make up a major portion of the European Union (EU) economy[1]. They are, unfortunately, the group that is most vulnerable to cyberattacks and cybercrimes. The COVID-19 pandemic has made the situation even worse with the introduction of a new digital realm where telecommuting and online businesses are increasingly becoming the norm for SMEs' functioning. Additionally, the majority of SMEs also face resource limitations and other difficulties, such as low management awareness and commitment to cybersecurity[2], which restrict their ability to invest and develop capability in cybersecurity.

In such a situation, European SMEs might benefit from free and affordable security solutions resulting from the EU and its Member States' funded projects. However, most of such security solutions do not fulfil the need of SMEs, and some that may meet them do not reach the needful SMEs.

The Scene

Digitalisation and security ought to work together. The digital transformation of European SMEs is progressing rapidly. This transformation has been acknowledged as a critical component of competitiveness for businesses and an engine of growth and welfare for the European economy and territories[3]. While it is obvious that the digitalisation of European SMEs is paramount, there are many aspects that need to be considered in order to realise its opportunities. However, underlying all of that is cybersecurity, which is absolutely fundamental[4]. There is no efficient digitalisation without cybersecurity.

Therefore, cybersecurity should be a core component of SMEs' digital transformation strategy. The European SMEs must realise that the benefit of cybersecurity is not limited to defending businesses against cyber threats but is much more. Cybersecurity can help SMEs to gain customers' and business partners' trust and confidence which are of paramount importance to doing business in the digital era[5]. Additionally, cybersecurity-ready SMEs can have a strategic growth advantage over competitors since they will experience less business disruption as a result of cybersecurity issues and can therefore concentrate their resources on innovation and creating more valuable organisations.

The Implications

SMEs play a crucial role in the European economy and innovation. Thus, they cannot be left unprotected from ever-changing and growing cyber threats. This becomes more critical if considering the fact that for many SMEs, essentially, small-SME and micro-SME, sustaining a major cyberattack can be tremendously difficult; reputational damage, financial losses, and penalties levied after a cyber-attack could force them out of business. Additionally, many SMEs are connected to one another, as well as with large enterprises. Therefore, the consequences of a major cyberattack on one SME may not limit to that SME alone but also spread to many other associated businesses and communities.

A rapid progression of digitalisation in European SMEs and continuously growing cyber threats both in quantity and complexity, contribute to increasing attack surface and making SMEs increasingly susceptible. On the other hand, SMEs are still substantially behind in adopting cybersecurity.

The future of European SMEs cannot be deemed secure without significant action and assistance from the EU and the Member States. However, it is unlikely that the situation of the European SMEs could change unless some radical actions are taken to encourage SMEs' participation and engagement in projects as stakeholders, both as information providers and end-users of the results.

cybersec4europe.eu

Policy Recommendations

We offer the following two policies for EU funding instruments and the Member States to promote and uplift SMEs' cybersecurity and make them more competitive:

1) **Encourage cybersecurity research projects targeting sector-specific SMEs, as well as with efficient and actionable plans to attract relevant SMEs.**

Building cybersecurity solutions (e.g., cybersecurity technologies, guidelines, approaches, and standards) for SMEs require their satisfactory participation and consultation in the project to understand their requirements. This is of utmost significance for the project's outcomes and success. There are also industry-specific security needs. While certain threats are global in nature, many SMEs must fight against specialized threat actors. For example, healthcare must protect IT infrastructure, patient data, and smart medical devices, while retail & wholesale must secure the customer and payment card data. However, it appears that the majority of cybersecurity projects funded by the EU and its Members States are aimed at SMEs as a whole than at specific sectors. The same has been evident from the low usefulness and applicability of most project-produced cybersecurity solutions for SMEs that are funded by the EU and its Member States[2]. This poor-quality results from projects can also be attributed to the enormous difficulties of attracting and engaging with SMEs, which most projects do not adequately consider and plan for. The two potential strategies to address the quality issue of cybersecurity solutions produced from projects are as follows:

- It is well known and often has been acknowledged that the majority of SMEs lack adequate human and financial resources. Cybersecurity projects should therefore be well-publicised with the reassurance of clear and immediate benefits for the participating SMEs.
- Cybersecurity research projects should target sector-specific SMEs and have efficient and actionable plans to attract a large number of participants or relevant SMEs.

2) **Encourage cybersecurity research projects with efficient and actionable plans for large-scale dissemination of their results to relevant SMEs.**

The cybersecurity solutions developed by projects supported by the EU and its Member States should ideally reach and be adopted by all applicable SMEs to make the best use of the resources and efforts invested in them. Every relevant SME in the region is entitled to use and benefit from these project-produced cybersecurity resources. However, most EU and its Member States funded projects struggle to reach a few hundred, and in exceptional cases to a few thousand SMEs (this is insignificant given the number of SMEs in the millions) with the present dissemination methods or practices. Particularly, such projects to reach out to micro and small SMEs, who could greatly benefit from the project-produced cybersecurity solutions, as well as make their results accessible and attractive for them is a key challenge. These projects cannot continue to operate on the premise that relevant SMEs will find and utilise the cybersecurity solutions they have produced simply because these resources have been made available online on the websites. Therefore, cybersecurity research projects should have efficient and actionable plans for large-scale dissemination of their results, and such projects should receive high priority for funding.

References

[1] European Commission. (2022). Entrepreneurship and small and medium-sized enterprises (SMEs), https://single-market-economy.ec.europa.eu/smes_en

[2] ENISA (June 2021). Cybersecurity for SMES: Challenges and recommendations, ISBN: 978-92-9204-409-1 – DOI: 10.2824/770352

[3] Interreg Europe. (April 2022). Fostering the digital transformation of SMEs, https://www.interregeurope.eu/sites/default/files/2022-04/Policy%20brief%20on%20digital%20transformation.pdf

[4] World Economic Forum. (May 2017). There can be no digital economy without security, https://www.weforum.org/agenda/2017/05/there-can-be-nodigital-economy-without-security/

[5] G. Lloyd (February 2020). The business benefits of cyber security for SMEs, Computer Fraud & Security, Elsevier.

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact Person : Sunil Chaudhary sunil.chaudhary@ntnu.no | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors, and the Commission is not responsible for any use that may be made of the information it contains.

2.6 European Digital Identity Wallet

This policy brief deals with the control of the data for the EU Digital Identity Wallet (EUDIW). The main recommendations are:

- **The European Data Protection Supervisor should issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDIW in Article 6a section 2 of the eIDAS 2 proposal.** The EUDIW ecosystem is complex, because issuers can be Member States (Article 6a section 1), but can also be private entities (Article 6a section 2). In principle, insofar as personal data needs to be processed for the provision of the wallet app, these private entities would hold a role under the GDPR. Nevertheless, more challenging would be the circumstance where the wallet provider does not need to process any personal data (the desirable scenario), but still develops software that enables certain data processing activities. Under these circumstances, the allocation of the data controller role might be complicated. It should be considered that wallet providers, as the entities developing the wallet app, are concerned with the final purpose of the wallet, and although the user will hold a certain control (e.g., with which parties they share their data), this management will ultimately rely on the application created by the wallet provider. More specifically, the developers of the wallet app pre-define in technical terms how data is collected and for what potential purposes and they hold "interpretative control"; that is to say, they determine how to transform data into actionable decisions. It could still be challenging the fact that these entities might not physically process any personal data. However, it should be noted that the European Court of Justice has ruled in several cases that it is irrelevant whether a concerned party has actual access to the data when it comes to ascertaining its controllership (Case Fashion ID C-40/17, Case Jehovan todistajat C-25/17).
- **Support and provision of funding to conduct research on the impact of innovative technologies in EU regulatory frameworks.** The scenario presented above is not unique and technologies are challenging the way traditional legal concepts are understood. It would be worth investigating more in depth the application of traditional GDPR administrative roles (data controller/processor) to the scenarios raised by new technologies, like the EUDIW, but also others such as artificial intelligence or distributed ledger technologies. Such studies would be crucial to understanding if traditional legal concepts remain applicable to new technological developments and might suggest rethinking these concepts to cover upcoming advances.

Cyber Security for Europe

Policy Recommendation

Allocating controllership in the European Digital Identity Wallet

Context and Findings

The **eIDAS 2 proposal** enables the transition towards **new models for identity management (IdM)**, placing the user at the centre of the ecosystem and limiting the role of identity providers (providers of electronic attestations of attributes/ issuing authorities), to the provision of identity credentials (electronic attestations of attributes). In this context, **the European Digital Identity Wallet (EUDIW) emerges as a key piece to empower users in the control of their personal data**, enabling identification and authentication processes through the sharing of credentials with external parties.

The eIDAS 2 proposed ecosystem **displaces the responsibility of identity providers in the authentication process to the wallet**. However, **the wallet**, as a technology that should be managed exclusively under user control, **challenges the General Data Protection Regulation's (GDPR) traditional role for data controllers** as there is no entity, but the user, who should have actual access to the data.

There already exist multi-purpose digital wallets that enable the management of credentials containing users' personal data (e.g., Apple Wallet or Google Wallet). Nevertheless, **the scope of the eIDAS 2 proposal makes necessary legal certainty concerning the allocation of controllership and liability** for the personal data that will be stored in and managed via the European Digital Identity Wallet.

The Problem

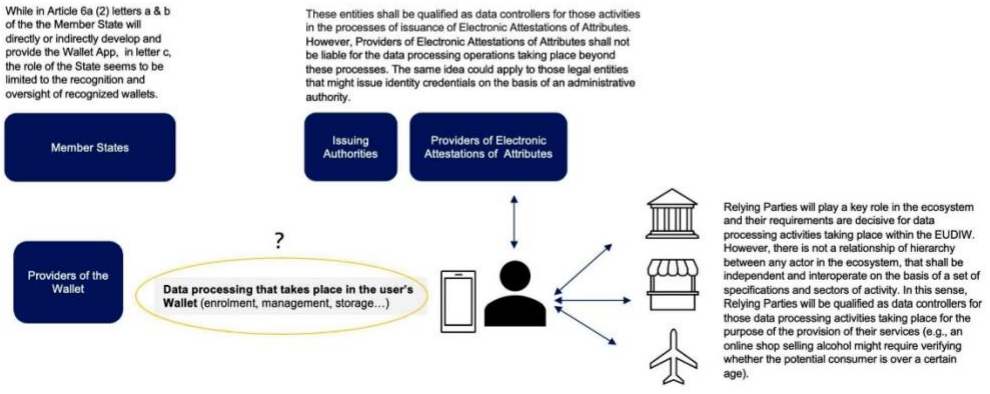
Ascertaining controllership over certain data processing activities is crucial to allocating GDPR obligations and responsibilities. Nevertheless, the EUDIW ecosystem is complex and encompasses different entities, holding various roles and who perform a set of data processing activities with separate purposes, but that are necessary or contribute to the overall functioning of the ecosystem. In particular, the data processing taking place in and via the EUDIW represents a challenge to traditional legal notions of a data controller and data processor according to the GDPR (Articles 4. (7)(8)).

The Scene

Article 6a, section 1, of the eIDAS 2 proposal establishes that "each Member State shall issue a European Digital Identity Wallet". However, section 2 of this Article envisages three different possibilities for the issuance of the EUDIW. More specifically, section 2(c) envisages the possibility of issuance by private entities and recognised by a Member State. In such a scenario, it will be crucial to determine to what extent implementing acts decide/rule the data processing conditions (regarding the issuance of the wallet app and the requirements in the wallet App itself); and what is the role of Member States is in providing such recognition.

The Implications

The allocation of controllership under the GDPR is essential to determining the obligations and responsibilities of the party that must and can successfully protect a user's personal data. These obligations should be clearly envisaged in the EUDIW ecosystem; in particular, account should be taken of the possibility of the provision by private entities. Otherwise, the security of a user's personal data could be left under their exclusive responsibility and in the event of errors, misfunctioning, etc, liability might be complicated to enforce.



cybersec4europe.eu

Policy Recommendations

The quick developments in the technological landscape require regulations to adapt faster than ever. The **lack of legal studies and adaptation of traditional regulations can be a brake to technology advances** due to the legal uncertainty and the risk for potential stakeholders to deploy a technology. On the other hand, the implementation of technologies without the adequate legal guarantees can result in a situation where there is an absence of legal rights. On this basis, the following recommendations are proposed:

1) **The European Data Protection Supervisor should issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDIW in Article 6a section 2 of the eIDAS 2 proposal.**

   The EUDIW ecosystem is complex, and despite according to Article 6a section 1, issuers of the EUDIW will be Member States, Article 6a section 2 envisages the possibility of the provision of wallet apps by private entities. In principle, insofar as personal data needs to be processed for the provision of the wallet app, these private entities would hold a role under the GDPR. Nevertheless, more challenging would be the circumstance where the wallet provider does not need to process any personal data (the desirable scenario), but still develops software that enables certain data processing activities. Under these circumstances, the allocation of the data controller role might be complicated.

   It should be considered that wallet providers, as the entities developing the wallet app, are concerned with the final purpose of the wallet, and although the user will hold a certain control (e.g., with which parties they share their data), this management will ultimately rely on the application created by the wallet provider. More specifically, the developers of the wallet app pre-define in technical terms how data is collected and for what potential purposes and they hold "interpretative control"; that is to say, they determine how to transform data into actionable decisions.

   It could still be challenging the fact that these entities might not physically process any personal data. However, it should be noted that the European Court of Justice has ruled in several cases that it is irrelevant whether a concerned party has actual access to the data when it comes to ascertaining its controllership (Case Fashion ID C-40/17, Case Jehovan todistajat C-25/17).

   In conclusion, this scenario might represent a less common approach to the concept of data controller, in particular, considering existing IdM ecosystems, where the identity provider has responsibility when personal data is being processed for identification and authentication processes. In the scenario of the wallet, despite wallet providers ideally not having access to personal data, they are still concerned with the final purpose of the wallet and therefore the data processing that takes place in and via the wallet.

2) **Support and provision of funding to conduct research on the impact of innovative technologies in EU regulatory frameworks.**

   The scenario presented above is not unique and technologies are challenging the way traditional legal concepts are understood. It would be worth investigating more in depth the application of traditional GDPR administrative roles (data controller / processor) to the scenarios raised by new technologies, like the EUDIW, but also others such as artificial intelligence or distributed ledger technologies. Such studies would be crucial to understanding if traditional legal concepts remain applicable to new technological developments and might suggest rethinking these concepts to cover upcoming advances.

References

1 D6.3 Final Pilot deployment and evaluation of User Experience and GDPR Compliance. **OLYMPUS Project** *(Oblivious identitY Management for Private and User-Friendly Services)* [Project Deliverable] pp.76-91. https://olympus-project.eu/wp-content/uploads/2021/10/Olympus_pu_d6_3_v1_2.pdf

2 OLYMPUS contributions and recommendations for improving cross-border identification in the European Union. **OLYMPUS Project** *(Oblivious identitY Management for Private and User-Friendly Services)* [Policy Brief]. https://olympus-project.eu/wp-content/uploads/2021/11/Olympus_pu_policy-brief_v1_0.pdf

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Professor Antonio Skarmeta skarmeta@um.es / Researcher Cristina Timón mariacristina.timon@um.es

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.

2.7 Vulnerability attribution

This policy brief deals with vulnerability attribution. The main recommendations are:

- **Fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks.** The fact that modern systems and services employ multiple components of different nature makes the detection of their vulnerabilities a highly non-trivial process. Thus, having available defences for up-to-date threats is not useful if we cannot effectively/efficiently (and automatically) determine from which specific vulnerabilities the tested systems suffer from. For this reason, the EU should fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks that are designed for being applicable to systems and services employing multiple components of different nature. Such frameworks should be easy to deploy by even non-experts in the security field who wish to incorporate different technological components into their applications.
- **Fund and support research towards the development of frameworks for assisting developers during the vulnerability patching procedure.** Solely detecting the vulnerabilities of modern systems and services comprised of multiple diverse components is likely not enough; we need to mitigate those vulnerabilities and restore those systems' security. In addition, it is worth mentioning that software developers are often non-experts with regard to the security aspect of every single component that they incorporate into their applications. Even if they are experts in certain components, they may not be aware of the potential security and privacy risks that arise when combining those components with other components of different nature. Thus, the EU should fund and support research towards the development of frameworks for assisting software developers into patching the vulnerabilities found in multi-component systems and services with state-of-the-art defences. The offered assistance can take the form of suggestions/guidelines or, where possible, the form of updates: that is, automatically patching the vulnerable system. Again, such frameworks should be easy to deploy by even non-experts in the security field who wish to improve their systems' resilience against state-of-the-art attacks.
- **Forming guidelines for the diffusion of accurate information regarding the risks and vulnerabilities of modern software systems and services.** The EU should fund and support research towards the formation of guidelines and suggestions for the dissemination of accurate information with regard to security/privacy vulnerabilities found in modern software systems and services. In particular, generic vulnerability attribution might cause misinformation and, as a consequence, the negative public opinion and/or security/privacy concerns towards the wrong technological component. For example, the reason that an authentication system has been bypassed might not be a vulnerability of the algorithm per se, rather than a buffer overflow (or the opposite). Thus, we need to form appropriate guidelines and suggestions that require the diffusion of the exact root cause(s) of each security incident. Doing so will facilitate the dissemination of accurate information to the public and avoid negative opinions and/or loss of people's trust towards recent technological advancements.

Cyber Security for Europe

Policy Recommendation

The need for proper vulnerability attribution/ characterisation and handling

Context and Findings

Security flaws, glitches or weaknesses (vulnerabilities) are increasingly being discovered in software systems and services.

Software vulnerabilities can be exploited by potential adversaries allowing them to **compromise sensitive data or computational resources**.

Different types of software vulnerabilities do exist, each of them **requiring a different handling approach for mitigation**.

The multi-component nature of modern software systems and services may introduce additional vulnerabilities, and thus increase the advantage of potential adversaries.

EU funding instruments should **support research towards the development of vulnerability attribution/characterization and patching frameworks.**

EU should fund and support research towards the formation of **guidelines and suggestions that ensure the diffusion of accurate information to the public** in regards to the risks and vulnerabilities found in systems and services employing multiple (diverse) components.

The Problem

Security flaws (vulnerabilities) are increasingly being discovered in software systems and services produced by even well-known software companies. These weaknesses can be exploited by skilled adversaries to compromise sensitive data or computational resources.

The multi-component nature of modern software systems and services has the potential to introduce a variety of additional vulnerabilities that increase the adversaries' advantage of exploiting them.

For example, a common system-based vulnerability, namely buffer overflow[1], occurs when the volume of input data exceeds the capacity of the memory buffer and overwrites adjacent memory locations. Buffer overflow can be mitigated using either stack canaries or safe functions instead of unsafe ones.

As another example consider SQL injection (SQLi)[2], which is a web-security vulnerability that allows an adversary to interfere with the queries that an application makes to its database. Conducting successful SQLi attacks may result in unauthorized access to personal/sensitive information (e.g., credit card numbers, passwords, health records), subvert an application's logic, etc. SQLi attacks can be prevented by using parameterized queries, validating the user's inputs, and enforcing appropriate privileges with strict access rights.

The aforementioned examples are just two instances of a large pool of possible vulnerabilities introduced by various components of different nature.

The Scene

We live in an era where the majority of systems and services are comprised of multiple (different) components. These components often have diverse characteristics, and thus require different handling approaches for mitigating their vulnerabilities and restoring the system's security. Simply put, different bugs require different handling methodologies.

What is important to note is that many of these vulnerabilities lack proper treatment that may result in increased security/privacy risk. This is mainly because the majority of security incidents are often characterized by general terms and descriptions, such as advanced persistent threat (APT), which fail to capture and report the exact root cause(s) that led to those incidents.

For example, consider an authentication system based on face recognition[3] that has been bypassed. The root cause of the bypass can be a buffer overflow[1], social engineering[4] or a model inversion attack[5]. Characterising the vulnerability that led to this security incident using a general (non-specific) term, such as APT, may result in an incomplete mitigation strategy as well as misinforming the public about the actual root cause of the problem.

Thus, while it is possible to handle bugs individually, there is a growing need for a generally applicable framework that accurately characterises/attributes the vulnerabilities of a system composed of multiple components of varying nature.

The Implications

Handling all types of vulnerabilities using the same approach/methodology will most likely result in an incomplete mitigation, and thus increased risk of exploitation. Especially in the case where security-critical and privacy-sensitive systems are exploited, the potential consequences can be severe, even causing fatalities.

Not only that, but a non-comprehensive vulnerability attribution framework may also result in the misinformation of the general public, which in turn might cause negative opinion or security/privacy concerns towards the wrong technological component.

As a result, it is crucial that the handling of different vulnerabilities must be made based on their type. This will result in a comprehensive solution that is devoid of any security, privacy, or ethical concerns.

cybersec4europe.eu

Policy Recommendations

If EU-supported funding initiatives do not change, we will probably end up with an environment that is hostile to the development and fruition of systems and services employing different types of technological components. This will probably have an adverse impact on the European software ecosystem, the development and fruition of novel inventions and eventually on European digital sovereignty. To reverse this trend, we have three policy recommendations:

1) **Fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks**
   The fact that modern systems and services employ multiple components of different nature makes the detection of their vulnerabilities a highly non-trivial process. Thus, having available defences for up-to-date threats is not useful if we cannot effectively/efficiently (and automatically) determine from which specific vulnerabilities the tested systems suffer from. For this reason, the EU should fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks that are designed for being applicable to systems and services employing multiple components of different nature. Such frameworks should be easy to deploy by even non-experts in the security field who wish to incorporate different technological components into their applications.

2) **Fund and support research towards the development of frameworks for assisting developers during the vulnerability patching procedure**
   Solely detecting the vulnerabilities of modern systems and services comprised of multiple diverse components is likely not enough; we need to mitigate those vulnerabilities and restore those systems' security. In addition, it is worth mentioning that software developers are often non-experts with regard to the security aspect of every single component that they incorporate into their applications. Even if they are experts in certain components, they may not be aware of the potential security and privacy risks that arise when combining those components with other components of different nature. Thus, the EU should fund and support research towards the development of frameworks for assisting software developers into patching the vulnerabilities found in multi-component systems and services with state-of-the-art defences. The offered assistance can take the form of suggestions/guidelines or, where possible, the form of updates: that is, automatically patching the vulnerable system. Again, such frameworks should be easy to deploy by even non-experts in the security field who wish to improve their systems' resilience against state-of-the-art attacks.

3) **Forming guidelines for the diffusion of accurate information regarding the risks and vulnerabilities of modern software systems and services**
   The EU should fund and support research towards the formation of guidelines and suggestions for the dissemination of accurate information with regard to security/privacy vulnerabilities found in modern software systems and services. In particular, generic vulnerability attribution might cause misinformation and, as a consequence, the negative public opinion and/or security/privacy concerns towards the wrong technological component. For example, the reason that an authentication system has been bypassed might not be a vulnerability of the algorithm per se, rather than a buffer overflow (or the opposite). Thus, we need to form appropriate guidelines and suggestions that require the diffusion of the exact root cause(s) of each security incident. Doing so will facilitate the dissemination of accurate information to the public and avoid negative opinions and/or loss of people's trust towards recent technological advancements.

References

[1] Larochelle, D., & Evans, D. (2001). Statically detecting likely buffer overflow vulnerabilities. In 10th USENIX Security Symposium (pp. 177–190).

[2] Boyd, S. W., & Keromytis, A. D. (2004, June). SQLrand: Preventing SQL injection attacks. In International conference on applied cryptography and network security (pp. 292-302). Springer, Berlin, Heidelberg.

[3] Bud, A. (2018). Facing the future: The impact of Apple FaceID. Biometric technology today, 2018(1), 5-7

[4] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, (pp. 113-122).

[5] Fredrikson, M., Jha, S., & Ristenpart, T. (2015, October). Model inversion attacks that exploit confidence information and basic countermeasures. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (pp. 1322-1333).

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Elias Athanasopoulos eliasathan@cs.ucy.ac.cy | cybersec4europe.eu

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the view of the authors and the Commission is not responsible for any use that may be made of the information it contains.

3 The Reactive Approach

Between M26 and M47, CyberSec4Europe researchers received several invitations to contribute[2] to various policy-related activities. Some of these are included below.

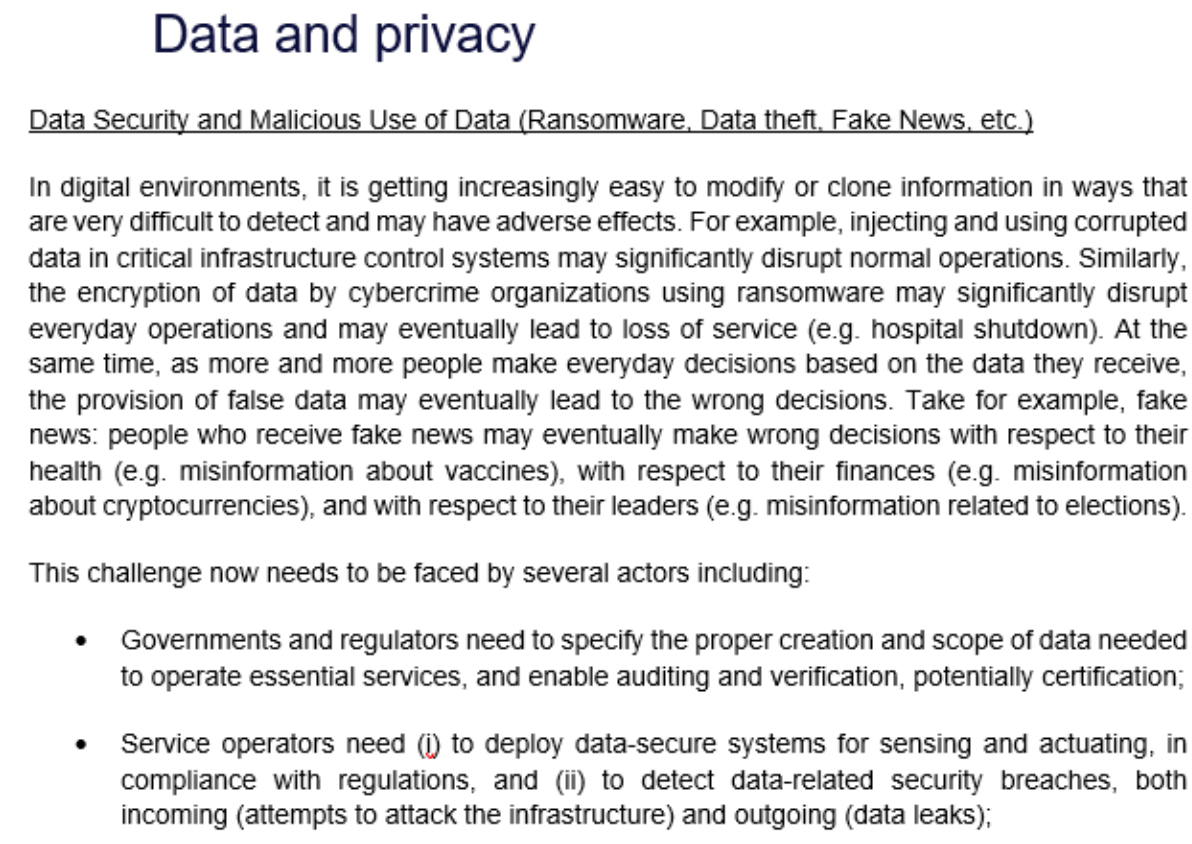
3.1 ECSO: The European Cyber Security Organisation

The project contributed to the ECSO's vision document on cyber security.

Figure 1: The project made contributions to ECSO's vision document

The main contributions were in the areas of data security and privacy.

[2] 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.



Data and privacy

Data Security and Malicious Use of Data (Ransomware, Data theft, Fake News, etc.)

In digital environments, it is getting increasingly easy to modify or clone information in ways that are very difficult to detect and may have adverse effects. For example, injecting and using corrupted data in critical infrastructure control systems may significantly disrupt normal operations. Similarly, the encryption of data by cybercrime organizations using ransomware may significantly disrupt everyday operations and may eventually lead to loss of service (e.g. hospital shutdown). At the same time, as more and more people make everyday decisions based on the data they receive, the provision of false data may eventually lead to the wrong decisions. Take for example, fake news: people who receive fake news may eventually make wrong decisions with respect to their health (e.g. misinformation about vaccines), with respect to their finances (e.g. misinformation about cryptocurrencies), and with respect to their leaders (e.g. misinformation related to elections).

This challenge now needs to be faced by several actors including:

- Governments and regulators need to specify the proper creation and scope of data needed to operate essential services, and enable auditing and verification, potentially certification;
- Service operators need (i) to deploy data-secure systems for sensing and actuating, in compliance with regulations, and (ii) to detect data-related security breaches, both incoming (attempts to attack the infrastructure) and outgoing (data leaks);

Figure 2: Excerpt from the contribution of the project to ECSO's vision document.

3.2 ENISA: European Union Agency for Cybersecurity

3.2.1 Research and innovation needs

On 11 July 2022 ENISA held a roundtable on "CYBERSECURITY RESEARCH AND INNOVATION NEEDS AND PRIORITIES". The project made a presentation on Artificial Intelligence – threats and opportunities.

The project proposed to give researchers easier access to the data:

Lack of Data leads to **asymmetric threats**

- Researchers have limited access to data
  - Data is usually collected by large companies that may or may not share
  - Researchers find it difficult to collect data
  - Researchers need to follow a strict and rigorous process to get (if at all) access to data
- **Attackers do not have to respect GDPR**
  - Or any other regulation
  - Attackers may collect data without any restrictions

This asymmetry implies that

→**Attackers can train their attack systems much better** than defenders can train their defense systems…

→ **Give Researchers easier access to data…**

The project also proposed to support proactive research:

Proactive Research Areas

- Use AI to **discover vulnerabilities** in systems (smart fuzzing)
  - And fix them
- Use AI to **mimic human behavior** (e.g. for fraud)
  - And develop algorithms that can detect this kind of fraud
- Use AI to develop **deep fakes**
  - And develop approaches to detect such fakes

15

3.3 JRC

Timelex contributed to the following Joint Research Center study: Study on APIs - Legal infrastructure in organizations - API viewpoint (JRC/IPR/2021/VLVP/2707). This is a legal study aiming to produce a report describing and comparing legal-organisational practises of data sharing through APIs. The Study analysed decision-making structures and models, roles and responsibilities, and coordination mechanisms (system and processes). The analysis was interview driven with specialised stakeholders, and covered practices in different sectors (public and private) and at different levels (European, national, regional, local), and both SMEs and big technological players.

3.4 DG JUST

Timelex contributed to the following DG JUST study: Study on model contract terms and fairness control in data sharing and in cloud contracts and on data access rights, JUST/2020/RCON/FW/CIVI/0098. This is a study examining current practices in relation to data sharing in data intensive sectors, and in cloud computing contracts. The objective is to define fairness assessment criteria, and to assess whether current practices are considered fair; with a view of assessing the potential impact of a fairness test that could be introduced under the future Data Act. In addition, the study will determine the potential of a model contract clauses for data sharing and/or cloud computing contracts, including identification of anticipated changes and modelling of economic impacts. Timelex leads the legal data collection and analysis.

3.5 European Parliament

The consortium under the leadership of GUF contributed to the Public hearing “European Digital Identity Wallet and Trust Services” of the European Parliament, ITRE Committee, on “The European Digital Identity Wallet”. The main points were:

- Identity management and wallets are an important infrastructure
  - Essential for trust in European digitalisation
  - Potentially a showcase how to do things
- Go for it but be aware of
  - The need to gain and preserve user trust
  - Technological challenges
  - Conflicting requirements
- Involve all communities, especially independent experts and civil society
- Have the decisions done with utmost transparency and by the most eligible entities
- Reserve sufficient resources (e.g. time and money)

3.6 Other contributions

University of Trento contributed the following article: "Building Principles for Lawful Cyber Lethal Autonomous Weapons" https://ieeexplore.ieee.org/document/9740711/. It deals with possible measures and design principles for lawful cyber lethal autonomous weapons.

Afonso Ferreira (UPS-IRIT) is part of two Groupes Thématiques Nationaux of the French Ministry for Research that follow Horizon Europe (HE): Cluster 3 and the Digital part of Cluster 4. As such, he contributes to the Work Programmes of HE (2023-24, currently). In addition, he contributes

European research and innovation policy for the CNRS as a whole (30,000 staff) and his National Institute for Digital Research (46 research laboratories), as Head of the Europe sector for Digital at the CNRS,.

4 Summary

Over the past four years, the partners of the CyberSec4Europe project have been doing research and development in the area of cybersecurity. The experience that they gained can be used not only in technical contributions for cybersecurity technologies but also in policy interventions. Towards this direction they have collected their policy recommendations in this deliverable. To disseminate them in a fast and easy way they have formatted the recommendations into two-page-long "policy briefs". Each policy brief deals with one issue: it presents the problem, the findings, and lists 2-3 policy interventions that can be used to address the problem. The policy briefs prepared are:

- Develop new funding instruments to support blue-sky research in the area of cybersecurity
- Support the design and development of new password-less authentication methods
- Institutionalize the Cybersecurity Competence Community
- Support projects working towards exploring the role of privacy enhancing technologies (PETs) in reducing risk and advancing European data protection policy to promote the use of advanced PETs
- Encourage cybersecurity research projects targeting sector-specific SMEs, as well as with efficient and actionable plans to attract relevant SMEs
- Encourage the European Data Protection Supervisor to issue an Opinion clarifying the application of the data controller role to the scenarios described for the issuance of the EUDIW in Article 6a (2) of the eIDAS2 Proposal.
- Fund and support research towards the development of comprehensive vulnerability attribution and characterization frameworks

In addition to the above the partners have made contributions to several European and Member States organizations and institutions including ECSO, ENISA, JRC, DG JUST, the European Parliament, and others.