The European watch
on cybersecurity & privacy

D2.8 Recommendations report on R&I needs

Author(s)	AEI CIBERSEGURIDAD
Status	Final
Version	v.1
Date	16/06/2021

Dissemination Level

☒ PU: Public

□ PP: Restricted to other programme participants (including the Commission)

□ RE: Restricted to a group specified by the consortium (including the Commission)

□ CO: Confidential, only for members of the consortium (including the Commission)

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

Document identifier: cyberwatching .eu – WP 2 – D2.8	
Deliverable lead	AEI CIBERSEGURIDAD
Related work package	WP2
Author(s)	M.RAMIREZ (AEI)
Contributor(s)	M. Miller (CONCEPTIVITY), D. Wallom (UOXF), N. Zazzeri (TRUST-IT)
Due date	30/04/2020
Actual submission date	16/06/2021
Reviewed by	N. Ferguson & N. Zazzeri (TRUST-IT) D. Wallom (UOXF)
Start date of Project	01/05/2017
Duration	51 months

Revision history

Version	Date	Authors	Notes
v0.1	30.04.2021	M.Ramirez (AEI Ciberseguridad)	First version
V0.2	17.05.2021	M. Miller (CONCEPTIVITY)	Internal review
V0.3	17.05.2021	Niccolò Zazzeri (Trust-IT)	Internal review
V1.0	18.05.2021	D. Wallom (UOXF)	Input regarding the Project Radar
V1.1	18.05.2021	M.Ramirez (AEI Ciberseguridad)	Changes following reviewer's comments and Executive Summary added
VFinal	16.06.2021	N. Ferguson (Trust-IT)	

Executive Summary

This deliverable presents the results of the **analysis of the Cybersecurity and Privacy European research projects and their results**, including the characterisation of the projects comprised in the Project Radar, the analysis of the Market and Technology Readiness Levels (MTRL) of those projects that interacted with Cyberwatching.eu by providing their MTRL self-assessment score and the analysis of the matrix of the identified technologies and services. The objective of this quantitative and qualitative analysis is to facilitate the connection between funded projects and future funding actions, so that organisations can take advantage of previous results to build new products and services, thus optimizing European funds invested in research.

The document itself can be seen as a **reference guide** for organisations to identify what has been done, how far it has been done and by whom. Along with the **clustering activities** that have been carried out to facilitate the creation of **synergies** between the projects, and which are also described in this document, this guide aims to promote knowledge transfer and collaboration between stakeholders.

Another important aspect that is included in the document refers to **less developed research spaces**, based on the priorities identified by ECSO in its WG6 in relation with the Security Research and Innovation Agenda (SRIA). By analysing the information of the projects, conclusions are reached about which are those less developed spaces, and where it is necessary to **increase the investment effort** to achieve better results and fill the gaps.

In addition, a complete list of the projects comprised in the Project Radar is included, with a brief reference to their specific results, a link to each project website (if applicable) and the classification of its results in relation to the priorities defined by ECSO.

This guide is a starting point, which can be actively followed by projects if the use of some of the tools developed within the project is promoted, such as the Project Radar or the Cyberwatching Marketplace, which allow, respectively, classify and analyse the results of each project and offer a first commercialization of those results, with the additional support of initiatives such as the Horizon Result Booster that favours collaboration between projects.

The conclusions and recommendations are derived from this analysis, together with the contributions received from the projects themselves in the framework of the clustering activities, where we proposed that they identify the greatest barriers to the commercialization of the results of their projects and how the EC could help overcome them.

Table of Contents

Table of tables

Table of figures

1 Introduction

This report provides an overview on the cybersecurity and privacy ecosystem, the projects and activities at a European level and areas of particular strength and possible weakness to ensure a minimal level of R&I within all areas.

This deliverable is the result of the *WP2 Research & Innovation observatory and* more specifically of the *Task 2.3 – Synergies & Convergence*. It comprises the analysis of the critical information acquired during the scoring and Principal Components Analysis (PCA) clustering processes carried out in Task 2.1 – Cybersecurity and Privacy Technology radar and *Task 2.2 – Mapping & clustering of R&I in EU & Associated Countries*, with the aim of facilitating the connection between funded projects and future funding actions to find synergies and convergences. The aim is to facilitate the uptake or re-use **of previous results to build new products and services**.

The European Union's "open science" model implies greater transparency and accessibility to the results and research data of the activities subsidized with public resources. This is reflected in the different policies at European level.

Horizon 2020 and Horizon Europe promote the opening of research results, both publications and data. The projects financed under the framework programmes have to openly deposit both the research results and the data - datasets - in an open access repository.

EOSC, European Open Science Cloud Declaration (2017) on Open Access to Scientific Data is an initiative of the European Commission, with the aim of promoting and supporting changes that accelerate the most effective transition to open science and innovation, eliminating barriers to the reuse of information and research tools.

The Horizon Results Booster is a package of specialised services delivered to FP7, H2020, HE projects at no cost and fully supported by the European Commission to maximise the impact of R&I public investment and further amplify the added value of the Framework Programmes (FPs).

And the recently launched the Open Research Europe platform, for the publication of scientific documents that can be freely accessed, will present the results of research funded by Horizon Europe, the EU's research and innovation program for 2021-2027, and by its predecessor, Horizon 2020.

For researchers to be able to reuse research results from projects in the field of cybersecurity, it is necessary to previously perform an accurate classification and analysis of the results, and this is precisely what is intended to be collected in this report, together with the identification of low developed spaces aligned with SRIA and Horizon Europe priorities.

2 Characterisation of projects

To achieve an accurate characterisation of the projects, Cyberwatching.eu proposed three activities that have been developed during the four years of the project. The first two are the basis for the development of the third one, and the following sections describe the relationship between them.

2.1 The Project Radar

The Project Radar is the method chosen to present the evaluations of the project outputs and how ready they are for use by users outside the project developing community. *D2.2 Technology Radar 1st report – Autumn 2018*[1] established the methodology, and how the Cyberwatching.eu project has adapted it to suit its needs. It then presented the first radar edition[2] – Autumn 2018 – and presented an analysis of the available data from **134 projects**. *D2.5 Cybersecurity Technology Radar 2nd Report*[3] *– Spring 2020* presented the analysis from **261 projects**, allowing to analyse trends and patterns in the funding landscape far more accurately than before, and taking into account the MTRL self-assessment. Now in Spring 2021, *D2.7 – Final Technology Radar Report* is being presented in parallel with this deliverable, with the analysis of **265** projects**.**

The Project Radar presents **six** segments, according to the Level 2 of the cyberwatching taxonomy described in *D2.1 A Taxonomy of Cybersecurity and Privacy.*

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

Table 1: Hierarchical arrangement of taxonomy categories and clusters

The Project Radar also presents **five** concentric rings, according to project lifecycle.

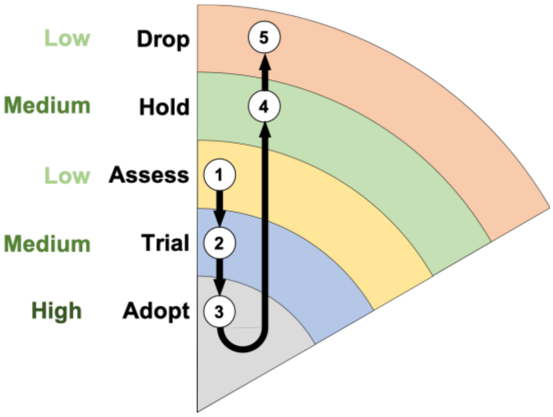


Figure 1: Mechanics of the technology radar

Finally, the Project Radar uses the MTRL self-assessment comparing the project score with the mean of the MTRL values within the same ring/segment to determine the readiness for the market. Traffic-light coloured dots for each project number show the project market and technology readiness level relative to the average of their lifecycle stage. Green showing fastest relative progress. To know more about how this relative performance is calculated, see D2.7. Final Technology Radar Report or visit [https://radar.cyberwatching .eu/doc/readiness](https://radar.cyberwatching.eu/doc/readiness).

[1] https://www.cyberwatching.eu/d22-cybersecurity-technology-radar-1st-report-autumn-2018

[2] https://radar.cyberwatching.eu/radar/autumn-2018

[3] https://www.cyberwatching.eu/d25-cybersecurity-technology-radar-2nd-report

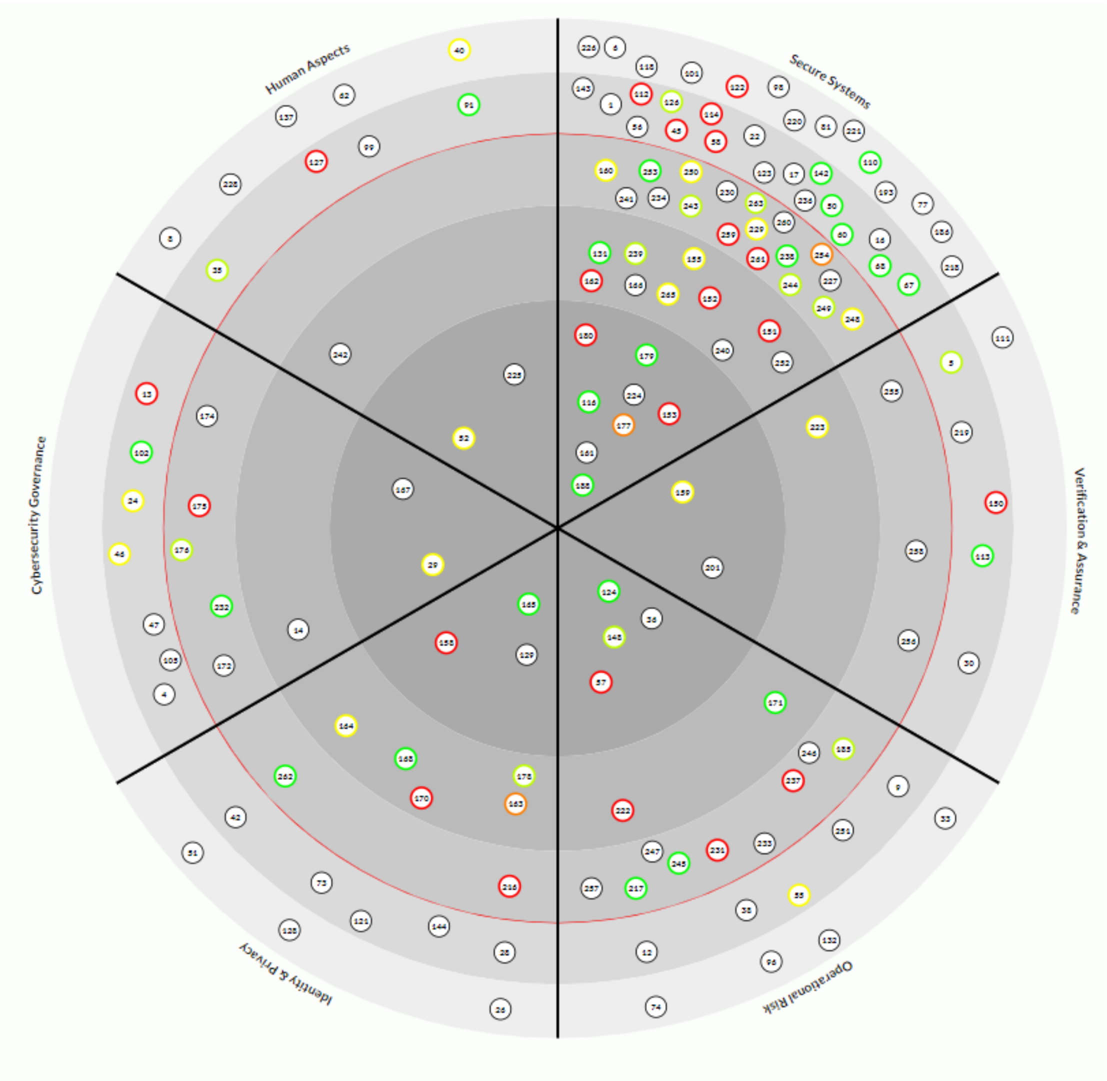


Figure 2: Live radar with MTRL self-assessment

The Project Radar has been analysed together with the MTRL self-assessment collection in 4 stable editions: Spring 2019, Autumn 2019, Spring 2020 and Autumn 2020 (Autumn 2018 edition did not include MTRL assessment).

The live version of the radar is compiled on-demand based on the latest information found in the database. Unlike stable editions, live radars are fluid in their content and display, although for this deliverable we have taken into account projects that have updated their MTRL status in the period from Autumn 2020 and Spring 2021.

When looking at the latest incarnation of the project radar it is clear that there are a number of sectors in which due to issues within COVID-19 pandemic etc that have had little or no investment recently, of particular note in this respect is Human Aspects of Cybersecurity for which all bar two of the projects in this sector are in either Hold or Drop. Unfortunately, neither of the two projects are still active have an MTRL self-assessment performance against them and so the current condition of their outcomes as products is unknown. In a similar condition are Cybersecurity Governance and Certification and Verification, both of whom are very sparsely populated. Cybersecurity Governance though has a majority of projects that have performed an MTRL self-assessment. Other areas, Operational Risk, Identity & Privacy and Secure Systems are overall very well populated with almost equal numbers of projects within each ring. Secure Systems is of course still the most populated sector though when comparing the live edition with that from Autumn 2019 there is still a perceptible trend towards the later rings, indicating that there is an interruption in the pipeline funding these types of projects as we would possibly expect. It is gratifying to see though that within the Secure Systems sector that a majority of projects have completed an MTRL self-assessment, for which a majority are performing well in terms of their readiness. Overall of the 145 projects displayed on the Live Radar on the 17th May 2021, 76 have performed MTRL self-assessments a rate of 52%. This compares with a rate of 37% for the Radar published Autumn 2020 (177:66) showing that not only are there more MTRL self-assessments occurring but the ratio of projects that are performing them is increasing.

2.2 Mapping and clustering of EC projects

Cyberwatching.eu fosters project collaboration, through a two-stage clustering of projects.

The first stage brings together those projects whose overall externally described are aligned, from the high-level goals of projects as described by their public descriptions.

The second stage clustering is around more technically focused capabilities or components within projects. The objective of this empirical analysis is to discover distinct smaller groups of projects that are consistent in their relationship to a set of defined general characteristics.

These clusters of projects are supposed to form the basis for identifying:

- Future collaboration and sharing of experience on common technical priorities.
- Re-use of project results by other current and future projects with components, technical ideas, methodologies or best practices identified by a repeatable statistical analysis rather than qualitative methodologies.
- Identify market positioning and potential exploitation opportunities with other projects.

The second stage clustering procedure is based on the outcome of a classic Principal Components Analysis (PCA)[4].

In *D2.4 - Statistical analysis of the Cybersecurity and Privacy ecosystem*[5] ¸**177 projects** were analysed and **56 of 67 active projects were clearly assigned to a cluster**. In *D2.6 Statistical analysis of the Cybersecurity and Privacy ecosystem*[6], **261 projects** were analysed, and 55 from **74 active projects were clearly assigned to a cluster**.

From this last analysis we can conclude that from the 261 projects, "Secure Systems and Technology" appears as the most dominating factor, while from the 74 active projects, the most dominant factors are "Secure Systems and Technology" and "National and international security & governance". With this PCA analysis, Cyberwatching.eu taxonomy is validated, as we can conclude that cohesion within the three correlation groups remains strong.

This analysis also provides an opportunity for the wider community and the EC to gain insight into where the projects are located within the cybersecurity and privacy landscape. The objective of this empirical analysis is to discover distinct smaller groups

[4] (a) Pearson, K. 1901. On Lines and Planes of Closest Fit to Systems of Points in Space. Philosophical Magazine, 2 (11): 559–572. (b) Hotelling, H. 1933. Analysis of a complex of statistical variables into principal components. Journal of Educational Psychology, 24, 417–441, and 498–520. (c) Jolliffe, I.T. 2002. Principal Component Analysis, 2nd edition, Springer-Verlag.

[5] https://www.cyberwatching.eu/d24-statistical-analysis-cybersecurity-and-privacy-ecosystem

[6] https://www.cyberwatching.eu/d26-statistical-analysis-cybersecurity-and-privacy-ecosystem

of projects that are consistent in their relationship to a set of defined general characteristics and hence where technical and other synergies not immediately obvious exist.

The clusters that arise from this mapping are the basis for designing specific activities to foster collaboration between projects. The list of clustered projects is included in APPENDIX 1.

Together with the MTRL evaluation, this first clustering of projects allows to deepen to a more concrete level of synergies, to carry out some sub-tasks like mutual presentation of achieved results; preparation of webinars and reports, assistance of mediation to one-on-one and one-on many meetings for collaboration, both from the scientific and the business opportunity preparation point of view. Those tasks effectively are the synergy-ignition levers of Cyberwatching.eu. These sub-tasks are introduced in section *3.2 MTRL and clustering activities* and their results are detailed in section *4.3 Catalogue of R&I services and clusters of projects*.

2.3 Description of projects outputs

Within this activity, a list has been prepared with the outputs from the projects included in the Project Hub[7], in order to evaluate their market maturity and their affinity with Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity[8]. This will make it possible to determine the alignment between the results obtained and the trends set by Europe, in order to determine whether it is necessary to maintain the established strategy or identify areas in which it is necessary to reinforce investment are identified.

From the total **282** projects in the hub, we have focused on the **204 projects** that, due to their scope, can be part (or have been part in the past) of the project radar, that is, that in some way they generate new technology, techniques, standards or policies.

The full list of the 204 project outputs that have been analysed for this deliverable is included in APPENDIX 2.

3 Analysis and identification of the MTRL of the different projects

One of the methods for identifying synergies and convergences of R&I projects is the analysis and identification of the closeness to the market. As it was appointed by EC in the M12 light review of Cyberwatching.eu, a TRL matrix would not help in identifying such synergies, as grants are given to projects to get to a TRL value based on the instruments.

At this point, Cyberwatching.eu developed a methodology to assess the closeness to the market, as it is described in D2.3 Methodology for the Classification of Projects/Services and Market Readiness, by analysing both the current state of TRL and MRL of a project.

[7] https://www.cyberwatching.eu/projects

[8] ECSO WG 6 – SRIA and Cybersecurity Technologies: Input to the Horizon Europe Programme 2021-2027: Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity

3.1 MTRL assessment

With the launch of the second edition of the radar (Spring 2019), Cyberwatching.eu started the MTRL collection from projects. The next table summarises the number of projects that participated in each MTRL collection, where a total of **80 projects have sent their MTRL status in at least one edition**, and only 31 of them are still ongoing by the time this deliverable is being developed:

	Spring 2019	Autumn 2019	Spring 2020	Autumn 2020	Spring 2021
N. Projects	29	44	40	19	33

Table 2: Evolution of MTRL collection

With the launch of the live radar edition[9] (Spring 2021), MTRL self-assessment was converted into an online tool[10], so that each project can complete the questionnaire and update their MTRL status whenever they consider there is a significative advance in TRL or MRL. MTRL collection has been transformed in a promotional activity, where Cyberwatching.eu consortium has to encourage projects to join the radar, adjust their JRC tags and update their MTRL status.

There has been just one project that have sent the MTRL status in the 5 editions: ECHO. Seven projects sent their MTRL status in 4 editions: STOP-IT, FENTEC, CYBER-TRUST, ASTRID, DEFEND, THREAT-ARREST and SECUREIOT. We have to take into account that finished project don't usually evolved their results, so it's **easier to get an engagement from active projects**.

Having said this, the MTRL analysis presented in this report has to be taken as a mere reference, as it takes the last MTRL updated from the projects (e.g. SAINT project finished by February 2021, but they sent their last MTRL in Spring 2019, so it's easy to deduce that their MTRL has evolved during the last 2 years).

Nevertheless, some conclusions can be drawn from the MTRL collected so far. Within the 80 projects that sent their MTRL score in any of the editions (Table 3), there were 1 CSA, 1 ECSEL-RIA, 1 ERC-SyG, 4 MSCA-RISE, 31 RIA and 42 IA. It seems that **the methodology is easier to apply in RIA projects and even more so in IA projects, so these types of projects are more willing to participate in the MTRL self-assessment**.

	Project hub	MTRL collection	%
CSA	7	1	14%
ECSEL-RIA	1	1	100%
ERC-SyG	1	1	100%
MSCA-RISE	6	4	67%
RIA	74	31	42%
IA	63	42	67%

Table 3: Type of instruments in the MTRL analysis

Regarding the representation of the segments designated in the Cyberwatching.eu taxonomy level 2 (Table 4), we notice a similar representation on the Project Hub and the Project Radar. The majority of the projects that have sent their MTRL score belong to **Security Systems segment**, not only because most of projects in the hub belong to this segment, but also because the relative percentage of projects in the hub sending their MTRL scores is higher in this segment (41%), although the relative percentage for projects in the **National and international security and governance** is even

[9] https://radar.cyberwatching.eu/radar/

[10] MTRL: Market and Technology Readiness

higher (47%). This could mean that **these types of projects are interested in assessing and improving their MTRL performance**.

	Project hub	MTRL collection	%
Operational Risk and Analytics	28	11	39%
Verification and Assurance	19	7	37%
Secure Systems and Technology	99	41	**41%**
Identity, Behaviour, Ethics and Privacy	25	8	32%
National and international security and governance	17	8	**47%**
Human Aspects of Cybersecurity	16	5	31%

Table 4: Number of projects per type of Level 2 taxonomy in the MTRL analysis

If we compare the TRL and MRL for projects in all the segments of level 2 of the Cyberwatching.eu taxonomy (Table 5 and Table 6), we can see that in general, TRL values are always higher than MRL values, which means that **all projects should invest more resources in marketing activities from the very beginning of the project**.

	TRL																																								
Operational Risk	1	2	3	3	4	6	6	6	7	7	9																														
Verification & Assurance	1	3	3	6	7	7	7																																		
Secure Systems	1	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	6	6	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	8	9
Identity & Privacy	3	3	3	3	3	6	6	7																																	
Cybersecurity Governance	3	6	7	7	7	7	7	9																																	
Human Aspects	3	6	7	7	7																																				

Table 5: TRL values classified by taxonomy level 2

	MRL																																								
Operational Risk	0	3	3	4	4	4	4	4	5	5	6																														
Verification & Assurance	1	2	2	3	4	4	5																																		
Secure Systems	1	1	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	5	6	6	7	7	7
Identity & Privacy	2	3	3	4	4	4	5	5																																	
Cybersecurity Governance	3	3	4	5	5	6	6	7																																	
Human Aspects	1	4	5	6	6																																				

Table 6: MRL values classified by taxonomy level 2

If we look at the "**mean"** (the average of a data set.) of the TRL and MRL scores of the projects in each segment (Table 6), we can see differences between TRL and MRL in the segments of the taxonomy. Considering that **National and international security and governance** and **Human Aspects of Cybersecurity projects** are supposed to involve less technology, the difference between TRL and MRL can make sense. More worrying is the difference in the **Verification and Assurance** segment, taking into account that it comprises risk management, that is a very important issue.

	TRL mean	MRL mean	Difference TRL-MRL
Operational Risk and Analytics	4,9	3,8	1,1
Verification and Assurance	4,9	3,0	**1,9**
Secure Systems and Technology	4,7	3,9	0,8
Identity, Behaviour, Ethics and Privacy	4,3	3,8	0,5
National and international security and governance	6,6	4,9	**1,8**
Human Aspects of Cybersecurity	6,0	4,4	**1,6**

Table 7: Average TRL and MRL scores for each segment of the taxonomy

So far, we have identified that a good target for **marketing capability actions** are projects in the **Verification and Assurance** segment, since they need to align their TRL advances with their MRL capabilities.

One important thing when evaluating the MTRL status of the projects is that it should be **self-assessed by the same person in the project**, because if we have a look at APPENDIX 3 EVOLUTION OF MTRL ASSESSMENT, we can see that there are many projects that have gone back and forth with their MTRL score, and the only reason for this behaviour is that different persons have been completing the questionnaire for each edition, so the performance in the long time is unclear. This also provides important information about consortia: **not all the members in a consortium share the same vision of the advances of the project**.

Looking at Table 8, attending to the **"mode"** (the most common number in a data set) of each individual question in the MTRL questionnaire, and focusing only in the 7 questions related to MRL (to assess the closeness to market), it remains clear that projects find the **major difficulties** in the **Go-To-Market area**, where most projects have just defined an initial business model and value proposition, but didn't carry out interviews with customers/beneficiaries to understand their needs, and the **Manufacturing/Supply chain**, where most projects have just started to identify potential suppliers, partners and customers and map them in an initial value chain analysis, but are far from manufacturing processes. The **strongest points are the Project Team**, where most of projects have a balanced team with technical and business experience within the consortium, and **Documentation**, where most of projects have developed position papers, press releases, etc. for dissemination.

As a conclusion, it is important to **carry out activities with projects related to the Go to market area and the Manufacturing/Supply chain, such as helping them to get in contact with potential clients and partners, so that they can adapt the results of the projects to the real needs of the consumers and can establish commercial relationships.**

Question		Most common answer	
Q3	PRODUCT DEFINITION/DESIGN	3	The product/service has been scaled from laboratory to pilot scale and issues that may affect achieving full scale have been identified.
Q4	COMPETITIVE LANDSCAPE	2	Primary market research to prove the product/service commercial feasibility has been completed and basic understanding of competitive products/services has been demonstrated.
Q5	TEAM	4	Balanced team with technical and business experience within the consortium.
Q6	DOCUMENTATION	4	Position papers, press releases, posters, etc. have been elaborated for the dissemination of the project outcomes.
Q7	INTELLECTUAL PROPERTY MANAGEMENT	2	Initial means of protection have been considered (or initial definition of exploitable assets has been considered).
Q8	GO-TO-MARKET	1	Initial business model and value proposition have been defined.
Q9	MANUFACTURING/SUPPLY CHAIN	1	Potential suppliers, partners and customers have been identified and mapped in an initial value chain analysis.

Table 8: Most common answers for questions related to MRL

For a detailed evolution of the MTRL self-assessment for each of the 80 projects according to the different collections carried out for each edition of the project radar, see APPENDIX 3.

3.2 MTRL and clustering activities

The specific sub-tasks carried out as synergy ignition levers started from the first clustering of projects developed in October 2019 by the University of Oxford as described in D2.4 - Statistical analysis of the Cybersecurity and Privacy ecosystem. To develop the sub-tasks, we focused on projects that belonged to one of the 5 identified clusters, were still active by that time and were in scope of the radar, since we need their MTRL status to start these MTRL activities.

In D2.4 (October 2019) we had 56 active clustered projects, but at the time that we started these activities (December 2019) we had 45 active projects, and only 37 were in the scope of the Radar. Therefore, the target at that moment was 37 projects.

Our **first action** was to try to collect MTRL values from all the 37 active and clustered projects that were in the scope of the radar, and invite them to a specific **webinar** focused on **how to improve their MRL with a few success stories**, taking into account the recommendation from EC in the M30 light review of building upon the Cyberwatching.eu experience and activities, promoting clusters and supporting internal cluster collaboration, given that marketing capabilities appeared weaker than technical capabilities.

To select the success stories, we analysed the results of the MTRL matrix in that moment, with 44 projects (29 were clustered, 15 were not).

Firstly, we focused on the 12 projects that had sent MTRL questionnaires both in Spring 2019 and Autumn 2019 editions, so we could compare the results, and from the evolution we observed that:

- 5 of them remained with the same values for both TRL and MRL.
- 5 of them increased their TRL but kept their MRL.
- 1 increased both TRL and MRL.
- 1 increased their MRL keeping the same TRL, but the increase was related to the team, not specifically to marketing issues.

This brought the following conclusions at that moment:

- Almost the half of the projects didn’t change their MTRL values in 6 months.
- More than 80% of the projects that increased their TRL didn’t increase their MRL.

After we focused on specific marketing capabilities, analysing the specific questions related to it in the MTRL questionnaire (Q3-Q9), and even more specifically those questions directly related to commercialization (Q8 - business model, value proposition, market and customer analysis, partnerships with stakeholders, and Q9 - relations with manufacturers and supply chain), we could see that, in absolute terms, from the 44 projects in the MTRL matrix for Autumn 2019 edition, the projects with highest values for Q8 and Q9 were **PROTECTIVE** (ended by August 2019) and **GHOST** (ended by April 2020) and that we also had acceptable values for Q8 and Q9 for other 5 projects.

N	Project	End	TRL	MRL	Cluster	Q8	Q9
102	PROTECTIVE	ago. 19	7	7	II	4	4
52	GHOST	abr. 20	7	5		4	4
110	SafeCloud	ago. 18	7	6		4	3
124	SMESEC	may. 20	8	6	IV	3	3
46	EU-SEC	dic. 19	7	5	II	3	3

60	LIGHTest	ago. 19	7	5		3	3
142	UNICORN	dic. 19	4	5	V	3	3

Table 9: Projects with higher values for questions related to commercialization in Autumn 2019

Then, we contacted these projects to check their interest in participating in the webinar to give some hints and advices in building marketing capabilities during project execution.

Finally, representatives from PROTECTIVE, GHOST and SMESEC projects accepted the invitation, and together with a representative from the EIC Accelerator (very market oriented funding instrument), a webinar took place on 11 March 2020 under the title "FROM RESEARCH TO MARKET: PROMISING OUTPUTS ARE NOT ENOUGH!". Following the webinar, a report[11] was prepared and published collecting the recommendations from the speakers for improving the market readiness.

Our **second action** to continue with the clustering activities was to organize **2 conference calls** (virtual meetings) in which we pretended to involve 2 groups of projects with similar Marketing Readiness Levels: one group of projects with MRL score between 3 and 4, and another group of projects with MRL scores between 6 and 7.

The goals for those meetings were:

- Identify common potential groups of clients, suppliers and partners that could be invited for next Cyberwatching.eu concertation meetings.
- Define common dissemination and networking strategies.
- Create partnerships to carry out additional research activities that can improve the commercial exploitation of partial results.
- Express their major barriers for commercialization, giving advice to EC in order to minimize these barriers.

With these goals in mind, we invited the projects identified in those 2 groups to participate in the meetings.

- Group 1 (9 projects): Active projects with MRL 3-4
  - SealedGRID
  - PANACEA
  - GUARD
  - SAPPAN
  - FENTEC
  - CYBER-TRUST
  - BPR4GDPR
  - PAPAYA
  - DEFEND

- Group 2 (12 projects): Active projects with MRL 5-6-7
  - POSEIDON
  - SECREDAS
  - InfraStress
  - CARAMEL
  - EnergyShield
  - CyberSec4Europe
  - ECHO
  - SCOTT
  - CS-AWARE

[11] R&I preparation for the market

- SecureIoT
- THREAT-ARREST
- STOP-IT

For both meetings, we invited Georgios Lyssandredis (Group 1) and Ada Matei (Group 2), from the **Common Competence Centre at DG RTD**, who presented **the Horizon Results Platform**[12], Michel Drescher from University of Oxford, who presented the new **live project radar** and Nick Ferguson from TRUST IT (and Cyberwatching.eu coordinator), who presented the **Cyberwatching.eu Marketplace** and the new **Horizon Results Booster service**[13].

In APPENDIX 4, you can find some conclusions drawn from the analysis of those projects that were exposed during the meetings, before starting the debate.

In the **first virtual meeting**, which took place on the 9th of July 2020 and involved 7 active R&I projects with an MRL score of between 3 and 4 (FENTEC, SealedGRID, PAPAYA, DEFEND, PANACEA, GUARD and SAPPAN), some starting points for collaboration emerged. One of them is the joint organisation of webinars focusing on three sectors:

- **Healthcare**: the theme was proposed by PANACEA with the aim to raise awareness of cybersecurity among hospital and public sector managers. The idea was supported by DEFEND and by SAPPAN.
- **Energy**: the theme was proposed by SealedGRID, which is oriented towards digital infrastructure and government and public authorities in the energy sector. The topic raised interest in the SAPPAN and DEFEND projects.
- **Financial**: the theme was proposed by FENTEC, which is working with Functional Encryption that can be applied to digital currency, motion detection, and stat analysis. This target sector raised lower interest compared to the previous two among projects joining the meeting.

During the **second cluster meeting**, which took place on the 16th of July 2020 and involved a group of projects with an MRL score of 5-6-7 (CS-AWARE, STOP-IT, PoSeIDon, CyberSec4Europe, ECHO, SecureIoT, SECREDAS, InfraStress, EnergyShield and CARAMEL) [14], a variety of thematic areas was discussed.

- **Threat intelligence and Information sharing**: the theme was proposed by ECHO, which is organising a table top exercise that will take place in October and will engage 20-25 organisations for incidents management, early warning and information sharing. The topic was welcomed by Cybersec4Europe, which is working on it in the context of banking with CONCORDIA. The CARAMEL project also showed some interest in information sharing for connected vehicles since the European Commission is putting great emphasis on data sharing in and out the vehicles. SECREDAS deals with the same field area (vehicles) and, during the meeting, proposed creating a larger group of interest and participating in a collaborative meeting.
- **Local Public Administration**: Cybersec4Europe and CS-AWARE, which is ending in August, are interested in organising a webinar or a workshop to engage public organisations and the two projects agreed to have a parallel discussion about this. CS-AWARE suggested the creation of a restrictive

[12] Horizon Results Platform

[13] Horizon Results Booster Service

[14] THREAT-ARREST project couldn't attend the meeting but sent the information for the analysis to be included in future meetings.

discussion group, including national organisations, focusing on COVID19 medium- and long-term impact on PA and its digitalisation process.

- **Finance/banking**: CS-AWARE aims to commercialise the Cybersecurity Awareness Solution for Local Public Administrations they developed within the project, and for this reason they are interested in creating synergies with partners working on the same topic, in order to find complementary solutions to reach the market.

Cyberwatching.eu offered support in the organisation, hosting and promotion of public webinars involving the projects clustered according to their target sectors. Cyberwatching.eu also proposed helping with a summary document showcasing the main outputs of the discussion groups, which can be sent to the European Commission.

The meetings were constructive and registered a high level of engagement among the projects, being the starting point for the collaboration of those two working groups that have continued to build and strengthen the research community with the support of Cyberwatching.eu, facilitating the connection between funded projects and future funding actions to find synergies and convergences.

In addition, we asked the projects what they thought were the **main barriers to commercialising their project results and how the EC could help minimise these barriers**. The results are shown in Table 10:

Barriers and EC role
Barriers: • Financial investments, National regulations and laws, Affordable prototype development, Weak communication. **EC could contribute with:** • Support, Intellectual property, Business Skills, Communication/Dissemination, R&D
Barriers: • Lack of awareness on: - cryptography as an efficient technology to protect individuals' privacy **- privacy as an important matter from an IT point of view** - GDPR importance • Difficulty for customers to understand the value proposition of cryptography in relation to current solutions **EC could contribute with:** • making **GDPR compliance easier for small enterprises** (start-ups and SMEs), that usually do not have the strength or the knowledge to understand what they shall do to be compliant
Barriers: • Components with different levels of maturity • Similar R&D projects on the race increases competition • Lack of demonstrated need for such tools: Desidentification tools are an emerging market • Big competitors specialized on privacy tools • Limited number of staff specialized in **privacy** as consequence of **low awareness.** **EC could contribute with:** • Collaboration between peer project promoted by EC • **Awareness creation from the EC** • EC can promote EU based solutions
Barriers:

Barriers and EC role
• Investment budgeting process in the HealthCare sector **EC could contribute with:** • **Pushing for a special treatment of cybersecurity budgets**? Cybersecurity 4.0?
Barriers: • The challenge of infrastructures and devices to implement and expose security capabilities in digital services. **EC could contribute with:** • Foster and coordinate standardization efforts towards new generation of cyber-security systems, which leverage the collaboration between providers of digital services and infrastructures. • Promote and foster the adoption of security capabilities as extensions to existing interfaces and APIs. • Promote the adoption of certification schemes and award those providers that give visibility of security features in their products.
Barriers: • **Internal:** Sales and marketing – consistent effort is required of professional sales/marketing for the next 6-9 months to commercialize CS-AWARE • **External:** Easier **access to EU administration/LPA** decision makers
Barriers: • **External:** The major barrier is the **lack of use of eID** by the citizenship. Moreover, this kind of SaaS must be **supported by PAs** that may launch a tender to contract the solution, which means a long and difficult process.
Barriers: • **Internal:** Providing visibility to our technical outputs from EC perspective will be essential to allow us a major diffusion of the solutions. In general, however, the answer depends on the specific technology we consider, since the project is developing multiple outputs.
Barriers: • **External:** More **standardisation** and common frameworks are needed to be adopted on IoT applications which are dispersed “silos” so far, and even more on Security / Cyberthreat common standards. EC could support with joint efforts on a common/standardised framework adopted by all “big players”.
Barriers: • **External: Lack of awareness**, Cyber security in energy sector and especially in EPES is not a well-established for advanced cybersecurity tools in the energy sector that go beyond firewalls and virus scanners (not very open to advanced solutions)
Barriers: • **External:** - Lack of investment in continuous human resource training reduces uptake of innovative solutions; - Lack of trust in research results; - Gaps between end user needs and available solutions; - Relatively new adoption of cyber- security services in the market; - Lack of appropriate decision support for cyber- security incidents; - Existing long-term service contracts and framework agreements may restrict rapid uptake of new technologies; - Lower-than- expected adoption of future connected vehicle technology
Barriers: • **External:** - Replacement of events by other activities. - Dissemination to other types of stakeholders: what, how.

Table 10: Main barriers for commercialization of projects results and EC role

After the first two meetings, other meetings took place around the topics of interest detected, and the successive meetings were also joined by other projects that had shown interest in the initiative, such as **Kraken**, **SDN-Microsense** or **Critical-Chains**, increasing the number of projects engaged.

And, consequently, some webinars were organised:

- **12 November 2020**: EPES AND SMART GRIDS: PRACTICAL TOOLS AND METHODS TO FIGHT AGAINST CYBER AND PRIVACY ATTACKS, with the participation of DEFeND, SDN-Microsense, SealedGRID and EnergySHIELD.
- **10 December 2020**: SECURITY AND PRIVACY BY DESIGN FOR HEALTHCARE, with the participation of PAPAYA, DEFeND and PANACEA.
- **14 December 2020**: FINANCIAL SECTOR INFRASTRUCTURE CYBER-PHYSICAL SECURITY AND REGULATORY STANDARDS WORKSHOP, organized by CRITICAL-CHAINS with the support of cyberwatching, with the participation of CS-AWARE, SOTER, CONCORDIA, CYBERSEC4EUROPE.

A fourth webinar (scheduled for 21 May) is in preparation regarding **Threat intelligence and Information Sharing** in the finance sector, with the participation of CONCORDIA, CYBERSEC4EUROPE and FINSEC projects.

Assisting the projects in their actions to disseminate results is an activity that arouses great interest among the projects, which have to comply with a plan for communication and dissemination of results. It is a way of putting projects with common interests in contact, so that they not only carry out joint dissemination efforts, but can also find synergies that drive research results.

To continue promoting collaboration between projects and favouring synergies between them, a new initiative aimed at clustering has been promoted, as described in section 4.3.

4 Synergies and convergences

Crossing the data obtained in the two previous sections drives us to the elaboration of a matrix that is T2.3 main output along with the analysis of this matrix. The goal is that both the matrix and its analysis will leverage future R&I activities and pave the way to establish a “reference guide” from which organizations will be able to start their developments without investing time and resources in an existing product or service.

4.1 Matrix of projects

From the MTRL analysis, the Matrix of projects has been constructed, as shown in APPENDIX 4, where the 80 projects that sent the MTRL at least once, are listed and classified attending their TRL scores, which classifies the technology readiness in each project in IDEA, PROTOTYPE, VALIDATION and PRODUCTION, and their MRL scores, which classifies the market readiness in Not marketable yet, Need to improve marketing, Ready to commercialize and Product stable (Table 11). It is also shown the taxonomy level 2 and they have been ordered by end date.

TRL
IDEA
PROTOTYPE
VALIDATION
PRODUCTION

MRL
Not marketable yet (NMY)
Need to improve marketing (NTIM)
Ready to commercialize (RTC)
Product stable (PS)

Table 11: TRL and MRL classification

From the table in APPENDIX 4, it is evident that most of projects that have already finished have a higher TRL and most of them are in VALIDATION phase while most of projects that still have a long way to go are in IDEA phase.

Table 12 shows a comparison between finished projects and ongoing projects in relation to their market readiness performance.

Only 8 out of the 51 finished projects are Ready to commercialise, 18 are not marketable and 25 Need to improve some marketing capabilities.

Already 3 out of the 51 ongoing projects are Ready to commercialise, 14 are not marketable and 12 Need to improve some marketing capabilities.

Taking a look at the relative percentages of completed and ongoing projects (Table 12), it is surprising to see that **the proximity to the market is similar in finished projects and ongoing projects**, which could indicate that **the message from the EC of the need to put more effort into the exploitation plans is permeating among the Projects**.

	Finished projects	%	Ongoing Projects	%
Not marketable yet (NMY)	18	35%	12	41%
Need to improve marketing (NTIM)	25	49%	14	48%
Ready to commercialize (RTC)	8	16%	3	10%

Table 12: MRL performance in finished and ongoing projects

Analysing the segment **Operational Risk and Analytics**, we found just one project ready to commercialise, with a high TRL, and all other projects need market improvement, even if they are in Validation Phase (TRL 6-7).

N	Project	End	IDEA	PROTO	VALID	PROD
57	IMPACT	21/01/2020	NMY			
231	SECONDO	01/12/2022	NMY			
148	FENTEC	01/12/2020	NTIM			
244	SPIDER	01/06/2022	NTIM			
185	PANACEA	31/12/2021		NTIM		
133	SUNFISH	17/12/2020			NTIM	
217	CUREX	01/11/2021			NTIM	
55	HERMENEUT	01/04/2019			NTIM	
222	RESISTO	01/04/2021			NMY	
124	SMESEC	01/05/2020			NTIM	
131	STOP-IT	01/05/2021				RTC

Table 13: MTRL scores for Operational Risk and Analytics segment

Analysing the segment **Verification and Assurance**, we find even a worse situation, where all projects need market improvement., with lower values for MRL in the IDEA phase.

N	Project	End	IDEA	PROTO	VALID	PROD
150	PROMETHEUS	01/12/2019	NMY			
159	FUTURE TPM	31/12/2020	NMY			
254	FORESIGHT	01/09/2022	NMY			
5	ANASTACIA	01/12/2019			NMY	
145	VisiOn	01/06/2017			NTIM	
223	SECREDAS	01/04/2021			NTIM	
113	SAINT	01/02/2021			NTIM	

Table 14: MTRL scores for Verification and Assurance segment

Analysing the segment **Secure Systems and Technology**, we see more correlation between TRL and MRL, where most of projects in IDEA phase (TRL 0-3) are not marketable yet (but we can also find projects with higher MRL), and projects in VALIDATION (TRL 6-7) or even PRODUCTION (TRL 8-9) PHASE have higher MRL values, finding 5 projects ready to commercialize.

N	Project	End	IDEA	PROTO	VALID	PROD
259	UP2DATE	22/12/2020	NMY			
112	SAFERtec	01/12/2019	NMY			
237	nIoVe	30/04/2022	NMY			
248	CyberSANE	01/08/2022	NTIM			
180	PROTASIS	01/04/2020	NMY			
153	YAKSHA	01/06/2020	NMY			
162	ASTRID	01/04/2021	NMY			
253	CARAMEL	01/09/2022	NMY			
177	ENACT	01/12/2020	NMY			
151	REACT	31/05/2021	NMY			
160	SealedGRID	01/12/2021	NMY			
229	SPHINX	31/12/2021	NMY			
261	SAPPAN	30/04/2022	NMY			
250	PHOENIX	31/08/2022	NMY			
249	Cyber-MAR	31/08/2022	NTIM			
238	GUARD	22/04/2020	NTIM			
245	EnergyShield	01/06/2022	NTIM			
114	SAURON	01/04/2019		NMY		
58	KONFIDO	01/10/2019		NMY		
71	MUSA	01/12/2017		NTIM		
265	M-SEC	30/09/2021		NTIM		
152	SerIoT	01/12/2020			NMY	
45	ENCASE	01/12/2019			NMY	
155	CYBER-TRUST	01/04/2021			NTIM	
243	SOTER	01/10/2021			NTIM	
263	SDN-microSENSE	30/04/2022			NTIM	
122	SHIELD	01/02/2019			NTIM	
50	FutureTrust	01/05/2019			NTIM	
68	MHMD	01/10/2019			NTIM	
67	mF2C	01/12/2019			NTIM	
142	UNICORN	01/12/2019			NTIM	
171	THREAT-ARREST	01/08/2021			RTC	
126	SODA	01/12/2019			NTIM	
227	SAFECARE	30/11/2021			NTIM	
60	LIGHTest	01/08/2019			NTIM	
239	InfraStress	01/05/2021			NTIM	
116	SCOTT	01/06/2020			RTC	
110	SafeCloud	01/08/2018			RTC	
188	SecureIoT	20/12/2020			RTC	
179	CYBERWISER	28/02/2021				RTC
232	TRINITY	30/06/2023				NTIM

Table 15: MTRL scores for Secure Systems and Technology segment

Analysing the segment **Identity, Behaviour, Ethics and Privacy** we have a very similar scenario to **Verification and Assurance**, although MRL values are a bit higher in this group:

N	Project	End	IDEA	PROTO	VALID	PROD
170	OLYMPUS	01/08/2021	NMY			
216	ASCLEPIOS	30/11/2021	NMY			
163	BPR4GDPR	01/04/2021	NTIM			
262	KRAKEN	30/11/2022	NTIM			
164	PAPAYA	01/04/2021	NTIM			
158	PRIVILEDGE	30/06/2021			NMY	
165	POSEIDON	01/10/2020			NTIM	
178	PDP4E	30/04/2021			NTIM	

Table 16: MTRL scores for Identity, Behaviour, Ethics and Privacy segment

Analysing the segment **National and international security and governance**, the performance is even better than the **Secure Systems and Technology** segment, where we find 3 projects ready to commercialise, and the MRL values are correlated to TRL values.

N	Project	End	IDEA	PROTO	VALID	PROD
175	CyberSec4Europe	22/07/2020	NMY			
176	ECHO	01/02/2023			NTIM	
24	COMPACT	01/10/2019			NTIM	
46	EU-SEC	01/12/2019			NTIM	
29	CS-AWARE	01/08/2020			RTC	
168	DEFEND	01/05/2021			RTC	
102	PROTECTIVE	01/08/2019			RTC	
13	CANVAS	01/08/2019				NMY

Table 17: MTRL scores for National and international security and governance segment

Analysing the segment **Human Aspects of Cybersecurity**, the performance is pretty similar to **National and international security and governance**, where we can find 2 projects ready to commercialise.

N	Project	End	IDEA	PROTO	VALID	PROD
127	SPECIAL	01/12/2019	NMY			
35	DECODE	01/12/2019			NTIM	
91	PrEstoCloud	01/12/2019			NTIM	
40	DOGANA	01/08/2018			RTC	
52	GHOST	01/04/2020			RTC	

Table 18: MTRL scores for Human Aspects of Cybersecurity segment

This matrix of projects, by itself, offers partial information about the performance of the projects in the different segments, but it is necessary an analysis comparing the results with some research priorities in order to determine these synergies and convergences, and this work is developed in the next section.

4.2 Identification of low developed spaces and SRIA priorities

In December 2020, ECSO WG6 published a document called "**Input to the Horizon Europe Programme 2021-2027 - Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity**" (already mentioned in section 2.3) which integrated the contributions received from ECSO members. This represents input into the Strategic Research and Innovation agenda priorities for the European Commission to consider for inclusion in the specific areas of the Horizon Europe Work Programme as mentioned above.

In that document ECSO identified **four main strategic areas for investment** in order to develop a comprehensive cybersecurity R&I strategy in Europe to thus increase digital autonomy and respond to the needs of our industrial sectors, while protecting European fundamental rights. These investments could be supported by the coming Horizon Europe Programme, from 2021 to 2027.

- The **first pillar** of the proposed R&I strategy identifies the importance to **create a sustainable ecosystem in Europe**.
- The **second pillar** of the R&I cybersecurity strategy focuses on the **digitisation of vertical sectors** and the need for **resilient infrastructures.**
- The **third pillar** builds on **data and economy.**
- The **fourth pillar** is the development of **basic and disruptive technologies.**

ECSO has continued to be a partner with the European Commission in the Cybersecurity Public Private Partnership and contributes inputs and feedback on a regular basis to the European Union work programmes. It is foreseen that ECSO will also do so not only for the Horizon Europe but also for the Digital Europe Programme as well. Furthermore, as ECSO's membership includes stakeholders from the public sector, the private sector, research and academic communities the broadest set of shared opinions can be stressed while ensuring appropriate representation across the different stakeholder communitites.

Based on the analysis of the results of the 204 projects that are included in the *APPENDIX 2*, together with the priorities established by ECSO's WG6 in those four pillars, another matrix has been prepared that determines which of the priorities suggested by ECSO have been or are being covered by the projects analysed.

4.2.1 Quantitative analysis

To determine if a project fits into any of the priorities defined by ECSO, **an individual assessment of the results of each project has been carried out**, so there may be some inaccuracies in the assessment. However, in the near future, the Project Radar will allow for an automatic assessment without error, as long as each project that is entered on the Radar appropriately tags its projects with the corresponding Cybersecurity domains, Sectors and Technology & Use cases tags.

Then, it will be enough to filter using the corresponding tags to identify which projects are working or have worked on those priorities, offering us an assessment of their state of technological and market maturity, even being able to analyse what economic effort the EC has made for certain priorities, as it is part of the information that is displayed on the radar.

The complete **matrix of projects Vs priorities**, divided into groups of 30 projects (due to its size), is shown in *APPENDIX 6*, while in this section we are going to draw the main conclusions derived from the analysis of this matrix, to identify which areas are already enough covered and which ones need further investments, and make some recommendations in section 5.2. The colours assigned to the title of some projects are the colours they have on the radar according to their relative performance[15].

In Figure 3, shows how many projects, out of the 204 analysed, have made or are making contributions to the priorities defined by ECSO, grouped by the four pillars, which gives us an idea of which priorities are covered the most and which are the least.

[15] Project readiness in the Cyberwatching Project Radar

In Figure 4, the same information is presented, but the priorities are shown sorted by the number of projects working on them.

This has to be considered as quantitative analysis.

It is clear that the priorities most addressed by the projects are **Approaches, methods, processes to support cybersecurity assessment, evaluation and certification** and **End-to-end privacy,** with more than 50 projects working on them**,** as those topics are the basis for Cybersecurity and Privacy, including risk assessment and privacy-preserving.

On the opposite side of the ranking are the priorities of **Secure and Trustworthy AI**, **Secure Quantum Infrastructures**, and the vertical sectors of **Robotics** and **Agrifood**, with very few projects working on it.

Going priority by priority, in sections 4.2.2 to 4.2.5, and analysing the MTRL scores of the projects included in APPENDIX 5, will help us to understand the current situation, and perform a qualitative analysis.

ECOSYSTEM, SOCIAL GOOD & CITIZENS	1	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification	53
	2	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	25
	3	Development of digital forensics mechanisms and analytical support	13
	4	Cyber ranges and simulation environments	14
	5	Cyber-physical systems security and cyber secure pervasive technology	23
APPLICATION DOMAINS & INFRASTRUCTURE	6	Cyber resilient digitised infrastructures	46
	7	Secure Quantum Infrastructures	4
	8	Cyber secure future communication systems and networks	26
	9	Vertical sectors cyber challenges	11
	10	Industry 4.0 and ICS	20
	11	Energy (oil, gas, electricity), and smart grids	28
	12	Transportation (road, rail, air; sea, space)	37
	13	Financial Services, e-payments and insurance	23
	14	Public services, e-government, digital citizenship	32
	15	Healthcare	44
	16	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities	18
	17	Robotics	4
	18	Agrifood	4
DATA & ECONOMY	19	Data security and malicious use of data	18
	20	End-to-end privacy	54
	21	Economic aspects of cybersecurity	20
BASIC & DISRUPTIVE TECHNOLOGIES	22	Secure and Trustworthy AIs	2
	23	Software and Hardware cybersecure engineering and assurance	45
	24	Cryptography	44
	25	Blockchains and DLTs	28
	26	IoT Security	37
	27	AI techniques for better security & malicious use of AI	38

Figure 3: Number or projects working on priorities identified by ECSO, grouped by pillars

20	End-to-end privacy	54
1	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification	53
6	Cyber resilient digitised infrastructures	46
23	Software and Hardware cybersecure engineering and assurance	45
15	Healthcare	44
24	Cryptography	44
27	AI techniques for better security & malicious use of AI	38
12	Transportation (road, rail, air; sea, space)	37
26	IoT Security	37
14	Public services, e-government, digital citizenship	32
11	Energy (oil, gas, electricity), and smart grids	28
25	Blockchains and DLTs	28
8	Cyber secure future communication systems and networks	26
2	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	25
5	Cyber-physical systems security and cyber secure pervasive technology	23
13	Financial Services, e-payments and insurance	23
10	Industry 4.0 and ICS	20
21	Economic aspects of cybersecurity	20
16	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities	18
19	Data security and malicious use of data	18
4	Cyber ranges and simulation environments	14
3	Development of digital forensics mechanisms and analytical support	13
9	Vertical sectors cyber challenges	11
7	Secure Quantum Infrastructures	4
17	Robotics	4
18	Agrifood	4
22	Secure and Trustworthy AIs	2

Figure 4: Number or projects working on priorities identified by ECSO, sorted from highest to lowest number of projects.

4.2.2 Ecosystem, Social Good & Citizens

Approaches, methods, processes to support cybersecurity assessment, evaluation and certification

There are 53 projects (26% of the projects on the radar) addressing this priority, although most of them are related to threat detection and mitigation tools and techniques: identifying potential threats, providing a list of prioritized response actions, and delivering a means to execute these responses. There are quite a lot projects developing tools for cyber risk assessment and even cyber culture assessment.

On the other hand, there are not so many projects that delve into certification and / or standardization schemes.

5	ANASTACIA	70	MITIGATE	166	SPEAR	223	SECREDAS
7	ARMOUR	71	MUSA	168	DEFEND	225	CYBERSECURITY
14	certMILS	73	NeCS	172	CONCORDIA	227	SAFECARE
24	COMPACT	98	PRIVACY FLAG	174	SPARTA	229	SPHINX
30	CYBECO	105	REASSURE	175	CyberSec4Europe	231	SECONDO
33	CYRail	124	SMESEC	176	ECHO	236	D-FENCE
36	DEFENDER	131	STOP-IT	178	PDP4E	239	InfraStress
40	DOGANA	132	STORM	185	PANACEA	242	CYBERCULT
46	EU-SEC	134	SUPERCLOUD	188	SecureIoT	245	EnergyShield
50	FutureTrust	143	VESSEDIA	201	CyberSure	250	PHOENIX
52	GHOST	146	WISER	207	CLTRe	263	SDN-microSENSE
55	HERMENEUT	155	CYBER-TRUST	209	GO 4G		
58	KONFIDO	159	FUTURE TPM	217	CUREX		
64	MAS2TERING	165	POSEIDON	222	RESISTO		

Table 19: Projects in the priority "Approaches, methods, processes to support cybersecurity assessment, evaluation and certification"

Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP

There are 25 projects (26% of the projects on the radar) addressing this priority. Many of them are aimed at detecting vulnerabilities and proposing countermeasures, but fewer propose self-healing techniques or include automation.

5	ANASTACIA	123	SISSDEN	197	ThreatMark	240	ODIX 2.0
29	CS-AWARE	151	REACT	221	TrueProactive	241	C4IIoT
36	DEFENDER	153	YAKSHA	222	RESISTO	261	SAPPAN
69	MIKELANGELO	162	ASTRID	227	SAFECARE	263	SDN-microSENSE
71	MUSA	175	CyberSec4Europe	229	SPHINX		
101	ProBOS	191	PANOPTESEC	238	GUARD		
120	SHARCS	196	ConnectProtect	239	InfraStress		

Table 20: Projects in the priority "Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP"

Development of digital forensics mechanisms and analytical support

There are 13 projects (12% of the projects on the radar) addressing this priority. These projects are more oriented to incident analysis, collected from multiple sources, but only 2 out of them are using AI, that was one of the gaps identified by ECSO.

29	CS-AWARE	16	CIPSEC	122	SHIELD	256	LOCARD
123	SISSDEN	73	NeCS	166	SPEAR		
153	YAKSHA	74	OCGN	219	AF-Cyber		
162	ASTRID	100	PRIVACY4FORENSICS	251	DAN		

Table 21: Projects in the priority "Development of digital forensics mechanisms and analytical support"

Cyber ranges and simulation environments

There are 14 projects (6% of the projects on the radar) addressing this priority. Cyber ranges are relatively new platforms, and only half of the projects are working with cyber ranges. The other half works with simulation and virtualization environments, with defined scenarios, including gaming.

70	MITIGATE	172	CONCORDIA	179	CYBERWISER	254	FORESIGHT
151	REACT	174	SPARTA	244	SPIDER	258	AERAS
155	CYBER-TRUST	175	CyberSec4Europe	248	CyberSANE		
171	THREAT-ARREST	176	ECHO	249	Cyber-MAR		

Table 22: Projects in the priority “Cyber ranges and simulation environments”

Cyber-physical systems security and cyber secure pervasive technology

There are 23 projects (7% of the projects on the radar) addressing this priority. Most of them are oriented to assess and mitigate. Only one project address information sharing and there is not a single project that uses Meta Attack Language.

5	ANASTACIA	112	SAFERtec	160	SealedGRID	238	GUARD
7	ARMOUR	114	SAURON	174	SPARTA	239	InfraStress
9	ATENA	115	SCISSOR	188	SecureIoT	241	C4IIoT
14	certMILS	116	SCOTT	222	RESISTO	246	CRITICAL-CHAINS
36	DEFENDER	119	SERECA	227	SAFECARE	260	1-SWARM
52	GHOST	131	STOP-IT	233	RADDICS		

Table 23: Projects in the priority “Cyber-physical systems security and cyber secure pervasive technology”

4.2.3 Application Domains & Infrastructure

Cyber resilient digitised infrastructures

There are 46 projects (23% of the projects on the radar) addressing this priority, which is a high number. There are several projects addressing the cyber and physical world through a holistic security perspective, and including real time analysis. None mention digital twins, and just one project takes 5G into account.

9	ATENA	75	OCTAVE	172	CONCORDIA	239	InfraStress
16	CIPSEC	105	REASSURE	174	SPARTA	243	SOTER
17	CITADEL	107	REDSENTRY	175	CyberSec4Europe	245	EnergyShield
29	CS-AWARE	114	SAURON	179	CYBERWISER	248	CyberSANE
31	CyberWiz	115	SCISSOR	180	PROTASIS	249	Cyber-MAR
33	CYRail	119	SERECA	185	PANACEA	250	PHOENIX
36	DEFENDER	121	SHIELD (Health)	192	SERENITI	252	vACCINE
46	EU-SEC	131	STOP-IT	222	RESISTO	254	FORESIGHT
67	mF2C	146	WISER	227	SAFECARE	258	AERAS
69	MIKELANGELO	159	FUTURE TPM	233	RADDICS	259	UP2DATE
70	MITIGATE	164	PAPAYA	234	FeatureCloud		
73	NeCS	166	SPEAR	238	GUARD		

Table 24: Projects in the priority “Cyber resilient digitised infrastructures”

Secure Quantum Infrastructures

There are 4 projects (2% of the projects on the radar) addressing this priority. Most projects are using Quantum for improving security, but they generally do not delve into the advancement of quantum technology.

86	PQCRYPTO	150	PROMETHEUS	159	FUTURE TPM	175	CyberSec4Europe

Table 25: Projects in the priority “Secure Quantum Infrastructures”

Cyber secure future communication systems and networks

There are 26 projects (13% of the projects on the radar) addressing this priority. Most projects focus on cloud. IoT is well represented as well. However, there are less projects researching in 5G.

5	ANASTACIA	95	PRISM CODE	134	SUPERCLOUD	244	SPIDER
10	BEACON	104	RAPID	138	TREDISEC	253	CARAMEL
16	CIPSEC	110	SafeCloud	152	SerIoT	255	5GZORRO
52	GHOST	111	SAFEcrypto	211	TFence	257	INSPIRE-5Gplus
62	MAMI	112	SAFERtec	222	RESISTO	260	1-SWARM
73	NeCS	122	SHIELD	223	SECREDAS		
91	PrEstoCloud	123	SISSDEN	232	TRINITY		

Table 26: Projects in the priority "Cyber secure future communication systems and networks"

Vertical sectors cyber challenges

There are 11 projects (5% of the projects on the radar) addressing this priority. We have included in this category the projects that are facing interoperability and interdependence in the vertical sectors. There are a lack of projects researching in interdependencies between critical sectors and multi-organisation and cross borders information sharing.

12	C3ISP	64	MAS2TERING	172	CONCORDIA	249	Cyber-MAR
29	CS-AWARE	67	mF2C	176	ECHO	263	SDN-microSENSE
61	LV-Pri20	116	SCOTT	239	InfraStress		

Table 27: Projects in the priority "Vertical sectors cyber challenges"

Industry 4.0 and ICS

There are 20 projects (10% of the projects on the radar) addressing this priority. Most projects focus on protecting ICS and SCADA systems with analysis of threats and proposal of countermeasures. There's a need to research in a holistic approach, including cyber culture of the staff.

38	DiSIEM	137	TOREADOR	180	PROTASIS	241	C4IIoT
115	SCISSOR	151	REACT	188	SecureIoT	248	CyberSANE
116	SCOTT	152	SerIoT	220	SIGAGuard	249	Cyber-MAR
124	SMESEC	175	CyberSec4Europe	232	TRINITY	260	1-SWARM
131	STOP-IT	176	ECHO	239	InfraStress	265	M-SEC

Table 28: Projects in the priority "Industry 4.0 and ICS"

Energy (oil, gas, electricity), and smart grids

There are 28 projects (14% of the projects on the radar) addressing this priority. There are not many projects that mention cascading effects and information sharing. Most of the pilots are focused on EPES and smart-grids, and very few on oil or gas.

9	ATENA	115	SCISSOR	171	THREAT-ARREST	239	InfraStress
14	certMILS	124	SMESEC	175	CyberSec4Europe	244	SPIDER
31	CyberWiz	151	REACT	176	ECHO	245	EnergyShield
32	CYCLONE	160	SealedGRID	178	PDP4E	248	CyberSANE
36	DEFENDER	161	SEMIoTICS	179	CYBERWISER	250	PHOENIX
52	GHOST	166	SPEAR	192	SERENITI	263	SDN-microSENSE
64	MAS2TERING	168	DEFEND	233	RADDICS	265	M-SEC

Table 29: Projects in the priority "Energy (oil, gas, electricity), and smart grids"

Transportation (road, rail, air; sea, space)

There are 37 projects (18% of the projects on the radar) addressing this priority. Most projects focus on automotive and rail. There are a few in maritime and just one project addressing space.

6	ARIES	112	SAFERtec	177	ENACT	241	C4IIoT
8	ASAP	114	SAURON	178	PDP4E	247	MALAGA
14	certMILS	116	SCOTT	179	CYBERWISER	248	CyberSANE
15	CHOReVOLUTION	120	SHARCS	180	PROTASIS	249	Cyber-MAR
16	CIPSEC	151	REACT	186	symbIoTe	252	vACCINE
22	COEMS	152	SerIoT	188	SecureIoT	253	CARAMEL
33	CYRail	163	BPR4GDPR	222	RESISTO	259	UP2DATE
70	MITIGATE	174	SPARTA	223	SECREDAS		
75	OCTAVE	175	CyberSec4Europe	237	nIoVe		
91	PrEstoCloud	176	ECHO	238	GUARD		

Table 30: Projects in the priority “Transportation (road, rail, air; sea, space)”

Financial Services, e-payments and insurance

There are 23 projects (11% of the projects on the radar) addressing this priority. There are several projects working on information sharing for the financial sector. There are a lack of projects researching on eIDAS integration.

13	CANVAS	127	SPECIAL	170	OLYMPUS	206	UNFRAUD
29	CS-AWARE	148	FENTEC	172	CONCORDIA	231	SECONDO
30	CYBECO	151	REACT	175	CyberSec4Europe	243	SOTER
65	MATTHEW	158	PRIVILEDGE	178	PDP4E	246	CRITICAL-CHAINS
75	OCTAVE	159	FUTURE TPM	197	ThreatMark	248	CyberSANE
107	REDSENTRY	168	DEFEND	203	LocationWise		

Table 31: Projects in the priority “Financial Services, e-payments and insurance”

Public services, e-government, digital citizenship

There are 32 projects (16% of the projects on the radar) addressing this priority. Most projects are oriented to privacy-preserving for citizens, authentication and information sharing.

6	ARIES	81	PANORAMIX	127	SPECIAL	168	DEFEND
13	CANVAS	96	PRISMACLOUD	129	SPOOC	170	OLYMPUS
15	CHOReVOLUTION	101	ProBOS	133	SUNFISH	172	CONCORDIA
24	COMPACT	102	PROTECTIVE	145	VisiOn	174	SPARTA
29	CS-AWARE	103	Ps2Share	150	PROMETHEUS	175	CyberSec4Europe
35	DECODE	111	SAFEcrypto	155	CYBER-TRUST	176	ECHO
60	LIGHTest	113	SAINT	163	BPR4GDPR	206	UNFRAUD
77	OPERANDO	124	SMESEC	165	POSEIDON	238	GUARD

Table 32: Projects in the priority “Public services, e-government, digital citizenship”

Healthcare

There are 44 projects (22% of the projects on the radar) addressing this priority. Many projects propose a holistic approach, with privacy-preserving of sensitive data, protection of devices, networks and staff awareness.

13	CANVAS	126	SODA	176	ECHO	223	SECREDAS
16	CIPSEC	128	SpeechXRays	177	ENACT	227	SAFECARE
22	COEMS	134	SUPERCLOUD	185	PANACEA	229	SPHINX
51	GenoPri	151	REACT	188	SecureIoT	230	SERUMS
52	GHOST	158	PRIVILEDGE	200	CHINO	234	FeatureCloud
58	KONFIDO	161	SEMIoTICS	201	CyberSure	238	GUARD
68	MH-MD	163	BPR4GDPR	211	TFence	239	InfraStress
96	PRISMACLOUD	164	PAPAYA	212	UltraFiBi	248	CyberSANE
116	SCOTT	168	DEFEND	216	ASCLEPIOS	258	AERAS
120	SHARCS	171	THREAT-ARREST	217	CUREX	262	KRAKEN
121	SHIELD (Health)	175	CyberSec4Europe	222	RESISTO	265	M-SEC

Table 33: Projects in the priority “Healthcare”

Smart cities and smart buildings (convergence of digital services for citizens) and other utilities

There are 18 projects (9% of the projects on the radar) addressing this priority. This type of projects are more related to IoT (connected devices) and digital services, more than smart buildings.

5	ANASTACIA	73	NeCS	124	SMESEC	188	SecureIoT
15	CHOReVOLUTION	91	PrEstoCloud	131	STOP-IT	198	Eye-O-T
24	COMPACT	96	PRISMACLOUD	171	THREAT-ARREST	265	M-SEC
52	GHOST	105	REASSURE	175	CyberSec4Europe		
64	MAS2TERING	116	SCOTT	186	symbIoTe		

Table 34: Projects in the priority “Smart cities and smart buildings (convergence of digital services for citizens) and other utilities”

Robotics

There are 4 projects (2% of the projects on the radar) addressing this priority. This is a very under represented sector, even if it has a lot do with Industry 4.0.

188	SecureIoT	232	TRINITY	233	RADDICS	260	1-SWARM

Table 35: Projects in the priority “Robotics”

Agrifood

There are 4 projects (2% of the projects on the radar) addressing this priority. Agrifood is a very under represented sector for pilots.

8	ASAP	151	REACT	152	SerIoT	175	CyberSec4Europe

Table 36: Projects in the priority “Agrifood”

4.2.4 Data & Economy

Data security and malicious use of data

There are 18 projects (9% of the projects on the radar) addressing this priority. There are some projects caring for provenance and integrity of data. There are also projects assuring data sharing with trusted third parties. But there are no projects working on fake news.

12	C3ISP	57	IMPACT	126	SODA	188	SecureIoT
18	CLARUS	73	NeCS	138	TREDISEC	229	SPHINX
35	DECODE	95	PRISM CODE	158	PRIVILEDGE	238	GUARD
45	ENCASE	103	Ps2Share	164	PAPAYA		
52	GHOST	110	SafeCloud	168	DEFEND		

Table 37: Projects in the priority “Data security and malicious use of data”

End-to-end privacy

There are 54 projects (26% of the projects on the radar) addressing this priority. Most projects in this priority work on GDPR compliance, privacy-preserving and data leakage.

34	DAPPER	110	SafeCloud	147	WITDOM	200	CHINO
51	GenoPri	116	SCOTT	155	CYBER-TRUST	213	ProtonSuite
65	MATTHEW	121	SHIELD (Health)	163	BPR4GDPR	216	ASCLEPIOS
73	NeCS	126	SODA	164	PAPAYA	217	CUREX
75	OCTAVE	127	SPECIAL	165	POSEIDON	224	ELIoT Pro
77	OPERANDO	129	SPOOC	167	SMOOTH	229	SPHINX
79	PaaSword	133	SUNFISH	168	DEFEND	230	SERUMS
81	PANORAMIX	137	TOREADOR	170	OLYMPUS	232	TRINITY
95	PRISM CODE	138	TREDISEC	174	SPARTA	234	FeatureCloud
96	PRISMACLOUD	140	TYPES	175	CyberSec4Europe	246	CRITICAL-CHAINS
98	PRIVACY FLAG	141	U2PIA	176	ECHO	261	SAPPAN

99	Privacy&Us	142	UNICORN	178	PDP4E	262	KRAKEN
102	PROTECTIVE	144	VIRT-EU	188	SecureIoT		
103	Ps2Share	145	VisiOn	193	SecureCloud		

Table 38: Projects in the priority “End-to-end privacy”

Economic aspects of cybersecurity

There are 20 projects (10% of the projects on the radar) addressing this priority. Here we find some projects that are just focusing on the economic aspects of cybersecurity and other that are integrating this analysis as part of the projects, either analysing the economic impact of cyber-threats or assessing business models for their solutions.

37	DISCOVERY	67	mF2C	146	WISER	217	CUREX
42	e-Sides	99	Privacy&Us	153	YAKSHA	231	SECONDO
47	EUNITY	102	PROTECTIVE	166	SPEAR	242	CYBERCULT
55	HERMENEUT	113	SAINT	194	ASCEMA	254	FORESIGHT
63	MAPPING	124	SMESEC	199	PerfectDashboard 2.0	262	KRAKEN

Table 39: Projects in the priority “Economic aspects of cybersecurity”

4.2.5 Basic & Disruptive Technologies

Secure and Trustworthy AI

There are 2 projects (1% of the projects on the radar) addressing this priority. This is the least represented category. Just a couple of projects are researching on the threats related to using AI.

174	SPARTA	178	PDP4E

Table 40: Projects in the priority “Secure and Trustworthy AI”

Software and Hardware cybersecure engineering and assurance

There are 45 projects (22% of the projects on the radar) addressing this priority. This is a trend, and more and more projects are taking into account security and privacy by design, and there are a few tools that help developers to do the same.

5	ANASTACIA	147	WITDOM	178	PDP4E	241	C4IIoT
14	certMILS	148	FENTEC	180	PROTASIS	245	EnergyShield
22	COEMS	151	REACT	185	PANACEA	247	MALAGA
30	CYBECO	152	SerIoT	186	symbIoTe	250	PHOENIX
71	MUSA	159	FUTURE TPM	188	SecureIoT	253	CARAMEL
79	PaaSword	160	SealedGRID	192	SERENITI	255	5GZORRO
112	SAFERtec	161	SEMIoTICS	193	SecureCloud	257	INSPIRE-5Gplus
117	SCR	163	BPR4GDPR	217	CUREX	259	UP2DATE
120	SHARCS	166	SPEAR	218	V-SPHERE	265	M-SEC
138	TREDISEC	168	DEFEND	224	ELIoT Pro		
142	UNICORN	174	SPARTA	232	TRINITY		
143	VESSEDIA	175	CyberSec4Europe	239	InfraStress		

Table 41: Projects in the priority “Software and Hardware cybersecure engineering and assurance”

Cryptograph

There are 44 projects (22% of the projects on the radar) addressing this priority. There are many projects using cryptographic techniques within their projects, but there are not so many projects researching specifically on cryptography.

6	ARIES	65	MATTHEW	127	SPECIAL	170	OLYMPUS
26	CREDENTIAL	68	MH-MD	129	SPOOC	175	CyberSec4Europe
28	CryptoCloud	79	PaaSword	133	SUNFISH	188	SecureIoT
35	DECODE	81	PANORAMIX	138	TREDISEC	216	ASCLEPIOS
43	ECRYPT-CSA	86	PQCRYPTO	147	WITDOM	224	ELIoT Pro
45	ENCASE	96	PRISMACLOUD	148	FENTEC	226	Blocknetwork
51	GenoPri	105	REASSURE	150	PROMETHEUS	230	SERUMS
53	HEAT	111	SAFEcrypto	158	PRIVILEDGE	241	C4IIoT
54	HECTOR	115	SCISSOR	159	FUTURE TPM	245	EnergyShield

56	HIPS	119	SERECA	162	ASTRID	246	CRITICAL-CHAINS
58	KONFIDO	126	SODA	164	PAPAYA	262	KRAKEN

Table 42: Projects in the priority "Cryptograph"

Blockchains and DLT

There are 28 projects (14% of the projects on the radar) addressing this priority. Despite the fact that the blockchain is a technology that has been researched for years, it is not fully implemented globally. Most projects use blockchain as a mean to reach the goals of their projects, but not as the main focus of their projects.

35	DECODE	155	CYBER-TRUST	226	Blocknetwork	246	CRITICAL-CHAINS
36	DEFENDER	158	PRIVILEDGE	230	SERUMS	250	PHOENIX
52	GHOST	160	SealedGRID	231	SECONDO	255	5GZORRO
58	KONFIDO	165	POSEIDON	234	FeatureCloud	256	LOCARD
68	MH-MD	172	CONCORDIA	237	nIoVe	257	INSPIRE-5Gplus
133	SUNFISH	175	CyberSec4Europe	241	C4IIoT	262	KRAKEN
152	SerIoT	217	CUREX	243	SOTER	265	M-SEC

Table 43: Projects in the priority "Blockchains and DLT"

IoT Security

There are 37 projects (18% of the projects on the radar) addressing this priority. A few projects focused on security for devices. Not many mention anonymisation.

ANASTACIA	98	PRIVACY FLAG	159	FUTURE TPM	224	ELIoT Pro
ARMOUR	105	REASSURE	161	SEMIoTICS	232	TRINITY
CHOReVOLUTION	116	SCOTT	174	SPARTA	237	nIoVe
COEMS	118	SecIoT	176	ECHO	238	GUARD
GHOST	119	SERECA	186	symbIoTe	241	C4IIoT
KONFIDO	124	SMESEC	188	SecureIoT	246	CRITICAL-CHAINS
LV-Pri20	143	VESSEDIA	198	Eye-O-T	265	M-SEC
mF2C	144	VIRT-EU	211	TFence		
NeCS	152	SerIoT	222	RESISTO		
PQCRYPTO	155	CYBER-TRUST	223	SECREDAS		

Table 44: Projects in the priority "IoT Security"

AI techniques for better security & malicious use of AI

There are 38 projects (19% of the projects on the radar) addressing this priority. They are using Machine learning, Deep learning and even Reinforcement learning, for threat analysis, predictive analysis and information sharing.

29	CS-AWARE	164	PAPAYA	220	SIGAGuard	248	CyberSANE
52	GHOST	165	POSEIDON	230	SERUMS	250	PHOENIX
64	MAS2TERING	172	CONCORDIA	233	RADDICS	252	vACCINE
101	ProBOS	174	SPARTA	234	FeatureCloud	253	CARAMEL
122	SHIELD	175	CyberSec4Europe	237	nIoVe	255	5GZORRO
127	SPECIAL	178	PDP4E	241	C4IIoT	257	INSPIRE-5Gplus
128	SpeechXRays	185	PANACEA	244	SPIDER	261	SAPPAN
131	STOP-IT	195	LipVerify	245	EnergyShield	265	M-SEC
137	TOREADOR	197	ThreatMark	246	CRITICAL-CHAINS		
151	REACT	206	UNFRAUD	247	MALAGA		

Table 45: Projects in the priority "AI techniques for better security & malicious use of AI"

4.2.6 MTRL analysis

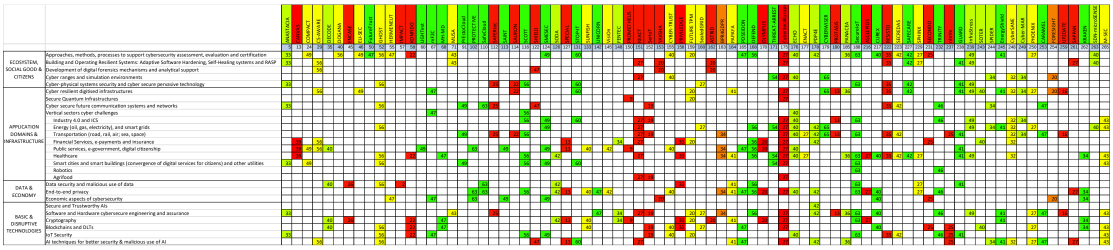
To complete the **qualitative analysis**, in those projects for which we have been able to obtain the MTRL self-assessment, the weighted average of the TRL and MRL values is included in the matrix in order to determine the maturity of the solutions provided by the projects to the different priorities.

The weighted average of the TRL and MRL values is calculated based on the number of questions asked in the questionnaire of each type, so that we have two questions to obtain the TRL value and seven questions to obtain the MRL value, so the formula to obtain that weighted MTRL value, consistently with which is described for the Project Radar[16], is:

$$\textbf{MTRL score} = 7 \times \textbf{MRL} + 2 \times \textbf{TRL}$$

This will give us an integer value between 0 and 81, which will allow us to evaluate the state of global maturity (MTRL) of each priority.

As a reference, that matrix will look like Figure 5, a mess of numbers and colours, that need to be sorted to get the important information.



		ANASTACIA	CANVAS	COMPACT	CS-AWARE	DECODE	DOGANA	ENCASE	EU-SEC	FutureTrust	GHOST	HERMENEUT	IMPACT	KONFIDO	LIGHTest	mF2C	MH-MD	MUSA	PrEstoCloud	PROTECTIVE
		5	13	24	29	35	40	45	46	50	52	55	57	58	60	67	68	71	91	102
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification	33		49			56		49	47	56	47		22				43		
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	33			56													43		
	Development of digital forensics mechanisms and analytical support				56															
	Cyber ranges and simulation environments																			
	Cyber-physical systems security and cyber secure pervasive technology	33									56									
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures				56				49							47				
	Secure Quantum Infrastructures																			
	Cyber secure future communication systems and networks	33									56								49	
	Vertical sectors cyber challenges															47				
	Industry 4.0 and ICS																			
	Energy (oil, gas, electricity), and smart grids										56									
	Transportation (road, rail, air; sea, space)																		49	
	Financial Services, e-payments and insurance		39		56															
	Public services, e-government, digital citizenship		39	49	56	40									49					63
	Healthcare		39								56			22			47			
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities	33		49							56								49	
	Robotics																			
	Agrifood																			
DATA & ECONOMY	Data security and malicious use of data					40		26			56		2							
	End-to-end privacy																			63
	Economic aspects of cybersecurity											47				47				63
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																			
	Software and Hardware cybersecure engineering and assurance	33																43		
	Cryptography					40		26						22			47			
	Blockchains and DLTs					40					56			22			47			
	IoT Security	33									56			22		47				
	AI techniques for better security & malicious use of AI				56						56									

		SafeCloud	SAFERtec	SAINT	SAURON	SCOTT	SHIELD	SMESEC	SODA	SPECIAL	STOP-IT	SUNFISH	UNICORN	VisiOn	FENTEC	PROMETHEUS	REACT	SerIoT
		110	112	113	114	116	122	124	126	127	131	133	142	145	148	150	151	152
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification							49			60							
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP																27	
	Development of digital forensics mechanisms and analytical support						47											
	Cyber ranges and simulation environments																27	
	Cyber-physical systems security and cyber secure pervasive technology		25		22	56					60							
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures				22						60							
	Secure Quantum Infrastructures															9		
	Cyber secure future communication systems and networks	63	25				47											19
	Vertical sectors cyber challenges					56												
	Industry 4.0 and ICS					56		49			60						27	19
	Energy (oil, gas, electricity), and smart grids							49									27	
	Transportation (road, rail, air; sea, space)		25		22	56											27	19
	Financial Services, e-payments and insurance									13					34		27	
	Public services, e-government, digital citizenship			49				49		13		40		42		9		
	Healthcare					56			42								27	
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities					56		49			60							
	Robotics																	
	Agrifood																27	19
DATA & ECONOMY	Data security and malicious use of data	63							42									
	End-to-end privacy	63				56			42	13		40	47	42				
	Economic aspects of cybersecurity			49				49										
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																	
	Software and Hardware cybersecure engineering and assurance		25										47		34		27	19
	Cryptography								42	13		40			34	9		
	Blockchains and DLTs											40						19
	IoT Security					56		49										19
	AI techniques for better security & malicious use of AI						47			13	60						27	

		YAKSHA	CYBER-TRUST	PRIVILEDGE	FUTURE TPM	SealedGRID	ASTRID	BPR4GDPR	PAPAYA	POSEIDON	DEFEND	OLYMPUS	THREAT-ARREST	CyberSec4Europe	ECHO	ENACT	PDP4E	CYBERWISER
		153	155	158	159	160	162	163	164	165	168	170	171	175	176	177	178	179
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification		40		20					47	56			27	40		42	
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	20					20							27				
	Development of digital forensics mechanisms and analytical support	20					20											
	Cyber ranges and simulation environments		40										54	27	40			65
	Cyber-physical systems security and cyber secure pervasive technology					27												
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures				20				41					27				65
	Secure Quantum Infrastructures				20									27				
	Cyber secure future communication systems and networks																	
	Vertical sectors cyber challenges														40			
	Industry 4.0 and ICS													27	40			
	Energy (oil, gas, electricity), and smart grids					27					56		54	27	40		42	65
	Transportation (road, rail, air; sea, space)							34						27	40	27	42	65
	Financial Services, e-payments and insurance			33	20						56	20		27			42	
	Public services, e-government, digital citizenship		40					34		47	56	20		27	40			
	Healthcare			33				34	41		56		54	27	40	27		
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities												54	27				
	Robotics																	
	Agrifood													27				
DATA & ECONOMY	Data security and malicious use of data			33					41		56							
	End-to-end privacy		40					34	41	47	56	20		27	40		42	
	Economic aspects of cybersecurity	20																
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																42	
	Software and Hardware cybersecure engineering and assurance				20	27		34			56			27			42	
	Cryptography			33	20		20		41			20		27				
	Blockchains and DLTs		40	33		27				47				27				
	IoT Security		40		20										40			
	AI techniques for better security & malicious use of AI								41	47				27			42	

		PROTASIS	PANACEA	SecureIoT	ASCLEPIOS	CUREX	RESISTO	SECREDAS	SAFECARE	SPHINX	SECONDO	TRINITY	nIoVe	GUARD	InfraStress	SOTER	SPIDER	EnergyShield	CyberSANE	Cyber-MAR	PHOENIX	CARAMEL	FORESIGHT	UP2DATE	SAPPAN	KRAKEN	SDN-microSENSE	M-SEC
		180	185	188	216	217	222	223	227	229	231	232	237	238	239	243	244	245	248	249	250	253	254	259	261	262	263	265
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification		36	63		40	35	42	42	27	25				49			41			27						40	
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP						35		42	27				41	49										27		40	
	Development of digital forensics mechanisms and analytical support																											
	Cyber ranges and simulation environments																34		32	34			20					
	Cyber-physical systems security and cyber secure pervasive technology			63			35		42					41	49													
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures	13	36				35		42					41	49	40		41	32	34	27		20	16				
	Secure Quantum Infrastructures																											
	Cyber secure future communication systems and networks						35	42				46					34					47						
	Vertical sectors cyber challenges																											
	Industry 4.0 and ICS	13		63								46			49				32	34								43
	Energy (oil, gas, electricity), and smart grids														49		34	41	32		27						40	43
	Transportation (road, rail, air; sea, space)	13		63			35	42					25	41					32	34		47		16				
	Financial Services, e-payments and insurance										25					40			32									
	Public services, e-government, digital citizenship													41														
	Healthcare		36	63	27	40	35	42	42	27				41	49				32							34		43
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities			63																								43
	Robotics			63								46																
	Agrifood																											
DATA & ECONOMY	Data security and malicious use of data			63						27				41														
	End-to-end privacy			63	27	40				27		46													27	34		
	Economic aspects of cybersecurity					40					25												20			34		
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																											
	Software and Hardware cybersecure engineering and assurance	13	36	63		40						46			49			41			27	47		16				43
	Cryptography			63	27													41								34		
	Blockchains and DLTs					40					25		25			40					27					34		43
	IoT Security			63			35	42				46	25	41														43
	AI techniques for better security & malicious use of AI		36										25				34	41	32		27	47			27			43

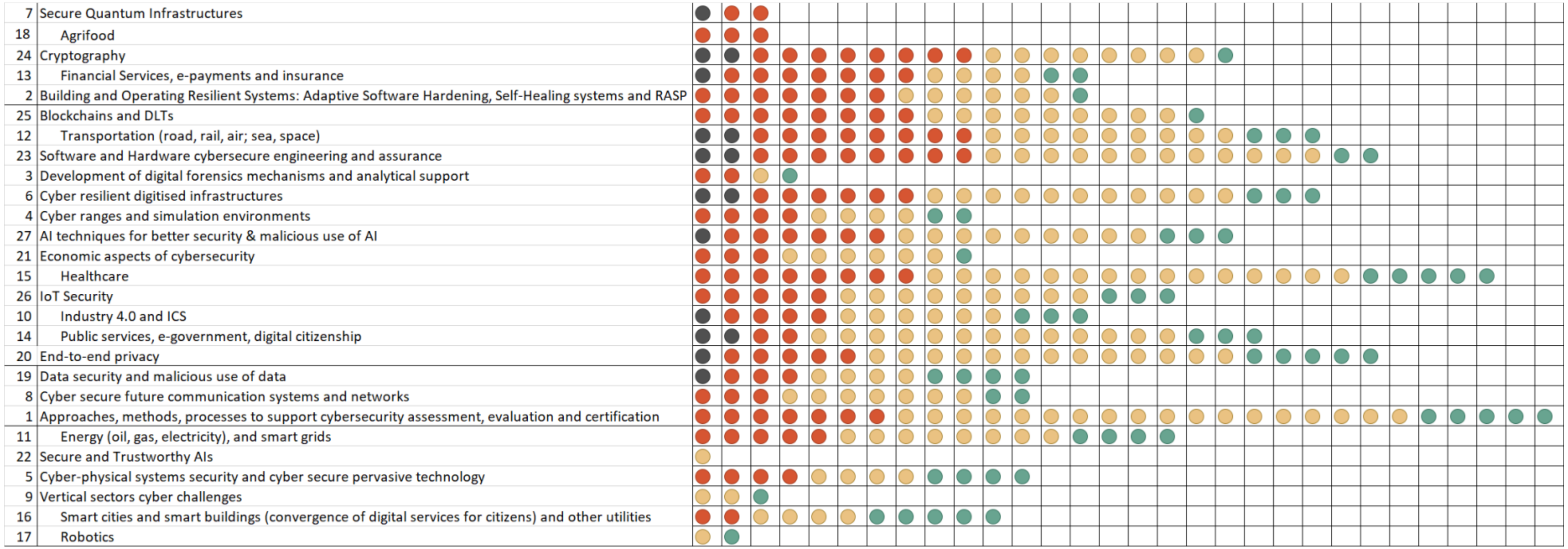
Figure 5: Matrix of MTRL self-assessed projects Vs SRIA priorities (qualitative analysis)

Sorting the MTRL score individually for each priority, we get to the graphic shown in Figure 6: Maturity of each priority identified by ECSO according to MTRL assessed projects, where we can observe:

- ***Secure Quantum Infrastructures*** priority is not only the priority with fewest projects on the radar (4), but also the assessed projects (3) have a very low average MTRL score.
- ***Agrifood*** is the least represented vertical sector among the projects on the radar (4) and the few projects evaluated (3) also have a low MTRL score.
- There are seven priorities with a similar maturity: half of the assessed projects are very far from market and the other half are closer:
  - ***Cryptography***, with 44 on the radar and 19 self-assessed.
  - ***Financial Services, e-payments and insurance***, with 33 projects on the radar and 14 projects self-assessed.
  - ***Building and Operating Resilient Systems***: Adaptive Software Hardening, Self-Healing systems and RASP, with 25 projects on the radar and 14 projects self-assessed.
  - ***Blockchains and DLTs***, with 28 projects in the radar and 18 self-assessed
  - **Transportation (road, rail, air; sea, space)**, with 37 projects on the radar and 22 self-assessed.
  - ***Software and Hardware cybersecure engineering and assurance***, with 45 projects on the radar and 24 self-assessed.
  - ***Development of digital forensics mechanisms and analytical support***, with 13 projects on the radar and 4 projects self-assessed.
- ***Cyber resilient digitised infrastructures*** priority is represented by a high number of projects in the radar (46) and the performance of the self-assessed projects (22) is medium-high, with less than half of the projects furthest from the market, but more than half somewhat more mature.
- ***Cyber ranges and simulation environments*** priority has a low representation on the radar (14 projects), and the assessed projects (10) performs similar to the previous priority.

[16] https://radar.cyberwatching.eu/doc/readiness

- ***AI techniques for better security & malicious use of AI priority***, with 38 projects on the radar, and 19 assessed, presents more projects near the market than far.
- ***Economic aspects of cybersecurity***, with 20 projects on the radar, is a priority with less than the 30% of the assessed projects (10) very far from the market.
- ***Healthcare***, with 44 projects on the radar, is the most represented vertical sector. Within the assessed projects (28), the maturity is quite high in 2/3 of them.
- ***IoT Security***, with 37 projects on the radar, and 17 projects assessed, presents the same behaviour than the previous priority: high maturity for 2/3 of the assessed projects.
- ***Industry 4.0 and ICS***, with 20 projects on the radar, and 14 of them assessed, have 40% of projects with low maturity and 60% with high maturity.
- ***Public services, e-government, digital citizenship***, with 32 projects on the radar, and 20 assessed, presents high maturity of most of the projects.
- ***End-to-end privacy***, with 54 projects on the radar and 24 assessed, has a maturity similar to the previous priority.
- ***Data security and malicious use of data***, with 18 projects on the radar and 12 assessed, presents 2/3 of projects with relative high maturity.
- ***Cyber secure future communication systems and networks***, with 26 projects on the radar and 12 assessed, have 75% of projects with high maturity.
- ***Approaches, methods, processes to support cybersecurity assessment, evaluation and certification***, with 53 projects in the radar and 30 assessed, presents almost an 80% of the projects with high maturity.
- ***Energy (oil, gas, electricity)****, and smart grids*, with 28 projects on the radar and 17 assessed, presents 70% of the projects with high maturity.
- ***Secure and Trustworthy Ais***, the least represented priority on the radar with just 2 projects, one of them assessed with a medium maturity.
- ***Cyber-physical systems security and cyber secure pervasive technology***, with 23 projects in the radar and 12 assessed, presents 1/3 with low maturity, 1/3 with medium maturity and 1/3 with high maturity.
- ***Vertical sectors cyber challenges***, with 11 projects on the radar and 3 assessed, present medium-high maturity for the 3 projects.
- ***Smart cities and smart buildings (convergence of digital services for citizens) and other utilities***, with 18 projects on the radar and 11 assessed, has a very good performance, with most of the projects with medium to high maturity,
- ***Robotics***, with 4 projects on the radar and 2 assessed, presents a good relative performance, with both projects near the market.



7	Secure Quantum Infrastructures	⚫	🔴	🔴																											
18	Agrifood	🔴	🔴	🔴																											
24	Cryptography	⚫	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢											
13	Financial Services, e-payments and insurance	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟢																
2	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟢																
25	Blockchains and DLTs	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢												
12	Transportation (road, rail, air; sea, space)	⚫	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢								
23	Software and Hardware cybersecure engineering and assurance	⚫	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢						
3	Development of digital forensics mechanisms and analytical support	🔴	🔴	🟡	🟢																										
6	Cyber resilient digitised infrastructures	⚫	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢								
4	Cyber ranges and simulation environments	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟢																				
27	AI techniques for better security & malicious use of AI	⚫	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢											
21	Economic aspects of cybersecurity	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟢																				
15	Healthcare	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢		
26	IoT Security	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢													
10	Industry 4.0 and ICS	⚫	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢																
14	Public services, e-government, digital citizenship	⚫	⚫	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢										
20	End-to-end privacy	⚫	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢						
19	Data security and malicious use of data	⚫	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢																		
8	Cyber secure future communication systems and networks	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢																		
1	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢
11	Energy (oil, gas, electricity), and smart grids	🔴	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢													
22	Secure and Trustworthy AIs	🟡																													
5	Cyber-physical systems security and cyber secure pervasive technology	🔴	🔴	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢																		
9	Vertical sectors cyber challenges	🟡	🟡	🟢																											
16	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities	🔴	🔴	🟡	🟡	🟡	🟡	🟢	🟢	🟢	🟢	🟢																			
17	Robotics	🟡	🟢																												

Figure 6: Maturity of each priority identified by ECSO according to MTRL assessed projects

4.3 Catalogue of R&I services and clusters of projects

By establishing and continuously updating an online catalogue of R&I services of projects and generated knowledge, organisations will be able to identify who has made what, when, where, as well as the way to contact them. This fosters knowledge transfer and collaboration among stakeholders.

With the aim of boosting synergies between projects, Cyberwatching.eu has created a new section on the website to accommodate project clusters around topics of common interest, giving new projects the option to join existing clusters or propose a new cluster around a specific sector or technology related to cybersecurity. This section has been called CYBERSECURITY AND PRIVACY PROJECT CLUSTERS.

Cyberwatching.eu offers support in the organisation, hosting and promotion of public webinars involving the projects clustered according to their target sectors. Cyberwatching.eu has proposed helping with a summary documents showcasing the main outputs of the discussion groups, which can be sent to the European Commission.

So far, six cluster has been created:

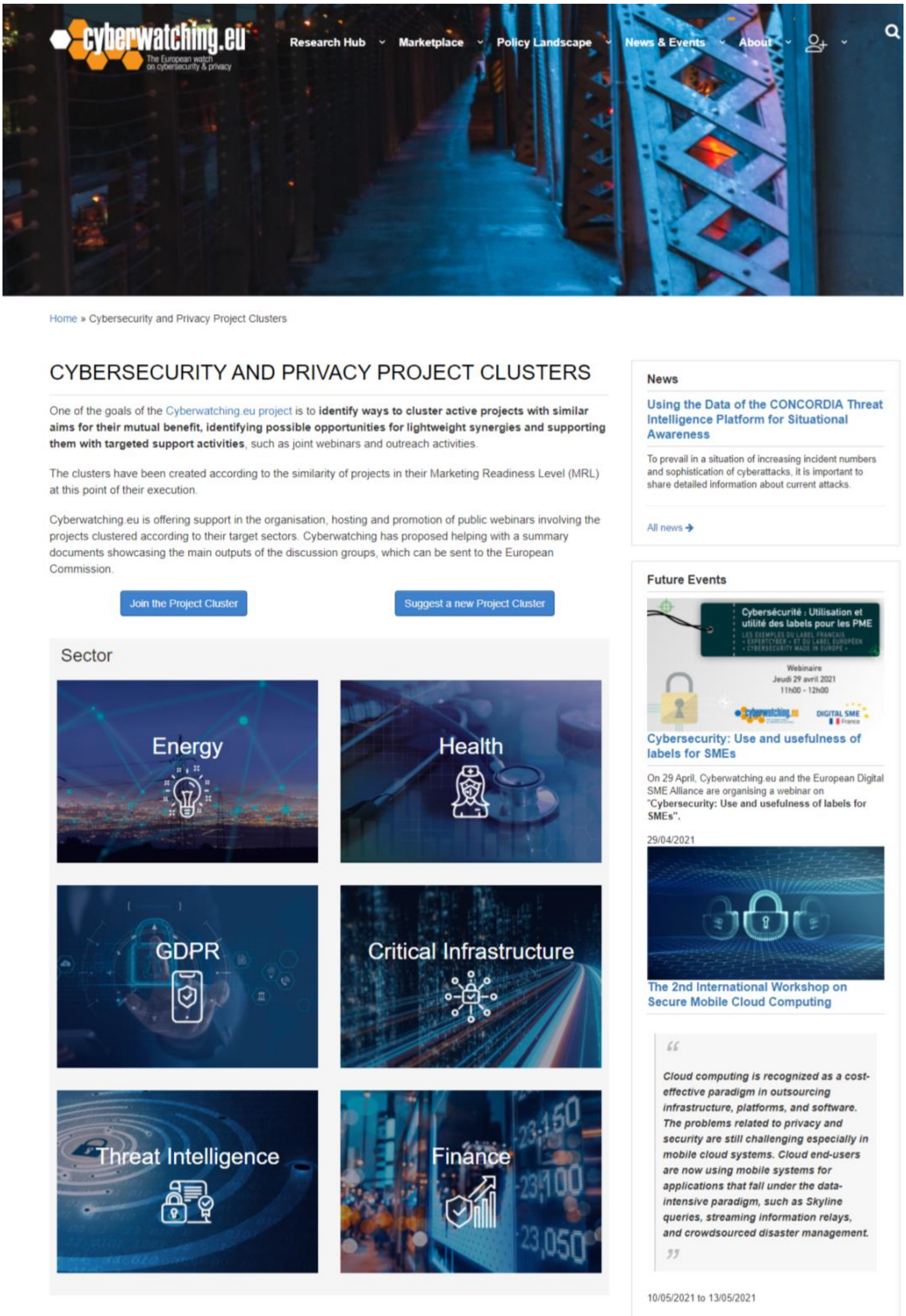
- Energy: Currently with SDN-microSENSE, EnergyShield, SealedGRID and DeFEND.
- Health: Currently with DEFeND, PANACEA and PAPAYA (and CUREX has applied to join).
- GDPR: Currently with BPR4GDPR, CUREX, DEFeND, PAPAYA, PDP4E, PoSeID-on and SMOOTH.
- Critical infrastructure: Currently with CRITICAL-CHAINS, CYBERSANE, CYBERWISER, ENERGYSHIELD, FINSEC, INFRASTRESS, PANACEA, ReAct, RESISTO, SDN-MICROSENSE and STOP-IT.
- Threat Intelligence: Currently with CONCORDIA, CYBERSEC4EUROPE and FINSEC.
- Finance: Currently with CONCORDIA, CRITICAL-CHAINS, CS-AWARE, CYBERSEC4EUROPE, DEFeND, ENSURESEC, FENTEC, FINSEC, INFINITECH and SOTER.

Each cluster section presents the following information:

- Introduction, with an overview of the cluster of projects.
- Cluster Objectives
- Challenges
- Who benefits?
- Innovations and solutions
- Impacts

Additionally, links to each project mini-site in **the Project Hub** is included, with the logo of each project. Ideally, this cluster section should include direct links to the solutions of each project included in the marketplace, news, links to related webinars and publications. But this is something that should be discussed in the actions for sustainability of the project assets.

By creating this section, we intend to generate a pull effect for other projects to join a cluster of their interest and, this way, the **engagement mechanism** is activated, and the projects enter into a wheel of collaboration: registering new projects in the catalogue of R&I services, activating the project on the project radar with the appropriate tags, completing and periodically updating its MTRL status and, finally, including commercial solutions into the marketplace. And along the way generating synergies between them.



Home » Cybersecurity and Privacy Project Clusters

CYBERSECURITY AND PRIVACY PROJECT CLUSTERS

One of the goals of the Cyberwatching.eu project is to **identify ways to cluster active projects with similar aims for their mutual benefit, identifying possible opportunities for lightweight synergies and supporting them with targeted support activities**, such as joint webinars and outreach activities.

The clusters have been created according to the similarity of projects in their Marketing Readiness Level (MRL) at this point of their execution.

Cyberwatching.eu is offering support in the organisation, hosting and promotion of public webinars involving the projects clustered according to their target sectors. Cyberwatching has proposed helping with a summary documents showcasing the main outputs of the discussion groups, which can be sent to the European Commission.

News

Using the Data of the CONCORDIA Threat Intelligence Platform for Situational Awareness

To prevail in a situation of increasing incident numbers and sophistication of cyberattacks, it is important to share detailed information about current attacks.

All news ➔

Future Events

Cybersecurity: Use and usefulness of labels for SMEs

On 29 April, Cyberwatching.eu and the European Digital SME Alliance are organising a webinar on "**Cybersecurity: Use and usefulness of labels for SMEs**".

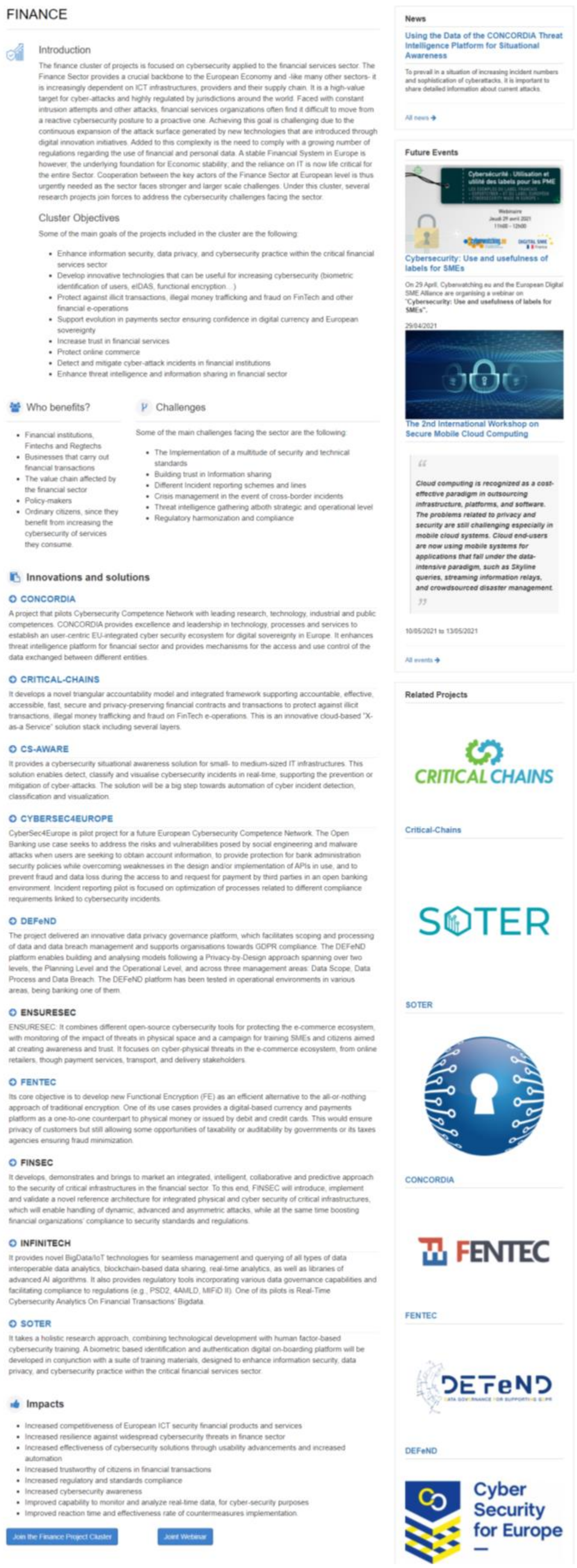
29/04/2021

The 2nd International Workshop on Secure Mobile Cloud Computing

> *Cloud computing is recognized as a cost-effective paradigm in outsourcing infrastructure, platforms, and software. The problems related to privacy and security are still challenging especially in mobile cloud systems. Cloud end-users are now using mobile systems for applications that fall under the data-intensive paradigm, such as Skyline queries, streaming information relays, and crowdsourced disaster management.*

10/05/2021 to 13/05/2021

Figure 7: Landing page of clusters of projects section



FINANCE

Introduction

The finance cluster of projects is focused on cybersecurity applied to the financial services sector. The Finance Sector provides a crucial backbone to the European Economy and -like many other sectors- it is increasingly dependent on ICT infrastructures, providers and their supply chain. It is a high-value target for cyber-attacks and highly regulated by jurisdictions around the world. Faced with constant intrusion attempts and other attacks, financial services organizations often find it difficult to move from a reactive cybersecurity posture to a proactive one. Achieving this goal is challenging due to the continuous expansion of the attack surface generated by new technologies that are introduced through digital innovation initiatives. Added to this complexity is the need to comply with a growing number of regulations regarding the use of financial and personal data. A stable Financial System in Europe is however, the underlying foundation for Economic stability; and the reliance on IT is now life critical for the entire Sector. Cooperation between the key actors of the Finance Sector at European level is thus urgently needed as the sector faces stronger and larger scale challenges. Under this cluster, several research projects join forces to address the cybersecurity challenges facing the sector.

Cluster Objectives

Some of the main goals of the projects included in the cluster are the following:

- Enhance information security, data privacy, and cybersecurity practice within the critical financial services sector
- Develop innovative technologies that can be useful for increasing cybersecurity (biometric identification of users, eIDAS, functional encryption…)
- Protect against illicit transactions, illegal money trafficking and fraud on FinTech and other financial e-operations
- Support evolution in payments sector ensuring confidence in digital currency and European sovereignty
- Increase trust in financial services
- Protect online commerce
- Detect and mitigate cyber-attack incidents in financial institutions
- Enhance threat intelligence and information sharing in financial sector

Who benefits?

- Financial institutions, Fintechs and Regtechs
- Businesses that carry out financial transactions
- The value chain affected by the financial sector
- Policy-makers
- Ordinary citizens, since they benefit from increasing the cybersecurity of services they consume.

Challenges

Some of the main challenges facing the sector are the following:

- The Implementation of a multitude of security and technical standards
- Building trust in Information sharing
- Different Incident reporting schemes and lines
- Crisis management in the event of cross-border incidents
- Threat intelligence gathering atboth strategic and operational level
- Regulatory harmonization and compliance

Innovations and solutions

CONCORDIA

A project that pilots Cybersecurity Competence Network with leading research, technology, industrial and public competences. CONCORDIA provides excellence and leadership in technology, processes and services to establish an user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe. It enhances threat intelligence platform for financial sector and provides mechanisms for the access and use control of the data exchanged between different entities.

CRITICAL-CHAINS

It develops a novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations. This is an innovative cloud-based "X-as-a Service" solution stack including several layers.

CS-AWARE

It provides a cybersecurity situational awareness solution for small- to medium-sized IT infrastructures. This solution enables detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber-attacks. The solution will be a big step towards automation of cyber incident detection, classification and visualization.

CYBERSEC4EUROPE

CyberSec4Europe is pilot project for a future European Cybersecurity Competence Network. The Open Banking use case seeks to address the risks and vulnerabilities posed by social engineering and malware attacks when users are seeking to obtain account information, to provide protection for bank administration security policies while overcoming weaknesses in the design and/or implementation of APIs in use, and to prevent fraud and data loss during the access to and request for payment by third parties in an open banking environment. Incident reporting pilot is focused on optimization of processes related to different compliance requirements linked to cybersecurity incidents.

DEFeND

The project delivered an innovative data privacy governance platform, which facilitates scoping and processing of data and data breach management and supports organisations towards GDPR compliance. The DEFeND platform enables building and analysing models following a Privacy-by-Design approach spanning over two levels, the Planning Level and the Operational Level, and across three management areas: Data Scope, Data Process and Data Breach. The DEFeND platform has been tested in operational environments in various areas, being banking one of them.

ENSURESEC

ENSURESEC: It combines different open-source cybersecurity tools for protecting the e-commerce ecosystem, with monitoring of the impact of threats in physical space and a campaign for training SMEs and citizens aimed at creating awareness and trust. It focuses on cyber-physical threats in the e-commerce ecosystem, from online retailers, though payment services, transport, and delivery stakeholders.

FENTEC

Its core objective is to develop new Functional Encryption (FE) as an efficient alternative to the all-or-nothing approach of traditional encryption. One of its use cases provides a digital-based currency and payments platform as a one-to-one counterpart to physical money or issued by debit and credit cards. This would ensure privacy of customers but still allowing some opportunities of taxability or auditability by governments or its taxes agencies ensuring fraud minimization.

FINSEC

It develops, demonstrates and brings to market an integrated, intelligent, collaborative and predictive approach to the security of critical infrastructures in the financial sector. To this end, FINSEC will introduce, implement and validate a novel reference architecture for integrated physical and cyber security of critical infrastructures, which will enable handling of dynamic, advanced and asymmetric attacks, while at the same time boosting financial organizations' compliance to security standards and regulations.

INFINITECH

It provides novel BigData/IoT technologies for seamless management and querying of all types of data interoperable data analytics, blockchain-based data sharing, real-time analytics, as well as libraries of advanced AI algorithms. It also provides regulatory tools incorporating various data governance capabilities and facilitating compliance to regulations (e.g., PSD2, 4AMLD, MIFiD II). One of its pilots is Real-Time Cybersecurity Analytics On Financial Transactions' Bigdata.

SOTER

It takes a holistic research approach, combining technological development with human factor-based cybersecurity training. A biometric based identification and authentication digital on-boarding platform will be developed in conjunction with a suite of training materials, designed to enhance information security, data privacy, and cybersecurity practice within the critical financial services sector.

Impacts

- Increased competitiveness of European ICT security financial products and services
- Increased resilience against widespread cybersecurity threats in finance sector
- Increased effectiveness of cybersecurity solutions through usability advancements and increased automation
- Increased trustworthy of citizens in financial transactions
- Increased regulatory and standards compliance
- Increased cybersecurity awareness
- Improved capability to monitor and analyze real-time data, for cyber-security purposes
- Improved reaction time and effectiveness rate of countermeasures implementation.

News

Using the Data of the CONCORDIA Threat Intelligence Platform for Situational Awareness

To prevail in a situation of increasing incident numbers and sophistication of cyberattacks, it is important to share detailed information about current attacks.

Future Events

Cybersécurité : Utilisation et utilité des labels pour les PME
Webinaire
Jeudi 29 avril 2021
11h00 - 12h00

Cybersecurity: Use and usefulness of labels for SMEs

On 29 April, Cyberwatching.eu and the European Digital SME Alliance are organising a webinar on "**Cybersecurity: Use and usefulness of labels for SMEs**".

29/04/2021

The 2nd International Workshop on Secure Mobile Cloud Computing

> *Cloud computing is recognized as a cost-effective paradigm in outsourcing infrastructure, platforms, and software. The problems related to privacy and security are still challenging especially in mobile cloud systems. Cloud end-users are now using mobile systems for applications that fall under the data-intensive paradigm, such as Skyline queries, streaming information relays, and crowdsourced disaster management.*

10/05/2021 to 13/05/2021

Related Projects

Critical-Chains

SOTER

CONCORDIA

FENTEC

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR
Cyber Security for Europe

DEFeND

Figure 8: Finance cluster section

There are already some **European Cluster Initiatives**, and Cyberwatching.eu will seek for synergies also with them, avoiding to overlap functions, and collaborating for the best future for projects in the different clusters.

Some of these clustering initiatives are the following:

- **The European GDPR Cluster Projects**: EU projects on the H2020 DS-08-2017 topic, namely BPR4GDPR, DEFeND, SMOOTH, PDP4E, PAPAYA, and PoSeID-on hosted a webinar where they presented their work and provided demos of their results.
- **TRUSTEE (daTa pRivacy and cloUd SecuriTy clustEr Europe)**: A network of 11 research projects funded by the European Union that was established within the Common Dissemination Booster initiative. The cluster is coordinated by CREDENTIAL, and furthermore subsumes the following projects: MUSA, PRISMACLOUD, SecureCloud, SERECA, SPECS, SUNFISH, SWITCH, TREDISEC, UNICORN, and WITDOM, which are all performing cutting-edge research and innovation in different domains of cloud security and privacy, ranging from secure and privacy-friendly authentication over encrypted and distributed solutions for data sharing and cloud storage to data integrity, authenticity, and availability. The ambition of TRUSTEE is to consolidate the distributed and fragmented nature of currently ongoing European research initiatives and to serve as a central contact point which for software vendors, customers, research colleagues, and decision makers that are interested in leading-edge technologies and solutions.
- **Cyber-Range Network**: a collaboration initiative created jointly from three EU funded projects: FORESIGHT, Cyber-MAR and SPIDER. The aforementioned projects created the "Cyber-Range Network" having as main objectives:
    - to promote collaboration and to facilitate exchange of knowledge among them;
    - to showcase their respective project results to a wider audience;
    - to perform joint dissemination activities;
    - to improve awareness regarding cybersecurity preparedness and training.
- **ECSCI (European Cluster for Securing Critical Infrastructures)**: to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities will focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. To promote the activities of the cluster, ECSCI will organize international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission. The member projects of the cluster are: FINSEC, ANASTACIA, CYBERSANE, DEFENDER, ENSURESEC, FeatureCloud, INFRASTRESS, PHOENIX, RESISTO, SAFECARE, SATIE, SECUREGAS, SmartResilience, SOTER, SPHINX, STOP-IT and 7SHIELD.

Cyberwatching.eu was already contacted by **FINSEC project** to seek for synergies and sustainability between ECSCI and the Critical Infrastructure cluster of Cyberwatching.eu.

Looking at the **sustainability of this clustering activity**, there is an interesting European initiative to accommodate activities to support clusters of projects: The Horizon Result Booster.

This initiative is a new package of three specialised services delivered to all ongoing and closed FP7 and H2020 projects at no cost and fully supported by the European

Commission. Projects funded by other Programmes than the FP7 and H2020 are eligible too if they join a Project Group led by a project funded under the FP7 and H2020 programme.

The Horizon Results Booster (HRB) aims to provide a tangible contribution to the dissemination of results and recommendations of research projects related to the European Commission Priority areas.

HRB offers a great opportunity for the identified clusters of projects, and new ones that may arise in the future, to access services that allow them to improve their results. Cyberwatching.eu has already begun to promote this service, considering this promotion as part of the clustering activities.

5 Conclusions and recommendations

After the quantitative and qualitative analysis carried out on the 204 radar projects and their alignment with the priorities defined by ECSO, it is necessary to collect the least developed spaces to obtain conclusions and suggest recommendations on where it is necessary to invest more efforts to fill the gaps.

5.1 Conclusions

Many of the priorities are related and interconnected, and it's not easy to give a separated diagnosis. For the same reason, most projects do not focus in only one priority.

There have been many advances in Approaches, methods, processes to support cybersecurity assessment and evaluation, but there is still work to do in **certification**.

There are not many projects working on **self-healing techniques** and their solutions are not very prepared to market yet.

There are not many projects developing **digital forensics mechanisms** and analytical support, and they are not using AI techniques.

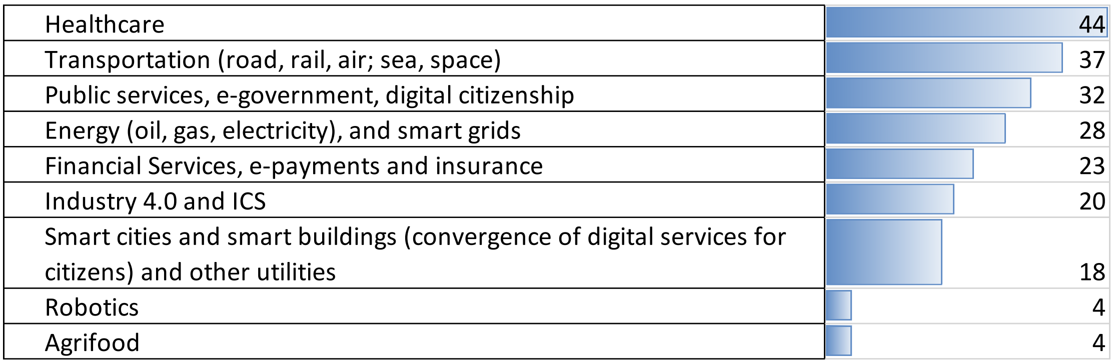
Cyber ranges play an important role in training and improving the digital capacities, and currently there are not many projects working on these developments, although the maturity of the partial results is not bad.

Projects working on **CPS systems** are evolving pretty good in closeness to market, but there, but they should keep researching in information sharing and Meta Attack Language. The maturity is worse in **Cyber resilient digitised infrastructures**, as half of the projects are far from market, but 5G and digital twins are not sufficiently used in this priority.

The priority of **Secure Quantum Infrastructures** is hardly being addressed by projects and the few that exist are not very mature.

The projects working on **Cyber secure future communication systems and networks** are very mature, but mostly in cloud and IoT, so they need to advance in 5G.

Regarding the vertical sectors, as it is shown in Figure 9, there are some sectors that are underrepresented in number of projects.



Healthcare	44
Transportation (road, rail, air; sea, space)	37
Public services, e-government, digital citizenship	32
Energy (oil, gas, electricity), and smart grids	28
Financial Services, e-payments and insurance	23
Industry 4.0 and ICS	20
Smart cities and smart buildings (convergence of digital services for citizens) and other utilities	18
Robotics	4
Agrifood	4

Figure 9: Number of projects in vertical sectors

Regarding **Data security and malicious use of data, the** projects caring for provenance and integrity of data and assuring data sharing with trusted third parties are pretty mature. But there are no projects working on fake news.

There are many projects working on **End-to-end privacy**, mainly focused on GDPR compliance, privacy-preserving and data leakage, and most of them are mature.

Some projects are just focusing on the **economic aspects of cybersecurity** and other are integrating this analysis as part of the projects, either analysing the economic impact of cyber-threats or assessing business models for their solutions. Most of them are not so far from the market.

Just a couple of projects are researching on the **threats related to using AI**, and they are not mature.

More and more projects are taking into account **security and privacy by design**, and there are a few tools that help developers to do the same. Nevertheless, not all are mature enough, and only 50% are relatively close to market.

There are many projects using **cryptographic techniques** within their projects, but there are not so many projects researching specifically on cryptography. Again, not all are mature enough, and only 50% are relatively close to market.

Despite the fact that the **blockchain** is a technology that has been researched for years, it is not fully implemented globally. Most projects use blockchain as a mean to reach the goals of their projects, but not as the main focus of their projects, and only 50% are relatively close to market.

A few projects focus on **security for IoT devices**, although they are pretty mature. Not many mention anonymisation.

Artificial intelligence is increasingly widespread, by using Machine learning, Deep learning and even Reinforcement learning, for threat analysis, predictive analysis and information sharing, and presents more projects near the market than far.

5.2 Recommendations

Below is a list of recommendations for the EC:

R1. Give value to the results of projects already developed, not only forcing to incorporate a section on previous initiatives in the Horizon Europe proposals, but also promoting among organisations the different tools that allow consulting and taking advantage of the results of previous projects, such as the Cyberwatching.eu Project Radar[17], the Horizon Results Platform[18] or the Horizon Result Booster[19].

R2. Promote clustering activities as a way to encourage collaboration between projects, joint dissemination and exchange of good exploitation practices, including the possibility of joint exploitation or joint future developments.

R3. Encourage projects to do intermediate self-evaluations, beyond the mandatory reviews with the EC, to check that their project is progressing correctly at the technological and market level. The self-assessment should be done by the same person in the project.

R4. Promote activities for projects related to developing skills in areas like Go to market and the Manufacturing/Supply chain, such as helping them to get in contact with potential clients and partners, so that they can adapt the results of the projects to the real needs of the consumers and can establish commercial relationships.

R5. Robotics and agrifood should be considered as preferred sectors for pilots and use cases.

R6. Industry 4.0 could also be a recommended sector for pilots, due to the priority of digital transformation by companies.

R7. Research in Secure and Trustworthy AIs must be encouraged, considering the growing use of AI for improving cybersecurity and privacy.

R8. Development of certification schemes and standards should be encouraged.

R9. Cyber ranges have to continue to be promoted and improved their market maturity,

R10. Information sharing and Meta Attack Language in CPS systems should be further researched.

R11. 5G and digital twins should be further researched in Cyber resilient digitised infrastructures. Also, 5G has to be researched in Cyber secure future communication systems and networks.

R12. Secure Quantum Infrastructures has to be intensively promoted.

R13. Regarding Data security and malicious use of data, research in fighting fake news should be carried out.

R14. Research on threats related to using AI should be highly encouraged.

R15. Research on new and advanced cryptographic techniques should improve their matureness.

R16. Blockchain should be integrated in cross- border and cross-domain settings.

Other **recommendations from the projects**, collected during the clustering activities.

- Support, Intellectual property, Business Skills, Communication/Dissemination, R&D.
- Make GDPR compliance easier for small enterprises (Start-ups and SMEs), that usually do not have the strength or the knowledge to understand what they shall do to be compliant.

[17] https://radar.cyberwatching.eu/radar

[18] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform

[19] https://www.horizonresultsbooster.eu/

- Collaboration between peer project promoted by EC.
- Privacy awareness creation from the EC.
- EC can promote EU based solutions.
- Push for a special treatment of cybersecurity budgets, such as Cybersecurity 4.0
- Foster and coordinate standardization efforts towards new generation of cyber-security systems, which leverage the collaboration between providers of digital services and infrastructures.
- Promote and foster the adoption of security capabilities as extensions to existing interfaces and APIs.
- Promote the adoption of certification schemes and award those providers that give visibility of security features in their products.
- Ease the access to EU administration/LPA decision makers.
- Foster the use of eID by the citizenship.
- More standardisation and common frameworks are needed to be adopted on IoT applications which are dispersed “silos” so far, and even more on Security / Cyberthreat common standards. EC could support with joint efforts on a common/standardised framework adopted by all “big players.
- Improve the investment in continuous human resource training to facilitate the uptake of innovative solutions.

6 List of Acronyms

Acronyms	Explanation
AAI	Authentication and Authorisation Infrastructure
AI	Artificial Intelligence
ASV	Automatic Speaker Verification
BDA	Big Data Analytics
BP	Business Process
CAV	Connected and Autonomous Vehicles
CERT	Computer emergency response team
CI	Critical Infrastructures
CPS	Cyber Physical Systems
CSA	Coordination and Support Action
CSIRT	Computer Security Incident Response Team
DEM	Digital evidence management
DL	Deep Learning
EC	European Commission
ECSEL-RIA	Electronic Components and Systems for European Leadership RIA
ECSO	European Cyber Security Organisation
EOSC	European Open Science Cloud Declaration
EPES	Electrical Power and Energy System
ERC-SyG	European Research Council Synergy Grants
FE	Functional Encryption
GDPR	General Data Protection Regulation
HRB	Horizon Results Booster
IA	Innovation action
IaaS	Infrastructure as a Service
ICS	industrial control systems
IDP	International Driving Permit
IDS	Intrusion Detection System
IPR	Intellectual Property Rights
IT	information technology
LPA	Local Public Administrations
MCCPS	Mixed-Criticality Cyber-Physical Systems
ML	Machine Learning
MOOC	massive open online course
MPC	MultiParty Computation
MRL	Market Readiness Levels
MSCA-RISE	Marie Skłodowska-Curie Actions Research and Innovation Staff Exchange
MTRL	Market and Technology Readiness Levels
NCS	Networked Critical Infrastructures
NFC	Near Field Communication
NFV	Network Functions Virtualisation
NIS-D	Network and Information Security Directive
OCC	offensive cyber capabilities
OSINT	Open Source Intelligence

Acronyms	Explanation
OSNs	online social networks
OT	operational technology
PA	Public Administrations
PaaS	Platform as a Service
PCA	Principal Component Analysis
QoS	Quality of Service
QR	Quantum-Resistant
RASP	runtime application self-protection
R&I	Research and Innovation
RIA	Research and Innovation Action
SaaS	Software as a Service
SC	Supply Chains
SCADA	Supervisory Control and Data Acquisition
SDL	Systems Development Lifecycle
SDN	Software Defined Networking
SG	Smart Grids
SIEM	Security Information and Event Management
SOC	Security Operation Center
TPM	Trusted Platform Module
TRL	Technology Readiness Levels
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything

APPENDIX 1. CLUSTERED PROJECTS

Cluster I (12 members):			SEGMENT IN RADAR
14	certMILS	I	Cybersecurity Governance
29	CS-AWARE	I	Cybersecurity Governance
163	BPR4GDPR	I	Identity & Privacy
167	SMOOTH	I	Cybersecurity Governance
168	DEFEND	I	Cybersecurity Governance
174	SPARTA	I	Cybersecurity Governance
175	CyberSec4Europe	I	Cybersecurity Governance
176	ECHO	I	Cybersecurity Governance
242	CYBERCULT	I	Human Aspects
261	SAPPAN	I	Secure Systems

Cluster II (5 members):			SEGMENT IN RADAR
113	SAINT	II	Verification & Assurance
131	STOP-IT	II	Operational Risk
148	FENTEC	II	Operational Risk
170	OLYMPUS	II	Identity & Privacy
178	PDP4E	II	Identity & Privacy
222	RESISTO	II	Operational Risk
233	RADDICS	II	Operational Risk

Cluster III (14 members):			SEGMENT IN RADAR
57	IMPACT	III	Operational Risk
201	CyberSure	III	Verification & Assurance
217	CUREX	III	Operational Risk
223	SECREDAS	III	Verification & Assurance
231	SECONDO	III	Operational Risk
244	SPIDER	III	Operational Risk
245	EnergyShield	III	Secure Systems
246	CRITICAL-CHAINS	III	Operational Risk
247	MALAGA	III	Operational Risk
248	CyberSANE	III	Secure Systems
249	Cyber-MAR	III	Secure Systems

Cluster IV (6 members):			SEGMENT IN RADAR
159	FUTURE TPM	IV	Verification & Assurance
162	ASTRID	IV	Secure Systems
237	nIoVe	IV	Secure Systems
239	InfraStress	IV	Secure Systems
240	ODIX 2.0	IV	Secure Systems
252	vACCINE	IV	Secure Systems
253	CARAMEL	IV	Secure Systems

Cluster V (9 members):			SEGMENT IN RADAR
151	REACT	V	Secure Systems
152	SerIoT	V	Secure Systems
155	CYBER-TRUST	V	Secure Systems

238	GUARD	V	Secure Systems
241	C4IIoT	V	Secure Systems
250	PHOENIX	V	Secure Systems
259	UP2DATE	V	Secure Systems

Cluster VI (9 members):			**SEGMENT IN RADAR**
129	SPOOC	VI	Identity & Privacy
160	SealedGRID	VI	Secure Systems
161	SEMIoTICS	VI	Secure Systems
164	PAPAYA	VI	Identity & Privacy
165	POSEIDON	VI	Identity & Privacy
166	SPEAR	VI	Secure Systems
177	ENACT	VI	Secure Systems
216	ASCLEPIOS	VI	Identity & Privacy
227	SAFERCARE	VI	Secure Systems
229	SPHINX	VI	Secure Systems
230	SERUMS	VI	Secure Systems
232	TRINITY	VI	Secure Systems
234	FeatureCloud	VI	Secure Systems
260	1-SWARM	VI	Secure Systems

APPENDIX 2. LIST OF EC PROJECTS OUTPUTS

1	AARC2	Authentication and Authorisation For Research and Collaboration	Integrated cross-discipline Authentication and Authorisation Infrastructure (AAI) framework, built on federated access production services (eduGAIN). - A secure and scalable Blueprint Architecture - A Policy Development Kit (PDK) that provides introductory information, training materials, template documents, and detailed guidelines on policy for AAIs. - A set of AARC in Action case studies, that provide examples and a reference to help organisations understand what solution could best fits their needs.
4	AEGIS	Accelerating EU-US DialoGue for Research and Innovation in CyberSecurity and Privacy	AEGIS proposes a multi-stakeholder approach to engage relevant communities from both sides of the Atlantic to accelerate EU-US cooperation in cybersecurity and privacy research and innovation. The AEGIS project has created a Cybersecurity Reflection Group, a multi-stakeholder collaboration platform that brings together high level experts from Europe and US to address challenges in cybersecurity and privacy R&I through regular meetings and events.
5	ANASTACIA	Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures	Anastacia platform: A holistic solution enabling trust and security by-design, addressing all the phases of the ICT Systems Development Lifecycle (SDL), for Cyber Physical Systems (CPS) based on IoT and Cloud architectures: - Security Development Paradigm - Distributed Trust and Security Enablers - Dynamic Security and Privacy Seal The ANASTACIA cyber-security framework will provides self-protection, self-healing and self-repair capabilities through novel enablers and components. USE CASE 1: Mobile Edge Computing applications USE CASE 2: Smart building

6	ARIES	reliAble euRopean Identity EcoSystem	Framework for reliable e-identity ecosystem comprising new technologies, processes and security features that ensure highest levels of quality in eID based on trustworthy security documents and biometrics for highly secure and privacy-respecting physical and virtual identity management, with the specific aim to tangibly achieve a reduction in levels of identity theft, fraud and associated crimes. ARIES will leverage virtual and mobile IDs cryptographically derived from strong eID documents in order to prevent identity theft and related crimes in the physical (e.g. an airport) and virtual (e.g eCommerce) domains.
7	ARMOUR	Large-Scale Experiments of IoT Security Trust	Solutions that allow the occasional testing, test environment and certification of large-scale IoT deployments validating the Security, Privacy and Confidence of new deployments. ARMOUR developed a certification methodology based on the ETSI proposal by combining the two approaches of testing and risk assessment and it applies model-based testing approaches to large-scale IoT systems.
8	ASAP	Adaptive Security and Privacy	It developed a dynamic open-source execution framework for scalable data analytics. Within the project, the consortium focused on the real-time analysis of Web content and telecommunications data. Currently extended as part of the EVOLVE big data project (Horizon 2020) and applied to a range of different use cases such as agriculture, mobility and maritime services, the content processing capabilities will also form the basis for planned Horizon Europe submissions.
9	ATENA	Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures	Objective 1 – Develop a Unified Modelling Framework and with ad-hoc models to control physical flow efficiency and improve resilience across CIs against threats of their IACSs and related ICT infrastructures Objective 2 – Define dynamic security paradigms for resilience of Cyber-Physical systems. Objective 3 – Develop new anomaly detection algorithms and risk assessment methodologies within a distributed Cyber-Physical environment. Objective 4 – Develop a suite of integrated ICT networked components for detection and reaction in presence of adverse events in industrial distributed systems. Objective 5 – Validate the ATENA models and tool suite in significant Use Cases: Electricity domain, Gas domain, Water domain, ICT domain As tangible results, the ATENA project will produce a set of tools that, implementing innovative models, methodologies and algorithms for security assurance, and interacting with the available smart components of a CI, will increase the level of cyber-physical security and resilience of underpinning CI & IACS.

10	BEACON	Enabling Federated Cloud Networking	A homogeneous virtualization layer, on top of heterogeneous underlying physical networks, computing and storage infrastructures, providing enablement for automated federation of applications across different clouds and datacenters
12	C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection	Define a collaborative and confidential information sharing, analysis and protection framework as a service for cyber security management. C3ISP paradigm is collect, analyse, inform, and react. Established Pilots: - Internet Service Providers (ISPs) Pilot - CERT Pilot - Enterprise Pilot - SME Pilot
13	CANVAS	Constructing an Alliance for Value-driven Cybersecurity	The CANVAS Consortium unifies technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. CANVAS has a particular focus on three domains of application: the health system, finance, and law enforcement / national security. Among others, CANVAS created a reference curriculum for value-driven cybersecurity, briefing packages for policy stakeholders, and a MOOC (massive open online course) on value-driven cybersecurity. An integrative view on the ethical and regulatory issues of cybersecurity
14	certMILS	Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats	A security certification methodology for Cyber-physical systems (CPS). The "MILS" in certMILS stands for "Multiple Independent Levels of Safety/Security", indicating that certMILS uses a special kind of operating systems called "separation kernel" (SK). This kind of operating system focuses being highly deterministic and reliable and puts user functionality into the application layer. Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats: - MILS Security Architecture Templates - Strategy for Security Certification of the Development and Product Lifecycle in High Assurance Industrial Cyber-Physical Systems - A Platform Approach for Fusing Safety and Security on a Solid Foundation Pilots: Smart grid, railway, subway

15	CHOReVOLUTION	Automated Synthesis of Dynamic and Secured Choreographies for the Future internet	CHOReVOLUTION aims to provide an environment allowing interactions between various services currently provided by local authorities, to deliver advanced applications based for example on traffic conditions or local weather. The CHOReVOLUTION IDRE offers dynamic and secured choreographies of services through a distributed coordination. This approach is useful in the development and management of complex interactions, such as intelligent transportation systems, IoT and smart city applications.
16	CIPSEC	Enhancing Critical Infrastructure Protection with innovative SECurity framework	Unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of Cis. As part of this framework CIPSEC will offer a complete security ecosystem of additional services that can support the proposed technical solutions to work reliably and at professional quality. These services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs) forensics analysis, standardization and protection against cascading effects. All solutions and services will be validated in three pilots performed in three different CI environments (transportation, health, environment). CIPSEC will also develop a marketing strategy for optimal positioning of its solutions in the CI security market.
17	CITADEL	Critical Infrastructure Protection using Adaptive MILS	The research and development work within the CITADEL project is focused on extending MILS for use in protecting critical infrastructures. The MILS approach has two aspects, or phases: 1) the development of a policy architecture that accomplishes a desired goal, and, 2) the implementation of that policy architecture upon a platform that manages shared resources in a way that the fundamental assumptions of any policy architecture are satisfied.
18	CLARUS	A FRAMEWORK FOR USER CENTRED PRIVACY AND SECURITY IN THE CLOUD	The main objective of CLARUS is to enhance trust in cloud computing services by developing a secure framework for the storage and processing of data outsourced to the cloud that allows end users to monitor, audit and retain control of the stored data without impairing the functionality and cost-saving benefits of cloud services. The CLARUS solution will provide the end user with a dedicated proxy located in a trusted domain implementing security and privacy features towards the cloud provider. The proxy is intended to be deployed within the client computer, in a server within the user’s domain, in an edge device (e.g. a router), or in any other location trusted by the user. CLARUS will also provide a set of security auditing services enabling the user to supervise the security operations performed by the CLARUS framework as well as other trust-enhancing features.

19	CloudSocket	Business and IT-Cloud Alignment using a Smart Socket	CloudSocket envisions the idea of "Business Process as a Service", where domain-specific business processes like employee registration at social insurance, tax report, or legal verification are supported by workflows that optimally match the ICT support for the selected process. The ICT support is expected to be realized by available platforms or software components from PaaS or SaaS platforms. CloudSocket introduces the concept BPaaS that fulfills the business process needs thanks to smart alignment techniques, packages this BPaaS as "extended Cloudlets" that are autonomously deployable and include adaptive rules to appropriately react in a multi-cloud environment by keeping SLAs and process-based billing. Hence, the vision is to "plug business" into the "Cloud". The tools section contains software prototypes and tools that are useful not only when implementing a CloudSocket Broker but also span across the lifespan of a Business Process (BP) and integrate seamlessly in a BP's lifecycle (execution, design, allocation & evaluation activity).
22	COEMS	Continuous Observation of Embedded Multicore Systems	A platform with supporting verification methods for software systems is created. COEMS tackles the issues of detection and identification of non-deterministic software failures caused by race conditions and access to inconsistent data. It gives insight to the system's actual behaviour without affecting it allowing new verification methods. An efficient real-time access and analysis as a critical element for operating safe systems will be developed and validated by COEMS. Moreover, a cross-layer programming approach supporting failure detection will be proposed. COEMS aims at shortening the development cycle by considerably increased test efficiency and effectivity, by increased debug efficiency (especially for non-deterministically occurring failures) and by supporting performance optimization. COEMS improves the reliability of delivered systems, enabling software developers to identify, understand, and remove software defects before release, as well as improving efficiency of software for multi/many-core computing systems in terms of performance, real-time behaviour, and energy consumption. It addressess the domains of safety-critical medical applications, automation and automotive industry, as well as the Internet of Things.

24	COMPACT	COmpetitive Methods to protect local Public Administration from Cyber security Threats	COMPACT delivered an integrated platform with 17 tools grouped by 4 different typologies (risk assessment, education, monitoring and knowledge sharing), most of them characterized by a high degree of usability by non IT experts and automation.
26	CREDENTIAL	Secure Cloud Identity Wallet	The main idea and ambition of CREDENTIAL is to enable end-to-end security and improved privacy in cloud identity management services for managing secure access control. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms. To make this ambition come true CREDENTIAL comprises following fields of core innovations: - Novel efficient cryptography to enable advanced trust models in the cloud - Methods for strong authentication to the cloud - Holistic privacy models for user protection and secure data sharing - Dedicated usability and HCI models for wide user adoption and maximum impact - Secure, efficient, and portable implementations of components and protocols - Piloting and testing on a European scale
28	CryptoCloud	Cryptography for the Cloud	The ERC CryptoCloud Project has studied several cryptographic primitives to reduce the privacy risks. First, new secure multi-party computation protocols have been proposed, as efficient alternative to the famous, but inefficient, Fully Homomorphic Encryption. Some tailored homomorphic constructions have also been designed for specific use-cases. Basically, this allows to players to make computations on encrypted inputs, and the result can be open by a target user only. But the main outcome of the project is definitely the variants of Functional Encryption: given a functional decryption key associated to a function f, applied on a ciphertext of x, one gets f(x) and nothing else. The multi-client setting has been defined, which allows aggregations of private inputs coming from distrustful sources. This a very technical primitive that has already found concrete instantiations with applications to real use-cases. The dynamic setting will find even more applications. Eventually, to reduce trust assumptions, we studied traceability feature that allows to trace back a defrauder in case of abuse, even if anonymity is a priori guaranteed.

29	CS-AWARE	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis	It provides a cybersecurity situational awareness solution for small- to medium-sized IT infrastructures. This solution enables detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber-attacks. The solution will be a big step towards automation of cyber incident detection, classification and visualization. It provides resilience as part of a self-healing mechanism that allows to automatically invoke predefined mitigation actions in case a threat was detected.
30	CYBECO	Supporting Cyberinsurance from a Behavioural Choice Perspective	CYBECO will research, develop, demonstrate, evaluate and exploit a new framework for managing cybersecurity risks, one that is focusing on cyberinsurance, as key risk management treatment. CYBECO integrates multidisciplinary research methods from Behavioural Economics, Statistics, Game and Decision Theory, Security Engineering and Behavioural Psychology in order to develop new concepts and models that are combined within a prototype software architecture (CYBECO Toolbox 2.0).
31	CyberWiz	Cyber-Security Visualization and CAD-Tool for the Vulnerability Assessment of Critical Infrastructures	The project will deliver and validate a tool that helps to 1) better understand current cyber security levels across complex enterprise-wide architectures, including relationships and interdependencies between systems, 2) prioritize areas to address and cyber security investments to pursue and 3) proactively manage cyber security e.g. when building or modifying architectures. The solution is based on a cybersecurity metamodel that 1) describes the qualitative structure (which assets, attacks and defences that should be included, and how these should be associated and 2) populates this qualitative structure with quantitative data (how likely different attacks are to succeed given the system parameter values and the presence or absence of different defences, using Bayesian networks). The tool generates a vulnerability “heat map” for each system configuration, allowing a user-friendly and visual comparison of the different alternatives. The project will validate the tool in 2 pilots with energy utilities in Sweden and Germany.
32	CYCLONE	Complete Dynamic Multi-cloud Application Management	CYCLONE provides an integrated software stack that enables a wealth of functionality, such as multi-cloud deployment and scaling of federated applications, secure access control using federated identities, as well as software-defined networking functions. In the CYCLONE testbed it is integrated with eduGAIN, allowing easy use of those academic identities for authentication, authorization, and other purposes. Use cases: Bioinformatics, Energy, Entrance and Internet of Services Lab (IoSL)

33	CYRail	Cybersecurity in the RAILway sector	An analysis of threats targeting Railway infrastructures was developed as well as innovative, attack detection and alerting techniques. Adapted mitigation plans and countermeasures were defined, taking into account their potential impact on operations. Protection Profiles for railway control and signalling applications were delivered to ensure security by design of new rail infrastructures.
34	DAPPER	Doing Anonymization Practically, Privately, Effectively and Reusably	The project considered the whole data release process, from the data owner to the data user. It laid out a set of principles for privacy tool design that highlight the requirements for interoperability, extensibility and scalability. The aim of the project was in Delivering Anonymization Practically, Privately, Effectively and Reusably (DAPPER)
35	DECODE	Decentralised Citizens Owned Data Ecosystem	The aim of the project to develop decentralised technologies (such as blockchain and cryptography) to give people greater control over their data. DECODE explores how to build a data-centric digital economy where data that is generated and gathered by citizens, the Internet of Things (IoT), and sensor networks is available for broader communal use, with appropriate privacy protections. As a result, innovators, startups, NGOs, cooperatives, and local communities can take advantage of that data to build apps and services that respond to their needs and those of the wider community. Four pilots: Digital Democracy and Data Commons, Citizen Science Data Governance, Digital Register - age check with municipal census data and Neighbourhood Online
36	DEFENDER	Defending the European Energy Infrastructures	DEFENDER addresses the emerging challenges associated with the proactive protection and fast restoration to mitigate physical or cyber incidents or attacks and most importantly combined cyberphysical attacks of the power transmission and distribution grid network infrastructure, which lies at the heart of any Critical Energy Infrastructure (CEI). Novel concepts for Critical Energy Infrastructures' security lifecycle assessment by design based on protective and lifecycle Closed Control Loops. Robustness, resiliency and self-healing as embedded Critical Energy Infrastructure characteristics, based on virtualization, reconfiguration and energy rerouting concepts.

37	DISCOVERY	Dialogues on ICT to Support COoperation Ventures and Europe-North AmeRica (Canada and USA) sYnergies	The goal is to create the Transatlantic ICT Forum as a sustainable mechanism to support dialogues for EU-North America cooperation in the field of ICTThe Transatlantic ICT Forum will promote policy debate and provide opinions and recommendations on crucial issues facing the EU-US and EU-Canada dialogues in ICT. Under the umbrella of the ICT Forum, three Working Groups have been established on funding mechanisms, ICT policy and regulations, and cybersecurity.
38	DiSIEM	Diversity Enhancements for SIEMs	The core idea of the project is to enhance existing SIEM systems with several diversity mechanisms, representing five main advances in the state of the art: - Integrate diverse OSINT (Open Source Intelligence) data sources. This data needs to be fetched, analysed, normalised and fused to identify relationships, trends and anomalies and hence help reacting to new vulnerabilities to the new infrastructure or even predict possible emerging threats against the infrastructure monitored by the SIEM. - Develop novel probabilistic security models and risk-based metrics to help security analysts to decide which infrastructure configurations offer better security guarantees and increase the capacity of SOCs to communicate the status of the organisation to C-level managers. - Design novel visualisation methods to present the diverse live and archival data sets, to better support the decision-making process - Integrate diverse, redundant and enhanced monitoring capabilities to the SIEM ecosystem to increase the value of the events fed to the system - Add support for long term archival of events in public cloud storage services
40	DOGANA	aDvanced sOcial enGineering And vulNerability Assesment Framework	a comprehensive tool-chain to perform cyber-risk assessments related to social engineering; a Framework to efficiently perform users' training in innovative and long-lasting ways; a law enforcement component aiming at addressing country specific and Europe-wide legal aspects.

42	e-Sides	Ethical and Societal Implications of Data Sciences	The principal scope of e-SIDES is to: 1 - Involve the complete value chain of big data stakeholders to reach a common vision for an ethically sound approach to big data processing. 2 - Improve the dialogue between data subjects and big data communities (industry, research, policy makers, regulators) and, thereby, to improve the confidence of citizens towards big data technologies and data markets. It will prepare and widely disseminate community shared conclusions and recommendations highlighting the best way to ultimately build confidence of citizens and businesses towards big data and the data economy.
43	ECRYPT-CSA	European Coordination and Support Action in Cryptology	The goal of this CSA is to strengthen European excellence in the area of cryptology and to build on the Network of Excellence ECRYPT and ECRYPT II to achieve a durable integration and structuring of the European cryptography community, involving academia, industry, law enforcement and defence agencies.
45	ENCASE	EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors	ENCASE aims to (ENhancing seCurity and privAcy in the Social wEb) aims at leveraging the latest advances in usable security and privacy toto design and implement a browser-based architecture for the protection of minors from malicious actors in online social networks (OSNs). The ENCASE user-centric architecture consists of three distinct services, which can be combined to form an effective protective net against cyberbullying, racist and hateful memes, sensitive content distribution, sexually abusive acts, and fake activity: a) a browser add-on with its corresponding intelligent web-proxy and scalable back-end software stack that collects the users" online actions to unveil incidents of aggressive or distressed behavior; b) a browser add-on with its associated web-proxy and back-end software stack that analyses social web data to detect fraudulent and fake activity and alert the user; and c) a browser add-on that detects, together with the intelligent web-proxy, when a user is about to share sensitive content with inappropriate audiences and protects it. The third add-on has usable controls that enable users to protect their content by suggesting suitable access lists, by watermarking, and by securing the content via cryptography or steganography.

46	EU-SEC	The European Security Certification Framework	Framework for multiparty recognition between trustworthy cloud services security certification: The framework defines the principles, criteria, processes and technical capabilities for the mutual recognition between various National, International and sector specific cloud security certifications and attestations. Continuous Auditing based security certification for trustworthy cloud services: Continuous auditing based certification relies on tools, methods and processes that allow for security properties of cloud services being checked with a frequency that depends on the service level/qualitative objectives (SLO & SQO) agreed upon between the parties. The EU-SEC aims to enhancing trustworthiness and transparency in the ICT supply chain through business cases developed and piloted by industrial partners.
47	EUNITY	Cybersecurity and privacy dialogue between Europe and Japan	EUNITY aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions.
50	FutureTrust	Future Trust Services for Trustworthy Global Transactions	FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the standardisation process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications. In particular the FutureTrust project will extend the existing European Trusted List (TL) infrastructure towards a “Global Trust List”, develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals and will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment.
51	GenoPri	Quantifying and Protecting the Privacy of Genomic Data	The two main objectives of this project are (i) to develop a new unifying framework for quantification of genomic privacy of individuals and (ii) to establish a complete framework for privacy-preserving utilization, sharing, and verification of genomic data under real-life threat models. Graph-based, iterative algorithms previously developed by the applicant to efficiently analyze big data and make inference from it will be the foundation for the new quantification framework. To achieve the holistic genomic privacy objective, cryptographic tools, techniques from information theory, and statistics (differential privacy) will be used.

52	GHOST	Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control	GHOST project provides a usable and autonomous solution for cyber security assessment in IoT-enabled smart home solutions. Ghost will contribute to boost European IoT home market, bringing next-generation security systems for domestic applications (based on technologies like blockchain or deep packet inspection) to all users, independently of their previous knowledge. The project mission is to deliver the first generation of disruptive software-enabled usable security network solution for Smart-Home occupants. GHOST software will be embedded in home network gateways to perform network analysis and deep packet inspection for suspicious pattern recognition, will apply machine learning and data analytics for malicious behaviour detection, will carry out context-aware real-time risk assessment, widely apply data analytics and visualization for effortless user comprehension and decision support, strengthen security defence through blockchain technology and smart contracts, while ensuring interoperability with various gateways and a wealth of IoT devices through a dedicated middleware layer.
53	HEAT	Homomorphic Encryption Applications and Technology	The HEAT project will develop advanced cryptographic technologies to process sensitive information in encrypted form, without needing to compromise on the privacy and security of the citizens and organizations that provide the input data. The core technology is based on homomorphic cryptography, which allows to perform computations on encrypted information without decrypting it. The main goal of HEAT is to produce a step change in the efficiency and applicability of this technology. The proposed outputs of HEAT are an open source software library to support applications that wish to use homomorphic cryptography.
54	HECTOR	HARDWARE ENABLED CRYPTO AND RANDOMNESS	The main objective of this project is to close the gap between the mathematical heaven of cryptographic algorithms and their efficient, secure and robust hardware implementations. It requires integrating secure cryptographic primitives such as random number generators (RNGs) and physically uncloneable functions (PUFs), together with physical attack countermeasures. Therefore we will study, design and implement RNGs and PUFs with demonstrable entropy guarantees and quality metrics. This includes on-the-fly entropy testing and physical attacks evaluations. This will enable more secure systems and easier certification.

55	HERMENEUT	Enterprises intangible Risks Management via Economic models based on simulatioN of modErn cyber-aTtacks	Fostering a culture of risk management, Hermeneut provides individual organisations as well as business sectors with an innovative methodology for the dynamic assessment of their vulnerabilities and corresponding tangible and intangible assets at risk. HERMENEUT delivers an Integrated estimation of the Enterprise's vulnerabilities for both the humans and technology, an innovative economic model, a holistic risk assessment model, a Web-based risk-driven cyber-security cost-benefit decision support tool, a validation of the potential of the proposed approach.
56	HIPS	High-Performance Secure Computation with Applications to Privacy and Cloud Security	A synergetic approach towards achieving high-performance secure computation. We will design new protocols while combining research from cryptography, algorithms and systems. In this way, issues like load balancing, memory management, cache-awareness, bandwidth bottlenecks, utilisation of parallel computing resources, and more, will be built into the cryptographic protocol and not considered merely as an afterthought. If successful, HIPS will enable the application of the beautiful theory of secure computation to the problems of privacy in the digital era, cloud security and more.
57	IMPACT	imPACT – Privacy, Accountability, Compliance, and Trust in Tomorrow's Internet	The imPACT project addresses the challenge of providing privacy, accountability, compliance and trust (PACT) in tomorrow's Internet, using a cross-disciplinary and synergistic approach to understanding and mastering the different roles, interactions and relationships of users and their joint effect on the four PACT properties. The focus is on principles and methodologies that are relevant to the needs of individual Internet users, have a strong potential to lead to practical solutions and address the fundamental long-term needs of the future Internet.

58	KONFIDO	KONFIDO - Secure and Trusted Paradigm for Interoperable eHealth Services	KONFIDO provides a set of tools that improve the security of cross-border exchange of eHealth data using OpenNCP. - The Trusted Execution Environment tool ensures secure communication among NCPs nodes belonging to the community. - p-PUF devices will be employed in the NCP that will operate as true random number generators and key generators for specific Homomorphic Encryption (HE) schemes. - The homomorphic encryption component used for protecting the exchange and the processing over sensitive patient data provides services at NI level, while for the NCP it is based on a new and ameliorated version of Cingulata (previously known as Armadillo), a crypto-compiler and run-time environment developed by CEA. - The KONFIDO SIEM is able to analyse information and events collected using a holistic approach at the different levels of the monitored system to discover possible ongoing attacks, or anomalous situations. - The blockchain-based auditing mechanism developed in the framework of KONFIDO is a legally binding system that allows to prove that scientific eHealth data have been requested by a legitimate entity and whether they have been provided or not. - OpenNCP is extended to provide eIDAS-compliant authentication for its users.
60	LIGHTest	Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes.	The objective of LIGHTest is to create a global cross-domain trust infrastructure that renders it transparent and easy for verifiers to evaluate electronic transactions. By querying different trust authorities world-wide and combining trust aspects related to identity, business, reputation etc. it will become possible to conduct domain-specific trust decisions. There is a LIGHTest community promoting the use of the results of LighTest project.

61	LV-Pri20	Logic-based Verification of Privacy-Preservation in Europe's 2020 ICT	Objective I has been the development of privacy-expressing formalisms to be used in the automatic verification of ICT/IoT systems; these formalisms were mainly based on applied logics. Objective II has been the development of new algorithms and automatic tools for the verification of security and privacy properties, with a focus of privacy properties; these tools were mainly based on applied logics. Objective III has been the analysis of classes of applications/systems, against their security and privacy properties with a focus on their privacy properties. Objective IV has envisaged redesigning systems/applications that had been found vulnerable during the explorations undertaken to achieve the third objective, into versions that are provably secure. Where possible, prototype implementations of the new designs have been envisaged. The systems tackled are manifold: lightweight authentication systems, C-like programs, real-life authenticated key-exchange infrastructures based on every-day-use protocols like TLS.
62	MAMI	Measurement and Architecture for a Middleboxed Internet	The MAMI project seeks to restore balance among end-user privacy concerns in the face of pervasive surveillance, innovation in network protocols in the face of increasing ossification, and the provision of in-network functionality in a cooperative way. The MAMI project aims to rearchitect the Internet to allow explicit cooperation between endpoints and middleboxes, restoring the promise and innovation potential of the original end-to-end architecture of the Internet while enabling appropriate in-network services to ease management and scalability of ever more demanding applications. To ensure the applicability of the protocol, it will develop it on a background of middlebox behaviour models, derived from large-scale measurements of middleboxes in the public Internet conducted on top of the MONROE testbed. After evaluating the fitness of proposed MCP by assessing its applicability to a set of real-world use cases for transport layer evolution, it will focus on incremental deployability in the presence of both cooperative and uncooperative middleboxes by experimentation in the Internet utilising the facilities provided by MONROE. The MAMI project is very active in standardisation with a focus on transport protocol work in the IETF. MAMI results are being considered for application to mobile edge and core as well as Software Defined Networking (SDN)-based network management approaches.

63	MAPPING	Managing Alternatives for Privacy, Property and INternet Governance	MAPPING's goal is to create an all-round and "joined-up" understanding of the many and varied economic, social, legal and ethical aspects of the recent developments on the Internet, and their consequences for the individual and society at large. MAPPING specifically investigates and debates the existing innovation policies, business models and legal framework related to the implementation of the Digital Agenda for Europe and the changes needed to set up an improved governance structure for the EU innovation ecosystem. More specifically MAPPING looks at current issues in Internet Governance, Privacy, Personality and Business Models and Intellectual Property Rights (IPR) in an online environment.
64	MAS2TERING	Multi-Agent Systems and Secured coupling of Telecom and EnErgy gRIds for Next Generation smartgrid services	It aimed at developing an innovative information and communication technology (ICT) platform for the monitoring and optimal management of low-voltage distribution grids by integrating last mile connectivity solutions with distributed optimisation technologies, while enhancing the security of increased bi-directional communications. MAS2TERING combines an original business vision, aimed at the enablement of local energy aggregation markets, with a set of enabling technologies from the artificial intelligence, communication and security domains. Development of software tools, for integration into the MAS2TERING Multi-Agent Systems platform, to investigate risks of breach of privacy and security, and reliability and QoS from insecure authentication in a heterogeneous environment where legacy standards and applications need to remain in operation alongside advanced standards. To deliver software modules, for them to be integrated into the MAS2TERING Multi-Agent Systems platform, to identify and quantify loss of data, breach of privacy and vulnerability from heterogeneous communication infrastructure (wireless, wired, PLC) and their impacts on grid reliability and QoS.
65	MATTHEW	Multi-entity-security using active Transmission Technology for improved Handling of Exportable security credentials Without privacy restrictions	The objective of MATTHEW is to develop novel, privacy-preserving security applications with Anonymity and Attribute Based Credentials (ABC) being transferable over various mobile platforms like smart phones and tablets using Near Field Communication (NFC). MATTHEW results will be demonstrated by a transferable payment application and a multi-key access control system. An ABC-based cryptographic API will provide pseudonyms for privacy.

67	mF2C	Towards an Open, Secure, Decentralized and Coordinated Fog-to-Cloud Management Ecosystem	mF2C provides a novel framework that increases the efficiency of resources' usage taking into consideration not only service requirements but also user demands. mF2C is agnostic of the application domain, meaning that the solution proposed can solve the needs of different verticals of different sizes, leveraging the European industries' competitiveness, enabling businesses to scale on the principles of sharing economy in a cooperative framework. In more details, the mF2C framework provides a coordinated management of traditional cloud architectures and novel fog ones, offering unique capabilities for distributed execution of applications throughout IoT, fog and cloud environments across a wide variety of industry verticals. Furthermore, mF2C facilitates the efficient usage of resources within the stack built from the edge up to the cloud, taking into consideration services' requirements (e.g. immediate data collection and processing, low latency) and user demands (e.g. security and QoS).
68	MH-MD	My Health - My Data	MyHealth-MyData is developing a permissioned blockchain network allowing biomedical data exchanges from hospitals and individual users to research centres and industries for academic or industrial research purposes. The platform is equipped with smart contracts to implement data transactions, identity and consent management tools (i.e., blockchain wallets, dynamic consent mechanisms), data anonymisation/encryption and secure computation tools, and some big data analytics for knowledge discovery on anonymised datasets.
69	MIKELANGELO	MIcro KErneL virtualizAtioN for hiGh pErfOrmance cLOud and hpc systems	The goal of MIKELANGELO is to provide improved responsiveness, flexibility and security of virtual infrastructure through novel components, supporting different setups or variants of the HPC, Cloud and HPC-Cloud. MIKELANGELO relies on optimisation of guest, hypervisor, their joint collaboration and on the set of approaches, devised to simplify and increase performance in virtual IO. the OSv management software has been significantly improved and is now under one brand Lightweight Execution Environment Toolbox - LEET. This includes complete OSv management utilities, which have been accepted into DellEMC's UniK project (https://github.com/emc-advanced-dev/unik) and into MirantisIT's Virtlet project (https://github.com/Mirantis/virtlet). MIKELANGELO is targeting to develop hypervisor-level security mechanisms for monitoring and mitigating cache side-channel attacks.

70	MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs	207Despite the importance of Critical Information Infrastructures (CIIs) and dynamic ICT-based maritime supply chains (SCs) for port operations, state-of-the-art Risk Management (RM) methodologies for maritime environments pay limited attention to cyber-security and do not adequately address security processes for international SCs. Motivated by these limitations, MITIGATE will introduce, integrate, validate and commercialize a novel RM system, which will empower stakeholders' collaboration for the identification, assessment and mitigation of risks associated with cyber-security assets and SC processes. This collaborative system will boost transparency in risk handling, while enabling the generation of unique evidence about risk assessment and mitigation. At the heart of the RM system will be an open simulation environment enabling stakeholders to simulate risks and evaluate risk mitigation actions. This environment will allow users to model, design, execute and analyze attack-oriented simulations. Emphasis will be paid on the estimation of cascading effects in SCs, as well as on the prediction of future risks.
71	MUSA	MUlti-cloud Secure Applications	The main objective of MUSA is to support the security-intelligent lifecycle management of distributed applications over heterogeneous cloud resources, through a security framework that includes: security-by-design mechanisms to allow application self-protection at runtime, and methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications. The project produced an open source tool suite composed of: a) A Kanban-style Integrated SecDevOps Dashboard for MultiCloud systems, b) MultiCloud systems Modeller, c) Riks Assessment tool for multiCloud systems, d) Security SLA generator for multiCloud systems, e) SIEM for mulitCloud systems. All the MUSA tools are integrated in the MUSA SecDevOps Framework, a single kanban-style Dashboard that enables multi-disciplinary DevOps teams to collaborate in the application life-cycle. MUSA offers an easily extendable Catalogue of security mechanisms already prepared to be deployed to work with your application components.

73	NeCS	European Network for Cyber-security	The European Network for Cyber Security (NECS) addresses the training and development of a European talent pool to help implement and support the European Cyber-security strategy as highlighted in the EC's Digital Agenda. NeCS research topics are: - Cybersecurity operations systems management: Including schemes for improving the efficiency of cyber security operations, for improving the protection and resilience of systems and data to cyber-attacks and the run-time adaptation of the protection and detection mechanisms of systems and processes while under attack as well as depending on risk and context of operation as well as to develop an improved understanding how cyber-attacks evolve including attacks that utilise new generations of malware, advanced evasion techniques and a fusion of computing and social engineering methods including those leveraging trust and influence in social networks. - Information exchange and sharing: to identify models, system architectures, interaction methods and processes to exchange information on cyber-security incidents of different nature (e.g. technical failures; human mistakes; natural events, malicious attacks) and on threats and vulnerabilities, in order to improve security operations and cyber-security intelligence in complex value chains and ecosystems, encompassing a large number of interconnected players and strongly interlinked information systems. - Risk management for cybersecurity: This will include training on methodologies, mathematical models, IT and telecommunications system architectures and solutions for risk management, especially applied for critical infrastructures. Research in this area also targets cyber-security metrics and their ability to correctly estimate risks for the cyber systems. Moreover, this area includes the management of the interactions between cyber-security risk management and the overall risk management/continuity plan of an organisation. In particular, a novel and rapidly gaining attention topic13 on cyber-insurance, as an alternative of risk mitigation strategy, will be considered.

74	OCGN	Traditional Organised Crime and the Internet: The changing organization of illegal gambling networks	The project examines online gambling and extortion networks. The objectives of this research are: - establish tools and technique that facilitate management of internal/external cyber-threats to online gambling sector - validate tools and techniques that will facilitate the management of internal/external cyber-threats to online gambling sector - set standards of information management - set standards of dissemination and flows of information to cybersecurity centres from online gambling sector in EU This is to be achieved by: - interviews with key individuals (systems managers at online sites and law enforcement) - analyse data for information flows and breaking down volume of information into accessible data for internal and external use. - analyse current decision-making processes/systems and processing information - analyse exchange of data to improve and implement best practice available in cybersecurity across EU online gambling sites
75	OCTAVE	Objective Control for TAlker VErification	Automatic Speaker Verification (ASV) as a Service. Solutions will be installed in data-sensitive and mission-critical services and validated in two real commercial trials: banking services and physical access within a critical airport infrastructure.
77	OPERANDO	Online Privacy Enforcement, Rights Assurance and Optimization	Specify, Implement, field test, validate and exploit an innovative privacy enforcement framework that will enable the Privacy as a Service (PaS) business paradigm and create a broad market for online privacy services online. Two available services: Operando G2C and Operando Consumer Privacy

79	PaaSword	A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications	A holistic data privacy and security by design framework enhanced by sophisticated context-aware policy access models and robust policy access, decision, enforcement and governance mechanisms, which will enable the implementation of secure and transparent Cloud-based applications and services that will maintain a fully distributed and totally encrypted data persistence layer, and, thus, will foster customers' data protection, integrity and confidentiality, even in the case wherein there is no control over the underlying third-party Cloud resources utilized. Distributed encryption and virtual database middleware technologies
81	PANORAMIX	Privacy and Accountability in Networks via Optimized Randomized Mix-nets	The main goal of PANORAMIX is to provide privacy via mix-networks. Mix-nets for Private Electronic Voting Protocols. FREE criptography softwares https://panoramix-project.eu/software/
86	PQCRYPTO	Post-quantum cryptography for long-term security	PQCRYPTO will allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things. PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

91	PrEstoCloud	PrEstoCloud - Proactive Cloud Resources Management at the Edge for Efficient Real-Time Big Data Processing	The goal of PrEstoCloud is to make substantial research contributions in the Cloud computing and real-time Big Data technologies in order to provide a dynamic, distributed architecture for proactive cloud resources management reaching the extreme edge of the network for efficient real-time big data processing and to deploy and validate it in several challenging, complementary and commercially-very promising use cases. In particular, PrEstoCloud aims to combine real-time Big Data, Cloud computing and Fog computing research in a unique way in order to provide an innovative solution for, as above elaborated, very complex problem of cloud-based adaptive real-time Big Data processing. TELEMATICS USE CASE: A vehicle/fleet management processes real-time information and alerts – based on data streams from GPS, on-board diagnostics, tire sensors and others. SURVEILLANCE USE CASE: A surveillance solution combines real-time data streams from cameras and pre-processing results from groups of unmanned aerial vehicles. MEDIA USE CASE: A media prosumer platform offers personalized and flexible consumption of real-time stories by combining freelance reporting, traditional broadcasting and social media streams.
95	PRISM CODE	Privacy and Security for Mobile Cooperative Devices	Design some of the fundamental tools for privacy and security of the upcoming distributed services, which are built upon the cooperation of mobile personal devices like smartphones, PDAs, or tablets. In analogy with the geometric prism which is built on two parallel bases, we believe that a wide adoption of cooperative services for mobile devices is possible only on the following two bases, to be present at the same time: privacy, to give to the users and other stakeholders some confidence that no private information will be disclosed by taking part in those services; and security, to guarantee (to some extent) that the services will not be exploited in a malicious way (e.g. having no money loss for stakeholders).
96	PRISMACLOUD	PRIvacy and Security MAintaining services in the CLOUD	Enabling secure and trustworthy cloud-based services by improving and adopting novel tools from cryptographic research. The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users. The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and provide tools to protect their privacy with the best technical means possible - by cryptography. The evaluation and validation of the developed methods and tools will be done in three pilots from three different domains, namely e-Health, Smart City and e-Government.

98	PRIVACY FLAG	Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments	Privacy Flag is developing a set of tools to enable citizens to check whether their rights as data subjects are being respected, and tools and services to help companies comply with personal data protection requirements. - app, addon and IoT tool + Privacy Flag Observatory are avilable and FREE: https://privacyflag.eu/pf-tools/ - Privacy Pact: https://privacyflag.eu/pf-tools/privacy-pact/ - Privacy Certification: https://privacyflag.eu/pf-tools/privacy-certification-scheme/ - Privacy Portal: https://www.privacyportal.eu/ - Privacy Flag Mobile App: https://privacyflag.eu/pf-tools/pf-mobile-application/ - Privacy Flag Browser Add on: https://privacyflag.eu/pf-tools/browser-add-on/ - IoT Tool: https://privacyflag.eu/pf-tools/iot-tool/ - Privacy Flag Observaroty https://privacyflag.eu/pf-tools/privacy-flag-observatory/ USE CASES: Mobile Application and IoT Tool, Browser Add-On, Website And Backend Management Platform
99	Privacy&Us	Privacy and Usabiliy	The PRIVACY.US innovative training network will train thirteen creative, entrepreneurial and innovative early stage researchers (ESRs) to be able to reason, design and develop innovative solutions to questions related to the protection of citizens' privacy, considering the multidisciplinary and intersectoral aspects of the issue. ESRs will be trained to face both current and future challenges in the area of privacy and usability. PRIVACY.US offers a combination of research-related and transferable competence skills that will enhance the career perspectives of the ESRs in both the academic and non-academic sectors.
100	PRIVACY4FORENSICS	A Formal Rule-Processing Engine for Privacy-Respecting Forensic Investigation	The key goal was to develop a rule-processing engine that extracts privacy properties of collected data and investigation search warrant(s), detects conflicting or uncertain situations and labels collected data accordingly, and monitors and controls investigator access to collected data in accordance with the assigned labels.

101	ProBOS	Protection Beyond Operating System - Development of the next generation cyber security solution	Next generation cyber security protection solution –ReaQta-core - that can revolutionise the IT security market by offering a higher level of protection to governments and private organisations. ReaQta-core is the first to apply a novel approach that incorporates a unique NanoOS and an Artificial Intelligence Engine to protect endpoints from the most advanced and sophisticated cyberthreats. They developed 2 products and 1 service: - ReaQta-Hive: Autonomous Detection & Response platform that eliminates any threat. - ReaQta-EON: Cloud-delivered NGAV+ with anti-ransomware capabilities - ReaQta-MDR: Augment your security team with 24/7 threat monitoring and response.
102	PROTECTIVE	Proactive Risk Management through Improved Cyber Situational Awareness	The PROTECTIVE system is designed to provide solutions for public domain CSIRTs and SME's who both have needs outside the mainstream of cyber security solution provision. PROTECTIVE will develop a comprehensive solution to raise organisational cyber situational awareness (CSA) through - enhancement of security alert correlation and prioritisation - linking of the relevance/criticality of an organizations assets to its business/mission - establishment of a threat intelligence sharing community Two pilots will be conducted to evaluate and validate the PROTECTIVE outcomes with CSIRTs from 3 National Research and Educational Networks (NRENs) and with SMEs via a managed security service provider (MSSP). GDPR compliance through development of run-time monitoring.
103	Ps2Share	Participation, Privacy and Power in the Sharing Economy	Ps2Share is concerned with questions of participation, privacy, and power in the sharing economy. The sharing economy promises to provide more inclusive business opportunities for individuals of various skills levels and resource endowment. However, the public rhetoric of chances, growth, and inclusion frequently contrasts with the risks, concerns, disadvantages, and exclusion in the experience of a variety of users. These platforms, extending into the private and physical realm of their users, create compound privacy risks and increase the potential for exclusion and discrimination through ratings-based sanctioning. Our overarching objective is to identify key challenges of the sharing economy and improve Europe's digital services through providing recommendations to Europe's institutions. These will include schools and companies, as well as governmental and non-governmental organisations.

104	RAPID	Heterogeneous Secure Multi-level Remote Acceleration Service for Low-Power Integrated Systems and Devices	RAPID proposes the development of an efficient heterogeneous CPU-GPU cloud computing infrastructure, which can be used to seamlessly offload CPU-based and GPU-based (using OpenCL API) tasks of applications running on low-power devices such as smartphones, notebooks, tablets, portable/wearable devices, robots, and cars to more powerful devices over a heterogeneous network (HetNet). In addition, RAPID proposes a secure unified model where almost any device can operate as an accelerated entity and/or as an accelerator serving other less powerful devices. Finally, a RAPID device can probe a Directory Server, which includes information for the accelerators, in order to automatically find and connect to the appropriate accelerators.

105	REASSURE	Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience	Many of the elements described below can be freely downloaded through the Resources tab. Regarding improvements of evaluation schemes, we delivered, based on a detect-map-exploit approach, a novel evaluation strategy that works “backwards’’ from an idealized and well-defined worst-case adversary. This strategy has the potential to maximise the assurance in evaluations by, per default, instantiating adversaries whose success can be bounded. We also significantly contributed to the understanding of the radically new attack vectors based on deep learning, and to the use of leakage detection tools in the context of our structured testing regime. In order to help IoT developers, we assessed the suitability of shortcut formulas as techniques enabling efficient a priori approximation of attack outcomes; we thoroughly analysed the use of leakage detection for conformance testing; we analysed how to automate leakage detection, which is one of the first steps of an evaluation. We also delivered a free introductive training on side-channel attacks, as well as a more advance training on leakage detection, first delivered during a workshop aligned with CARDIS 2018, before becoming a free self-led online training course. Many of the aforementioned results were integrated into tools, as targeted by our third objective. To help developers and researchers test attacks, and to improve the comparability of results, we published four reference data sets (for AES and ECC), one software implementation for AES and a corresponding set of data sets for deep learning (the ASCAD database). We also released an open-source leakage simulator (ELMO) based on instruction-level profiles for a processor relevant for the IoT (used by NCSC, NXP, now underpins the ROSITA tool), an open source toolbox for SCA (JuliaSCA), an open source implementation for shortcut formulas, scripts related to shortcut formulas for ECC implementations, keyless rank estimation and local random probing model (belief propagation) for the worst-case analysis of ECC countermeasures. Finally, we developed Inspector Cloud, an online tool allowing to perform side-channel attacks
107	REDSENTRY	Proactive Operational Intelligence Cybersecurity Platform for the Financial Services Industry	REDSENTRY aims to provide a flexible, scalable and open solution to the ever-changing threat landscape faced by the financial services sector. REDSENTRY will provide a real-time networking monitoring platform to provide the ability to detect and manage any type of threat. By focusing on network monitoring REDSENTRY will provide enable financial sector institutions to manage their infrastructure in real time, proactively and with automatic security response protocols.

110	SafeCloud	Secure and Resilient Cloud Architecture	SafeCloud will re-architect cloud infrastructures to ensure that data transmission, storage, and processing can be: partitioned in multiple administrative domains that are unlikely to collude, so that sensitive data can be protected by design; entangled with inter-dependencies that make it impossible for any of the domains to tamper with its integrity. These two principles (partitioning and entanglement) are applied holistically across the entire data management stack, from communication to storage and processing. Users will control the choice of non-colluding domains for partitioning and the tradeoffs between entanglement and performance, and thus will have full control over what happens to their data. This will make users less reluctant to manage their personal data online due to privacy concerns and will generate important benefits for privacy-sensitive online applications such as distributed cloud infrastructures and medical record storage platforms.
111	SAFEcrypto	Secure Architectures of Future Emerging Cryptography	It provides a new generation of practical, robust and physically secure post-quantum cryptographic solutions that ensure long-term security for future ICT systems, services and applications. Novel public-key cryptographic schemes (digital signatures, authentication, identity-based encryption (IBE), attribute-based encryption (ABE)) will be developed using lattice problems as the source of computational hardness. The project will involve novel algorithmic and design optimisations, and implementations of the lattice-based cryptographic schemes addressing the cost, energy consumption, performance and physical robustness needs of resource-constrained applications, such as mobile and battery-operated devices, and of real-time applications, such as network security, satellite communications and cloud. Use cases: Network Space-based Entities, Public Safety Communications, Privacy-preserving Municipal Data Analytics

112	SAFERtec	Security Assurance FramEwoRk for neTworked vEhicular teChnology	The main output is a security assurance framework for connected vehicles. As such the focus of the project is not a high-TRL system to be presented to customers. An online SW toolkit could serve as a potential product but has been rather foreseen as a more practical way to use the proposed security assurance framework. Provide a security assurance Framework enabled to cover the whole System Development Life Cycle (i.e., planning, design, implementation, operation and maintenance) of ICT-based Connected Vehicles The SAFERtec project will put under the microscope two highly pervasive instances of the Automotive communications (i.e., RSU- and cloud- communications) and consider a broad range of the related security-assurance issues.
113	SAINT	SYSTEMIC ANALYZER IN NETWORK THREATS	SAINT proposes to analyse and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cybercriminal activity, associated markets and revenues will drive the development of a framework of business models appropriate for the fighting of cybercrime. SAINT will provide to a clear set of methodologies, regulatory recommendations, behaviour protocols, and best practices to all relevant stakeholders including policy makers, regulators, governmental authorities, law enforcement agencies, and relevant market operators. Global Security Map: https://globalsecuritymap.com/ A series of deliverables on networking cybersecurity https://project-saint.eu/deliverables
114	SAURON	Scalable multidimensionAl sitUation awaReness sOlution for protectiNg european ports	Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe and put the focus on protection of EU Ports under Transport Infrastructure and means of transportation type of CI. The main outcome of SAURON is the multidimensional yet installation-specific Situational Awareness (SA) platform which helps port operators to anticipate and to withstand potential cyber, physical or combined threats to their business. The SAURON platform consists of the following components: (a) Physical Situational Awareness application (PSA); (b) Cyber Situational Awareness application (CSA); (c) Hybrid Situational Awareness application (HSA); and (d) SAURON Emergency Population Warning System (EPWS)

115	SCISSOR	Security In trusted SCADA and smart-grids	SCISSOR designs a new generation SCADA security monitoring framework, comprising four layers: i) a monitoring layer supporting traffic probes providing programmable traffic analyses up to layer 7, new ultra-low cost/energy pervasive sensing technologies, system and software integrity verification, and smart camera surveillance solutions for automatic detection and object classification; ii) a control and coordination layer adaptively orchestrating remote probes/sensors, providing a uniform representation of monitoring data gathered from heterogeneous sources, and enforcing cryptographic data protection, including certificate-less identity/attribute-based encryption schemes; iii) a decision and analysis layer in the form of an innovative SIEM fed by both highly heterogeneous monitoring events as well as the native control processes' signals, and supporting advanced correlation and detection methodologies; iv) a human-machine layer devised to present in real time the system behaviour to the human end user in a simple and usable manner. SCISSOR's framework will leverage easy-to-deploy cloud-based development and integration, and will be designed with resilience and reliability in mind (no single point of failure). SCISSOR will be assessed via i) an off-field SCADA platform, to highlight its ability to detect and thwart targeted threats, and ii) an on-field, real world deployment within a running operational smart grid, to showcase usability, viability and deployability.

116	SCOTT	Secure COnnected Trustable Things	Building user trust will be a real competitive advantage for technologies, products and services in the IoT market. SCOTT involves technology, human and social sciences, and will build trustable things that securely communicate‘, interconnected by dependable wireless technology, which do care about the end-users‘ privacy desires. USE CASES: Air quality monitoring for healthy indoor environments Vehicle-as-a-sensor within smart infrastructure Managed wireless for smart infrastructure Secure wireless avionics intra communications for sensing and actuation Secure connected facilities management Safe freight and traffic management in intermodal logistic hubs Logistics management using collaborative robots and DevOps methodologies Autonomous wireless network for rail logistics and maintenance Secure cloud services for novel connected mobility applications Smart train composition coupling Ubiquitous testing of automotive systems Trustable warning system for critical areas Trustable wireless in-vehicle communication network Assisted living and community care Secure Car Access solutions Publications: https://scottproject.eu/media/publications/
117	SCR	Disruptive Cybersecurity SaaS for SMEs and freelance developers	Our system automates the vulnerability scanning of software assets and reduces the effort required for development teams to adopt security best practices.
118	SecIoT	Cybersecurity Threat Detection for Internet of Things Connected Devices	The EU-funded SecIoT project helped close the security gap. Experts in IoT security are relatively scarce, while demand for IoT security consultations is growing. Hence, the project team developed a plan for an automated cybersecurity expert system, intended for companies manufacturing IoT devices. The system will ultimately allow manufacturers to test their products for vulnerability and make necessary improvements.

119	SERECA	Secure Enclaves for REactive Cloud Applications	The Secure Enclaves for REactive Cloud Applications (SERECA) project aims to remove technical impediments to secure cloud computing, and thereby encourage greater uptake of cost-effective and innovative cloud solutions in Europe. It proposes to develop secure enclaves, a new technique that exploits secure commodity CPU hardware for cloud deployments, empowering applications to ensure their own security without relying on public cloud operators. Secure enclaves additionally support regulatory-compliant data localisation by allowing applications to securely span multiple cloud data centres. Although secure enclaves are a general mechanism, SERECA focuses on a particularly important and rapidly growing class of applications: reactive applications for the Internet of Things (IoT), Cyber-Physical Systems (CPS), augmented reality, gaming, computer-mediated social interaction. SERECA is validating its results through the development of two innovative and challenging industry-led use cases. One concerns the monitoring of a civil water supply network, a critical infrastructure targeted by malicious attacks. The other concerns a commercial software-as-a-service (SaaS) application for analysing the performance of cloud-deployed applications. Such a service collects sensitive performance metrics about live usage, assets that must be protected from industrial espionage and other criminal activities.
120	SHARCS	Secure Hardware-Software Architectures for Robust Computing Systems	A framework for designing, building and demonstrating secure-by-design applications and services, that achieve end-to-end security for their users. SHARCS will achieve this by systematically analysing and extending, as necessary, the hardware and software layers in a computing system. This holistic approach is necessary, as no system can truly be secure unless every layer is secured, starting from the lowest one. We will measure the effectiveness of the SHARCS framework by using it on a diverse set of security-critical, real-word applications. The applications have been chosen from three different domains, medical, cloud and automotive, to demonstrate the platform independence capabilities of SHARCS. SHARCS will provide a powerful foundation for designing and developing trustworthy, secure-by-design applications and services for the Future Internet.

121	SHIELD (Health)	European Security in Health Data Exchange	SHiELD will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it. This will make it possible to provide better health care to mobile citizens across European borders, and facilitate legitimate commercial uses of health data. SHiELD will address these security and compliance challenges: • providing models and analysis tools for automated identification of end-to-end security risks and compliance issues and supporting privacy and 'by design'; • defining an open and extensible data exchange architecture based on epSOS, able to support security measures to address these risks; • developing security mechanisms to deal with new and emerging risks, such as inference attacks on sensitive data, and risks from relatively unprotected mobile edge devices; • providing faster and more cost effective methods to verify and monitor compliance with multiple sets of applicable regulations;

122	SHIELD	Securing against intruders and other threats through a NFV-enabled environment	Nowadays, cybercrime is one of the most relevant and critical threats to both the economy and society in Europe. The SHIELD project proposes a universal solution for dynamically establishing and deploying virtual security infrastructures into ISP and corporate networks. SHIELD builds on the huge momentum of Network Functions Virtualisation (NFV), as currently standardised by ETSI, in order to virtualise security appliances into virtual Network Security Functions (vNSFs), to be instantiated within the network infrastructure using NFV technologies and concepts, effectively monitoring and filtering network traffic in a distributed manner. DATA ANALYSIS AND REMEDIATION ENGINE (DARE) An information-driven IDPS platform capable of predicting specific vulnerabilities and attacks by relying on Big Data, Threat Monitoring and Machine Learning to analyse the output produced by vNSFs. Pattern discovery techniques analyse data to identify current malicious behaviours or predict likely threats. Analysis' results are accessible by systems and security administrators via a dashboard. NETWORK FUNCTIONS VIRTUALISATION (NFV) AND VIRTUAL NETWORK SECURITY FUNCTIONS (VNSFS) NFV enables the virtualisation of network and security appliances. The resulting virtual appliances, named vNSFs, are instantiated within the network infrastructure by a vNSFs orchestrator in order to effectively monitor and filter network traffic in a distributed manner. Advertisement, browsing, selection and trading of vNSFs in a secure manner is provided by a logically centralised repository, named vNSFs store. TRUSTED COMPUTING (TC) The trustworthiness of the secure SHIELD framework is implemented by relying on TC technologies. The infrastructure attestation binds the vNSFs and the network configuration with the store and orchestration of the network. The key components of the secure SHIELD framework will be protected by using the TPM, a TC hardware that assures the integrity of the software and the configuration.

123	SISSDEN	Secure Information Sharing Sensor Delivery event Network	The core of SISSDEN is a worldwide sensor network for situational awareness and sharing of actionable information. This passive threat data collection mechanism will be complemented by behavioural analysis of malware and multiple external data sources. Actionable information produced by SISSDEN will be used for the purposes of no-cost victim notification and remediation via organizations such as National CERTs, ISPs, hosting providers and Law Enforcement Agencies such as EC3. It will especially benefit SMEs and citizens, which do not have the capability to resist threats alone, allowing them to participate in this global effort, and profit from the improved information processing, analysis and exchange of security intelligence, to effectively prevent and counter security breaches.
124	SMESEC	Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework	The main goal of SMESEC is to identify what are the needs from the SME perspective and translate them into requirements for a unified framework, which will eventually consist of the SMESEC partners' contributed products. The products can cover a wide range of security market segments, and it is expected that the unification will bring even higher added value to the products and the Framework. High quality cyber-security solutions attractive to companies and organizations with restricted budget; increase protection by focusing on increasing awareness and training for SMEs and their "insiders"; consolidating international and European links and harmonizing solutions with general standards and directives; ready to market solutions. The suite supports SMEs in managing network information security risks and threats and identifying opportunities for implementing secure, innovative technologies for the digital market. As a benefit, the framework shall allow SMEs not only look at cyber-security as an obstacle but also as an opportunity for business. USE CASES: Smart City, Industrial IoT, Smart Grid, E-voting
126	SODA	Scalable Oblivious Data Analytics	The SODA project will enable practical privacy-preserving analytics of information from multiple data assets using multi-party computation techniques. Secure MultiParty Computation (MPC) for Big Data Analytics. GOAL 1: Develop techniques for analyzing encrypted data GOAL 2: Protect data from leakage of individual data GOAL 3: Demonstrate functionality HEALTHCARE will be our first use case.

127	SPECIAL	Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance	We develop technology that: - supports the acquisition of user consent at collection time and the recording of both data and metadata (consent policies, event data, context) according to legislative and user-specified policies; - caters for privacy-aware, secure workflows that include usage/access control, transparency and compliance verification; - demonstrates robustness in terms of performance, scalability and security, all of which are necessary to support privacy preserving innovation in Big Data environments; and - provides a dashboard with feedback and control features that make privacy in Big Data comprehensible and manageable for data subjects, controllers, and processors. USE CASES: - Proximus is a Belgian telecommunications provider offering telephony (landline and mobile), internet and Internet TV. Their use case foresees the creation of a tourist recommendation tool on the basis of customer interest profiles. The tool is aimed at visitors of the Belgian coast. - Deutsche Telekom is a leading European telecommunications provider and involved in the SPECIAL project with a focus at exploring various possible use cases. One of them is aimed at municipality road layout optimisation and traffic management. Furthermore, a use case includes traffic alert information for customers based on their commuting behaviour and other geolocation data. - The project partner Thomson Reuters Limited (TR) located in the United Kingdom is focused on supporting Know Your Customer requirements in the financial sector. To this end, TR provides end-to-end client identity and verification services that enable financial institutions to fulfil their compliance and due diligence obligations against financial crimes based e.g. on international and national anti-money laundering laws and regulations Special privacy Dashboard: https://www.specialprivacy.eu/platform

128	SpeechXRays	Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face	The SpeechXRays project will develop and test in real-life environments a user recognition platform based on voice acoustics analysis and audio-visual identity verification. SpeechXRays will outperform state-of-the-art solutions in the following areas: · Security: high accuracy solution (cross over accuracy of 1/100 i.e. twice the commercial voice/face solutions) · Privacy: biometric data stored in the device (or in a private cloud under the responsibility of the data subject) · Usability: text-independent speaker identification (no pass phrase), low sensitivity to surrounding noise · Cost-efficiency: use of standard embedded microphone and cameras (smartphones, laptops). The project will combine and pilot two proven techniques: acoustic driven voice recognition (using acoustic rather than statistical only models) and multi-channel biometrics incorporating dynamic face recognition (machine vision analysis of speech, lip movement and face). The vision of the SpeechXRays project is to provide a solution combining the convenience and cost-effectiveness of voice biometrics, achieving better accuracies by combining it with video, and bringing superior anti-spoofing capabilities. The technology will be deployed on 2000 users in 3 pilots: a workforce use case, an eHealth use case and a consumer use case.
129	SPOOC	Automated Security Proofs of Cryptographic Protocols: Privacy, Untrusted Platforms and Applications to E-voting Protocols	The goals of the Spooc project are to develop solid foundations and practical tools to analyse and formally prove security properties that ensure the privacy of users as well as techniques for executing protocols on untrusted platforms. - develop foundations and practical tools for specifying and formally verifying new security properties, in particular privacy properties; - develop techniques for the design and automated analysis of protocols that have to be executed on untrusted platforms; - apply these methods in particular to novel e-voting protocols, which aim at guaranteeing strong security guarantees without need to trust the voter client software.

131	STOP-IT	Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats	STOP-IT provides technological solutions, a risk -based mutlidisciplinary methodology and training material to support strategic/tactical planning, real-time/operational decision making and post-action assessment to protect the key parts of the water infrastructure against cyber and physical threats and their combination. - Real time anomaly detection on cyber-physical infrastructures using machine learning and signature-based detection of abnormal behaviours within the network. - Cross Layer Security Information and Event Management (XL-SIEM). This tool receives events coming from different sources to generate correlated alarms that indicate the risk level, and detailed information about the event (description, IP source and destination, Port source and destination, Protocols). . Network Traffic Sensors and Analysers (NTSA). It incorporates five categories of sensors able to identify different malicious patterns such as TTL-based attacks, brute force attacks, DNS answer attacks, time-based attacks, and domain-based attacks. RESULTS: The STOP-IT platform, Strategic and Tactical Risk Assessment & Treatment Framework, Toolbox for IT & SCADA Security, Physical Threats Toolbox, Cyber Threat Sharing Service, Public Warning Notification System, Reasoning Engine, Other results
132	STORM	The first cybersecurity management system providing evidence based metrics for cyber risk at the business asset level in real-time	InnoSec’s main product, STORM, is the only Cyber Risk Management application that provides evidence based metrics defining cyber risk at the business asset level in real-time, using a flexible risk modeling method, while improving the overall user experience.

133	SUNFISH	SecUre iNFormation SHaring in federated heterogeneous private clouds	The SUNFISH project aims to reduce the management cost of private clouds owned by Public Administrations, and - beyond pure costs savings – to accelerate the transition to 21st century interoperable and scalable public services, boosting enforcement of the European Digital Single Market. Cloud federations allow access to Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) from different public or private clouds over the internet, introducing the concept of Federation as a Service (FaaS) in a hybrid cloud environment. The SUNFISH platform therefore focuses on enabling the sharing of data between potentially untrusted entities while protecting the sensitive data of each entity. SUNFISH Platform Components are: - Identity Management (IDM). - Data Security (DS). - Federated Administration and Monitoring (FAM). - Intelligent Workload Management (IWM). - Data Masking (DM). - Anonymization (ANM). - Federated Runtime Monitoring (FRM). - Federated Security Audit (FSA). - Secure Multi-party Computation (SMC). - Service Ledger (SL).

134	SUPERCLOUD	USER-CENTRIC MANAGEMENT OF SECURITY AND DEPENDABILITY IN CLOUDS OF CLOUDS	SUPERCLOUD proposes new security and dependability infrastructure management paradigms that are : 1) user-centric, for self-service clouds-of-clouds where customers define their own protection requirements and avoid lock-ins; and 2) self-managed, for self-protecting clouds-of-clouds that reduce administration complexity through automation. -Self-Service Security: Implementation of a cloud architecture that gives users the flexibility to define their own protection requirements and instantiate policies accordingly. -Self-Managed Security: Development of an autonomic security management framework that operates seamlessly over compute, storage and network layers, and across provider domains to ensure compliance with security policies. -End-to-End Security: Proposition of trust models and security mechanisms that enable composition of services and trust statements across different administrative provider domains. -Resilience: Implementation of a resource management framework that composes provider-agnostic resources in a robust manner using primitives from diverse cloud providers. The SUPERCLOUD methodology will be validated by testbed integration for real-world use cases in the healthcare domain. The consortium is industry-led with partners actively involved in promotion of open source cloud technologies and contributing to major standardization bodies in cloud security, inter-cloud architectures, security protocols, and SDN.
137	TOREADOR	TrustwOrthy model-awaRE Analytics Data platfORm	TOREADOR takes a model-based BDA-as-a-service (MBDAaaS) approach, providing models of the entire Big Data analysis process and of its artefacts. TOREADOR open, suitable for-standardisation models will support substantial automation and commoditisation of Big Data analytics, while enabling it to be easily tailored to domain-specific customer requirements. Besides models for representing all aspects of BDA, TOREADOR will deliver an architectural framework and a set of components for model-driven set-up and management of Big Data analytics processes
138	TREDISEC	Trust-aware, REliable and Distributed Information SEcurity in the Cloud.	It leverages existing or novel cryptographic protocols and system security mechanisms, which offer strong data confidentiality, integrity and availability guarantees while permitting efficient storage and data processing across multiple tenants. From a practical standpoint, the ambition of this project is to develop systems and techniques that make the cloud a secure and efficient place to store data.

140	TYPES	Towards transparencY and Privacy in the onlinE advertising businesS	It plans to demonstrate solutions that protect individuals' privacy while empowering the users to control how their data is used by service providers for advertising purposes. At the same time, TYPES will make it easier to verify whether users' online rights are respected and if personal data is exchanged for a reasonable value-added to users. Results: - Social Media Data Valuation Tool – Would you like to know the money you are generating for Facebook? - eyeWnder – Real Time Web Advertisement Analyser - TestYourPrivacy - Data Valuation Portal - Survey Tool - User Configuration Panel - Online Advertising Price Comparison Portal - Data Broker - YouTube Video Valuation Tool
141	U2PIA	Universal application 2 conduct Privacy Impact Assessment analysis and reports	A disruptive cloud platform designed to enable the creation of in-depth analysis of the risks which Personal Data are subject to through a Privacy Impact Assessment (PIA).

142	UNICORN	A NOVEL FRAMEWORK FOR MULTI-CLOUD SERVICES DEVELOPMENT, ORCHESTRATION, DEPLOYMENT AND CONTINUOUS MANAGEMENT FOSTERING CLOUD TECHNOLOGIES UPTAKE FROM DIGITAL SMES AND STARTUPS	- Unified DevOps Tool: Offer a single tool for application development, deployment, and management during the whole application lifecycle - Monitoring & Resource Adaptation: Unicorn elasticity library supports apps to elastically (de)allocate resources and provides real-time monitoring and analytics - True Multi-Cloud Deployments: Unicorn supports transparent and automated multi-cloud deployments for services to span across cloud zones and geographical regions - Privacy & Security Adoption: Unicorn security and privacy design libraries prevent data breaches and ensure customer privacy
143	VESSEDIA	VERIFICATION ENGINEERING OF SAFETY AND SECURITY CRITICAL DYNAMIC INDUSTRIAL APPLICATIONS	VESSEDIA proposes to enhance and scale up modern formal methods-based software analysis tools to enable using them on a wider range of applications than embedded safety-critical applications (in the Nuclear, Transportation, Energy supply, Process control and Space areas). Developers will benefit rapidly from the outcome of the project when developing connected applications. At the forefront of connected applications is the Internet of Things (IoT), whose growth is exponential and whose security and safety risks are real (for instance in hacked smart phones or smart home devices). VESSEDIA will take this domain as a target for demonstrating the benefits of using our tools on connected applications. Impacts on quality assurance, security evaluation and certification, from tooling and methodological standpoints. USE CASES: - Contiki OS environment (operating system for the IoT) - CEA's use case, MPL routing - DA's use case: several interacting applications (an experimental Aircraft Maintenance System application prototype, a datalink (DL), a blockchain application, a software gateway and a security proxy)

144	VIRT-EU	Values and ethics in Innovation for Responsible Technology in EUrope	Our goals are to (1) understand how IoT innovators enact ethics as they design future devices and to (2) generate a new framework for Privacy, Ethical and Social Impact Assessment (PESIA), which will proactively position ethical self-assessments in the development process of IoT technologies. The VIRT-EU TOOLKIT offers practical help in developing ethically informed technology: - The Ethical Stack is a series of tools to support creators of new connected technology to reflect on their product's ethical and social impacts. - PESIA is a questionnaire that helps developers and designers assess their privacy, ethical, and social impacts. - Our workshop materials are designed to convene difficult conversations about ethics in technology development
145	VisiOn	Visual Privacy Management in User Centric Open Environments	The VisiOn project developed a visual privacy platform to help public entities deliver safe and privacy-enhanced e-government services that meet the highest privacy standards and nowadays necessities, and offer citizens greater and personalised control over their data. A validated set of business plans and models for the commercial exploitation of the project results (tools, services, platform), along with strategies of reaching potential customers.
146	WISER	Wide-Impact cyber SEcurity Risk framework	WISER delivers a cyber-risk management framework able to assess, monitor and mitigate the risks in real time, in multiple industries. WISER incorporates socio-economic impact aspects, building on current state of the art methodologies and tools, and leveraging best practices from multiple industries and international initiatives (e.g: NIS). WISER aims at implementing an impressive series of 9 short experiments, in the form of Early Assessment Pilots (EAPs) to test the resilience of different risk management frameworks (taken from different industries and intended broadly) with regards to both traditional and advanced cybersecurity threats. The WISER framework will ensure cyber risk management becomes an integral part to good business practice in both critical infrastructure & process owners and ICT-intensive SMEs by offering two delivery modes: a pre-packaged solution for addressing basic cyber risk management needs (i.e. SMEs), and a Risk Platform as a Service (RPaaS) mode of operation of the platform, intended for critical infrastructures or highly complex cyber systems requiring the implementation of special controls within the ICT system to be monitored

147	WITDOM	empoWering prIvacy and securiTy in non-trusteD envirOnMents	Efficient and practical privacy enhancing techniques and efficient signal and data processing in the encrypted domain, and develop a holistic security-by-design framework for quantitative evaluation of end-to-end security and privacy, aiming at guaranteeing efficient and verifiable provision of privacy in the context of ICT services owned by third-party providers of distributed processing and storage, thereby maximizing independence from stated security and privacy commitments by respective providers.
148	FENTEC	Functional Encryption Technologies	Its core objective is to develop new Functional Encryption (FE) as an efficient alternative to the all-or-nothing approach of traditional encryption. Privacy-preserving and auditable Digital Currency: This use-case provides a digital-based currency as a one-to-one counterpart to physical money or issued by debit and credit cards. This would remove the privacy issues but still allowing some opportunities of taxability or auditability by governments or its taxes agencies. Motion Detection and Local Decision Making: In this use case where FENTEC wants to detect motion at the gateway level on an encrypted video stream coming from security cameras. Privacy-Preserving Statistical Analysis: This use case addresses the privacy-preserving computation of data analytics, focusing on the computation of statistics over large usage data.
150	PROMETHEUS	PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms Using latticeS	PROMETHEUS aims to provide post-quantum signature schemes, encryption schemes and privacy-preserving protocols relying on lattice. - Cryptographic foundations. - Basic tools related to lattices - Signature and encryption schemes - Privacy-preserving protocols

151	REACT	REactively Defending against Advanced Cybersecurity Threats	to fight software exploitation, and mitigate such Advanced Cybersecurity Threats in a timely fashion, based on four complementary actions: - Probes actively, and in a transparent and ethical way, the network for identifying unknown vulnerabilities. - Once aware of new vulnerabilities, automatically patches all vulnerable hosts of an organization, using software instrumentation, and secures them temporarily, until the official patch of the vulnerability is published. - Detects exploited hosts and immediately isolates them from the rest of the network to limit malware propagation. - Analyzes security incidents for forecasting future cybersecurity threats. Actions of all four components are projected through a visual interface, which increases situational awareness for the entire life cycle of the product.
152	SerIoT	Secure and Safe Internet of Things	SerIoT aims to provide a useful open & reference framework for real-time monitoring of the traffic exchanged through heterogeneous IoT platforms within the IoT network in order to recognize suspicious patterns, to evaluate them and finally to decide on the detection of a security leak, privacy threat and abnormal event detection, while offering parallel mitigation actions that are seamlessly exploited in the background. SerIoT technology will be installed, deployed and validated in emerging IoT-enabled application areas (i.e. Smart Transportation, Surveillance & Flexible Manufacturing/Industrie 4.0 as core business areas and & Food & Supply chain) through-out its lifetime, enabling the conduction of pioneer R&D for the delivery of horizontal IoT end-to-end security platform in Europe.
153	YAKSHA	Cybersecurity Awareness and Knowledge Systemic High-level Application	Develop and implement a software toolkit to improve Cybersecurity of organizations in the ASEAN region. YAKSHA aims to reinforce European Union (EU) and Association of South East Asian Nations (ASEAN) cooperation and build partnerships in the Cybersecurity domain by developing a solution tailored to specific users and national needs, leveraging EU Know-How and expertise. Develop and introduce the innovative concept of honeypots-as-a-service which will greatly enhance the process of gathering threat intelligence. YAKSHA Label of Excellence https://project-yaksha.eu/outcomes/

155	CYBER-TRUST	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things	The CYBER-TRUST project aims to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, to perform high quality interdisciplinary research in key areas for introducing novel concepts and approaches to tackle the grand challenges towards securing the ecosystem of IoT devices. The high-level project outcomes of the project are components/tools aiming at: (a) protecting the hardware and software configurations of IoT devices; (b) providing an inventory of authorized (and unauthorized) software; (c) effectively managing hardware devices on a network; (d) performing continuous vulnerability assessment and remediation; (e) protecting sensitive data and users' privacy. USE CASES: IoT device owners, Internet Service Providers (ISPs) and Law Enforcement Agencies (LEAs).
158	PRIVILEDGE	Privacy-Enhancing Cryptography in Distributed Ledgers	PRIViLEDGE realises cryptographic protocols supporting privacy, anonymity, and efficient decentralised consensus for DLTs. Results from PRIViLEDGE are demonstrated through four ledger-based solutions: - verifiable online voting; - contract validation and execution for insurance; - university diploma record ledger; - update mechanism for stake-based ledgers.

159	FUTURE TPM	Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module	The FutureTPM project is aimed at designing and developing a Quantum-Resistant (QR) Trusted Platform Module (TPM). FutureTPM will provide a new generation of TPM-based solutions including hardware, software and virtualization environments, by incorporating robust and physically secured Quantum-Resistant cryptographic primitives. This will allow long-term security, privacy and operational assurance for future ICT systems and services. FutureTPM solutions will also improve the security of Hardware Security Modules, Trusted Execution Environments, Smart Cards, and the Internet of Things. The goal is to enable a smooth transition from current TPM environments, based on existing widely used and standardised cryptographic techniques, to systems providing enhanced security through QR cryptographic functions, including secure authentication, encryption and signing functions. By designing an innovative portfolio of high-security QR algorithms for primitives such as Key Agreement, Encryption, Signature, Cryptographic Hashing, Message Authentication Code (MAC) Functions, and Direct Anonymous Attestation (DAA), FutureTPM will fill the gaps that currently threaten its long-term security properties. This will enable FutureTPM systems to generate a secure root of trust that can be used for interacting with Cloud services, accessing corporate services, performing banking and eCommerce transactions, along with a wide range of other services. USE CASES: Online banking, Activity tracking, Device management.
160	SealedGRID	Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID	SealedGRID, proposes a flexible architecture that provides security services at all levels of Smart GRID by implementing Trusted Execution Environments on their devices, together with advanced authentication and authorization mechanisms, as well as privacy preserving techniques.
161	SEMIoTICS	Smart End-to-end Massive IoT Interoperability, Connectivity and Security	SEMIoTICS develops a pattern-driven framework around existing IoT platforms to support secure/dependable actuation and IoT/IIOT semi-autonomic behaviour that support cross-layer and intelligent dynamic adaptation in renewable energy, healthcare, and smart sensing.

162	ASTRID	AddreSsing ThReats for virtualIseD services	ASTRID provides the technical framework for a cybersecurity application to “plug-in” a virtual service without manual operation, and to configure/manage a number of local agents that provide security services. Tackling the specific challenges brought by cloud-based services, the main target is defining a framework to improve the visibility over virtual applications in the cloud and NFV domains, pursuing more flexibility and dynamicity in creating and managing security services. ASTRID’s expected main product consists of a framework that supports current state-of-the-art detection/reaction algorithms and improves their effectiveness by: - giving them visibility over the service topology (virtual machines and virtual links); - feeding them with security-related context in a programmatic way; - automating actions consequent to the detection of threats/attacks. ASTRID will provide integration with tools for software orchestration (e.g., OpenBaton, Maestro, Kubernetes, etc.) and the ability to collect a broad and heterogeneous security context, possibly independently from the current orchestrator in use, which is essential to detect most recent forms of advanced, persistent, stealth, morphing, and zero-day attacks. To support legal and forensics investigation in virtualised environments.
163	BPR4GDPR	Business Process Re-engineering and functional toolkit for GDPR compliance	BPR4GDPR aims to provide solutions for GDPR compliance that cover the full process lifecycle addressing those major challenges and priorities. These address all stages within a process lifecycle, starting from its specification by an administrative user or its discovery based on event logs, its analysis and re-design, implementation, execution and monitoring, resulting eventually in possibly updated process models, adapted to real-time circumstances and other evolutionary factors— as well as preparatory tasks and operations that are horizontal, continuous, or process-independent, or deal with process-asynchronous enforcement of data subjects’ rights. In this way, the BPR4GDPR solutions will include requirements interpretation, broad territorial scope, accountability, security means enforcement, data subject’s rights and consent, unified data view and processing actions inventory, privacy by design, etc. Compliance-as-a-Service (CaaS). By design privacy-aware process models. Compliance-driven process re-engineering. USE CASES: e-Government services in the healthcare and social security sectors, Automotive market, Real estate agencies

164	PAPAYA	PlAtform for PrivAcY preserving data Analytics	The PAPAYA project is aiming to address the privacy concerns when data analytics tasks are performed by untrusted third-party data processors. Since these tasks may be performed obliviously on protected data (i.e. encrypted data), PAPAYA has designed and developed dedicated privacy preserving data analytics primitives that enable data owners to extract valuable information from this protected data, while being cost-effective and accurate. Specific innovations of the project include: - Privacy Engine; - Stress management service; - Arrhythmia detection service; - Mobile usage statistics service; - Mobile patterns analytics service; - Threat detection for sensitive data service; - Privacy-preserving Arrhythmia Classifier; - Compliance tools; - Privacy-preserving analytics platform; - Privacy-preserving data analytics modules; - Privacy-preserving collaborative training of neural networks; - Privacy-preserving training of neural networks.
165	POSEIDON	Protection and control of Secured Information by means of a privacy enhanced Dashboard	PoSeID-on will develop and deliver an innovative intrinsically scalable platform, namely the Privacy Enhancing Dashboard for personal data protection, as an integrated and comprehensive solution aimed to safeguard the rights of data subjects, exploiting the cutting-edge technologies of Smart Contracts and Blockchain, as well as support organizations in data management and processing while ensuring GDPR compliance. Through Artificial Intelligence and Machine Learning algorithms, PoseID-on will monitor privacy risks (Personal Data Analyser module). The PoSeID-on platform will also include a Risk Management module. Privacy Enhanced Dashboard as a Service (PEDaaS).

166	SPEAR	SPEAR: Secure and PrivatE smArt gRid	It aims at developing an integrated platform of methods, processes, and tools for: - timely detecting evolved security attacks using big data analytics, advanced visual-aided anomaly detection tools, and smart node trust management schemes; - developing an advanced forensic readiness framework for collecting attack traces and preparing the necessary legal evidence in court, while preserving user private information; - implementing an anonymous smart grid channel for mitigating the lack of trust in exchanging sensitive information about cyberattack incidents; - performing risk analysis and awareness through cyber hygiene frameworks, while empowering EU-wide consensus, by collaborating with European and global security organizations, standardization bodies, industrial groups and smart grid operators; - exploiting the research outcomes to more critical infrastructure domains, while creating competitive business models for utilizing the implemented security tools in smart grid operators and actors across Europe.
167	SMOOTH	GDPR Compliance Cloud Platform for Micro Enterprises	SMOOTH project assists Micro enterprises to adopt and be compliant with the General Data Protection Regulation (GDPR) by designing and implementing easy-to-use and affordable tools to generate awareness on their GDPR obligations and analysing their level of compliance with the new data protection regulation.

168	DEFEND	Data Governance for Supporting GDPR	It provides an innovative data privacy governance platform which supports healthcare organizations towards GDPR compliance using advanced modelling languages and methodologies for privacy-by-design and data protection management. Specific innovations of the project include: - the development of advanced modelling languages and methodologies for privacy-by-design and data protection management; - Automated methods and techniques to elicit, map and analyse data that organizations hold for individuals; - Integrated encryption and anonymisation solutions for GDPR; - methods and automation techniques for the specification, management and enforcement of personal data consent; - a modular solution that covers different aspects of GDPR. The DEFeND platform provides 5 main services to organisations and relevant stakeholders: Data Scope Management Service, Data Process Management Service, Data Breach Management Service, GDPR Planning Service and GDPR Reporting Service. IMPLEMENTING PRIVACY BY DESIGN/PRIVACY ENGINEERING. CONDUCTING PRIVACY RISK ASSESSMENTS (PIAS/DPIAS USE CASES: banking, energy, healthcare, public administration.
170	OLYMPUS	Oblivious identitY Management for Private and User-friendly Services	OLYMPUS will address the challenges associated to the use of privacy-preserving identity management solutions by establishing an interoperable European identity management framework based on novel cryptographic approaches applied to currently deployed identity management technologies. In particular, OLYMPUS will employ distributed cryptographic techniques to split up the role of the online IDP over multiple authorities, so that no single authority can impersonate or track its users. By not requiring users to store any long-lived credentials, the OLYMPUS framework will not rely on any protected hardware or software environments on user devices and will be able to offer a much better streamlined user experience. Rather, users will obtain short-lived access tokens after authenticating to the system using readily available and platform-independent mechanisms such as passwords or biometrics. USE CASES: Mobile Driving Licence and Credit File

171	THREAT-ARREST	THREAT-ARRESTCyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training	THREAT-ARREST aims to develop an advanced training platform incorporating emulation, simulation, serious gaming and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model driven approach where cyber threat and training preparation (CTTP) models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training. The platform will also support trainee performance evaluation and training programme evaluation and adapt training programmes based on them. The effectiveness of the framework will be validated using a prototype implementation interconnected with real cyber systems pilots in the areas of smart energy, healthcare and shipping, and from technical, legal and business perspectives. Use cases: Smart Energy, Shipping, Healthcare
172	CONCORDIA	Cyber security cOmpeteNce fOr Research anD Innovation	A project that pilots Cybersecurity Competence Network with leading research, technology, industrial and public competences. CONCORDIA provides excellence and leadership in technology, processes and services to establish an user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe. It enhances threat intelligence platform for financial sector and provides mechanisms for the access and use control of the data exchanged between different entities. The CONCORDIA H2020 project releases the KYPO Cyber Range Platform (KYPO CRP) as open source

174	SPARTA	Strategic programs for advanced research and technology in Europe	SPARTA will create a long-lasting community capable of collaboration to define, develop, share, and evolve solutions that will help practitioners prevent cybercrime and enhance cybersecurity. SPARTA establishes a strategic research and innovation roadmap to stimulate the development and deployment of key technologies in cybersecurity and to retain digital sovereignty and autonomy of the European industries. SPARTA PROGRAMS: - T-SHARK: Full-spectrum cybersecurity awareness - CAPE: Continuous assessment in polymorphous environments - HAAI-T: High-assurance intelligent infrastructure toolkit - SAFAIR: Secure and reliable AI systems for citizen Other services: Education Map, Curricula designer
175	CyberSec4Europe	Cyber Security Network of Competence Centres for Europe	The project demonstration cases will address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation. In addition to the demonstration of the governance structure and the operation of the network, CyberSec4Europe will develop a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project.

176	ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations	- ECHO Security Certification Scheme: Development of sector specific security certification needs within EU Cybersecurity Certification Framework from ENISA. - ECHO Early Warning System: Most large organizations have set up a Computer Security Incident Response Team (CSIRT), Managed Security Services (MSS), Computer emergency response team (CERT) with an expert group that handles computer security incidents. Existing vulnerability and threat data feed (e.g. CVE, STIX), as well as cyber information sharing platforms (e.g. MISP), are already part of the expert team toolkits today. Knowledge sharing of known threats and vulnerabilities need to be combined with information on emerging threats to bolster the cyber defence posture. An early warning system will combine these information verticals to give the operators a view of the current attack surface, as well as the emerging ones. It will encourage pooling of resources across the organizational boundary to effectively combat cyber threats of today as well as the future. - ECHO Federated Cyber Range: The role of the ECHO Federated Cyber Range (E-FCR) is to interconnect existing cyber-range capabilities through a convenient portal operating as a broker between user requirements and a pool of available cyber range capabilities. A cyber-range has the potential to help strengthen the stability, security and performance of cyberinfrastructures and information technology (IT), operations technology (OT), and industrial control systems (ICS) by facilitating high-fidelity simulations of operational conditions in a virtual environment. - ECHO Multisector Assessment Framework: The overall goal of the activity is to foster the development and adoption of a Multi-Sector Assessment Framework, aiming to provide a structured method for multi-dimensional analysis and development of management processes for cybersecurity risks, leverage to guide actions and provide confidence on program and actions taken, help benchmark initiatives, provide an effective cybersecurity educational portfolio and training programmes, provide a shared definition of the transversal and cross-sectoral skills and qualifications needed by cyber-security actors. - ECHO Cyber Skills Framework: Contributes to European strategic autonomy and help build and strengthen cybersecurity capacities across the EU through delivery of a common reference model for cyberskills, along with a collection of cyber curricula involving training that spans both strategic and policy aspects as well as technology-oriented aspects. - ECHO Governance Model: A governance structure that is implemented, tested and validated

			through a collection of demonstration cases involving all partners in the network to showcase (in a measurable manner) its performance.
177	ENACT	Trustworthy and Smart Actuation in IoT systems	ENACT enables continuous delivery of IoT smart-systems, implementing toolkits for IoT systems into agile operations to facilitate trustworthiness and robustness that can be easily integrated into existing IoT services. The ENACT DevOps Framework: a set of loosely coupled enablers that can be easily integrated with existing IoT platforms. The ENACT enablers are categorized in three groups as follows: (i) the toolkit for the continuous delivery of smart IoT systems, (ii) the toolkit for the agile operation of smart IoT systems, and (iii) the ENACT facilities for trustworthiness. The set of enablers can be seamlessly combined and they can easily integrate with existing IoT platform services and enablers.
178	PDP4E	Methods and tools for GDPR compliance through Privacy and Data Protection Engineering	It provides software and system engineers with methods and software tools to systematically apply data protection principles in the projects they carry out, so that the products they create comply with the General Data Protection Regulation (GDPR), thus bringing the principles of Privacy and Data Protection by Design to practice. PDP4E will be assessed by two demonstration pilots on industries where privacy and data protection are especially relevant, one on novel financial applications and services (fintech application domain) and one on big data on smart grid (smart grid application domain). Paper “The Impact of Artificial Intelligence on Security: a Dual Perspective”: This paper analyses the impact of Artificial Intelligence (AI) on security processes. Through the analysis of risk maps (a risk analysis tool), we highlight two opposing views: Beneficial AI and Malicious AI.

179	CYBERWISER	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training	CYBERWISER.eu is an educational, collaborative, real-time civil cyber range platform where cybersecurity competitions will take place. They Currently Offer 4 Courses. They offer a SMEs cybersecurity best practices assessment. - Multilanguage Guide on NIS Directive - https://cyberwiser.eu/insights/nis-guides - Multilingual CS Glossary for beginners - https://cyberwiser.eu/insights/cyber-security-guide-novices - Free Risk Assessment Tool - https://cyberwiser.eu/cyberwiser-light - Free Socio Economic Impact Tool - https://cyberwiser.eu/cyberwiser-socio-economic-impact-tool - Paid Real Time Cyber Risk Monitoring services - https://cyberwiser.eu/cyberwiser-essential - https://cyberwiser.eu/cyberwiser-plus
180	PROTASIS	Restoring Trust in the cyber space: a Systems Security Proposal	PROTASIS aims to expand the reach of SysSec to the international community via a joint research program in the area of Systems Security spearheaded by the need to develop a computing infrastructure that will be trusted by the citizens and the organizations they use it. Through a novel international and intersectoral program the participants will advance the state-of-the art in the area of security and privacy and will sharpen their skills using the most advanced methods for cyberattacks and malware.

185	PANACEA	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people	The PANACEA project provides all healthcare actors with an assessment and system monitoring audit workflow to easily run conformity assessment and engineering assessment. The PANACEA project has developed, with three European Healthcare Centres, a people-centric toolkit of nine tools, to assess and improve the cybersecurity readiness of healthcare socio-technical systems (ICT, networked medical devices, staff) and of medical device/system lifecycles. It includes software-based innovative tools: - dynamic risk assessment, based on a multi-layer attack graph model including "human" and "business" layers, and automatic generation of mitigation recommendations, - inter-organizational secure information and heavy images sharing, - regulatory compliant security-by-design and certification of systems/medical devices, - machine-to-machine and smartphone-based facial identification (also with masks). It also includes non-technical tools, influencing staff behaviour and supporting the management through: - contextualized risk governance models, - educational voiceless videos, - methodology to produce behavioural "nudges", - methodology to maximize cybersecurity return-on-investment, - guidance for contextualized deployment of previous tools. Potential integrated use of the nine tools' is a further innovative feature, supporting full plan-do-check-act and multi-disciplinary approaches to cybersecurity preparedness.

186	symbIoTe	Symbiosis of smart objects across IoT environments	The main goal of symbIoTe (symbiosis of smart objects across IoT environments) is to foster a simplified IoT application and service development process over interworking IoT platforms. This will be accomplished by 1) providing the means to create and manage virtual IoT environments across various IoT platforms, 2) implementing high-level APIs –enablers– leveraging such virtual environments to offer specialized services (e.g., localization in indoor spaces or unified access to environmental data gathered from various sources), tailored to the needs of symbIoTe-specific use cases, 3) offering the means for creating dynamic and self-configurable smart spaces, and 4) implementing a secure interworking protocol between the platforms in accordance with recommendations from standardization bodies. This will support SMEs and new entrants in the IoT domain to build innovative IoT services within short development life cycles. Business cases: Smart Residence, EduCampus, Smart Stadium, Smart Mobility, Smart Yachting
188	SecureIoT	Predictive Security for IoT Platforms and Networks of Smart Objects	Security Risk Assessment and Mitigation as a Service for IoT applications and devices: Focused specifically on IoT architectures, applications, sensors, assets and modalities, this framework of cybersecurity threat analysis, assessment, evaluation and viable mitigation proposals, is innovatively offered remotely as a service and computes vulnerability likelihood factors. SecureIoT will provide implementations of security data collection, security monitoring and predictive security mechanisms to offer integrated services for risk assessment, compliance auditing against regulations and directives (e.g. GDPR, NIS, ePrivacy), as well as to support the IoT developers. Foretelling and anticipation of security behaviour of IoT entities, is the main concept emphasised by SecureIoT. The provided services span security compliance auditing, automated risk assessment and mitigation, as well as support for IoT security-aware programming. Sceneraios: industry 4.0, social assisted robots, connected cars. SecureIoT's turn-key solutions will be offered in the form of three integrated SECaaS services: - Risk Assessment services - Compliance services (incl. GDPR) - Developers support services

191	PANOPTESEC	Dynamic Risk Approaches for Automated Cyber Defence	A prototype of a cyber defence decision support system, demonstrating a risk based approach to automated cyber defence that accounts for the dynamic nature of information and communications technologies (ICT) and the constantly evolving capabilities of cyber attackers.
192	SERENITI	Cyber Security and Resilience of Networked Critical Infrastructures	The project aims at elaborating novel methodologies for the design of security and resilience-aware ICT infrastructures for Networked Critical Infrastructures, e.g., water plants, oil and gas pipelines, power grid, and the emerging Smart Grid. It addresses several research gaps by providing: - A new approach for designing more secure and resilient NCI. In particular the project will develop unique techniques to aid engineers in designing their networks according to a wide set of requirements. - A novel Distributed IDS (DIDS) that glues together existing cyber and physical IDS. - A novel approach for DIDS placement in NCI that takes into account security and resilience design requirements.
193	SecureCloud	Secure Big Data Processing in Untrusted Clouds	SecureCloud is an ecosystem of cloud facilities characterized by superior security guarantees, providing protection from attacks by privileged users (e.g. the cloud provider or the system administrator) and software (e.g. the hypervisor). Protection relies on new security extensions recently introduced into commercially available off-the-shelf CPUs. The current implementation is based on Intel SGX, but support for additional platforms might become available in the future. SecureCloud is customizable, since it enables developers to build a cloud-based computing environment based on SGX-enabled containers that matches their personal preferences. SecureCloud is modular, because it allows developers to pick and use only the features that they need/want. SecureCloud is flexible, since it can satisfy a wide range of customers-specific requirements including big data processing, secure intra-cloud communication, precise microservice scheduling and reliable data storage. SecureCloud is interoperable, in that its facilities can be seamlessly integrated with best of breed offerings from the Open Source community
194	ASCEMA	ASCEMA: Content Aware Technology for IP Protection in Supply Chains	A feasibility study of bringing to market a novel solution for protecting intellectual property across enterprise boundaries and will support a go to market plan for Ascema for Supply Chains, a patented technology that protects high value content across enterprise boundaries, including a full business plan, to verify the technological, practical and economic viability of GeoLang's novel Ascema for Supply Chains data loss prevention platform.

195	LipVerify	Feasibility study on the development of LipVerify - a new viseme based user authentication service.	Feasibility of commercialising a new service which provides secure access to sensitive data, applications and physical areas via a unique biometric authentication technique - based on analysis of the users lip movements. Health: Patients with tracheostomies, laryngectomies and/or prolonged intubation have great difficulty speaking. SRAVI helps these patients convey important information quickly. SRAVI can also be used at home and to help with a range of speech debilitating conditions. Keyword spotting in silent video, e.g. CCTV
196	ConnectProtect	A total cyber protection service to Small Businesses operating critical infrastructure and Residential customers	This project focuses on cyber-security and aims to address any form of internal or external malware and cyber-attacks, a total cyber protection service for SMEs and residential customers.
197	ThreatMark	Advanced Fraud Detection System - Protecting digital transactions against cyber attacks	ThreatMark vision is to secure the assets of people/companies by better protection of digital transaction systems against cyber-attacks. Advanced machine learning and unique algorithms of ThreatMark make the detection of advanced threats and behavioural anomalies more sensitive and reliable while lowering the cost of operation. We challenge the conventional methods of transaction protection by bringing usually fragmented features under one roof: (online) fraud detection systems, web fraud detection, web application firewall, malware detection, criminal and account takeover detection.
198	Eye-O-T	Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes.	The Eye-O-T enables the operators to monitor and analyse in real time a large number of IoT networks, distributed over many remote sites and running different local communication protocols. The system is composed by plug & play probes that capture Smart Home IoT edge and gateway traffics and send it to the cloud through the existing broadband infrastructure; and an intuitive real-time dashboard. The Eye-O-T security system not only enables Smart Home owners to minimise their house and privacy vulnerability to security breaches and malicious attacks, but also reduces the Smart Home maintenance cost for operators
199	PerfectDashboard 2.0	First single platform for efficient and security aware management of CMS based websites	A tool for web administrators to prevent potential attacks on majority of web pages managed with CMS such as Joomla and WordPress. With our application already proven by individual web admins one may not only introduce necessary changes in the code mitigating the risk of a security breach much faster than ever before, but can ensure the final effect does not impact on the web page layout and its contents.

200	CHINO	The Health Data Security Platform for EU Developers Enterprises	Data Security Platform as a Service (PaaS) that helps digital health developers to ensure compliance with EU GDPR and US HIPAA data protection laws.
201	CyberSure	CYBER Security InSURancE — A Framework for Liability Based Trust	It is a programme of collaborations and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance policy for cyber systems. The purpose of creating such policies will be to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches in them. The framework will be supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems. The development of the CyberSure platform will be driven by certification, risk analysis and cyber insurance scenarios for cyber system pilots providing cloud and e-health services.
203	LocationWise	LocationWise Payment Card Validation: A cloud based location verification system that willsignificantly lower cost of payment card cyber security	We have designed and developed a mobile location solution to technology readiness level 6 and defined applications for banks, financial institutions and payment service providers. We have shown the commercial viability of our services to validate and authenticate customer transactions, which will allow financial institution clients to enhance their digital financial services offerings. Planning a pilot test with a bank, big e-commerce, enterprise, telecommunication company and public administration
206	UNFRAUD	An advanced online anti-fraud software equipped with deep learning Artificial Intelligence thatcan face and detect, current fraudulent techniques and their continued evolution in a cost effective man	A cybersecurity software that prevents potential online fraud scenarios through deep learning algorithms that are the cutting-edge techniques of artificial intelligence

207	CLTRe	The Cybersecurity Behavioural Toolkit	CLTRe Toolkit is assessing the actual ideas, habits and behaviours of the employees in order to measure and improve the security culture of an organisation. The solution stores behavioural assessments over time to provide the organization with trend analysis in order to understand behavioural change over time. The phase 1 project will validate the technical and commercial feasibility of a cybersecurity behavioural toolkit offered as Software as a Service.
209	GO 4G	InvizBox Go 4G - Security and Privacy, Everywhere	InvizBox Go 4G provides an innovative approach to securing data on the internet and protecting user privacy with ease. InvizBox Go 4G addresses a major market opportunity by bringing to market a solution for cyber-security that currently is only available to companies and consumers by installing and configuring software on each and every device that they wish to protect. The Go 4G project will look to conduct a full technical and economic feasibility study of InvizBox Go 4G and develop a business strategy that ensures that the product's commercial potential is maximized.
211	TFence	A patent pending solution/microchip for the IoT cybersecurity market requirements: no access toonline software updates, very small size, inexpensive hardware, low energy consumption.	High-tech and critical systems, such as medical devices, implants and IoT devices are vulnerable. Penetration of medical devices would have a devastating impact, including substantial economic damage, injury and loss of life. Similarly, Penetration of IoT in the industry would cause large economic damage. Current solutions are clunky, expensive and do not fit the large variety of small medical devices, wearables and IoT appliances. Terafence is developing a state-of-the-art hardware silicon solution/FPGA/Chip based device, TFence, for cyber-secured connectivity (patent pending) based on unidirectional net flow from and to IoT devices and networks of IoT devices.
212	UltraFiBi	Next-generation Strong Ultrasonic Fingerprint Biometrics	UltraFiBi was to conceive a comprehensive business plan for MODULEUS' entry to markets initially in Europe, through two main activities: mapping of the market and technology assessment, based on the strong expertise by MODULEUS in the overall value chain of advanced ultrasound systems development, i.e. application, platforms, software, electronic boards, and components. MODULEUS focuses on advanced ultrasound fingerprint sensors for reliable and secure authentication, as current fingerprint recognition systems do not detect the liveness (hence even a play-doh hack works), but ultrasound does.

213	ProtonSuite	The world's largest secure collaboration suite	cloud-based cybersecure collaboration platform that provides users with end-to-end secure communication channels and collaboration tools.
216	ASCLEPIOS	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare	The vision of ASCLEPIOS is to maximize and fortify the trust of users on cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. ASCLEPIOS is using several modern cryptographic approaches to build a cloud-based eHealth framework that protects users' privacy and prevents both internal and external attacks. ASCLEPIOS offers the ability to users to verify the integrity of their medical devices before receiving them while receiving simultaneously certain guarantees about the trustworthiness of their cloud service provider. Furthermore, ASCLEPIOS offers a novel solution through which healthcare practitioners and medical researchers are able to calculate statistics on medical data in a privacy-preserving way.
217	CUREX	seCUre and pRivate hEalth data eXchange	The vision of CUREX is to safeguard patient privacy and increase their trust in the currently vulnerable critical healthcare information infrastructures, especially in cases where data is exchanged among healthcare stakeholders within any business, operational and systemic cross-border environment. By leveraging novel methods on ontological health data modelling, vulnerability discovery, threat intelligence, cybersecurity, and privacy risk assessment methodologies, and state-of-the art in blockchain technologies for health data, CUREX aims at enabling secure and authorized sensitive health data exchange. CUREX will achieve its objectives by empowering healthcare institutions to efficiently, accurately and effectively assess and address their cybersecurity and privacy risks associated with health data exchange and enhance their cybersecurity and privacy awareness among the organization personnel. By capitalizing on technologies developed for the well-known H2020 project MyHealthMyData (MHMD), CUREX will offer a secure-by-design business network based on the MHMD blockchain technologies and software that will provide accountability and auditability functionalities that will increase trust among hospitals and care centres. CUREX will provide GDPR compliant tools and applications targeted towards healthcare professionals and individuals, offering a secure and private-by-design environment to access and exchange data. To conduct techno-economic, market and legal analysis and propose business and application models.

218	V-SPHERE	Vulnerability Search and Prevention through Holistic End-to-end Risk Evaluation	The EU-funded V-SPHERE project developed a software tool that enables the design of genuinely secure computer systems. The tool, named PROSA, supports the crucial initial phases of system specification and design. PROSA does so by enabling security-by-design. In practice this means helping programmers and architects create system models, simplifying documentation of system design and implementation and, at the same time, performing a comprehensive and trustworthy threat analysis.
219	AF-Cyber	Logic-based Attribution and Forensics in Cyber Security	The AF-Cyber project, hosted by Imperial College London, UK, has sought to strengthen our defences against cyberattacks with the development of a logic-based analytical tool. This project's goal was to help analysts in their assessments and attributions of cyberattacks. Karafili studied how past attacks were assessed and attributed. Attribution is the process of identifying where the attack came from, and who the perpetrator of the attack was. A thorough analysis was performed, with all evidence categorised. Karafili next set about developing a tool to emulate the reasoning and investigation process typically followed by security analysts. Karafili therefore focused most of her work on providing analytical support, through the suggestion of probable investigation paths to follow, possible crucial missing evidence and possible explanations for the given results.
220	SIGAGuard	Cybersecurity anomaly detection solution for critical infrastructures	SIGA OT Solutions provides Operational Technology monitoring and anomaly detection for ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition) in industrial and critical infrastructure applications. SIGA's SigaPlatform is a comprehensive process anomaly detection system that monitors critical assets using electrical signal-based predictive analysis and artificial intelligence. It cannot be hacked or manipulated from the operational network and it can be used for operational needs as well as for cybersecurity. SIGA is designated for organizations that rely on their OT hardware to maintain operations: Water treatment, oil & gas, industrial production plants and building management systems.
221	TrueProactive	ROMAD TrueProactive - a next generation cyber defence software for European SMEs	TrueProactive project aimed to transform the approach to identifying cyberthreats with a groundbreaking next-generation endpoint defence platform. The platform proactively detects and blocks new strains.

222	RESISTO	RESIlience enhancement and risk control platform for communication infraSTructure Operators	RESISTO is an innovative solution for Communication Infrastructure providing holistic (cyber/physical) situation awareness and enhanced resilience. RESISTO will help Communications Infrastructures Operators to take the best countermeasures and reactive actions exploiting the combined use of risk and resilience preparatory analyses, detection and reaction technologies, applications and processes in the physical and cyber domains. SOME USE CASES: - MARITIME SAFETY AND EMERGENCY CASE. - Healthcare scenario - 5G NETWORK RESPONSE TO A SECURITY BREACH. - Protection of Cloud Storage Services: Smart Manufacturing
223	SECREDAS	Cyber Security for Cross Domain Reliable Dependable Automated Systems	SECREDAS stands for “Product Security for Cross Domain Reliable Dependable Automated Systems”. It looks at security, safety and privacy across multiple application domains: Road, Rail and Health. The project consortium will build a reference architecture for Secure and Safe Automated systems compliant with the new GDPR Regulation. It will develop a framework for multi-concerned security-safety verification and testing. Increased safety and privacy of IoT devices integrated in vehicles. A prototype of a radar/5G component capable of operating in the 76-81 GHz frequency band. Develop guidelines for continuous multi-concern (safety and security) certification including assessment methods.
224	ELIoT Pro	KEEPING YOUR CONNECTED SMART DEVICES PROTECTED AGAINST HACKERS AND CYBER ATTACKS	The EU-funded ELIoT Pro project developed a reliable solution, by replacing a key IoT weakness of fixed passwords with a one-time password used in the IoT system administrator authentication protocol also in device-to-device authentication and encryption. These protocols are also designed to be very computationally lightweight, suitable for even simple IoT devices.
225	CYBERSECURITY	Cyber Security Behaviours	Our main scientific achievement was the development of a theoretical model that can explain cybersecurity behaviour. Using different research methods – interviews, survey questionnaire and modelling – we examined the individuals’ ability to neutralise threats as well as computer self-efficacy. The latter pertains to individuals’ judgment of their capabilities to use computers in various situations to perform a task successfully,

226	Blocknetwork	Blocknetwork - Fusing Big Data and Implementing Novel Cyber Security Solutions	Blocknetwork is DataUniTor's unique implementation of blockchain schemes. The number of applications related to "secure information from Big Data" is almost endless, but includes healthcare, public sector, retail, manufacturing and modern cities. A self-organized cryptographic Blocknetwork with an evolutionary extension model is the future and the next logical step for blockchain to track complex transactions – gaining flexibility and scalability. The DataUniTor's Blocknetwork scheme retrieves information from the data collected by various data sources and fuses the information into a knowledgebase while also offering additional security features - handling larger volumes, taking fewer instructions and providing a simpler and faster response.
227	SAFECARE	SAFEguard of Critical heAlth infrastructure	The aim of SAFECARE is to provide solutions for the health services that will improve physical and cyber security in a seamless and cost-effective way. Thereby, it promotes new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. SAFECARE is conducting research in four areas: - Healthcare infrastructure threat assessment and solution requirements - Physical security solutions for Healthcare infrastructure - Cybersecurity solutions for Healthcare infrastructure - Integrated Cyber-Physical security solutions for Healthcare infrastructure
228	ADVERSARY	Digital platform for hands-on cybersecurity training	Our platform provides tools for hands-on cybersecurity training through a gamified experience." In this platform, the user can take on the role of the hacker in real-world scenarios. This helps to reduce security risks as developers are kept up to date with the latest threats and attacks.
229	SPHINX	A Universal Cyber Security Toolkit for Health-Care Industry	SPHINX aims to introduce a health tailored Universal Cyber Security Vulnerability Assessment and Certification Toolkit, thus enhancing the cyber protection of the Health and Care IT Ecosystem and ensuring patients' data privacy and integrity. A Holistic Cyber Security vulnerability assessment toolkit, that will be able to proactively assess and mitigate cyber-security threats known or unknown, imposed by devices and services within a corporate ecosystem.

230	SERUMS	Securing Medical Data in Smart Patient-Centric Healthcare Systems	The goal of the SERUMS project is to put patients at the centre of future health-care provision, enhancing their personal care, and maximizing the quality of treatment that they can receive, while ensuring trust in the security and privacy of their confidential medical data. - To develop new techniques that will ensure the security and protection of personal medical data sharing. - To integrate personal medical data from multiple sources into a single coherent smart patient record, including smart devices. - To develop new data analytic techniques. - To develop/enhance authentication and trust mechanisms. - Legal compliance (including GDP) Technologies: - Blockchain and Metadata Extraction for Smart Patient Health Records. - Distributed Differential Privacy Deep Learning Models. - Data Masking, Data Fabrication and Semantic-Preserving Encryption.
231	SECONDO	a Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyonD 2020 netwOrking era	SECONDO will support professionals who seek cyber security investments, developed to support human decision making, and a complete well-founded security strategy. This is a timely research problem, as the rapid growth of cyber-attacks is expected to continue its upwards trajectory. Such growth presents a prominent threat to normal business operations and the EU society itself. On the other hand, an interesting, well-known, finding is that an organisation's computer systems may be less secure than a competitor's, despite having spent more money in securing them. Budget setting, cyber security investment choices and cyber insurance, in the face of uncertainties, are highly challenging tasks with massive business implications. Cyber Security Investments and Blockchain. Cyber Insurance and Smart Contracts. SECONDO aims to make impact on the operation of EU businesses who often: (i) have a limited cyber security budget; (ii) ignore the importance of cyber insurance.

232	TRINITY	Digital Technologies, Advanced Robotics and increased Cyber-security for Agile Production in Future European Manufacturing Ecosystems	The main objective of TRINITY is to create a network of multidisciplinary and synergistic local digital innovation hubs (DIHs) composed of research centers, companies, and university groups that cover a wide range of topics that can contribute to agile production: advanced robotics as the driving force and digital tools, data privacy and cyber security technologies to support the introduction of advanced robotic systems in the production processes.
233	RADDICS	Reliable Data-Driven Decision Making in Cyber-Physical Systems	The RADDICS project seeks to design novel RL (Reinforcement Learning) algorithms that are provably reliable, even when deployed on high-stakes applications. Our approach hinges upon marrying nonparametric statistical learning with robust optimization. In particular, we use Bayesian approaches to quantify uncertainty in the prediction, in a way that yields valid high-probability (Frequentist) confidence estimates about the unknown dynamics and rewards, even under some possibly adversarial circumstances. We then act safely under all plausible models, by employing tools from robust optimization and control theory. Additional observations contract the posterior, allowing to learn and improve policies over time in a safe manner. Beyond developing new algorithms and theory, we seek to demonstrate our approach on several real-world applications, ranging from robotics over energy systems to scientific applications.
234	FeatureCloud	Privacy preserving federated machine learning and blockchaining for reduced cyber risks in a world of distributed healthcare	FeatureCloud is an EU-funded consortium project that is creating a novel artificial intelligence (AI) platform, the FeatureCloud AI Store, based on the ground-breaking idea to use a federated infrastructure for integrating local AI globally without transferring any primary medical data or personal information. FeatureCloud is privacy-enhancing by default. For a world of unrestricted research. For accelerated development of cures and treatments. For maximal security and privacy. - To develop a highly innovative integrated software platform and app store implementing a privacy-aware federated approach - To provide proof of principle for federated machine learning fostering client-side computing as an effective cybersecurity measure - To offer a blockchain-based data access control system - To provide secure feature sharing, rather than raw data sharing, between healthcare organizations

236	D-FENCE	D-FENCE: Deceptive Monitored Environments for Cybersecurity in Enterprises	The new digitisation era envisages a world where all electronic devices are part of a single network known as the Internet of Things (IoT). D-FENCE is an advanced cybersecurity solution that applies Cyber Deception to ‘cheat the hackers’. D-FENCE creates lures (credentials, HTML tags, cookies…) and distributes them across the real production systems. These lures point to our decoys, i.e. false endpoints (PCs, servers…) that mimic real assets. When attackers try to access the decoys, an alarm is immediately triggered, so it is possibly to rapidly detect, monitor, analyse and counteract any attack. Meanwhile, the real assets are safe from the attacker, who is tangled in our deceptive virtual environment.
237	nIoVe	A Novel Adaptive Cybersecurity Framework for the Internet-of-Vehicles	nIoVe aims to deploy a novel multi-layered interoperable cybersecurity solution for the Internet-of-Vehicles (IoV), with emphasis of the Connected and Autonomous Vehicles (CAVs) ecosystem by employing an advanced cybersecurity system enabling all relevant stakeholders and incident response teams to share cyber threat intelligence, synchronize and coordinate their cybersecurity strategies, response and recovery activities. To do so the project develops a set of in-vehicle and V2X data collectors that will feed nIoVe’s machine learning platform and tools for threat analysis and situational awareness across the IoV ecosystem. Advanced visual and data analytics are further enhanced and adapted to boost cyber-threat detection performance under complex attack scenarios, while IoV stakeholders are jointly engaged in incident response activities through trusted mechanisms. The proposed approach is supported by interoperable data exchange between existing and newly proposed cybersecurity tools. nIoVe solution will be demonstrated and validated in 3 pilots: Hybrid execution environment, simulated environment and real-world conditions.

238	GUARD	A cybersecurity framework to GUArantee Reliability and trust for Digital service chains	A complete framework that demonstrate the feasibility of managing service integrity and data sovereignty for complex chains of digital services. The framework is composed of the following main components: 1) A set of programmable monitoring, inspection and detection agents that fulfil most of common needs of SIEM tools. A local agent should expose security properties and capabilities in each digital service, as well as integrate with internal AAA tools for giving access to external security providers. 2) A flexible platform that discovers, connects to, and collects data from security agents deployed in related digital services. The platform will include several algorithms for detection and data tracking. In addition, demonstration of the platform in two realistic Use Cases is also planned, including a smart mobility application and an eHealth service. Cyber-physical systems including IoT devices and deployments in the cloud are the primary environments for Use Case demonstration.

239	InfraStress	Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system	The integrated InfraStress framework consists of a number of different components and services developed by the InfraStress H2020 project and enabling Sensitive Industrial Plants and Sites (SIPS) to improve their resilience and security, in particular adopting a holistic approach towards cyber-physical threats. It integrates solutions for cyber and physical threat detection and data acquisition, providing services for physical and logical security data sources and sensor/detection systems; integrated cyber/physical situational awareness, as the core of the framework enabling to correlate information and extract operational and user-oriented/user-dependent knowledge to build and maintain situational pictures and insights on SIPS protection and resilience; CIP Services including applications which implement protection features and deliver them to users: it supports a variety of Human Computer Interfaces (HCI), as well as more effective and innovative interaction with end users (e.g. through AR). Situational picture for integrated cyber-physical protection of industrial sensitive sites and plants. Cyber and physical threat intelligence and prediction. CIP Monitoring and early warning services. Response, mitigation and recovery decision support services. Information sharing and distribution to relevant stakeholder USE CASES: - Motoroil - Sensitive fiber production plant - Petrol storage - Coastal chemical storage terminal - Medical device manufacturing & supply
240	ODIX 2.0	A revolutionary cybersecurity SaaS helping small-medium business (SMEs) to protect their networks like large corporates do!	odix`s file sanitization regime leverages our proprietary True Content Disarm and Reconstruction (True CDR™) technology. We call the process “odixing”, which purges electronic media of malware by processing all incoming files using set policies. Files from a wide range of file types are tested to confirm that they match the respective file type standards. Then, the odix CDR Engine disarms and neutralizes subspecies code and then rebuilds files into clean versions that are sent to end users for immediate use. Unlike traditional anti malware technologies, odixing is effective against both known and unrecognized malware. odix solutions are ideal for organizations that rely on ongoing incoming and outgoing file-based data exchange for productivity. Such exchanges provide numerous opportunities for hacking and insertion of malicious software including viruses, trojans, and worms.

241	C4IIoT	Cyber security 4.0: protecting the Industrial Internet Of Things	C4IIOT will design, build and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems. C4IIOT bridges cyber assurance and protection, machine (deep) learning (ML/DL), edge/cloud computing, blockchain and Big Data technologies to provide a viable scheme for enabling security and accountability, preserving privacy, enabling reliability and assuring trustworthiness within evolving IIoT applications and processes (e.g. automotive). C4IIOT novel cybersecurity mechanisms are carefully orchestrated across all infrastructure elements involved within an IIoT system (e.g., IIoT devices, field gateways, cloud resources) and is based upon analysis of various data flows (e.g., IIoT device data, encrypted network flows).
242	CYBERCULT	Strategic Cultures of Cyber Warfare	It studies the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel and the United States. It will also review the cultural, socio-political, historical and ideational factors involved. Focusing on these countries as well as Estonia, Germany, Japan, New Zealand and the United Kingdom, it will explore the perceptions of OCC.
243	SOTER	cyberSecurity Optimization and Training for Enhanced Resilience in finance	It takes a holistic research approach, combining technological development with human factor-based cybersecurity training. A biometric based identification and authentication digital on-boarding platform will be developed in conjunction with a suite of training materials, designed to enhance information security, data privacy, and cybersecurity practice within the critical financial services sector. Proposed blockchain implementation of the SOTER platform.
244	SPIDER	a cyberSecurity Platform for vIrtualiseD 5G cybEr Range services	The SPIDER solution will be offered as an innovative cutting-edge Cyber Range as a Service (CRaaS) platform for training cyber security professionals in responding appropriately on modern cyber security incidents. This platform will take into account all relevant advancements and latest trends and will capitalize on current state of the art offering a synthetic and sophisticated war-gaming environment that will provide to the training users the ability of playing the part either of the attacker either of the defender. Furthermore, SPIDER's vision is to address the needs of both experts and non-experts' trainees. This virtual cyber environment will be used for enhancing users' skills, through gamification and generation of various cybersecurity simulation scenarios that will offer to the trainees the chance to participate in various types of cyber tests (both pre-built and customised).

245	EnergyShield	Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures	The VA module has a threat model (attack vectors and probabilities) and the software proposed integrates vulnerability assessment tool based on Foreseeti's SecuriCAD. The SBA module is Software as a Service (SaaS) and improves the security culture audit tool based on National Technical University of Athens's security culture toolkit. It enable the use of detailed socio-cultural characteristics (e.g. security behaviour analysis of individual users or departments) to produce accurate heatmaps of vulnerabilities across an organization The Anomaly Detection module is a software + hardware tool that uses machine learning to enable the real-time detection of anomalies covering the monitoring part Distributed Denial of Service Mitigation is a SaaS DDoS mitigation tool based on L7Defense's Ammune technology and uses known attack pattern (multi-vector attacks) to predict and protect against cascading effects, taking care of the protection level. The tool proposed for this area is Security Information and event Management (SIEM) and has the role of providing feedback on the proposed attack vectors via enabling real-time incident logging and analysis for immediate sharing throughout the industry (decision-support tools to coordinate cyberdefender response across the EPES value chain). The EnergyShield toolkit will combine the latest technologies for vulnerability assessment (automated threat modelling), monitoring & protection (anomaly detection and DDoS mitigation) and learning & sharing (security information and event management).

246	CRITICAL-CHAINS	IOT- & Blockchain-Enabled Security Framework for New Generation Critical Cyber-Physical Systems In Finance Sector	Critical-Chains is a 3-year research and innovation programme funded with the support of the European Commission Horizon 2020 Programme with a focus on IOT & Blockchain-Enabled Security Framework for Fintech Integrated New Generation Cyber-Physical Systems to support the Financial Sector. The Critical-Chains Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector. The project aims at developing a novel triangular accountability model and integrated framework supporting accountable, effective, accessible, fast, secure and privacy-preserving financial contracts and transactions to protect against illicit transactions, illegal money trafficking and fraud on FinTech e-operations. This is an innovative cloud-based "X-as-a Service" solution stack including several Cyber-Pysical Security Layers already validated through the first pilots, as follows: - Multi-Factor Hardware-Assisted Authentication as-a-Service (Auth-as-a-Service) - Blockchain Core Data Integrity Layer (Blockchain-as-a-Service (BCaaS) - Cryptography-as-a-Service (CRYPTaaS) - Data and Information Security and Privacy preservation at all layers of cloud through Hardware (HW) Security Module (HSM) and effective IoT connectivity enhanced with beyond Bluetooth Low Energy 5.0 chip combined within "as-a-Service" model (HwSaaS) and Transactions Flow Modelling As-a-Service (FMaaS).
247	MALAGA	Applying Machine Learning to Cyber Risk Analysis and Mitigation	The EU-funded MALAGA project will use machine learning (ML) technology to investigate cybersecurity risks, as well as find ways to reduce risks in the CAV field. With ML, the project will predict risks and price insurance policies to pave the way for innovation and entrepreneurial activity in Europe. The research will examine Connected and Autonomous Vehicles (CAV) cybersecurity risks and mitigation using Machine Learning (ML) techniques to predict future risks, price insurance policies and thereby foster innovation and entrepreneurial activity in Europe. The research will go beyond the SoA and implement models in ML like ensemble models and deep learning to forecast the risks of CAV technology. A network model of interactions will be trained and evaluated to study cascading of risks and threats in the CAV environment.

248	CyberSANE	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures	Optimisation of collaboration and the promotion of effective interaction among CII operators. Development of Advanced Persistent Threats taxonomy and models for CIIs. Uniting Web crawling and data aggregation technologies for necessary semantic structure, representation, convention and tool creation for data pulling, cleansing, analysis and interlinking. Development of Correlation Techniques for optimisation of automatic analysis of huge quantities of events, information and evidence combining both structure and unstructured data in a privacy-aware manner for malicious action identification in cyber assets such as abnormal behaviour. Specification of appropriate forecasting procedures and models which assist CII operators and security experts. Establishment of a Simulation Environment allowing investigators to design, model and execute simulations for the detection, analysis, visualisation, containing and eradication of security events and propagation effects. Enabling identification and standardisation of required information for sharing with relevant parties. Promotion and facilitation of trusted, secure and privacy aware data communication, maintenance and storage of forensic artefacts and evidential data. Integration of CyberSANE components into the CyberSANE system (TRL6) Deployment and Validation of the CyberSANE system in real operational environments.
249	Cyber-MAR	Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain	The main output is a platform consisting of networked cyber ranges and additional components providing advanced capabilities such as financial impact estimation, cert/csirts information sharing and decision support on potential cyber-attacks. The platform main aim is to act as a cost efficient training solution for cyber security professionals primarily in the maritime logistics domain.

250	PHOENIX	Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks	PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost. PHOENIX will realise 3 strategic goals: (1) Strengthen EPES cybersecurity preparedness by employing security a) "by design" via novel protective concepts for resilience, survivability, self-healing and accountability, and b) "by innovation" via adapting, upgrading and integrating a number of TRL5 developments to TRL7-8 and validating them in real-live large scale pilots; (2) Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level, a novel fully decentralized inter-DLTs/blockchain based near real-time synchronized cybersecurity information awareness platform, among authorized EPES stakeholders, utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group; (3) Accelerate research and innovation in EPES cybersecurity by a novel deploy, monitor, detect and mitigate DevSecOps mechanism, a secure gateway, privacy preserving federated Machine Learning algorithms and establishment of certification methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.
251	DAN	High-performance, kiosk-solution for forensic darknet analysis to gain cyber threat intelligence for companies and greatly enhance efficiency and capabilities of European investigation authorities	Mh SERVICE developed DAN, a Kiosk solution for darknet analysis. It includes high-performance hardware, pre-installed and pre-configured intuitive software, as well as user training and seminars. The acquired data is isolated from the possibility of foreign access or manipulation by third persons to ensure the chain of evidence for investigation authorities and privacy for companies. During the feasibility study of DAN, we tested the prototype at several customers and now optimise and redesign the DAN to perfectly fulfil the user needs from both segments.

252	vACCINE	AeronautiCal Cyber INtrusion dEtection mechanism	The vACCINE Project aims to enhance the resilience of existing aeronautical systems against cyber-attacks by designing an onboard machine learning based anomaly detector applied to ATC datalink communications. The detector will monitor data from ground before it enters the avionics domain and be able to detect anomalies caused by intrusion attempts or malfunction.
253	CARAMEL	Artificial Intelligence based cybersecurity for connected and automated vehicles	The EU-funded CARAMEL project is developing cybersecurity solutions for the new generation of cars: i) autonomous cars, ii) 5G connected vehicles, and iii) electromobility. The project applies a proactive method based on artificial intelligence and machine learning techniques to mitigate cybersecurity-originated safety risks on roads. Considering the entire supply chain, CARAMEL aims to introduce innovative anti-hacking intrusion detection/prevention systems for the European automotive industry. - Analysis of Security and Privacy Requirements of CCAM: The security and privacy aspects of the next generation mobility ecosystem - Anti Hacking Device: Innovative anti-hacking intrusion detection/prevention systems for the European automotive industry. - AI based geolocation attacks detection and mitigation: Man-in-the-middle attack called “location spoofing” attack. - V2X message and OBU tampering attacks detection and mitigation: man-in-the-middle attack and vehicle bus (through radio interface) attack & attack on key certificates storage, malicious firmware update, attack on exploiting OSS vulnerabilities.

254	FORESIGHT	Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments	1) Delivery of a state-of-the-art platform that considerably extends the capabilities of existing cyber-ranges by allowing them to be part of a cyber-range federation, where current and future cyber-ranges and simulation training environments of varying TRLs contribute by adding domain specificities (apart from those considered during the project's lifetime) and allowing complex cross-domain (i.e. hybrid) scenarios to be built. 2)Development of realistic and dynamic scenarios based on identified and forecasted trends and needs in terms of cyber-attacks and vulnerabilities (along with their cascading effects), based on cyber-threat intelligence that is gathered from various online sources and the dark web, to enable cyber-security professionals to rapidly adapt to an evolving threat landscape. 3) Development of advanced risk analysis and econometric models, constantly updated with real-life incidents, that will assist organisations to estimate the impact of cyber-risks, select the most appropriate and affordable security measures to protect valuable assets, and minimise the cost and time to recover from cyber-attacks. 4)Delivery of innovative training curricula, going far beyond those individual domains considered in the project, guiding cyber-security professionals to implement and combine security measures in innovative ways by using new technologies; established learning methodologies will be employed to maximise the outcome of training (that will be linked to professional certification programs), which will be efficiently supported by learning platforms to establish a rich cyber-security FORESIGHT knowledge base.
255	5GZORRO	Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks.	5GZORRO will develop these envisaged solutions for zero-touch service, network and security management in multi-stakeholder environments (ubiquitous), making use of Smart contracts based on Distributed Ledgers Technologies to implement required business agility. 5GZORRO consortium envisions the evolution of 5G to achieve truly production-level support of diverse vertical applications, which coexist on a highly pervasive shared network infrastructure, through automated end-to-end network slicing, across multiple operators and infrastructure/resource providers, who can share heterogeneous types of resources (spectrum, virtualized radio access, virtualized edge/core). 5GZORRO uses distributed Artificial Intelligence (AI) to implement cognitive network orchestration and management with minimal manual intervention (Zero-Touch Automation). Distributed Ledger Technologies (DLT) are adopted to implement flexible and efficient distributed security and trust across the various parties involved a 5G end-to-end service chain.

256	LOCARD	Lawful evidence collecting and continuity platform development	The project aims to provide a holistic platform for chain of custody assurance along the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata in a blockchain, supporting permission policies for selectively sharing access to digital evidence with other platform nodes. This will be powered by an immutable storage and an identity management system to protect privacy and handle access to evidence data using a Trusted Execution Environment.
257	INSPIRE-5Gplus	INtelligent Security and PervasIve tRust for 5G and Beyond	INSPIRE-5Gplus aims to make a radical shift in the security management of 5G networks and beyond at the level of platforms and vertical applications and services. To meet this goal, INSPIRE-5Gplus will devise and implement a fully automated end-to-end smart network and service security management framework that empowers not only protection but also trustworthiness and liability in managing 5G network infrastructures across multi-domains. INSPIRE-5Gplus will ensure that the provided security is compliant with the expected Security Service Level Agreement (SSLA) and the regulation requirements.
258	AERAS	A CybEr range tRaining platform for medicAl organisations and systems Security	AERAS aims to develop a realistic and rapidly adjustable cyber range platform for systems and organisations in the critical healthcare sector, to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical cyber-systems and organizations against advanced, known and new cyber-attacks, and reduce their security risks.
259	UP2DATE	Intelligent software-UPDATE technologies for safe and secure mixed-criticality and high performance cyber physical systems	a software paradigm for SAfety and SEcurity (SASE) software updates for intelligent and resource intensive Mixed-Criticality Cyber-Physical Systems (MCCPS). Two use cases: Automotive and railway.

260	1-SWARM	Integrated development and operations management framework for cyber-physical systems of systems under the paradigm of swarm intelligence	a methodological and technological framework, modular and re-usable (“Swarm Intelligence DevOps Framework”), for the engineering of the three major aspects of CPSoS: - The HW/SW runtime platform that sustains their operations; - The distributed and orchestrated Intelligence that guarantees their autonomic behavior; - The extension of their “existence” into the cyber-domain for a full life-cycle approach. Key to the exploitability of 1-SWARM’s result is the demonstration of its potentialities for 4 different application scenarios, food packaging, logistics for reconfigurable material handling, intelligent AGVs and aerial drones for monitoring of retails shops.
261	SAPPAN	Sharing and Automation for Privacy Preserving Attack Neutralization	a platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. SAPPAN will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. SAPPAN will enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches: (1) privacy-preserving aggregation and data analytics including advanced client-side abstractions; (2) federated threat detection based on sharing of anonymised data and sharing of trained machine learning models; (3) standardisation of knowledge in the context of incident response and recovery to enable reuse and sharing; (4) visual, interactive support for Security Operation Center operators.

262	KRAKEN	Brokerage and market platform for personal data	a trusted and secure personal data platform with state-of-the-art privacy aware analytics methods (with guarantees on metadata privacy, including query privacy). KRAKEN project aims to enable the sharing, brokerage, and trading of potentially sensitive personal data, by returning the control of this data to citizens (data providers) throughout the entire data lifecycle. KRAKEN will standardize different IT solutions thanks to featuring the (privacy-preserving) integration of independently obtained data sources from subjects consenting to different analyses. The project combines, interoperates, and extends the best results from two existing mature computing platforms developed within two H2020 actions: CREDENTIAL and MyHealthMyData. Creating economic value and innovative business models for 'personal data spaces' and supporting the Digital Single Markets' data economy by incentivizing parties, in particular SMEs, to actively engage in the data market. WP3 Decentralised Ledger Solutions: implementation core Technologies WP4 Crypto technologies and Analytics: implementation core Technologies Two pilots: Education and Health.
263	SDN-microSENSE	SDN - microgrid reSilient Electrical eNergy SystEm	SDN-microSENSE intends to provide a set of secure, privacy-enabled and resilient to cyberattacks tools, thus ensuring the normal operation of EPES as well as the integrity and the confidentiality of communications. - a resilient, multi-layered and SDN-enabled microgrid architecture, which will leverage the global system visibility for preventing and addressing disruptions to the underlying SCADA and ICS infrastructure - a risk assessment and management framework, - security applications, self-healing attack-resilient - a secure and flexible energy trading platform - an anonymous channel for information sharing among energy operators and actors - a privacy-preserving framework for enhancing EPES against data breaches - a policy recommendation framework.

265	M-SEC	Multi-layered Security technologies to ensure hyper connected smart cities with Blockchain, BigData, Cloud and IoT	- M-Sec IoT infrastructure: based on IoT, cloud, Big Data and blockchain to develop and operate new IoT applications for smart cities on top of smart objects. - M-Sec Marketplace: Our open market of applications, data and services will facilitate the exchange of value and information between IoT devices and people through virtual currencies.

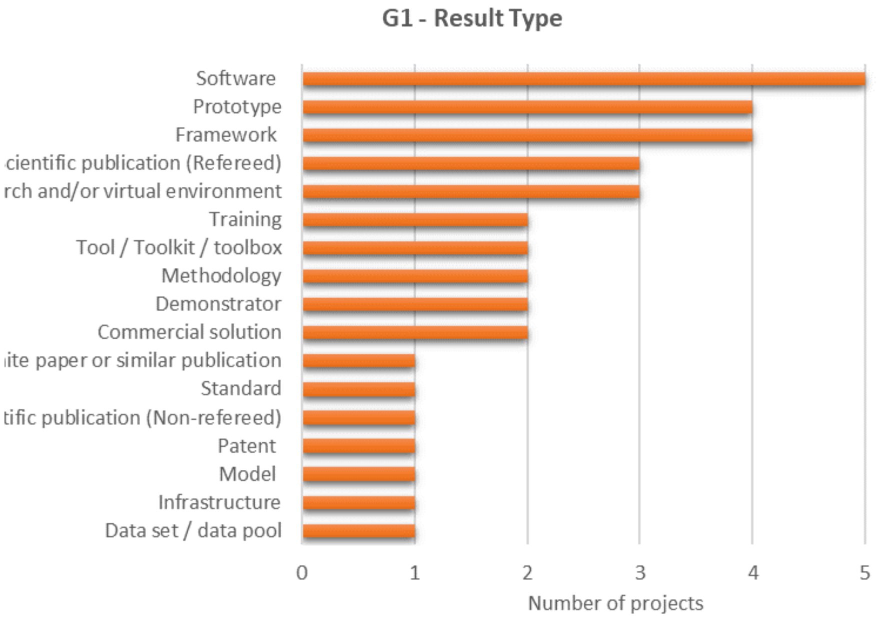
APPENDIX 3. EVOLUTION OF MTRL ASSESSMENT

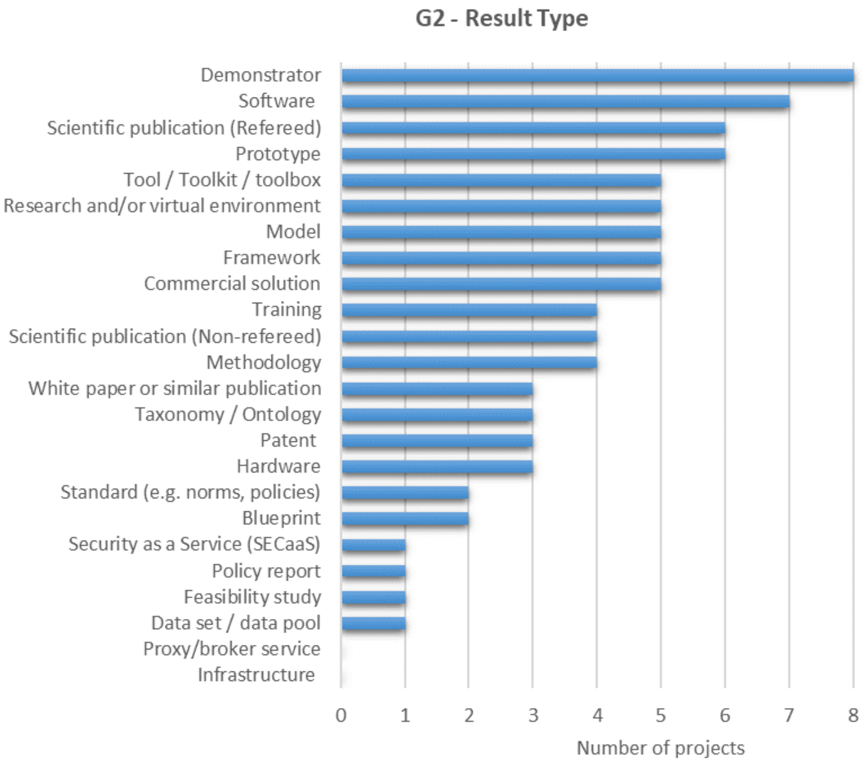
N.	Project	End date	T	M	T	M	T	M	T	M	T	M	Type	Taxonomy L2	Cluster
5	ANASTACIA	1/12/2019	6	3									RIA	Verification & Assurance	
13	CANVAS	1/08/2019			9	3							CSA	Cybersecurity Governance	
24	COMPACT	1/10/2019			7	4	7	5					IA	Cybersecurity Governance	
29	CS-AWARE	1/08/2020					7	6			7	6	IA	Cybersecurity Governance	I
35	DECODE	1/11/2019	6	4									RIA	Human Aspects	
40	DOGANA	1/08/2018	7	6									IA	Human Aspects	
45	ENCASE	1/12/2019	4	2	6	2							MSCA-RISE	Secure Systems	
46	EU-SEC	1/12/2019	7	5									IA	Cybersecurity Governance	
50	FutureTrust	1/05/2019	6	5									IA	Secure Systems	
52	GHOST	1/04/2020			7	5	7	6					IA	Human Aspects	
55	HERMENEUT	1/04/2019	6	5			6	5					RIA	Operational Risk	
57	IMPACT	1/01/2021					1	0					ERC-SyG	Operational Risk	III
58	KONFIDO	1/10/2019	4	2									RIA	Secure Systems	
60	LIGHTest	1/08/2019	7	5	7	5							IA	Secure Systems	
67	mF2C	1/12/2019			6	5							RIA	Secure Systems	
68	MH-MD	1/10/2019	6	5	6	5							RIA	Secure Systems	
71	MUSA	1/12/2017					4	5					RIA	Secure Systems	
91	PrEstoCloud	1/12/2019			7	5							RIA	Human Aspects	
102	PROTECTIVE	1/08/2019			7	7							IA	Cybersecurity Governance	
110	SafeCloud	1/08/2018			7	6	7	7					IA	Secure Systems	
112	SAFERtec	1/12/2019	2	3									RIA	Secure Systems	
113	SAINT	1/02/2021	7	5									RIA	Verification & Assurance	II
114	SAURON	1/04/2019			4	2							IA	Secure Systems	
116	SCOTT	1/06/2020			6	5	7	6			7	6	IA	Secure Systems	
122	SHIELD	1/02/2019			6	5							IA	Secure Systems	
124	SMESEC	1/05/2020	8	6	8	6	7	6			7	5	IA	Operational Risk	
126	SODA	1/12/2019	7	4									RIA	Secure Systems	

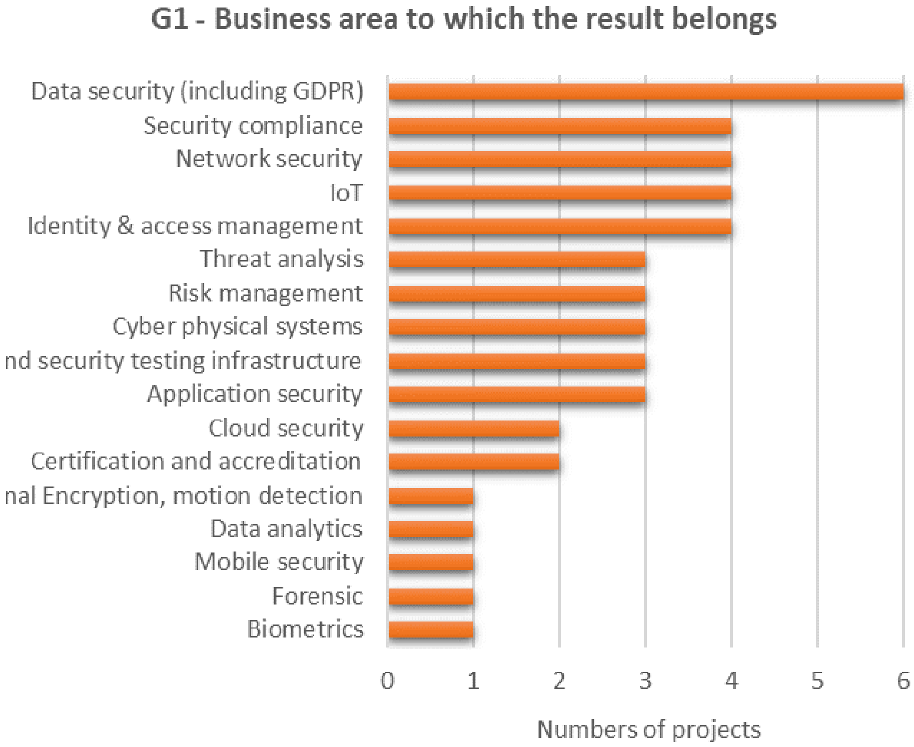
N.	Project	End date	T	M	T	M	T	M	T	M	T	M	Type	Taxonomy L2	Cluster
127	SPECIAL	1/12/2019	3	1									RIA	Human Aspects	
131	STOP-IT	1/05/2021			7	6	7	7	7	7	9	6	IA	Operational Risk	II
133	SUNFISH	1/12/2017					6	4					RIA	Operational Risk	
142	UNICORN	1/12/2019	6	5									IA	Secure Systems	
145	VisiOn	1/06/2017					7	4					IA	Verification & Assurance	
148	FENTEC	1/12/2020	3	3	3	3	3	4	3	4			RIA	Operational Risk	II
150	PROMETHEUS	1/12/2019	1	1									RIA	Verification & Assurance	V
151	REACT	1/05/2021	1	1							3	3	RIA	Secure Systems	V
152	SerIoT	1/12/2020	2	1	6	1							RIA	Secure Systems	
153	YAKSHA	1/06/2020	3	2									IA	Secure Systems	
155	CYBER-TRUST	1/04/2021	3	1	3	3	6	4	6	4			RIA	Secure Systems	V
158	PRIVILEDGE	1/12/2020									6	3	RIA	Identity & Privacy	
159	FUTURE TPM	1/12/2020									3	2	RIA	Verification & Assurance	IV
160	SealedGRID	1/12/2021	1	2	2	2	3	3					MSCA-RISE	Secure Systems	VI
162	ASTRID	1/04/2021			2	1	3	2	3	3	3	2	RIA	Secure Systems	IV
163	BPR4GDPR	1/04/2021					3	4					IA	Identity & Privacy	I
164	PAPAYA	1/04/2021					3	4	3	5			IA	Identity & Privacy	VI
165	POSEIDON	1/10/2020	3	4	6	4	6	5					IA	Identity & Privacy	VI
168	DEFEND	1/05/2021	2	3	3	3	3	4			7	6	IA	Cybersecurity Governance	I
170	OLYMPUS	1/08/2021	2	2	2	2	3	2					IA	Identity & Privacy	II
171	THREAT-ARREST	1/08/2021			6	6	6	6	6	6	6	6	IA	Secure Systems	
175	CyberSec4Europe	1/07/2022	2	4			3	5			3	3	RIA	Cybersecurity Governance	I
176	ECHO	1/02/2023	1	3	7	4	6	5	6	5	6	4	RIA	Cybersecurity Governance	I
177	ENACT	1/12/2020	3	3									RIA	Secure Systems	VI
178	PDP4E	1/01/2021									7	4	IA	Identity & Privacy	II
179	CYBERWISER	28/02/2021									8	7	IA	Secure Systems	
180	PROTASIS	1/04/2020									3	1	MSCA-RISE	Secure Systems	
185	PANACEA	1/12/2021			3	2	3	3			4	4	RIA	Operational Risk	
188	SecureIoT	1/12/2020			6	5	7	6	7	6	7	7	RIA	Secure Systems	

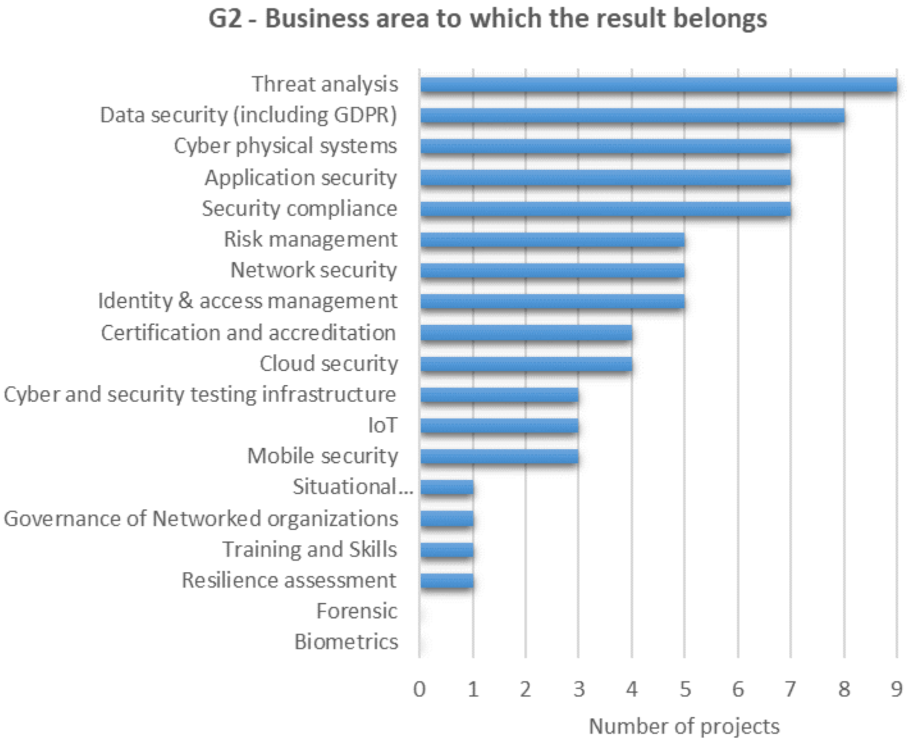
N.	Project	End date	T	M	T	M	T	M	T	M	T	M	Type	Taxonomy L2	Cluster
216	ASCLEPIOS	1/11/2021									3	3	RIA	Identity & Privacy	VI
217	CUREX	1/11/2021					2	1	6	3	6	4	RIA	Operational Risk	III
222	RESISTO	1/04/2021					7	3					IA	Operational Risk	II
223	SECREDAS	1/04/2021					6	5	7	4	7	4	ECSEL-RIA	Verification & Assurance	III
227	SAFECARE	1/08/2021									7	4	IA	Secure Systems	VI
229	SPHINX	1/12/2021									3	3	RIA	Secure Systems	VI
231	SECONDO	1/12/2022					1	2	2	3			MSCA-RISE	Operational Risk	III
232	TRINITY	1/12/2022									9	4	IA	Secure Systems	VI
237	nIoVe	1/04/2022									2	3	IA	Secure Systems	IV
238	GUARD	1/04/2022					2	3	3	5			IA	Secure Systems	V
239	InfraStress	1/05/2021					6	5			7	5	IA	Secure Systems	IV
243	SOTER	1/10/2021									6	4	IA	Secure Systems	
244	SPIDER	1/06/2022					1	1	3	3	3	4	IA	Operational Risk	III
245	EnergyShield	1/06/2022					3	5	3	5	3	5	IA	Secure Systems	III
248	CyberSANE	1/08/2022					1	2	2	3	2	4	IA	Secure Systems	III
249	Cyber-MAR	1/08/2022					3	2			3	4	IA	Secure Systems	III
250	PHOENIX	1/08/2022									3	3	IA	Secure Systems	V
253	CARAMEL	1/03/2022					6	5	6	5			IA	Secure Systems	IV
254	FORESIGHT	1/09/2022							3	4	3	2	IA	Verification & Assurance	
259	UP2DATE	1/12/2022					1	2					RIA	Secure Systems	V
261	SAPPAN	30/04/2022					3	3					IA	Secure Systems	I
262	KRAKEN	30/11/2022					1	3	3	4			IA	Identity & Privacy	
263	SDN-microSENSE	30/04/2022							6	4			IA	Secure Systems	
265	M-SEC	30/09/2021									4	5	RIA	Secure Systems	

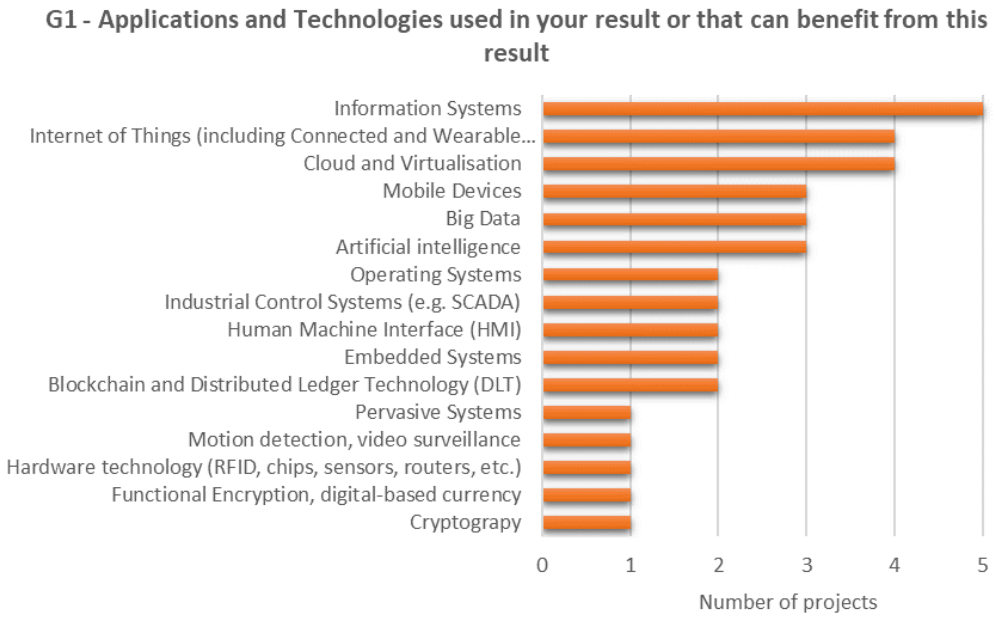
APPENDIX 4. RESULTS FROM ANALYSING GROUPS 1 AND 2 FOR CLUSTERING ACTIVITIES

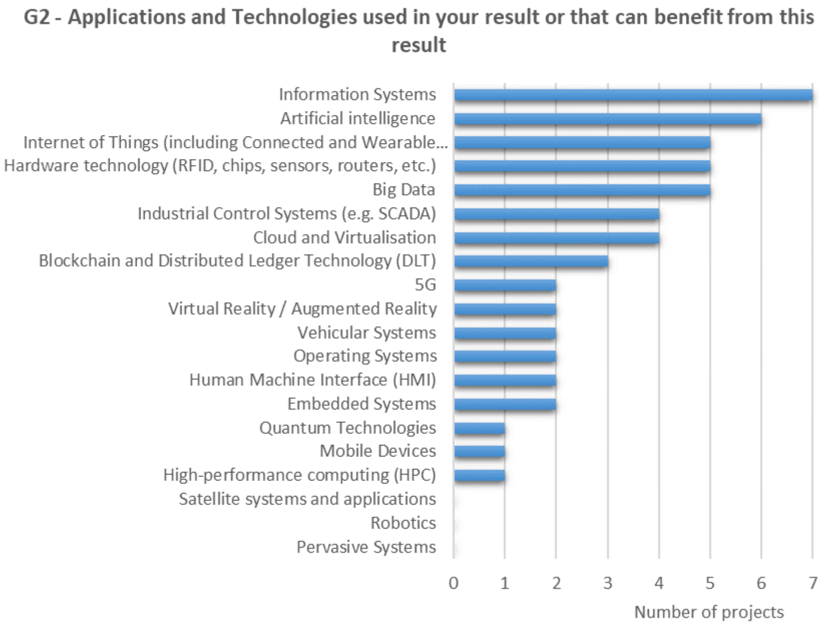


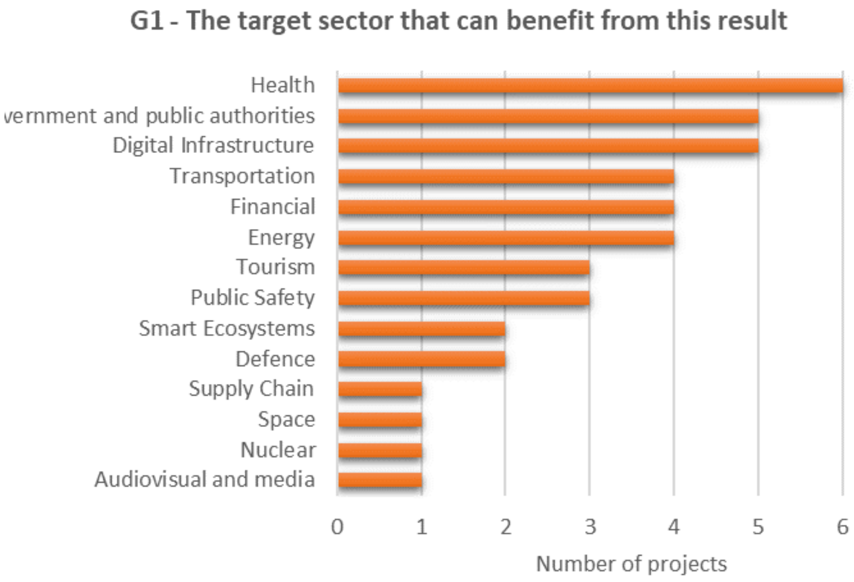


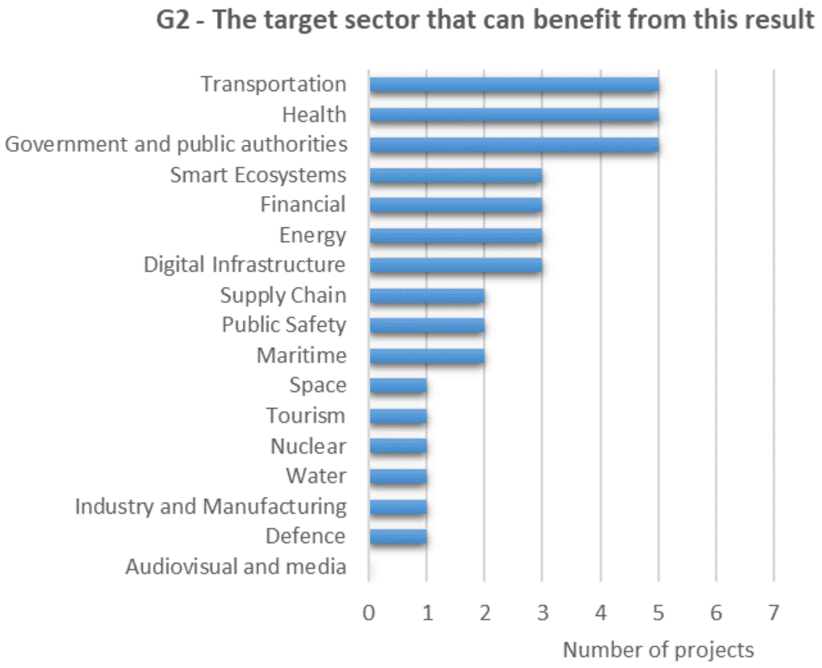

G1 - Business area to which the result belongs
Data security (including GDPR)
Security compliance
Network security
IoT
Identity & access management
Threat analysis
Risk management
Cyber physical systems
nd security testing infrastructure
Application security
Cloud security
Certification and accreditation
nal Encryption, motion detection
Data analytics
Mobile security
Forensic
Biometrics
0
1
2
3
4
5
6
Numbers of projects

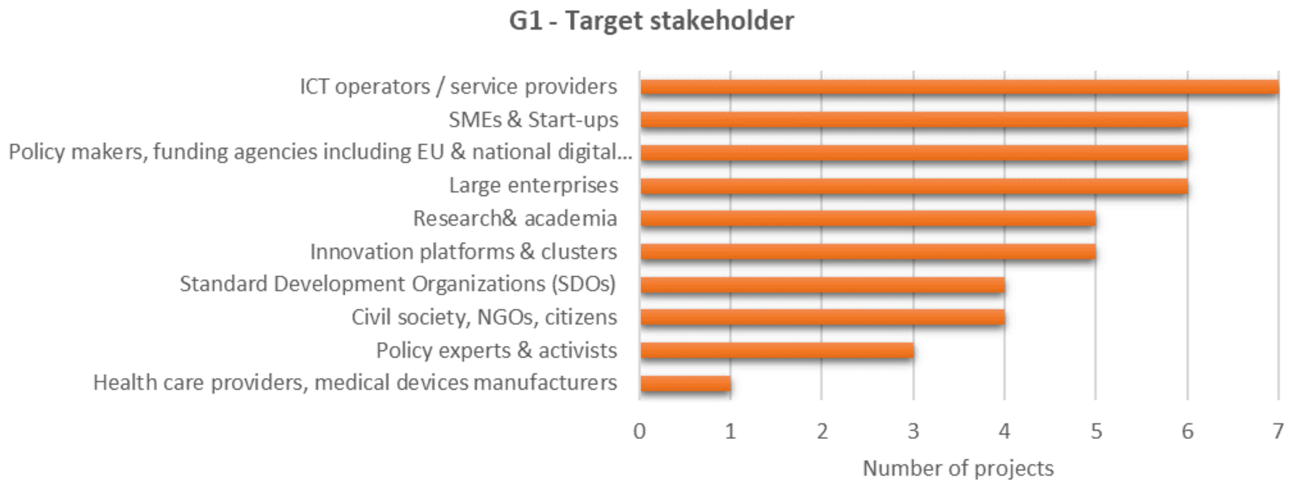

G2 - Business area to which the result belongs
Threat analysis
Data security (including GDPR)
Cyber physical systems
Application security
Security compliance
Risk management
Network security
Identity & access management
Certification and accreditation
Cloud security
Cyber and security testing infrastructure
IoT
Mobile security
Situational...
Governance of Networked organizations
Training and Skills
Resilience assessment
Forensic
Biometrics
0
1
2
3
4
5
6
7
8
9
Number of projects

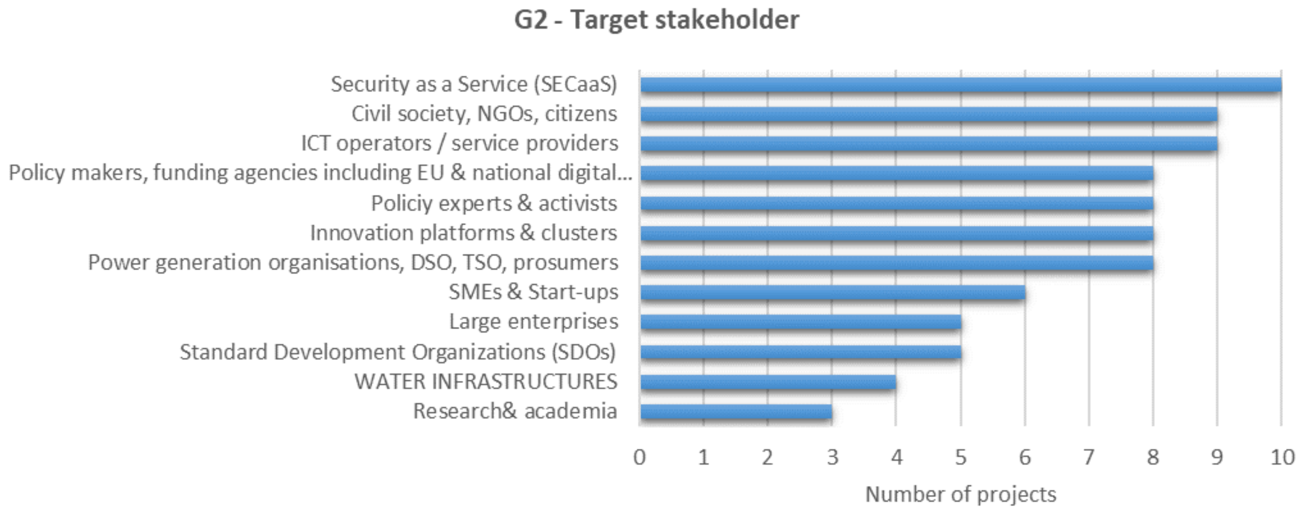

G1 - Applications and Technologies used in your result or that can benefit from this result
Information Systems
Internet of Things (including Connected and Wearable...
Cloud and Virtualisation
Mobile Devices
Big Data
Artificial intelligence
Operating Systems
Industrial Control Systems (e.g. SCADA)
Human Machine Interface (HMI)
Embedded Systems
Blockchain and Distributed Ledger Technology (DLT)
Pervasive Systems
Motion detection, video surveillance
Hardware technology (RFID, chips, sensors, routers, etc.)
Functional Encryption, digital-based currency
Cryptograpy
0
1
2
3
4
5
Number of projects


G2 - Applications and Technologies used in your result or that can benefit from this result
Information Systems
Artificial intelligence
Internet of Things (including Connected and Wearable...
Hardware technology (RFID, chips, sensors, routers, etc.)
Big Data
Industrial Control Systems (e.g. SCADA)
Cloud and Virtualisation
Blockchain and Distributed Ledger Technology (DLT)
5G
Virtual Reality / Augmented Reality
Vehicular Systems
Operating Systems
Human Machine Interface (HMI)
Embedded Systems
Quantum Technologies
Mobile Devices
High-performance computing (HPC)
Satellite systems and applications
Robotics
Pervasive Systems
0
1
2
3
4
5
6
7
Number of projects


G1 - The target sector that can benefit from this result
Health
vernment and public authorities
Digital Infrastructure
Transportation
Financial
Energy
Tourism
Public Safety
Smart Ecosystems
Defence
Supply Chain
Space
Nuclear
Audiovisual and media
0
1
2
3
4
5
6
Number of projects


G2 - The target sector that can benefit from this result
Transportation
Health
Government and public authorities
Smart Ecosystems
Financial
Energy
Digital Infrastructure
Supply Chain
Public Safety
Maritime
Space
Tourism
Nuclear
Water
Industry and Manufacturing
Defence
Audiovisual and media
0
1
2
3
4
5
6
7
Number of projects


G1 - Target stakeholder
ICT operators / service providers
SMEs & Start-ups
Policy makers, funding agencies including EU & national digital...
Large enterprises
Research& academia
Innovation platforms & clusters
Standard Development Organizations (SDOs)
Civil society, NGOs, citizens
Policy experts & activists
Health care providers, medical devices manufacturers
0
1
2
3
4
5
6
7
Number of projects


G2 - Target stakeholder
Security as a Service (SECaaS)
Civil society, NGOs, citizens
ICT operators / service providers
Policy makers, funding agencies including EU & national digital...
Policiy experts & activists
Innovation platforms & clusters
Power generation organisations, DSO, TSO, prosumers
SMEs & Start-ups
Large enterprises
Standard Development Organizations (SDOs)
WATER INFRASTRUCTURES
Research& academia
0
1
2
3
4
5
6
7
8
9
10
Number of projects

APPENDIX 5. MATRIX OF PROJECTS WITH MTRL ASSESSMENT

N	Project	Start	End	TRL	MRL	Taxonomy L2	Idea	Proto	Valid	Produ
145	VisiOn	01/07/2015	01/06/2017	7	4	Verification & Assurance			NTIM	
71	MUSA	01/01/2015	01/12/2017	4	5	Secure Systems		NTIM		
40	DOGANA	01/09/2015	01/08/2018	7	6	Human Aspects			RTC	
110	SafeCloud	01/09/2015	01/08/2018	7	7	Secure Systems			RTC	
122	SHIELD	01/09/2016	01/02/2019	6	5	Secure Systems			NTIM	
114	SAURON	01/05/2017	01/04/2019	4	2	Secure Systems		NMY		
55	HERMENEUT	01/05/2017	01/04/2019	6	5	Operational Risk			NTIM	
50	FutureTrust	01/06/2016	01/05/2019	6	5	Secure Systems			NTIM	
60	LIGHTest	01/09/2016	01/08/2019	7	5	Secure Systems			NTIM	
102	PROTECTIVE	01/09/2016	01/08/2019	7	7	Cybersecurity Governance			RTC	
13	CANVAS	01/09/2016	01/08/2019	9	3	Cybersecurity Governance				NMY
58	KONFIDO	01/11/2016	01/10/2019	4	2	Secure Systems		NMY		
68	MHMD	01/11/2016	01/10/2019	6	5	Secure Systems			NTIM	
24	COMPACT	01/05/2017	01/10/2019	7	5	Cybersecurity Governance			NTIM	
150	PROMETHEUS	01/01/2018	01/12/2019	1	1	Verification & Assurance	NMY			
112	SAFERtec	01/01/2017	01/12/2019	2	3	Secure Systems	NMY			
127	SPECIAL	01/01/2017	01/12/2019	3	1	Human Aspects	NMY			
45	ENCASE	01/01/2016	01/12/2019	6	2	Secure Systems			NMY	
5	ANASTACIA	01/01/2017	01/12/2019	6	3	Verification & Assurance			NMY	
35	DECODE	01/12/2016	01/12/2019	6	4	Human Aspects			NTIM	
67	mF2C	01/01/2017	01/12/2019	6	5	Secure Systems			NTIM	
142	UNICORN	01/01/2017	01/12/2019	6	5	Secure Systems			NTIM	
126	SODA	01/01/2017	01/12/2019	7	4	Secure Systems			NTIM	
46	EU-SEC	01/01/2017	01/12/2019	7	5	Cybersecurity Governance			NTIM	
91	PrEstoCloud	01/01/2017	01/12/2019	7	5	Human Aspects			NTIM	
57	IMPACT	15/02/2020	21/01/2020	1	0	Operational Risk	NMY			
180	PROTASIS	01/05/2016	01/04/2020	3	1	Secure Systems	NMY			
52	GHOST	01/05/2017	01/04/2020	7	6	Human Aspects			RTC	
238	GUARD	19/05/2020	22/04/2020	3	5	Secure Systems	NTIM			

N	Project	Start	End	TRL	MRL	Taxonomy L2	Idea	Proto	Valid	Produ
124	SMESEC	01/06/2017	01/05/2020	7	5	Operational Risk			NTIM	
153	YAKSHA	01/01/2018	01/06/2020	3	2	Secure Systems	NMY			
116	SCOTT	01/05/2017	01/06/2020	7	6	Secure Systems			RTC	
175	CyberSec4Europe	19/03/2020	22/07/2020	3	3	Cybersecurity Governance	NMY			
29	CS-AWARE	01/09/2017	01/08/2020	7	6	Cybersecurity Governance			RTC	
165	POSEIDON	01/05/2018	01/10/2020	6	5	Identity & Privacy			NTIM	
177	ENACT	01/01/2018	01/12/2020	3	3	Secure Systems	NMY			
148	FENTEC	01/01/2018	01/12/2020	3	4	Operational Risk	NTIM			
152	SerIoT	01/01/2018	01/12/2020	6	1	Secure Systems			NMY	
133	SUNFISH	15/01/2020	17/12/2020	6	4	Operational Risk			NTIM	
188	SecureIoT	18/01/2020	20/12/2020	7	7	Secure Systems			RTC	
259	UP2DATE	20/01/2020	22/12/2020	1	2	Secure Systems	NMY			
159	FUTURE TPM	01/01/2018	31/12/2020	3	2	Verification & Assurance	NMY			
113	SAINT	01/03/2017	01/02/2021	7	5	Verification & Assurance			NTIM	
179	CYBERWISER	01/09/2018	28/02/2021	8	7	Secure Systems				RTC
162	ASTRID	01/05/2018	01/04/2021	3	2	Secure Systems	NMY			
163	BPR4GDPR	01/05/2018	01/04/2021	3	4	Identity & Privacy	NTIM			
164	PAPAYA	01/05/2018	01/04/2021	3	5	Identity & Privacy	NTIM			
155	CYBER-TRUST	01/05/2018	01/04/2021	6	4	Secure Systems			NTIM	
222	RESISTO	01/05/2018	01/04/2021	7	3	Operational Risk			NMY	
223	SECREDAS	01/05/2018	01/04/2021	7	4	Verification & Assurance			NTIM	
178	PDP4E	01/05/2018	30/04/2021	7	4	Identity & Privacy			NTIM	
239	InfraStress	01/06/2019	01/05/2021	7	5	Secure Systems			NTIM	
168	DEFEND	01/06/2018	01/05/2021	7	6	Cybersecurity Governance			RTC	
131	STOP-IT	01/06/2017	01/05/2021	9	6	Operational Risk				RTC
151	REACT	01/06/2018	31/05/2021	3	3	Secure Systems	NMY			
158	PRIVILEDGE	01/01/2018	30/06/2021	6	3	Identity & Privacy			NMY	
170	OLYMPUS	01/09/2018	01/08/2021	3	2	Identity & Privacy	NMY			
171	THREAT-ARREST	01/09/2018	01/08/2021	6	6	Secure Systems			RTC	
265	M-SEC	01/07/2018	30/09/2021	4	5	Secure Systems		NTIM		
243	SOTER	01/07/2019	01/10/2021	6	4	Secure Systems			NTIM	

N	Project	Start	End	TRL	MRL	Taxonomy L2	Idea	Proto	Valid	Produ
217	CUREX	01/12/2018	01/11/2021	6	4	Operational Risk			NTIM	
216	ASCLEPIOS	01/12/2018	30/11/2021	3	3	Identity & Privacy	NMY			
227	SAFECARE	01/09/2018	30/11/2021	7	4	Secure Systems			NTIM	
160	SealedGRID	01/01/2018	01/12/2021	3	3	Secure Systems	NMY			
229	SPHINX	01/01/2019	31/12/2021	3	3	Secure Systems	NMY			
185	PANACEA	01/01/2019	31/12/2021	4	4	Operational Risk		NTIM		
237	nIoVe	01/05/2019	30/04/2022	2	3	Secure Systems	NMY			
261	SAPPAN	01/05/2019	30/04/2022	3	3	Secure Systems	NMY			
263	SDN-microSENSE		30/04/2022	6	4	Secure Systems			NTIM	
244	SPIDER	01/07/2019	01/06/2022	3	4	Operational Risk	NTIM			
245	EnergyShield	01/07/2019	01/06/2022	3	5	Secure Systems	NTIM			
248	CyberSANE	01/09/2019	01/08/2022	2	4	Secure Systems	NTIM			
250	PHOENIX	01/09/2019	31/08/2022	3	3	Secure Systems	NMY			
249	Cyber-MAR	01/09/2019	31/08/2022	3	4	Secure Systems	NTIM			
253	CARAMEL	01/10/2019	01/09/2022	3	2	Secure Systems	NMY			
254	FORESIGHT	01/10/2019	01/09/2022	3	2	Verification & Assurance	NMY			
262	KRAKEN	01/12/2019	30/11/2022	3	4	Identity & Privacy	NTIM			
231	SECONDO	01/01/2019	01/12/2022	2	3	Operational Risk	NMY			
176	ECHO	01/03/2019	01/02/2023	6	4	Cybersecurity Governance			NTIM	
232	TRINITY	01/01/2019	30/06/2023	9	4	Secure Systems				NTIM

APPENDIX 6. MATRIX OF PROJECTS Vs SRIA PRIORITIES

		AARC2	AEGIS	ANASTACIA	ARIES	ARMOUR	ASAP	ATENA	BEACON	C3ISP	CANVAS	certMILS	CHOReVOLUTION	CIPSEC	CITADEL	CLARUS	CloudSocket	COEMS	COMPACT	CREDENTIAL	CryptoCloud	CS-AWARE	CYBECO	CyberWiz	CYCLONE	CYRail	DAPPER	DECODE	DEFENDER	DISCOVERY	DiSIEM
		1	4	5	6	7	8	9	10	12	13	14	15	16	17	18	19	22	24	26	28	29	30	31	32	33	34	35	36	37	38
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification			▨		▨						▨							▨				▨			▨			▨		
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP			▨																		▨							▨		
	Development of digital forensics mechanisms and analytical support													▨								▨									
	Cyber ranges and simulation environments																														
	Cyber-physical systems security and cyber secure pervasive technology			▨		▨		▨				▨																	▨		
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures							▨						▨	▨							▨		▨		▨			▨		
	Secure Quantum Infrastructures																														
	Cyber secure future communication systems and networks			▨					▨					▨																	
	Vertical sectors cyber challenges									▨												▨									
	Industry 4.0 and ICS																														▨
	Energy (oil, gas, electricity), and smart grids							▨				▨												▨	▨				▨		
	Transportation (road, rail, air; sea, space)				▨		▨					▨	▨	▨				▨								▨					
	Financial Services, e-payments and insurance										▨											▨	▨								
	Public services, e-government, digital citizenship				▨						▨		▨						▨			▨						▨			
	Healthcare										▨			▨				▨													
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities			▨									▨						▨												
	Robotics																														
	Agrifood						▨																								
DATA & ECONOMY	Data security and malicious use of data									▨						▨												▨			
	End-to-end privacy																										▨				
	Economic aspects of cybersecurity																													▨	
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																														
	Software and Hardware cybersecure engineering and assurance			▨								▨						▨					▨								
	Cryptography				▨															▨	▨							▨			
	Blockchains and DLTs																											▨	▨		
	IoT Security			▨		▨							▨					▨													
	AI techniques for better security & malicious use of AI																					▨									

		DOGANA	e-Sides	ECRYPT-CSA	ENCASE	EU-SEC	EUNITY	FutureTrust	GenoPri	GHOST	HEAT	HECTOR	HERMENEUT	HIPS	IMPACT	KONFIDO	LIGHTest	LV-Pri20	MAMI	MAPPING	MAS2TERING	MATTHEW	mF2C	MH-MD	MIKELANGELO	MITIGATE	MUSA	NeCS	OCGN	OCTAVE	OPERANDO
		40	42	43	45	46	47	50	51	52	53	54	55	56	57	58	60	61	62	63	64	65	67	68	69	70	71	73	74	75	77
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification	■				■		■		■			■			■					■					■	■	■			
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP																								■		■				
	Development of digital forensics mechanisms and analytical support																											■	■		
	Cyber ranges and simulation environments																									■					
	Cyber-physical systems security and cyber secure pervasive technology									■																					
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures					■																	■		■	■		■		■	
	Secure Quantum Infrastructures																														
	Cyber secure future communication systems and networks									■									■									■			
	Vertical sectors cyber challenges																	■			■		■								
	Industry 4.0 and ICS																														
	Energy (oil, gas, electricity), and smart grids									■											■										
	Transportation (road, rail, air; sea, space)																									■				■	
	Financial Services, e-payments and insurance																					■								■	
	Public services, e-government, digital citizenship																■														■
	Healthcare								■	■						■								■							
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities									■											■							■			
	Robotics																														
	Agrifood																														
DATA & ECONOMY	Data security and malicious use of data				■					■					■													■			
	End-to-end privacy								■													■						■		■	■
	Economic aspects of cybersecurity		■				■						■							■			■								
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																														
	Software and Hardware cybersecure engineering and assurance																										■				
	Cryptography			■	■				■		■	■		■		■						■		■							
	Blockchains and DLTs									■						■								■							
	IoT Security									■						■		■					■					■			
	AI techniques for better security & malicious use of AI									■											■										

		PaaSword	PANORAMIX	PQCRYPTO	PrEstoCloud	PRISM CODE	PRISMACLOUD	PRIVACY FLAG	Privacy&Us	PRIVACY4FORENS	ProBOS	PROTECTIVE	Ps2Share	RAPID	REASSURE	REDSENTRY	SafeCloud	SAFEcrypto	SAFERtec	SAINT	SAURON	SCISSOR	SCOTT	SCR	SecIoT	SERECA	SHARCS	SHIELD (Health)	SHIELD	SISSDEN	SMESEC
		79	81	86	91	95	96	98	99	100	101	102	103	104	105	107	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification							■							■																■
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP										■																■			■	
	Development of digital forensics mechanisms and analytical support									■																			■	■	
	Cyber ranges and simulation environments																														
	Cyber-physical systems security and cyber secure pervasive technology																		■		■	■	■			■					
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures														■	■					■	■				■		■			
	Secure Quantum Infrastructures			■																											
	Cyber secure future communication systems and networks				■	■								■			■	■	■										■	■	
	Vertical sectors cyber challenges																						■								
	Industry 4.0 and ICS																					■	■								■
	Energy (oil, gas, electricity), and smart grids																					■									■
	Transportation (road, rail, air; sea, space)				■														■		■		■				■				
	Financial Services, e-payments and insurance															■															
	Public services, e-government, digital citizenship		■				■				■	■	■					■		■											■
	Healthcare						■																■				■	■			
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities				■		■								■								■								■
	Robotics																														
	Agrifood																														
DATA & ECONOMY	Data security and malicious use of data					■							■				■														
	End-to-end privacy	■	■			■	■	■	■			■	■				■						■					■			
	Economic aspects of cybersecurity								■			■								■											■
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																														
	Software and Hardware cybersecure engineering and assurance	■																	■					■			■				
	Cryptography	■	■	■			■								■			■				■				■					
	Blockchains and DLTs																														
	IoT Security			■				■							■								■		■	■					■
	AI techniques for better security & malicious use of AI										■																		■		

		SODA	SPECIAL	SpeechXRays	SPOOC	STOP-IT	STORM	SUNFISH	SUPERCLOUD	TOREADOR	TREDISEC	TYPES	U2PIA	UNICORN	VESSEDIA	VIRT-EU	VisiOn	WISER	WITDOM	FENTEC	PROMETHEUS	REACT	SerIoT	YAKSHA	CYBER-TRUST	PRIVILEDGE	FUTURE TPM	SealedGRID	SEMIoTICS	ASTRID	BPR4GDPR
		126	127	128	129	131	132	133	134	137	138	140	141	142	143	144	145	146	147	148	150	151	152	153	155	158	159	160	161	162	163
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification					■	■		■						■			■							■		■				
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP																					■		■						■	
	Development of digital forensics mechanisms and analytical support																							■						■	
	Cyber ranges and simulation environments																					■			■						
	Cyber-physical systems security and cyber secure pervasive technology					■																						■			
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures					■												■									■				
	Secure Quantum Infrastructures																				■						■				
	Cyber secure future communication systems and networks								■		■												■								
	Vertical sectors cyber challenges																														
	Industry 4.0 and ICS					■				■												■	■								
	Energy (oil, gas, electricity), and smart grids																					■						■	■		
	Transportation (road, rail, air; sea, space)																					■	■								■
	Financial Services, e-payments and insurance		■																	■		■				■	■				
	Public services, e-government, digital citizenship		■		■			■									■				■				■						■
	Healthcare	■		■					■													■				■			■		■
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities					■																									
	Robotics																														
	Agrifood																					■	■								
DATA & ECONOMY	Data security and malicious use of data	■									■															■					
	End-to-end privacy	■	■		■			■		■	■	■	■	■		■	■		■						■						■
	Economic aspects of cybersecurity																	■						■							
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																														
	Software and Hardware cybersecure engineering and assurance										■			■	■				■	■		■	■				■	■	■		■
	Cryptography	■	■		■			■			■								■	■	■					■	■			■	
	Blockchains and DLTs							■															■		■	■		■			
	IoT Security														■	■							■		■		■		■		
	AI techniques for better security & malicious use of AI		■	■		■				■												■									

		PAPAYA	POSEIDON	SPEAR	SMOOTH	DEFEND	OLYMPUS	THREAT-ARREST	CONCORDIA	SPARTA	CyberSec4Europe	ECHO	ENACT	PDP4E	CYBERWISER	PROTASIS	PANACEA	symbIoTe	SecureIoT	PANOPTESEC	SERENITI	SecureCloud	ASCEMA	LipVerify	ConnectProtect	ThreatMark	Eye-O-T	PerfectDashboar	CHINO	CyberSure	LocationWise
		164	165	166	167	168	170	171	172	174	175	176	177	178	179	180	185	186	188	191	192	193	194	195	196	197	198	199	200	201	203
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification		■	■		■			■	■	■	■		■			■		■											■	
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP										■									■					■	■					
	Development of digital forensics mechanisms and analytical support			■																											
	Cyber ranges and simulation environments							■	■	■	■	■			■																
	Cyber-physical systems security and cyber secure pervasive technology									■									■												
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures	■		■					■	■	■				■	■	■				■										
	Secure Quantum Infrastructures										■																				
	Cyber secure future communication systems and networks																														
	Vertical sectors cyber challenges								■			■																			
	Industry 4.0 and ICS										■	■				■			■												
	Energy (oil, gas, electricity), and smart grids			■		■		■			■	■		■	■						■										
	Transportation (road, rail, air; sea, space)									■	■	■	■	■	■	■		■	■												
	Financial Services, e-payments and insurance					■	■		■		■			■												■					■
	Public services, e-government, digital citizenship		■			■	■		■	■	■	■																			
	Healthcare	■				■		■			■	■	■				■		■										■	■	
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities							■			■							■	■								■				
	Robotics																		■												
	Agrifood										■																				
DATA & ECONOMY	Data security and malicious use of data	■				■													■												
	End-to-end privacy	■	■		■	■	■			■	■	■		■					■			■							■		
	Economic aspects of cybersecurity			■																			■					■			
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs									■				■																	
	Software and Hardware cybersecure engineering and assurance			■		■				■	■			■		■	■	■	■		■	■									
	Cryptography	■					■				■								■												
	Blockchains and DLTs		■						■		■																				
	IoT Security									■		■						■	■								■				
	AI techniques for better security & malicious use of AI	■	■						■	■	■			■			■							■		■					

		UNFRAUD	CLTRe	GO 4G	TFence	UltraFiBi	ProtonSuite	ASCLEPIOS	CUREX	V-SPHERE	AF-Cyber	SIGAGuard	TrueProactive	RESISTO	SECREDAS	ELIoT Pro	CYBERSECURITY	Blocknetwork	SAFECARE	ADVERSARY	SPHINX	SERUMS	SECONDO	TRINITY	RADDICS	FeatureCloud	D-FENCE	nIoVe	GUARD	InfraStress	ODIX 2.0
		206	207	209	211	212	213	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	236	237	238	239	240
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification		■	■					■					■	■		■		■		■		■				■			■	
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP												■	■					■		■								■	■	■
	Development of digital forensics mechanisms and analytical support										■																				
	Cyber ranges and simulation environments																														
	Cyber-physical systems security and cyber secure pervasive technology													■					■						■				■	■	
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures													■					■						■	■			■	■	
	Secure Quantum Infrastructures																														
	Cyber secure future communication systems and networks				■									■	■									■							
	Vertical sectors cyber challenges																													■	
	Industry 4.0 and ICS											■												■						■	
	Energy (oil, gas, electricity), and smart grids																								■					■	
	Transportation (road, rail, air; sea, space)													■	■													■	■		
	Financial Services, e-payments and insurance	■																					■								
	Public services, e-government, digital citizenship	■																											■		
	Healthcare				■	■		■	■					■	■				■		■	■				■			■	■	
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities																														
	Robotics																							■	■						
	Agrifood																														
DATA & ECONOMY	Data security and malicious use of data																				■								■		
	End-to-end privacy						■	■	■							■					■	■		■		■					
	Economic aspects of cybersecurity								■														■								
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																														
	Software and Hardware cybersecure engineering and assurance								■	■						■								■						■	
	Cryptography							■								■		■				■									
	Blockchains and DLTs								■									■				■	■			■		■			
	IoT Security				■									■	■	■								■				■	■		
	AI techniques for better security & malicious use of AI	■										■										■			■	■		■			

		C4IIoT	CYBERCULT	SOTER	SPIDER	EnergyShield	CRITICAL-CHAINS	MALAGA	CyberSANE	Cyber-MAR	PHOENIX	DAN	vACCINE	CARAMEL	FORESIGHT	5GZORRO	LOCARD	INSPIRE-5Gplus	AERAS	UP2DATE	1-SWARM	SAPPAN	KRAKEN	SDN-microSENSE	M-SEC
		241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	265
ECOSYSTEM, SOCIAL GOOD & CITIZENS	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification		■			■					■													■	
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP	■																				■		■	
	Development of digital forensics mechanisms and analytical support											■					■								
	Cyber ranges and simulation environments				■				■	■					■				■						
	Cyber-physical systems security and cyber secure pervasive technology	■					■														■				
APPLICATION DOMAINS & INFRASTRUCTURE	Cyber resilient digitised infrastructures			■		■			■	■	■		■		■				■	■					
	Secure Quantum Infrastructures																								
	Cyber secure future communication systems and networks				■									■		■		■			■				
	Vertical sectors cyber challenges									■														■	
	Industry 4.0 and ICS	■							■	■											■				■
	Energy (oil, gas, electricity), and smart grids				■	■			■		■													■	■
	Transportation (road, rail, air; sea, space)	■						■	■	■			■	■						■					
	Financial Services, e-payments and insurance			■			■		■																
	Public services, e-government, digital citizenship																								
	Healthcare								■										■				■		■
	Smart cities and smart buildings (convergence of digital services for citizens) and other utilities																								■
	Robotics																				■				
	Agrifood																								
DATA & ECONOMY	Data security and malicious use of data																								
	End-to-end privacy						■															■	■		
	Economic aspects of cybersecurity		■												■								■		
BASIC & DISRUPTIVE TECHNOLOGIES	Secure and Trustworthy AIs																								
	Software and Hardware cybersecure engineering and assurance	■				■		■			■			■		■		■		■					■
	Cryptography	■				■	■																■		
	Blockchains and DLTs	■		■			■				■					■	■	■					■		■
	IoT Security	■					■																		■
	AI techniques for better security & malicious use of AI	■			■	■	■	■	■		■		■	■		■		■				■			■