D2.5 Cybersecurity Projects Radar 2nd Report Spring 2020

Author(s)	M Drescher & D Wallom , UOXF
Status	FINAL
Version	1.0
Date	6 August 2020

Dissemination Level

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

Abstract:

We present in this report a visualisation of EC supported activities in the area of Cybersecurity and Privacy that allows possible exploiters of the outputs of these projects to understand their status.

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 – WP2 – D2.2	
Deliverable lead	**UOXF**
Related work package	**WP2**
Author(s)	**M Drescher & D Wallom, UOXF**
Contributor(s)	**-**
Due date	**30/06/2020**
Actual submission date	**06/08/2020**
Reviewed by	**M Ramirez (AEI), M Miller (CPT)**
Start date of Project	**01/05/2017**
Duration	**48 months**

Revision history

Version	Date	Authors	Notes
0.1	1/10/2018	M Drescher (UOXF)	Core structure of the document agreed
0.2	13/07/2020	M Drescher (UOXF)	Radar analysis nearly complete
0.3	15/7/2020	M Drescher (UOXF)	First complete draft.
0.4	29/7/2020	D Wallom (UOXF)	UOXF Internal review.
0.5	04/08/2020	M Ramirez (AEI)	AEI Internal review
0.6	04/8/2020	M Miller (CPT)	CPT Internal review
1.0	06/8/2020	M Drescher (UOXF) N Zazzeri (Trust-IT)	Quality check and final version

Executive Summary

The European Commission has launched 115 calls which were either explicitly supporting projects in the domain of Cybersecurity and Privacy (CS & P), or from which projects in this area were supported. As such it is important that we consider what the outputs of these projects have been and where the products they have created have gone in terms of exploitation either by the projects themselves or by others who may reuse their outputs.

The previous deliverable D2.2 Technology Radar 1st report – Autumn 2018 established the methodology, and how the Cyberwatching.eu project has adapted it to suit its needs. It then presented the first radar edition – Autumn 2018 – and presented an analysis of the then available data.

Now, almost 2 years later, our data on projects has grown from 134 to 261 projects, across 113 funding calls (previously 34), providing Cyberwatching.eu with a dataset that allows to analyse trends and patterns in the funding landscape far more accurately than before.

Our data shows that in 2018 some radar sectors were underrepresented, thus having a factually larger impact than thought, and some sectors being overrepresented – with the consequence of their input being actually less influential that we previously thought.

Integrating MTRL score self-assessments provided by the included projects themselves into the Projects Radar allows Cyberwatching.eu to shortlist projects with potential for adoption from external domain stakeholders. This is one of the primary goals of the Cyberatching.eu projects.

The Spring 2020 Projects Radar continues to present a strong imbalance across the radar sectors. Where we previously thought that the Secure Systems sector was overrepresented with a 34% share overall in Autumn 2018, its actual share in project presence is now consistently at about 50% of all projects – the effect of Secure Systems being underrepresented in the Autumn 2018 Radar and now showing a stronger dominance than previously anticipated.

In this report, we combine the analysis of the now available data with the larger cyber threat landscape analysis, and raise attention to the lack of fundamental research available on the Human Aspects sector which, with appropriate funding and exploitation, we expect to address cybersecurity vulnerabilities at the root by increasing individual's resilience against and affinity to falling for social engineering attacks as a fundamentally preventative measure.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Introduction

"A large number of substantial investments have been made by both national governments and the European Commission to support co-ordinated programmes of research and innovation projects within the broad domain of cybersecurity and privacy. Since some of these programmes have now completed and as the European Commission has transitioned from Framework 7 to Horizon 2020, it is important that we are able to evaluate the impact that these programmes have had, and more specifically, how ready the outputs are for utilisation by persons from outside the developing community. As such, in an area such as Cybersecurity it is essential that we are able to consider and present to stakeholders in these enterprises (potential users of the technologies, processes and policies developed) the outputs from the projects alongside a systematic method of the evaluation of the outputs, with commentary on how easy these outputs are to use both generally and more importantly, outside of the team that originally developed them."

This quote from D2.2 Cybersecurity Technology Radar 1st Report – Autumn 2018 [1] holds true now as it held true nearly 2 years ago.

Since then, the methodology of assessing projects has not changed (refer to [1] for an in-depth explanation of the methodology), neither has the intent and purpose of the radar. What has changed, however, is the sample[1] of EU funded projects in the EU Cybersecurity and Privacy (CS & P) landscape, and with that interesting and noteworthy patterns emerge, as described in this deliverable.

It is important to reiterate that the Projects Radars do *not* visualise the entire data set: Each Radar includes only those projects that were either active or finished within 3 years of the radar's reference date. Any project that has not started by then, or is older than 3 years, is not included. Hence, Projects Radars represent *sliding windows* into the history of the EU's investment strategy in CS & P research.

Since the publication in [1] the four radar editions (Autumn 2018, Spring 2019, Autumn 2019, and Spring 2020) are available online in a first version prominently placed on the Cyberwatching.eu website [2]. While it demonstrates the usefulness and impact of the tool, it has several statistical and usability shortfalls, which are addressed in a second version that is due to be published after the production of this deliverable. The shortfall of the first online version of the Projects Radar tool are that it is susceptible to changes in the underpinning data set that should be out of scope for the radar editions, and since it requires significant manual labour to produce each edition, human errors in that process are likely. In that respect, the first online version can be seen as a proof of concept at TRL 4, the second online version will be at TRL 6, adding stability and reproducibility of the results with reasonable data quality constraints.

This edition of the Cyberwatching.eu Projects Radar will provide an analysis of the data available across four editions, spanning nearly two years of data gathering and analysis.

[1] Statistically speaking the Cyberwatching.eu project will only ever operate on samples of a data set, not a complete population of projects.

Glossary of Terms

Term	Description
CI	Critical Infrastructure(s)
CS & P	Cybersecurity and Privacy
H2020	Horizon 2020
MTRL	Market and Technology Readiness Level. Individual TRL and MRL (Market Readiness Level) scores conjoined into one data value, frequently noted as (MRL, TRL)
Projects Radar	Short term for Cyberwatching.eu CS & P Projects Radar

2 The analysed projects

In line with the process established in the first edition of the report [1] we collected projects from a total of 115 funding calls (Spring 2020; up by 90 from 25 in Autumn 2018). These calls are, in alphabetical order:

CIP-01-2016-2017	H2020-EU.3.7.4	MSCA-COFUND-2016
DRS-17-2014	H2020-FOF-2016	MSCA-IF-2014-EF
DS-01-2014	H2020-ICT-2014-1	MSCA-IF-2015-EF
DS-01-2016	H2020-ICT-2015	MSCA-IF-2016
DS-02-2014	H2020-ICT-2016-1	MSCA-IF-2017
DS-02-2016	H2020-ICT-2017-1	MSCA-IF-2018
DS-02-2016	H2020-INFRAEOSC-2018-1	MSCA-ITN-2014-ETN
DS-03-2015	H2020-IOT-2016	MSCA-ITN-2015-ETN
DS-03-2016	H2020-IOT-2017	MSCA-RISE-2015
DS-04-2015	H2020-MSCA-RISE-2015	MSCA-RISE-2016
DS-04-2016	H2020-MSCA-RISE-2017	MSCA-RISE-2018
DS-05-2015	H2020-SC1-FA-DTS-2018-1	MSCA-RISE-2019
DS-05-2016	H2020-SMEINST-1-2016-2017	PEOPLE-2007-4-3.IRG
DS-06-2014	H2020-SU-ICT-2018	S2R-OC-IP2-01-2015
DS-07-2015	H2020-SU-ICT-2018-2	SEC-2010.6.5-2
DT-ICT-02-2018	ICT-01-2019	SEC-2011.2.5-1
ECSEL-2016-2-IA-two-stage	ICT-06-2016	SEC-2011.3.4-1
ECSEL-2017-2	ICT-07-2014	SEC-2011.6.1-5
EE-13-2014	ICT-09-2014	SEC-2011.6.5-2
EIC-SMEInst-2018-2020	ICT-10-2016	SEC-2012.2.3-1
EINFRA-22-2016	ICT-12-2015	SEC-2012.6.1-2
ERC-2013-SyG	ICT-12-2016	SiS-2008-1.2.2.1
ERC-2018-COG	ICT-16-2015	SiS-2009-1.1.2.1
ERC-AG-PE6	ICT-18-2016	SiS.2013.1.2-1
ERC-CG-2013-PE6	ICT-20-2019-2020	SMEInst-01-2016-2017
ERC-CoG-2014	ICT-2007.1.4	SMEInst-02-2016-2017
ERC-SG-PE6	ICT-2007.6.2	SMEInst-09-2016-2017
EUB-1-2015	ICT-2009.1.4	SMEInst-10-2016-2017
FCT-09-2015	ICT-2013.1.5	SMEInst-13-2016-2017
FP7-ICT-2013-10	ICT-2013.10.1	SSH-2009-3.2.1.
FP7-PEOPLE-2011-IOF	ICT-2013.6.1	SU-DS01-2018
FP7-PEOPLE-2012-CIG	ICT-32-2014	SU-DS04-2018-2020
FP7-PEOPLE-2013-CIG	ICT-35-2016	SU-DS05-2018-2019
FP7-PEOPLE-2013-IIF	ICT-37-2014-1	SU-FCT02-2018-2019-2020
FP7-PEOPLE-IOF-2008	ICT-37-2015-1	SU-ICT-01-2018
FP7-SEC-2012-1	ICT-38-2015	SU-INFRA01-2018-2019-2020
H2020-DS-LEIT-2017	INNOSUP-02-2016	SU-TDS-02-2018
H2020-DS-SC7-2016	JTI-CS2-2018-CfP09-SYS-01-11	SU-TDS-03-2018
H2020-DS-SC7-2017		

Table 1: List of EC funding calls for projects included in the Projects Radar database

The database now includes a total number of 261 projects of which 34 are considered out of scope of the radar, in line with the criteria set out in [1]. These projects are:

3ants	DSSC	PRIPARE
CAPITAL	ECRYPT-NET	PROOFY
CE-IoT	FAR-EDGE	ReCRED
CloudTeam	FIDELITY	RPS
COLA	FORTIKA	SAFETY 4.0
CREATE-IoT	IPaCSO	SamurAI
CROSSMINER	LIMPET	SecureHospitals.eu
cyberwatching.eu	MELODIC	SOFIE
CYBERWISER.EU	OCRE	STAMP
DECODE	OPENREQ	SWITCH
DITAS	P5	TRUESSEC.EU
DOGANA II		

Table 2: Projects considered out of scope for the Projects Radar

Appendix 1 provides a complete list of all 261 projects included in the Projects Radar database.

3 The Spring 2020 Projects Radar

This second edition of the Projects Radar will include an analysis of not only the most recent snapshot of information, but also provide an analysis of trends across the now four available Radar editions since the first report [1] was published.
Reusing the same structure, we present an analysis sector by sector, followed by analysing the full radar history from Autumn 2018 to Spring 2020. However, this deliverable will not list the detailed tabulations of projects, or the visualisation of the radars, as these are available online at https://www.cyberwatching.eu/technology-radar

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	34	17	9	40	34	134
Spring 2019	69	15	32	48	11	175
Autumn 2019	67	22	34	52	16	191
Spring 2020	63	9	38	32	48	190

Table 3: Projects Radar editions

3.1 Results by sector

3.1.1 Secure Systems and Technology

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	12	7	3	17	8	47
Spring 2019	25	7	16	23	9	80
Autumn 2019	31	7	17	24	10	89
Spring 2020	30	3	15	16	23	87

Table 4: "Secure Systems and Technology" overview – Spring 2020

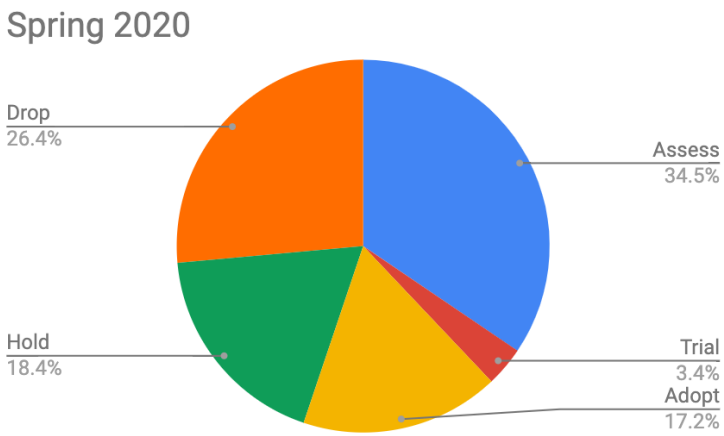

Figure 1: Distribution of projects by lifecycle stage in the "Secure Systems and Technology" sector – Spring 2020

"Secure systems and technology" is understandably the most popular area within the cybersecurity and privacy ecosystem, since it is what most would consider the front line in protecting resources, to develop new technological solutions to what can be a technology driven problem.

Anticipating the analysis of the entire Radar and its history, the huge jump on projects since Autumn 2018 is very atypical, given that 2018 sits well within the H2020 funding cycle. In our analysis we conclude that this is a consequence of our initial dataset being far too incomplete, which was then rectified with the second wave of data gathering of funded projects in the EU CS & P landscape.

Having said that, the continuous high level of projects in the pipeline (Assess ring) over the Radar editions is a reassuring sign of continued demonstration and perceived importance of research and innovation towards secure systems in an increasingly digital world.

There are clearly two waves of projects visible in the radar in 2020: More than a third of all projects are still active for at least six months, whereas almost half of all projects are now more than one year ('Hold') or two years ('Drop') old, and thus considered close to obsolescence (i.e. more than three years since the project ended).

These waves are visible going back in time through the radar editions albeit less obvious in previous iterations as they gradually progress through the project lifecycle rings.

Only one sixth (15 projects) have finished recently and are considered ready for adoption. Taking recent MTRL self-assessments into account, six of these projects appear particularly suited for immediate adoption:

#	Project	Type	TRL	MRL
50	FutureTrust	IA	6	5
60	LIGHTest	IA	7	5
67	mF2C	RIA	6	5
68	MH-MD	RIA	6	5
126	SODA	RIA	7	4
142	UNICORN	IA	6	5

Table 5: Projects addressing "Secure Systems and Technology" close to or ready for adoption

3.1.2 Verification and Assurance

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	2	1	1	4	8	16
Spring 2019	7	0	2	5	1	15
Autumn 2019	6	3	2	4	2	17
Spring 2020	8	0	3	2	5	18

Table 6: "Verification and Assurance" overview – Spring 2020

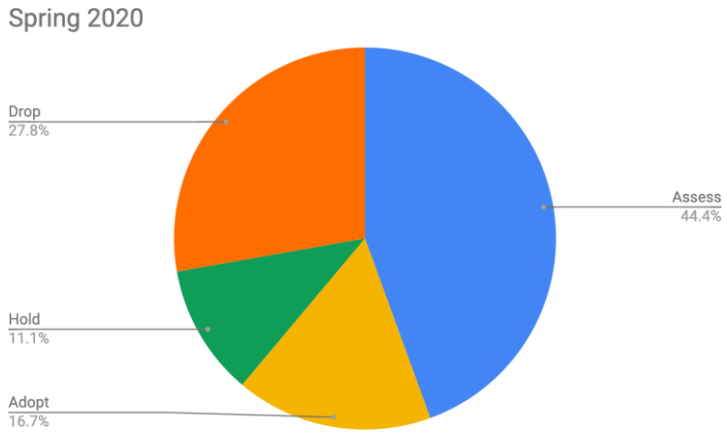

Figure 2: Distribution of projects by lifecycle stage in the "Verification & Assurance" sector – Spring 2020

While still one of the smallest sectors in Spring 2020, Verification and Assurance have maintained a steady amount of project "supply" to progress through this sector.
Interestingly enough, contrary to the uncharacteristic jump in projects in the "Secure Systems and Technology" sector, this sector sees a stable level of projects. While a significant amount of projects were dropped after the Autumn 2018 radar (a concern expressed in [1]) this sector presents a similar wave pattern of influx and outflux in projects across the board.
While in 2018 many projects (and with them their results) were close to obsolescence and have since been obsolete, a new wave of projects in this area are looking at cryptographic opportunities and weaknesses e.g. in the quantum cryptography domain: Nearly half of the projects (8) in this sector are still (very) active, and a sixth (3) are ready for adoption. Of these, one stands out as particularly ready for adoption:

#	Project	Type	TRL	MRL
5	ANASTACIA	RIA	6	3

Table 7: Projects addressing "Verification & Assurance " that are close to or ready for adoption

3.1.3 Operational Risk, Management and Analytics

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	6	3	2	6	3	20
Spring 2019	10	2	7	5	0	24
Autumn 2019	12	2	6	7	1	28
Spring 2020	12	1	4	7	5	29

Table 8: "Operational Risk, Management and Analytics" overview – Spring 2020

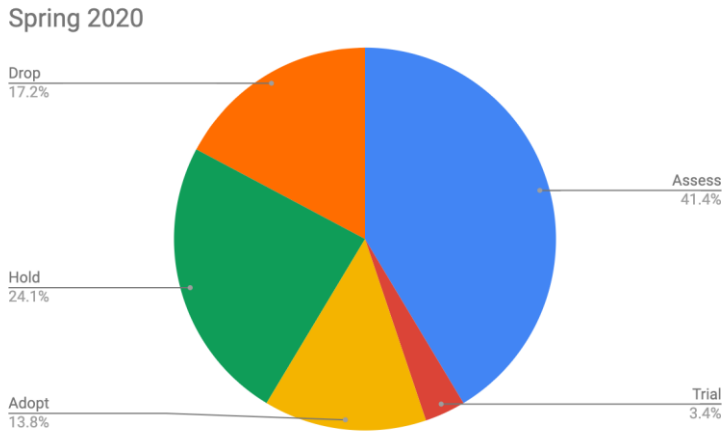

Figure 3: Distribution of projects by lifecycle stage in the "Operational Risk, Management and Analytics" sector – Spring 2020

A pattern similar to that for Secure Systems and Technology appears for Operational Risk, Management and Analytics. We again attribute this to an insufficient dataset at the time of analysis presented in [1].
Reassuringly, a stable pipeline of projects addressing operational risks in the CS & P landscape over the last three Radar raises hopes that in perhaps a year's time, significant advances in reducing operational risks and cybersecurity management will be available.
The heightened attention to cyber-attacks on CIs in the past years may be attributed to this continued supply of projects in this sector.
While there are five projects considered ready for adoption in this sector, we lack information to make a qualified statement about which would be most suitable for immediate adoption.

3.1.4 Identity, Behaviour, Ethics and Privacy

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	4	2	1	6	6	19
Spring 2019	11	2	1	10	0	24
Autumn 2019	8	3	2	9	2	24
Spring 2020	6	2	5	1	10	24

Table 9: "Identity, Behaviour, Ethics and Privacy" overview

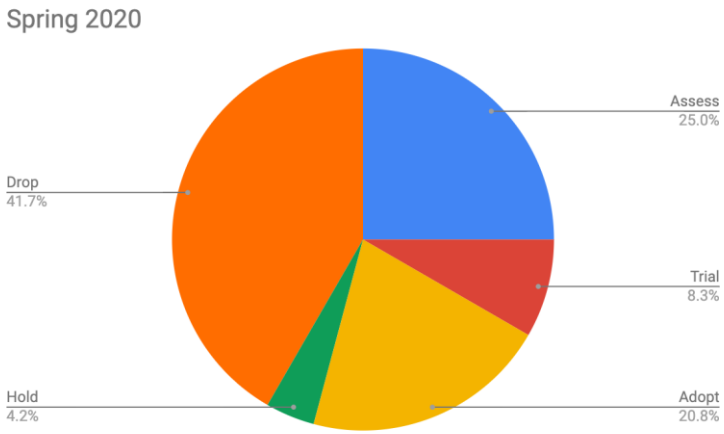

Figure 4: Distribution of projects by lifecycle stage in the "Identity, Ethics, Behaviour and Privacy" sector – Spring 2020

As with other sectors in this Radar, we see a jump in number of projects between the Autumn 2018 and Spring 2019 radar editions. This adds to the evidence of insufficient data for 2018.

However, the main concern identified in 2018 remains, in that this sector appears chronically underfunded even though the number of projects allocated to this sector appears stable. As clearly as for the most popular sector, we see a strong wave of projects about to become obsolete (i.e. dropping off the radar), while the influx of projects is dropping significantly (-50% within a year, from Spring 2019 to Spring 2020).

This is a worry, since analysis of cybersecurity incidents has clearly shown that the human factor appears to be the most significant and impactful factor: Colloquially speaking, the biggest cybersecurity risk sits in front of the computer.

A few projects are available for immediate adoption, but due to insufficient supporting data we cannot make a statement about their suitability.

3.1.5 National & international Security, Privacy and Governance

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	5	4	0	2	1	12
Spring 2019	10	4	1	2	0	17
Autumn 2019	8	2	5	2	0	17
Spring 2020	6	2	6	1	2	17

Table 10: "National & international Security, Privacy and Governance" overview

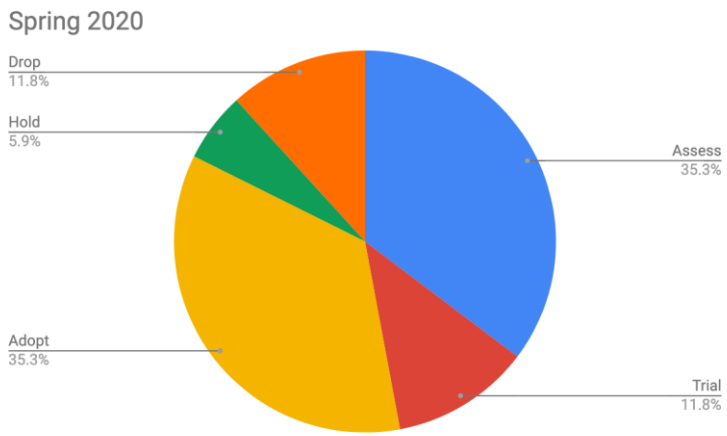

Figure 5: "National & international Security, Privacy and Governance" radar – Spring 2020

Again, more evidence that the data collected for the Autumn 2018 radar was too incomplete.
Differentiating out from the Spring 2019 radar, the figures now show a number of projects available for immediate adoption. While the number of projects in this sector at large remain stable, the drop in project "supply" to the pipeline gives cause for concern where the nature and pattern of cyber-attacks grows beyond company and indeed geographical and political borders. Reduced research and innovation in this sector may pose a threat to maintaining, let alone improving against multi-national and cross-organisational cybersecurity attacks.
One project available for adoption stands out with a remarkably high MTRL score:

#	Project	Type	TRL	MRL
102	PROTECTIVE	IA	7	7

Table 11: Projects addressing "Cybersecurity Governance" close to or ready for adoption

3.1.6 Human Aspects of Cybersecurity

Radar	Assess	Trial	Adopt	Hold	Drop	TOTAL
Autumn 2018	5	0	2	5	8	20
Spring 2019	6	0	5	3	1	15
Autumn 2019	2	5	2	6	1	16
Spring 2020	1	1	5	5	3	15

Table 12: "Human Aspects of Cybersecurity" overview – Spring 2020

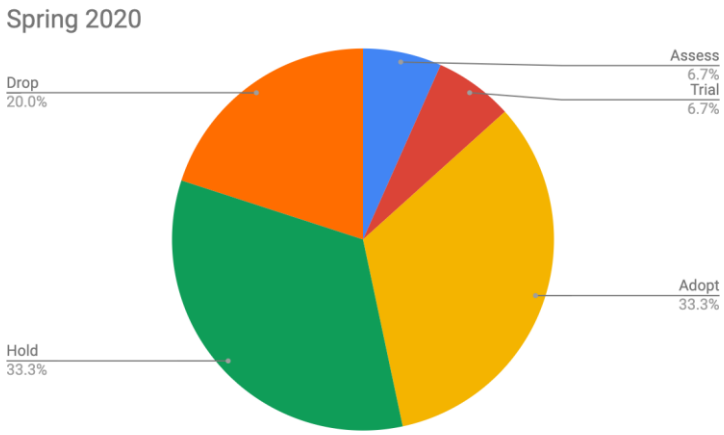

Figure 6: "Human Aspects of Cybersecurity" radar – Spring 2020

This sector is the only sector that presents a drop in number of included projects after the Autumn 2018 collection and analysis. Looking closer at the figures, we conjecture that this discrepancy is not only due to a large number of projects becoming obsolete, but also some projects being mis-classified as "Hold" when in fact they might have been classified as "Drop" in the first place in the Autumn 2018 radar. The reason for this might have been that in 2018, the corresponding assignment was performed manually, while in all other subsequent radars, assignments are calculated automatically.

On the basis of more accurate data, this sector is now the smallest of all six sectors in the radar. While the supply of new projects appeared reassuring one year ago (Spring 2019) it dramatically dropped, with many projects now moving closer to obsolescence, and a peak of 5 projects ready for adoption now.

Given the increasing popularity of social engineering in cybersecurity incidents, it is ever more important to understand and mitigate "the human factor" in any activities in the CS & P landscape. "Human Aspects of Cybersecurity" is the one sector in the radar that most clearly represents fundamental research. Yet, this most fundamental factor of effective cybersecurity appears to be orphaned.

Three out of five projects appear the most promising in terms of immediate adoption:

#	Project	Type	TRL	MRL
35	DECODE	RIA	6	4
52	GHOST	IA	7	6
91	PrEstoCloud	RIA	7	5

Table 13: Projects addressing "Secure Systems and Technology" close to or ready for adoption

3.2 The Autumn 2018 Technology Radar

3.2.1 Statistical analysis of 2 years of Projects Radar data gathering

Radar edition	Secure Systems	Verification & Assurance	Operational Risk	Identity & Privacy	Cybersecurity Governance	Human Aspects	TOTAL
Autumn 2018	47	16	20	19	12	20	134
Spring 2019	80	15	24	24	17	15	175
Autumn 2019	89	17	28	24	17	16	191
Spring 2020	87	18	29	24	17	15	190
Change[2]	7	3	5	0	0	0	15
Growth[3]	9%	20%	21%	0%	0%	0%	9%

Table 14: Distribution of projects per sector across Radars.

Since the first edition of the radar in Autumn 2018, when only one compiled data set was available, we are now in the position to analyse the landscape better, using the full set of four data sets compiled in 6-month cycles (see Table 14).
Looking at the growth of information about projects available to us, the "explosion" of project entries in our database, hence in our radar editions (from 134 in Autumn 2018 to 191 in Spring 2020, a growth of 43%, see Table 15), is a clear sign that in Autumn 2018 the project clearly did have only partial information available for analysis. While this ought to be true still at the time of writing, we expect that the gap between available information and information known to us is much smaller, and now resembles a statistically representative sample of projects in the EU CS & P landscape.

	Secure Systems	Verification & Assurance	Operational Risk	Identity & Privacy	Cybersecurity Governance	Human Aspects	TOTAL
Change	40	2	9	6	5	-5	57
Growth	85%	13%	45%	32%	42%	-25%	43%

Table 15: Growth figures from August 2018 to Spring 2020

The figures presented in Table 15 allows us to analyse the skew of representation in the Autumn 2018 radar.
The overall growth rate of projects in the radar editions is 43%. If the growth rates across all sectors would be equal, then the Autumn 2018 radar would still be a representative visualisation of the landscape. This is not the case though.
Looking at the growth rates for the individual sectors in the radar from Autumn 2018 to Spring 2020, we can state the following:

- Secure Systems was **underrepresented**.
- Verification & Assurance was **overrepresented**.
- Operational Risk was appropriately represented.
- Identity and Privacy was **overrepresented**.
- Cybersecurity Governance was appropriately represented.
- Human Aspects was **overrepresented**.

The impact of this misrepresentation has profound consequences in the analysis and statements made in the predecessor deliverable [1], in particular:

[2] Year on year, from Spring 2019 to Spring 2020

1. The domination of projects in the Secure Systems sector is stronger than initially thought, and the concern of overly focussing on technical solutions becomes even stronger.
2. The stated concern about the loss of representation hence understanding of "the human factor" in cybersecurity and privacy, as indicated by projects addressing Identity and Privacy, and Human Aspects, becomes even more exacerbated given that both sectors were overrepresented in the Autumn 2018 radar, and are in fact relatively speaking considerably smaller than we initially stated.

Looking at the growth figures year on year from Spring 2019 to Spring 2020 (Table 14) we can immediately see much more sustainable growth across the board.
While "Secure System" appears to grow in line with the overall increase in projects (by 9%), "Verification and Assurance" and "Operational Risk" grew disproportionally. This is a good sign in that this appears to reflect the need of much greater formal assurance and cryptographically stronger functions and services, as well as strengthening operational preparedness and management of cybersecurity risks. On the flipside, however, Identity & Privacy, Cybersecurity Governance, and Human Aspects fall behind with no growth at all.
Over the years, the distribution of projects across the six sectors of the radar (ignoring Autumn 2018 as not representative) remains remarkably stable (see Table 16) with three clear clusters of "market share":

1. **Secure Systems**
   Most dominant by far – almost 50% of all projects.
2. **Operational Risk, Identity & Privacy**
   Low interest; about 1/6 each in terms of projects
3. **Verification & Assurance, Cybersecurity Governance, Human Aspects**
   Lowest interest, not even 10% share of each sector across the radars

Radar edition	Secure Systems	Verification & Assurance	Operational Risk	Identity & Privacy	Cybersecurity Governance	Human Aspects	TOTAL
Autumn 2018	35%	12%	15%	14%	9%	15%	100%
Spring 2019	46%	9%	14%	14%	10%	9%	100%
Autumn 2019	47%	9%	15%	13%	9%	8%	100%
Spring 2020	46%	9%	15%	13%	9%	8%	100%
Growth[2]	-	1%	2%	-1%	-1%	-1%	

Table 16: Relative size of sectors per radar.

Radar edition	Secure Systems	Verification & Assurance	Operational Risk	Identity & Privacy	Cybersecurity Governance	Human Aspects	TOTAL
Autumn 2018	43%	8%	16%	11%	7%	14%	100%
Spring 2019	42%	13%	15%	8%	15%	7%	100%
Autumn 2019	46%	13%	14%	7%	13%	6%	100%
Spring 2020	45%	14%	15%	7%	13%	6%	100%
Growth[2]	3%	1%	-	-1%	-2%	-1%	

Table 17: Budget allocation across sectors and radar editions

An interesting pattern emerges, however, when comparing the distribution of projects across sectors throughout the radars (Table 16) with the distribution of project budgets on the same scales, i.e. radar sectors and radar editions as shown in Table 17. Within the margin of error, sectors appear consistently either relatively overfunded, underfunded, or adequately funded:

Overfunded	Adequately funded	Underfunded
Verification & Assurance	Secure Systems	Identity & Privacy
Cybersecurity Governance	Operational Risk	Human Aspects

Table 18: Funding balance across radar sectors – Spring 2020

We conjecture that the reason for this pattern lies in the EU's strategy of funding a several lighthouse projects in the relatively overfunded sectors. These are:

Radar sector	Project	Project budget	Sector budget
Secure Systems	SCOTT	39 M€	387 M€
Verification & Assurance	SECREDAS	51 M€	118 M€
Cybersecurity Governance	CyberSec4Europe	16 M€	109 M€
	SPARTA	16 M€	
	CONCORDIA	16 M€	
	ECHO	16 M€	

Table 19: Lighthouse projects impacting the funding distribution across radar sectors – Spring 2020

The SCOTT project's impact, while clearly a funding outlier within the Secure Systems sector, is mitigated by two factors: i) the size of the Secure Systems sector in the radars, and ii) the large number of SME-Instrument projects conducting feasibility studies in this area, that are short-lived with a budget of 71 k€ each. Both Verification & Assurance, and Cybersecurity Governance, are small sectors where large earmarked funding calls (close to or well above 50%) undoubtedly have a statistical impact.

3.2.2 Overview of the Projects Radar Spring 2020

Figure 7 shows the visual representation of the Spring 2020 edition of the Cyberwatching.eu Projects Radar. What is statistically most evident is reflected here as well, i.e. Secure Systems is by far the most dominant sector, hosting about 50% of all projects that are included in this edition. Compared to that, all other sectors look almost deserted.

All sectors bar one show an assuring pipeline of projects entering at the Assess stage. The exception to this pattern is Human Aspects, which is worrying, and may indicate funding for this fundamental aspect of cybersecurity to dry out soon.

The colour indication for projects show a good response rate for Cyberwatching.eu's efforts in engaging with projects it is supporting; and our strategy of focussing on projects that are still active bears fruit: About half of all projects in the inner three rings

(Assess, Trial, Adopt) have submitted MTRL self-assessments to Cyberwatching.eu Task 2.3.

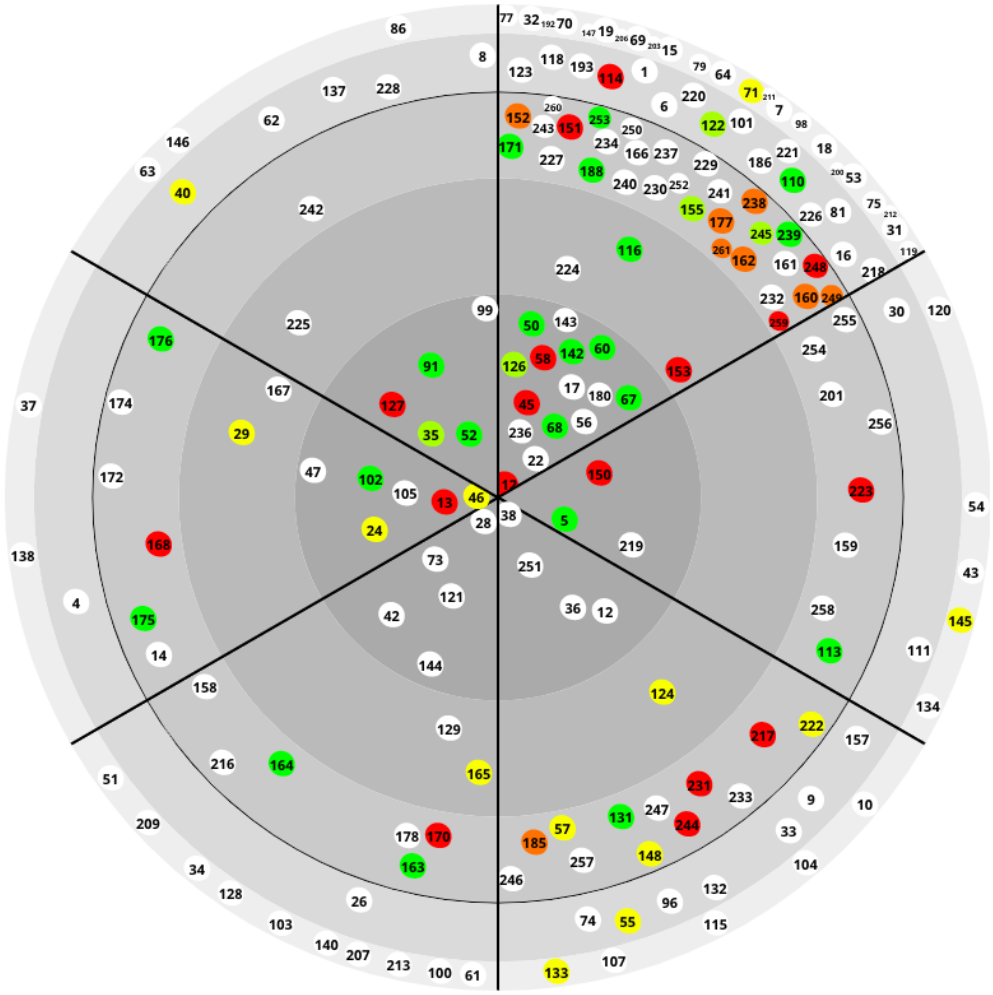

Figure 7: The Spring 2020 CS & P Projects Radar, segments from top right to top left: Secure Systems, Verification & Assurance, Operational Risk, Identity and Privacy, Cybersecurity Governance, Human Aspects

4 Commentary & next steps

Having four Projects Radar editions available for analysis has profoundly changed our perception of the EU CS & P landscape:

Where we considered the Secure Systems sector being overrepresented in Autumn 2018, the situation is in fact worse, given the more complete data available over the last three radar editions (from Spring 2019 to Spring 2020). Now, Secure Systems are the most important aspect for about 50% of all projects in any of the last three Projects Radars.

On the flip side, Human Aspects and Identity & Privacy were in fact overrepresented in Autumn 2018. Hence their actual relative contribution is in fact smaller than thought, something of significant concern.

We do not deny that it is important to research and innovate to provide more secure systems, but is “throwing technology at a social problem” really the best answer that can be found? Given that current threat analysis repeatedly states that social engineering was and still is the most popular attack vector, it begs the question why the two sectors that address this issue directly – Identity & Privacy, and Human Aspects – are not more prominent on the research agenda? How are individuals

supposed to counter or deal with attacks and influencing attempts that employ Deepfakes, Deepfake voice, synthetic identities, and fake news [3]? These are fundamentally social engineering techniques, attempting to make individuals believe in what is conveyed. Once that is achieved, the attack/influence was successful, making further information security and cyber security measures ever more difficult.
We therefore consider that the long-term funding strategy for cybersecurity and privacy should put more focus on Human Aspects, and Identity and Privacy, and less focus on technical solutions addressing the same issue.
Cyberwatching.eu will continue to collect project information from all sources accessible, and further produce editions of Projects Radars. Over the remaining time of the project, at least two more radar editions will be produced (Autumn 2020 and Spring 2021).
A brief simulation of recreating the Autumn 2018 Projects Radar with the current data set shows that it would contain around 70 projects more than when it was created. For consistency and comparison reasons, we kept the Autumn 2018 radar intact. However, given the significantly larger number of projects included in the simulation, we are considering to alter the Autumn 2018 project in our final revision of this deliverable in M48 (D2.7 Final Technology Radar Report).

5 References

1	D2.2 Technology Radar 1st report – Autumn 2018 D Wallom, M Drescher, UOXF, Cyberwatching.eu
2	The European Projects Radar on cyberwatching.eu web site: https://www.cyberwatching.eu/technology-radar
3	Cyberthreat trends: 15 cybersecurity threats for 2020, K Porter: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

6 Appendix 1: EC funded projects reference

The following projects were included and analysed in this deliverable, in alphabetical order:

Project	Call	Type	Start	End
1-SWARM	ICT-01-2019	RIA	Jan 2020	Dec 2022
3ants	SMEInst-13-2016-2017	SME-1	Jul 2017	Dec 2017
5GZORRO	ICT-20-2019-2020	RIA	Nov 2019	Apr 2022
AARC2	EINFRA-22-2016	RIA	May 2017	Apr 2019
ABC4Trust	ICT-2009.1.4	CP	Nov 2010	Feb 2015
ADDPRIV	SEC-2010.6.5-2	CP	Feb 2011	Mar 2014
ADVERSARY	EIC-SMEInst-2018-2020	SME-1	Nov 2018	Feb 2019
AEGIS	DS-05-2016	CSA	May 2017	Apr 2019
AERAS	MSCA-RISE-2019	MSCA-RISE	Dec 2019	Nov 2023
AF-Cyber	MSCA-IF-2016	MSCA-IF-EF-ST	Feb 2018	Jan 2020
ANASTACIA	DS-01-2016	RIA	Jan 2017	Dec 2019
ARIES	FCT-09-2015	RIA	Sep 2016	Feb 2019
ARMOUR	ICT-12-2015	RIA	Feb 2016	Jan 2018
ASAP	ERC-AG-PE6	ERC-AG	Oct 2012	Sep 2018
ASCEMA	SMEInst-01-2016-2017	SME-1	Jun 2016	Nov 2016
ASCLEPIOS	SU-TDS-02-2018	RIA	Dec 2018	Nov 2021
ASTRID	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021
ATENA	DS-03-2015	IA	May 2016	Apr 2019
BEACON	ICT-07-2014	RIA	Feb 2015	Jul 2017
BIOSEC	FP7-PEOPLE-IOF-2008	MC-IOF	Mar 2009	Feb 2012
Blocknetwork	EIC-SMEInst-2018-2020	SME-1	Sep 2018	Feb 2019
BPR4GDPR	H2020-DS-SC7-2017	IA	May 2018	Apr 2021
C3ISP	DS-04-2015	IA	Oct 2016	Sep 2019
C4IIoT	SU-ICT-01-2018	IA	Jun 2019	May 2022
CANVAS	DS-07-2015	CSA	Sep 2016	Aug 2019
CAPITAL	ICT-2013.1.5	CSA	Oct 2013	Sep 2015
CARAMEL	SU-ICT-01-2018	IA	Oct 2019	Mar 2022
CE-IoT	H2020-MSCA-RISE-2017	MSCA-RISE	Jul 2018	Jun 2022
certMILS	DS-01-2016	IA	Jan 2017	Dec 2020
CHINO	SMEInst-13-2016-2017	SME-1	Jan 2017	Jun 2017
CHOReVOLUTION	ICT-09-2014	RIA	Jan 2015	Dec 2017
CIPSEC	DS-03-2015	IA	May 2016	Apr 2019
CITADEL	DS-03-2015	IA	Jun 2016	May 2019
CLARUS	ICT-07-2014	RIA	Jan 2015	Dec 2017
CloudSocket	ICT-07-2014	RIA	Jan 2015	Dec 2017
CloudTeam	ICT-07-2014	IA	Mar 2015	Feb 2017
CLTRe	SMEInst-01-2016-2017	SME-1	Jun 2017	Nov 2017
COCKPITCI	SEC-2011.2.5-1	CP-FP	Jan 2012	Dec 2014
COEMS	ICT-10-2016	RIA	Nov 2016	Oct 2019
COLA	ICT-06-2016	IA	Jan 2017	Jun 2019
COMPACT	DS-02-2016	IA	May 2017	Oct 2019
CONCORDIA	H2020-SU-ICT-2018-2	RIA	Jan 2019	Dec 2022
ConnectProtect	SMEInst-13-2016-2017	SME-1	Jul 2016	Dec 2016
CONSENT	SSH-2009-3.2.1.	CP-FP	May 2010	Apr 2013
CREATE-IoT	H2020-IOT-2016	CSA	Jan 2017	Dec 2019

Project	Call	Type	Start	End
CREDENTIAL	DS-02-2014	IA	Oct 2015	Sep 2018
CRITICAL-CHAINS	SU-DS05-2018-2019	IA	Jul 2019	Jun 2022
CROSSMINER	ICT-10-2016	RIA	Jan 2017	Dec 2019
CryptoCloud	ERC-AG-PE6	ERC-AG	Jun 2014	May 2019
CS-AWARE	DS-02-2016	IA	Sep 2017	Aug 2020
CUREX	SU-TDS-02-2018	RIA	Dec 2018	Nov 2021
CYBECO	DS-04-2016	RIA	May 2017	Apr 2019
CYBECO II	H2020-DS-SC7-2016	RIA	May 2017	Apr 2019
Cyber-MAR	SU-DS01-2018	IA	Sep 2019	Aug 2022
CYBER-TRUST	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021
CYBERCULT	MSCA-IF-2018	MSCA-IF-EF-ST	Jul 2019	Jun 2021
CyberSANE	SU-ICT-01-2018	IA	Sep 2019	Aug 2022
CyberSec4Europe	H2020-SU-ICT-2018-2	RIA	Mar 2019	Jul 2022
CYBERSECURITY	MSCA-IF-2017	MSCA-IF-EF-ST	Aug 2018	Jul 2020
CyberSure	MSCA-RISE-2016	MSCA-RISE	Jan 2017	Dec 2020
cyberwatching.eu	DS-05-2016	CSA	May 2017	Apr 2021
CYBERWISER.EU	H2020-EU.3.7.4	IA	Sep 2018	Feb 2021
CyberWiz	DRS-17-2014	SME-2	Sep 2015	Aug 2017
CYCLONE	ICT-07-2014	IA	Jan 2015	Dec 2017
CYRail	S2R-OC-IP2-01-2015	Shift2Rail-RIA	Oct 2016	Sep 2018
D-FENCE	EIC-SMEInst-2018-2020	SME-1	May 2019	Aug 2019
DAN	EIC-SMEInst-2018-2020	SME-1	Oct 2019	Mar 2020
DAPPER	FP7-PEOPLE-2013-CIG	MC-CIG	Apr 2014	Mar 2018
DECODE	ICT-12-2016	RIA	Dec 2016	Nov 2019
DECODE	H2020-ICT-2016-1	RIA	Dec 2016	Dec 2019
DEFEND	H2020-DS-SC7-2017	IA	Jun 2018	May 2021
DEFENDER	CIP-01-2016-2017	IA	May 2017	Apr 2020
DISCOVERY	ICT-38-2015	CSA	Jan 2016	Dec 2017
DiSIEM	DS-04-2015	IA	Sep 2016	Aug 2019
DITAS	ICT-06-2016	RIA	Jan 2017	Dec 2019
DOGANA	DS-06-2014	IA	Sep 2015	Aug 2018
DOGANA II		IA	Jan 2017	Dec 2019
DSSC	MSCA-COFUND-2016	MSCA-COFUND-DP	May 2017	Apr 2022
e-Sides	ICT-18-2016	CSA	Jan 2017	Dec 2019
ECHO	H2020-SU-ICT-2018-2	RIA	Mar 2019	Feb 2023
ECRYPT-CSA	ICT-32-2014	CSA	Mar 2015	Feb 2018
ECRYPT-NET	MSCA-ITN-2014-ETN	MSCA-ITN-ETN	Mar 2015	Feb 2019
ELIoT Pro	EIC-SMEInst-2018-2020	SME-2	Jun 2018	May 2020
ENACT	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
ENCASE	MSCA-RISE-2015	MSCA-RISE	Jan 2016	Dec 2019
EnergyShield	SU-DS04-2018-2020	IA	Jul 2019	Jun 2022
EU-SEC	DS-01-2016	IA	Jan 2017	Dec 2019
EUNITY	DS-05-2016	CSA	Jun 2017	May 2019
Eye-O-T	SMEInst-13-2016-2017	SME-1	Aug 2016	Dec 2016
FAR-EDGE	H2020-FOF-2016	RIA	Oct 2016	Oct 2019
FeatureCloud	SU-TDS-02-2018	RIA	Jan 2019	Dec 2023
FENTEC	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
FIDELITY	SEC-2011.3.4-1	CP-IP	Feb 2012	Jan 2016
FORESIGHT	SU-DS01-2018	IA	Oct 2019	Sep 2022

Project	Call	Type	Start	End
FORTIKA	DS-02-2016	IA	Jun 2017	May 2020
FUTURE TPM	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
FutureTrust	DS-05-2015	IA	Jun 2016	May 2019
GenoPri	MSCA-IF-2015-EF	MSCA-IF-EF-ST	May 2016	Apr 2018
GHOST	DS-02-2016	IA	May 2017	Apr 2020
GO 4G	SMEInst-13-2016-2017	SME-1	Jul 2017	Dec 2017
GUARD	SU-ICT-01-2018	IA	May 2019	Apr 2022
HEAT	ICT-32-2014	RIA	Jan 2015	Dec 2017
HECTOR	ICT-32-2014	RIA	Mar 2015	Feb 2018
HERMENEUT	DS-04-2016	RIA	May 2017	Apr 2019
HIPS	ERC-CG-2013-PE6	ERC-CG	Oct 2014	Sep 2019
IMPACT	ERC-2013-SyG	ERC-SyG	Feb 2015	Jan 2021
InfraStress	SU-INFRA01-2018-2019-2020	IA	Jun 2019	May 2021
INSPIRE-5Gplus	ICT-20-2019-2020	RIA	Nov 2019	Oct 2022
IPaCSO	ICT-2013.1.5	CSA	Nov 2013	Oct 2015
KONFIDO	DS-03-2016	RIA	Nov 2016	Oct 2019
LAST	ERC-SG-PE6	ERC-SG	Oct 2009	Sep 2014
LIGHTest	DS-05-2015	IA	Sep 2016	Aug 2019
LIMPET	SMEInst-09-2016-2017	SME-1	Feb 2017	Jul 2017
LipVerify	SMEInst-13-2016-2017	SME-1	Jul 2016	Dec 2016
LOCARD	SU-FCT02-2018-2019-2020	RIA	May 2019	Apr 2022
LocationWise	SMEInst-13-2016-2017	SME-1	Mar 2017	Aug 2017
LV-Pri20	MSCA-IF-2014-EF	MSCA-IF-EF-CAR	Jun 2015	Jun 2017
MALAGA	MSCA-IF-2018	MSCA-IF-EF-ST	Sep 2019	Oct 2021
MAMI	ICT-12-2015	RIA	Jan 2016	Jun 2018
MAPPING	SiS.2013.1.2-1	CSA-SA	Mar 2014	Feb 2018
MAS2TERING	ICT-2013.6.1	CP	Sep 2014	Aug 2017
MATTHEW	ICT-2013.1.5	CP	Nov 2013	Oct 2016
MELODIC	ICT-06-2016	RIA	Dec 2016	Nov 2019
mF2C	ICT-06-2016	RIA	Jan 2017	Dec 2019
MH-MD	ICT-18-2016	RIA	Nov 2016	Oct 2019
MIKELANGELO	ICT-07-2014	RIA	Jan 2015	Dec 2017
MITIGATE	DS-06-2014	IA	Sep 2015	Feb 2018
MUSA	ICT-07-2014	RIA	Jan 2015	Dec 2017
NECOMA	ICT-2013.10.1	CP	Jun 2013	Mar 2016
NeCS	MSCA-ITN-2015-ETN	MSCA-ITN-ETN	Sep 2015	Aug 2019
nIoVe	SU-ICT-01-2018	IA	May 2019	Apr 2022
OCGN	MSCA-IF-2015-EF	MSCA-IF-EF-ST	May 2017	Nov 2018
OCRE	H2020-INFRAEOSC-2018-1	RIA	Jan 2019	Dec 2021
OCTAVE	DS-02-2014	IA	Jun 2015	Jul 2017
ODIX 2.0	EIC-SMEInst-2018-2020	SME-2	Jun 2019	Jun 2021
OLYMPUS	H2020-DS-SC7-2017	IA	Sep 2018	Aug 2021
OPENREQ	ICT-10-2016	RIA	Jan 2017	Dec 2019
OPERANDO	DS-01-2014	IA	May 2015	Apr 2018
P5	SEC-2012.2.3-1	CP-FP	Aug 2013	Oct 2016
PaaSword	ICT-07-2014	RIA	Jan 2015	Dec 2017
PACT	SEC-2011.6.5-2	CP-FP	Feb 2012	Jan 2015
PANACEA	H2020-SC1-FA-DTS-2018-1	RIA	Jan 2019	Dec 2021
PANOPTESEC	ICT-2013.1.5	CP	Nov 2013	Oct 2016

Project	Call	Type	Start	End
PANORAMIX	DS-01-2014	IA	Sep 2015	Aug 2018
PAPAYA	H2020-DS-SC7-2017	IA	May 2018	Apr 2021
PARIS	SEC-2012.6.1-2	CP-FP	Jan 2013	Feb 2016
PASS	PEOPLE-2007-4-3.IRG	MC-IRG	Dec 2008	Nov 2012
PATS	SiS-2008-1.2.2.1	CSA-SA	Aug 2009	Mar 2012
PDP4E	H2020-DS-SC7-2017	IA	May 2018	Jan 2021
PerfectDashboard 2.0	SMEInst-13-2016-2017	SME-1	Oct 2016	Dec 2016
PHOENIX	SU-DS04-2018-2020	IA	Sep 2019	Aug 2022
PICOS	ICT-2007.1.4	CP	Feb 2008	Jun 2011
POSEIDON	H2020-DS-SC7-2017	IA	May 2018	Oct 2020
PQCRYPTO	ICT-32-2014	RIA	Mar 2015	Feb 2018
PRACTIS	SiS-2009-1.1.2.1	CP-FP	Jan 2010	Mar 2013
PRECIOSA	ICT-2007.6.2	CP	Mar 2008	Aug 2010
PRESCIENT	SiS-2009-1.1.2.1	CP-FP	Jan 2010	Mar 2013
PreserviX	ICT-37-2014-1	SME-1	May 2015	Oct 2015
PrEstoCloud	ICT-06-2016	RIA	Jan 2017	Dec 2019
PrimeLife	ICT-2007.1.4	CP	Mar 2008	Jun 2011
PRIPARE	ICT-2013.1.5	CSA	Oct 2013	Sep 2015
PRISM	ICT-2007.1.4	CP	Mar 2008	May 2010
PRISM CODE	FP7-PEOPLE-2012-CIG	MC-CIG	Nov 2012	Oct 2016
PRISMACLOUD	ICT-32-2014	RIA	Feb 2015	Jul 2018
PRISMS	SEC-2011.6.5-2	CP-FP	Feb 2012	Jul 2015
PRIVACY FLAG	DS-01-2014	IA	May 2015	Apr 2018
Privacy.Us	MSCA-ITN-2015-ETN	MSCA-ITN-ETN	Dec 2015	Nov 2019
PRIVACY4FORENSICS	FP7-PEOPLE-2013-IIF	MC-IIF	Feb 2015	Mar 2018
PRIVILEDGE	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
ProBOS	SMEInst-13-2016-2017	SME-2	Oct 2016	Sep 2018
PROMETHEUS	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2019
PROOFY	SMEInst-01-2016-2017	SME-1	May 2017	Aug 2017
PROTASIS	H2020-MSCA-RISE-2015	MSCA-RISE	May 2016	Apr 2020
PROTECTIVE	DS-04-2015	IA	Sep 2016	Aug 2019
ProtonSuite	SMEInst-13-2016-2017	SME-1	Dec 2017	Mar 2018
Ps2Share	ICT-35-2016	RIA	Jan 2017	Dec 2017
RADDICS	ERC-2018-COG	ERC-COG	Jan 2019	Dec 2023
RAPID	ICT-07-2014	RIA	Jan 2015	Dec 2017
REACT	H2020-DS-SC7-2017	RIA	Jun 2018	May 2021
REASSURE	DS-01-2016	RIA	Jan 2017	Dec 2019
ReCRED	DS-02-2014	IA	May 2015	Apr 2018
REDSENTRY	H2020-SMEINST-1-2016-2017	SME-1	Jul 2017	Dec 2017
RESISTO	CIP-01-2016-2017	IA	May 2018	Apr 2021
RESPECT	SEC-2011.6.1-5	CP-FP	Feb 2012	May 2015
REVEN-X1	ICT-37-2015-1	SME-1	Jul 2015	Dec 2015
RPS	SMEInst-10-2016-2017	SME-1	Jan 2018	May 2018
SAFECARE	CIP-01-2016-2017	IA	Sep 2018	Aug 2021
SafeCloud	DS-01-2014	IA	Sep 2015	Aug 2018
SAFEcrypto	ICT-32-2014	RIA	Jan 2015	Dec 2018
SAFERtec	DS-01-2016	RIA	Jan 2017	Dec 2019
SAFETY 4.0	SMEInst-02-2016-2017	SME-1	Aug 2017	Nov 2017
SAINT	DS-04-2016	RIA	Mar 2017	Feb 2021

Project	Call	Type	Start	End
SamurAI	EIC-SMEInst-2018-2020	SME-1	May 2019	Aug 2019
SAPPAN	H2020-SU-ICT-2018	IA	May 2019	Apr 2022
SAURON	CIP-01-2016-2017	IA	May 2017	Apr 2019
SAWSOC	FP7-SEC-2012-1	CP-FP	Nov 2013	Apr 2016
SCISSOR	ICT-32-2014	RIA	Jan 2015	Dec 2017
SCOTT	ECSEL-2016-2-IA-two-stage	IA	May 2017	Jun 2020
SCR	SMEInst-13-2016-2017	SME-1	Jul 2016	Dec 2016
SealedGRID	H2020-MSCA-RISE-2017	MSCA-RISE	Jan 2018	Dec 2021
SecIoT	INNOSUP-02-2016	CSA	Sep 2017	Aug 2018
SECONDO	MSCA-RISE-2018	MSCA-RISE	Jan 2019	Dec 2022
SECREDAS	ECSEL-2017-2	ECSEL-RIA	May 2018	Apr 2021
SecureCloud	EUB-1-2015	RIA	Jan 2016	Dec 2018
SecureHospitals.eu	SU-TDS-03-2018	CSA	Dec 2018	Jan 2021
SecureIoT	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
SEMIoTICS	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
SERECA	ICT-07-2014	RIA	Mar 2015	Feb 2018
SERENITI	FP7-PEOPLE-2013-CIG	MC-CIG	Mar 2014	Feb 2018
SerIoT	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
SERUMS	SU-TDS-02-2018	RIA	Jan 2019	Dec 2021
SHARCS	ICT-32-2014	RIA	Jan 2015	Dec 2017
SHIELD	DS-04-2015	IA	Sep 2016	Feb 2019
SHiELD (Health)	DS-03-2016	RIA	Jan 2017	Dec 2019
SIGAGuard	SMEInst-13-2016-2017	SME-1	Apr 2018	Jul 2018
SISSDEN	DS-04-2015	IA	May 2016	Apr 2019
SMESEC	DS-02-2016	IA	Jun 2017	May 2020
SMOOTH	H2020-DS-SC7-2017	IA	May 2018	Oct 2020
SocialPrivacy	FP7-PEOPLE-2011-IOF	MC-IOF	Sep 2012	Aug 2015
SODA	ICT-18-2016	RIA	Jan 2017	Dec 2019
SOFIE	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
SOTER	SU-DS05-2018-2019	IA	Jul 2019	Oct 2021
SPARTA	H2020-SU-ICT-2018-2	RIA	Feb 2019	Jan 2022
SPEAR	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021
SPECIAL	ICT-18-2016	RIA	Jan 2017	Dec 2019
SPECS	FP7-ICT-2013-10	CP	Nov 2013	Apr 2016
SpeechXRays	DS-02-2014	IA	May 2015	Apr 2018
SPHINX	SU-TDS-02-2018	RIA	Jan 2019	Dec 2021
SPIDER	SU-DS01-2018	IA	Jul 2019	Jun 2022
SPOOC	ERC-CoG-2014	ERC-COG	Sep 2015	Aug 2020
STAMP	ICT-10-2016	RIA	Dec 2016	Nov 2019
STOP-IT	CIP-01-2016-2017	IA	Jun 2017	May 2021
STORM	EE-13-2014	RIA	Mar 2015	Aug 2018
SUNFISH	ICT-07-2014	RIA	Jan 2015	Dec 2017
SUPERCLOUD	ICT-07-2014	RIA	Feb 2015	Jan 2018
SurPRISE	SEC-2011.6.5-2	CP-FP	Feb 2012	Jan 2015
SWITCH	H2020-ICT-2014-1	RIA	Feb 2015	Jan 2018
symbIoTe	H2020-ICT-2015	RIA	Jan 2016	Dec 2018
SysSec	ICT-2009.1.4	NoE	Sep 2010	Nov 2014
TFence	SMEInst-13-2016-2017	SME-1	Aug 2017	Nov 2017
THREAT-ARREST	H2020-DS-SC7-2017	IA	Sep 2018	Aug 2021

Project	Call	Type	Start	End
ThreatMark	SMEInst-13-2016-2017	SME-1	Aug 2016	Nov 2016
TOREADOR	ICT-16-2015	RIA	Jan 2016	Dec 2018
TREDISEC	ICT-32-2014	RIA	Apr 2015	Mar 2018
TRINITY	DT-ICT-02-2018	IA	Jan 2019	Dec 2022
TrueProactive	EIC-SMEInst-2018-2020	SME-1	May 2018	Aug 2018
TRUESSEC.EU	DS-01-2016	CSA	Jan 2017	Dec 2018
TYPES	DS-01-2014	IA	May 2015	Oct 2017
U2PIA	SMEInst-13-2016-2017	SME-1	Nov 2016	Mar 2017
UltraFiBi	SMEInst-13-2016-2017	SME-1	Oct 2017	Mar 2018
UNFRAUD	SMEInst-13-2016-2017	SME-1	Jun 2017	Sep 2017
UNICORN	ICT-06-2016	IA	Jan 2017	Dec 2019
UP2DATE	ICT-01-2019	RIA	Jan 2020	Dec 2022
V-SPHERE	SMEInst-13-2016-2017	SME-1	Feb 2018	May 2018
vACCINE	JTI-CS2-2018-CfP09-SYS-01-11	CS2-IA	Oct 2019	Sep 2021
VESSEDIA	DS-01-2016	RIA	Jan 2017	Dec 2019
VIRT-EU	ICT-35-2016	RIA	Jan 2017	Dec 2019
VisiOn	DS-01-2014	IA	Jul 2015	Jun 2017
WISER	DS-06-2014	IA	Jun 2015	Nov 2017
WITDOM	ICT-32-2014	RIA	Jan 2015	Dec 2017
YAKSHA	H2020-ICT-2017-1	IA	Jan 2018	Jun 2020