D2.4 - Statistical analysis of the Cybersecurity and Privacy ecosystem

Author(s)	M. Drescher & D. Wallom, UOXF
Status	Final
Version	vFinal
Date	22 10/2019

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:

This deliverable offers an analysis of the landscape of EU funded projects in the Cybersecurity and Privacy research community using well-known statistical analysis methodologies. It compares the results for a full set of projects funded in the past with a subset of projects that at the time of writing are still active. The results are then condensed into a proposed clustering of active projects Cyberwatching.eu may further engage with in more tailored and focused communication.

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	**30/06/2019**
Actual submission date	**22/10/2019**
Reviewed by	**M Ramirez, AEI** **M Miller, Conceptivity** **N Ferguson, Trust-IT**
Start date of Project	**01/05/2017**
Duration	**48 months**

Revision history

Version	Date	Authors	Notes
v0.1	10 Oct 2019	M Drescher & D Wallom (UOXF)	Final draft
v0.2	10 Oct 2019	M Ramírez (AEI)	Internal review 1
v0.3	10 Oct 2019	M Miller (Conceptivity)	Internal review 2
v0.4	11 Oct 2019	M Drescher (UOXF)	Final document
v0.5	16 Oct 2019	N Ferguson (TRUST)	Internal review 3
vFinal	16 Oct 2019	M Drescher & D Wallom (UOXF)	Final version

Executive Summary

With more than 170 projects funded by the European Commission over the course of the FP7 and Horizon 2020 framework programmes in the cybersecurity and privacy sector over the course of a decade, it becomes increasingly challenging to maintain oversight of the state of play, and the landscape at large.

The Cyberwatching.eu project has been funded to "become *the* European observatory of research and innovation in the field of cybersecurity and privacy", to support the EU and Member States funded projects to meet, discover, and collaborate.

Among several tools and platforms is a statistical analysis of existing projects against an established taxonomy of terms that can help categorising and classifying projects with similar interests: What may be feasible to manually produce for a few tens of projects very quickly becomes an impossible task for a few hundred projects.

This deliverable continues the work done previously in a different domain. During the EC funded CloudWATCH2 project (grant agreement no. 644748) the statistical analysis was applied to a set of projects working in the domain of cloud computing, and project affinity was tested on the set of characteristics defined in a draft version of the NIST Definition of Cloud Computing (now ISO/IEC 17788). The results were also published as a scientific paper (Springer, OID 10.1186/s13677-017-0084-1).

In this deliverable, we apply the same methodology (commonly known as Principle Component Analysis, or PCA) to the landscape of EC funded cybersecurity and privacy projects. The deliverable compares the results of an analysis of all 177 EC funded projects (known to us at the time of writing) with the results of the subset of all projects that are still active.

Based on the analysis this deliverable suggests a set of clusters of active projects that, when engaged and supported, have a reasonable chance of building momentum and collaboration with measurable synergies.

Table of Contents

1 Introduction 5

2 Quantitative dimensions & clustering methodology 6

3 The analysed projects 8

4 The Landscape of Cybersecurity & Privacy Research 10

5 Commentary & next steps 14

5.1 Clustering projects 14

6 Appendix 1: EC funded projects reference 18

LIST OF FIGURES

Figure 1 Overview of the number of projects in the repository that have finished. For year 2019, 31 more will finish between the time of analysis and the end of the year.. 9
Figure 2 Biplot of all 177 EU funded projects (right) and biplot of still active projects (left) 10
Figure 3 Hierarchical dendrogram of all 177 projects (left) and hierarchical dendogram of all still active projects (right) 12
Figure 4 Cluster tree of still active projects in a 2-dimensional representation. 13

LIST OF TABLES

Table 1: The Cyberwatching.eu two-tier taxonomy 6
Table 2: Snapshot of first-level classification of EC funded projects against the taxonomy 6
Table 3: Snapshot of the second-level clustering 7
Table 4: Numerical transformation of ranking of the cybersecurity and privacy taxonomy 7
Table 5: The project ranking matrix in its final form for PCA consumption 8

1 Introduction

Cyberwatching.eu's mission is to "become *the* European observatory of research and innovation in the field of cybersecurity and privacy". Part of this mission is to create mechanisms and tools by which the EC and member states supported projects can come together to share outputs, methods and best practices.

One specific tool to enable projects in that way is a clustering methodology based on statistical analysis of commonalities and differences based on ordinal assessment data gathered on projects by Cyberwatching.eu. The generally accepted statistical analysis used for this report is called Principal Component Analysis. It is widely used in similar problem areas.

A detailed description of the methodology was published in the Journal of Cloud Computing in 2017[1] as part of the EC funded CloudWATCH project (grant agreement no. 610994) and will therefore not be described here.

The analysis was successfully applied numerous times in the CloudWATCH and CloudWATCH2 projects, and again in Cyberwatching.eu as illustrated in the first project review.

Finding commonalities in multi-dimensional ordinal assessment data of projects is difficult. Weighing these commonalities and discovering stable statistical correlations is even more difficult; PCA and associated methodologies as described in the academic paper referenced above are the right tools to discover these correlations in the data.

In the context of this project, the aim is to provide funded projects with an easy to understand means by which those with overlapping interests should easily find:

a) Ongoing Projects to collaborate with, and
b) Peruse outputs and results of projects in past funding cycles that share the same commonalities

The value of offering this work to funded projects is twofold:

a) Using the results as intended by Cyberwatching.eu – primarily saving time and resources on their own budget
b) Ingest and accept the work Cyberwatching.eu is doing as part of a 360 degree review of their own work and impact, along regular EC project reviews, external feedback and other chosen means of measuring or quantifying their project's impact on the wider community.

[1] https://link.springer.com/article/10.1186/s13677-017-0084-1

2 Quantitative dimensions & clustering methodology

Cyberwatching.eu uses a two-tier "Cybersecurity and privacy research taxonomy" (see Cyberwatching.eu deliverable "D2.1 A Taxonomy of Cybersecurity and Privacy to assess the coverage of developed landscape by EC and nationally funded projects"[2]) throughout its project work.

This taxonomy comprises of three level-1 areas. Each of these are then further refined in level 2, as follows:

Taxonomy Level 1	Taxonomy Level 2 terms
Foundations of technology & risk management	Operational Risk and Analytics
	Verification & Assurance
Applications & user-oriented services	Secure Systems and Technology
	Identity, Behaviour, Ethics and Privacy
Governance, Ethics and Trust	National & international security and governance
	Human Aspects of Cybersecurity

Table 1: The Cyberwatching.eu two-tier taxonomy

EC funded projects undergo a two-tier assessment against this taxonomy:

First, projects are *classified* against the taxonomy's first level.

This classification ranks each level 1 term in order of importance and applicability to the classified project. It is important to note that the ranking is incomplete by design, in that for some projects, not all level 1 taxonomy terms are in scope.

Therefore, while some projects may be classified in all three level 1 terms, most projects in fact are not.

As a result, for each project, insofar as within scope of this activity an ordered list of ranks of taxonomy terms exists, named "rank 1", "rank 2" and "rank 3" with each project having a level 1 taxonomy term at rank 1, and some having a second ranked term, and even fewer having all level 1 taxonomy terms ranked.

#	EC Project name	Rank 1	Rank 2	Rank 3
1	AARC2	Apps & user oriented services		
2	ABC4Trust	Apps & user oriented services	Governance, Ethics, Trust	
3	ADDPRIV	Found. of tech & risk management	Governance, Ethics, Trust	
4	AEGIS	Governance, Ethics, Trust		
5	ANASTACIA	Found. of tech & risk management	Apps & user oriented services	Governance, Ethics, Trust

Table 2: Snapshot of first-level classification of EC funded projects against the taxonomy

[2] https://www.cyberwatching.eu/d21-cybersecurity-and-privacy-ecosystem-model-report-taxonomy-cybersecurity-and-privacy-assess-coverage-developed-landscape-ec-and-nationally-funded-projects

Some projects were out of scope as none of the taxonomy terms would apply, and thus were removed from any further analysis.

Projects are then *clustered* according to the taxonomy's second level.

This subsequent clustering respects the results of the project classification conducted in the first step: Since the taxonomy is hierarchical and orthogonal, a different and independent ranking of second-level terms would violate the structure of the hierarchy.

Therefore, clustering on level 2 obeys the ranking of level 1 terms: For any given level 1 term ranked highest in step 1, only its corresponding level 2 terms may appear as first (on "rank 1.a") or second (in rank 1.b) in rank in the level 2 clustering.

Similarly, the clustering is incomplete: While for some projects both level 2 terms apply, for others only one applies. The resulting matrix of level 2 rankings may thus have "holes" where a respective level 2 taxonomy term would not apply, anywhere from rank 1.b to rank 3.a for the respective projects, as shown in the example in Table 3.

#	EC Project name	Rank 1.a	Rank 1.b	Rank 2.a	Rank 2.b	Rank 3.a	Rank 3.b
1	AARC2	Secure Systems	Identity & Privacy				
2	ABC4Trust	Secure Systems	Identity & Privacy	Cybersecurity Governance			
3	ADDPRIV	Verification & Assurance		Cybersecurity Governance	Human Aspects		
4	AEGIS	Cybersecurity Governance					
5	ANASTACIA	Verification & Assurance	Operational Risk	Secure Systems		Cybersecurity Governance	

Table 3: Snapshot of the second-level clustering

Normalisation of the results

This matrix result from the second step above is then normalised in a two-step process so that it is suitable for statistical analysis: The matrix resulting from step two above is a position-oriented ranking matrix, which is suitable for human consumption. To process this in a statistical manner, it needs to be transformed into a score-based ranking matrix (see Table 4). This is done in a two-step process as follows.

First, the initial ranking matrix A from step two is transformed into a matrix B with the level 2 taxonomy terms as fixed column names and project results organised in rows. The position of a taxonomy term in matrix A is reflected as a numerical value in the corresponding column in matrix B.

#	EC Project name	Secure systems	Identity & Privacy	Operational Risk	Verification & Assurance	Cybersecurity governance	Human Aspects
1	AARC2	1	2	0	0	0	0
2	ABC4Trust	1	2	0	0	3	0
3	ADDPRIV	0	0	0	1	3	4
4	AEGIS	0	0	0	0	1	0
5	ANASTACIA	3	0	2	1	5	0

Table 4: Numerical transformation of ranking of the cybersecurity and privacy taxonomy

Up to this point, this work is performed manually (supported by functions) in a spreadsheet. The data from the step above is transferred into a Matlab 2019a script, which further transforms this data into a PCA compatible matrix C by translating the rank numerical value into an importance value: A high rank indicated by a low number is consistently turned into a high importance value: Ranks 1 – 6 are consequently translated into importance values 6 – 1, with zero indicating the taxonomy term being not applicable at all, as given in **Error! Reference source not found.**.

#	EC Project name	Secure systems	Identity & Privacy	Operational Risk	Verification & Assurance	Cybersecurity governance	Human Aspects
1	AARC2	6	5	0	0	0	0
2	ABC4Trust	6	5	0	0	4	0
3	ADDPRIV	0	0	0	6	5	4
4	AEGIS	0	0	0	0	6	0
5	ANASTACIA	4	0	5	6	3	0

Table 5: The project ranking matrix in its final form for PCA consumption

3 The analysed projects

At the time of writing, 177 projects have been registered in the repository. The full list of projects can be found in Appendix 1.

Of these, 110 projects (62%) ended before 1 August 2019; the projects most recently started are ECHO and CyberSec4Europe (March 2019, call H2020-SU-ICT-2018-2). However, we believe that projects that have already finished still provide value in their legacy. We therefore will present two statistical analyses over all 177 projects in our registry, and the 67 projects (38%) that are still active.

This serves two purposes: To find out which projects may be still of value for an ongoing project (e.g. to find some legacy information) one would look at the analysis over all 177 projects. But to explore and find potential collaboration partner projects, one would better examine the analysis over the still active projects.

Arguably, very old projects might skew the result of the analysis. However, the vast majority (ca 75%, 79 projects) finished within the last two years (i.e. in 2017 or later), and only a quarter (31) finished in the years before. These figures become even more pronounced at the end of 2019 when an additional 31 projects will have finished – 20 projects will finish at the end of December 2019 alone.

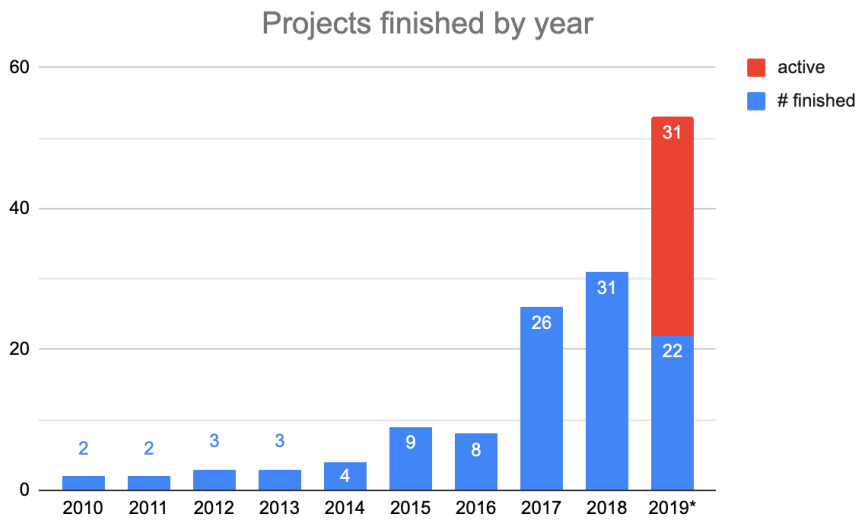

Figure 1 Overview of the number of projects in the repository that have finished. For year 2019, 31 more will finish between the time of analysis and the end of the year

4 The Landscape of Cybersecurity & Privacy Research

Understanding and interpreting the results of the multivariate analysis of the EU cybersecurity and privacy research landscape requires a reduction of dimensions involved – in this case six, stemming from the second level of the Cyberwatching.eu taxonomy – to a meaningful set of two dimensions (perhaps three) that can be visualised for further analysis.

The result of this first analysis are the two biplots presented below; these are presenting the mapping of the six-dimensional full landscape onto a two-dimensional representation respectively.

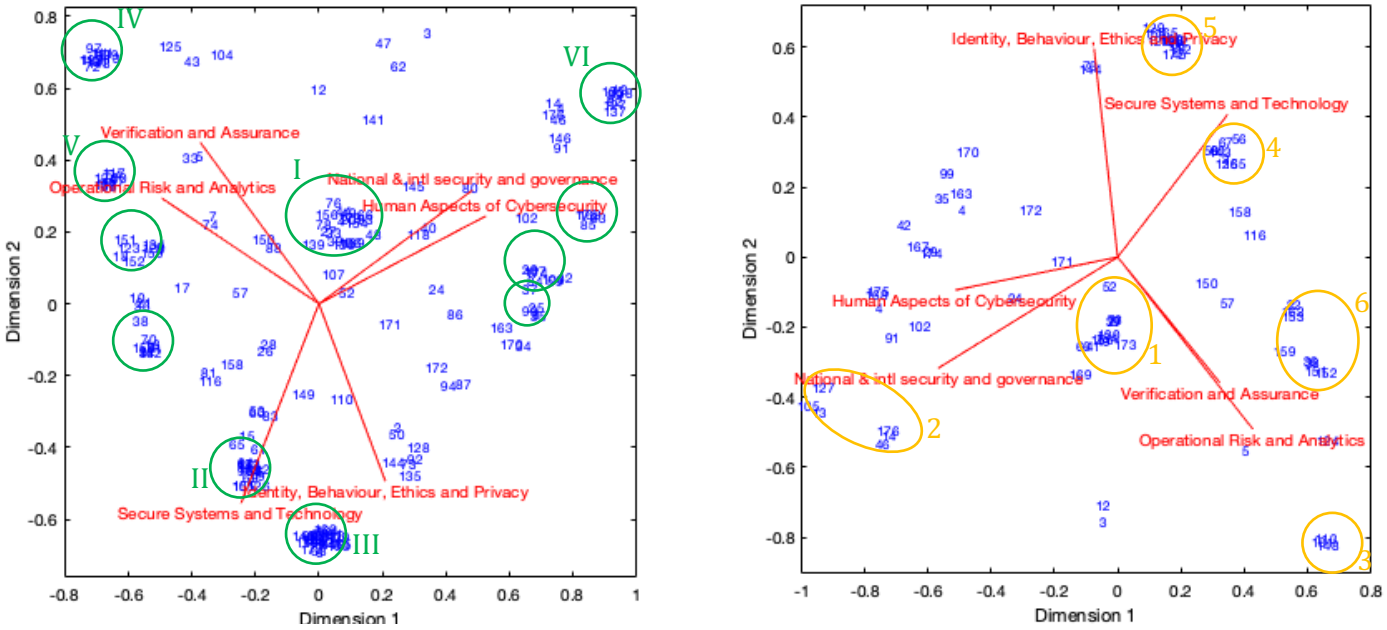

Figure 2 Biplot of all 177 EU funded projects (right) and biplot of still active projects (left)

Across all 177 projects, "Verification and Assurance", and "Secure Systems and Technology" appear to be the two dominating factors, albeit very weak. However, there are no weakly or non-contributing factors as all six taxonomy terms are near equally strong in their influence. This appears largely driven by a number of clearly identifiable clusters of closely correlated projects on the edge of the cloud of projects (see small green circles in Figure 2). This is complemented by a comparatively large but loosely coupled cluster (cluster I) of projects close to the centre of the biplot (see large circle) representing cross-cutting projects, often related to international collaboration (e.g. projects 139, 48, 78, 76 or 150).

The biplot demonstrates a stable correlation of cybersecurity aspects across the different project. These correlation groups are:

1. Operational Risk and Analysis, and
   Verification and Assurance;
2. National & int'l security and governance, and
   Human Aspects of Cybersecurity

3. Secure Systems and Technology, and
   Identity, Behaviour, Ethics and Privacy

These are driven by a number of very strong clusters of projects:

- One cluster (II) almost exclusively driving “Secure Systems and Technology”
- Very strong cluster III covering both "Secure Systems and Technology” and “Identity, Behaviour, Ethics and Privacy”
- Cluster IV driving “Verification and Assurance”
- “Operational Risk and Analytics driven by cluster V
- “National & int’l security and governance” driven by cluster VI

All three correlation groups appear orthogonal to each other without any direct antagonists, except when looking at individual aspects:

- “Verification and Assurance” and
  “Identity, Behaviour, Ethics and Privacy”, and
- “Secure Systems and Technology” and “National & int’l security and governance”

This is not to say that these aspects are antagonists in practice, it simply states that both aspects appear not to be included as research and innovation topics in the same project.

Looking at the biplot for the still active projects (see Figure 3, the landscape appears similar, yet carrying significant differences. Instead of two there are three aspects more significantly contributing to the project landscape:

- Operational Risk and Analytics
- National & int’l security and governance
- Identity, Behaviour, Ethics and Privacy

The weakest drivers of project scope are

- Verification and Assurance, and
- Human Aspects of Cybersecurity

The correlations between aspects of the cybersecurity and privacy taxonomy terms are maintained, albeit in a slightly different setup:

“Verification and Assurance” and “Operational Risk and Analytics” are virtually inseparable elements of projects, with “Operational Risk and Analytics” being the dominant factor. This is largely driven by cluster 3 and to some extend also cluster 6.

“Secure Systems and Technology” and “Identity, Behaviour, Ethics and Privacy” maintain a loose correlation. A similar setup of clusters (clusters 4 and 5) of still active projects maintains this correlation established by clusters II and III respectively, albeit naturally in smaller numbers.

"National & int'l security and governance", and "Human Aspects of Cybersecurity" show a much looser correlation that before with only cluster 2 contributing mostly to "National & int'l security and governance".

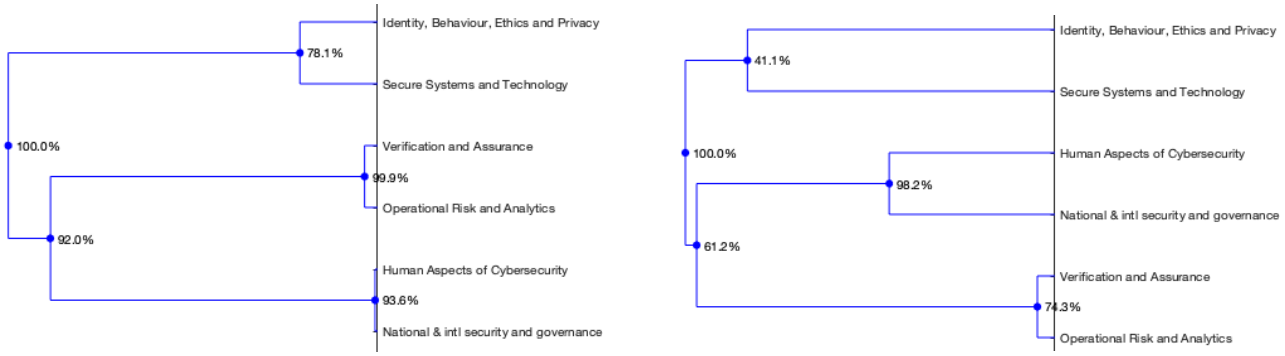

Figure 3 Hierarchical dendrogram of all 177 projects (left) and hierarchical dendogram of all still active projects (right)

Both dendrograms for all 177 projects (Figure 4), and the still active projects (Figure 5) support the observations of correlation between individual aspects of cybersecurity and privacy research in the EU.

However, the very high correlation factors (>> 50%) for each of the three correlation groups across all 177 projects (Figure 4) indicate almost no degree of freedom in the selection of topics chosen when proposing a project. This is compounded by the very high correlation factor (>> 50%) across correlation groups 1 and 2.

Looking at still active projects, the correlation factors are overall less but still significant in their trend: The correlation groups remain intact with significant correlation factors (98% and 74%, respectively) with the exception for group 3 where the correlation factor drops from nearly 80% to just about 41%.

Although much less than across all 177 projects (at 92%) six out of 10 of all active projects appear to combine either "Identity, Behaviour, Ethics and Privacy" or "Secure Systems and Technology" with a mix of topics from correlation groups 1 and 2.

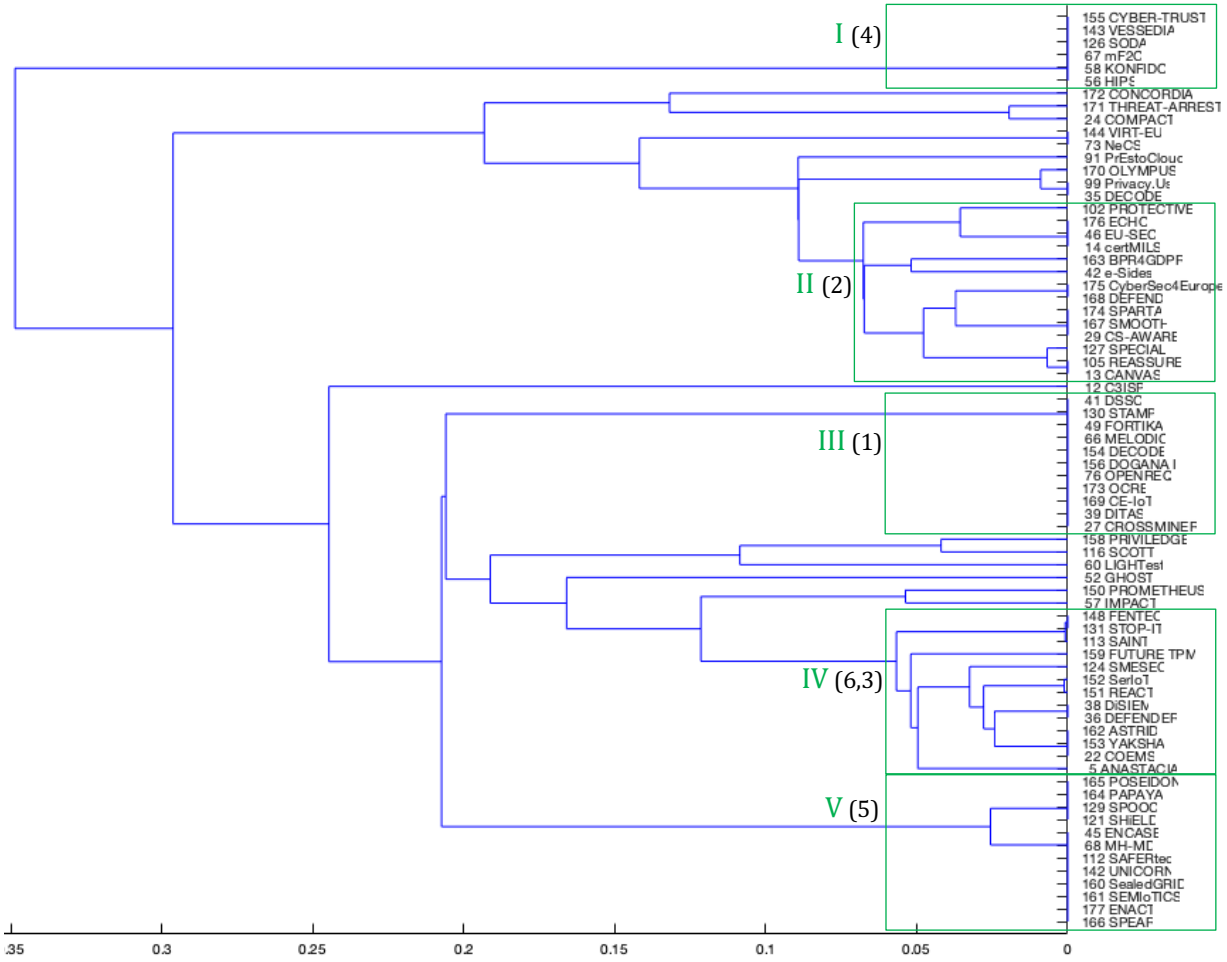

Figure 4 Cluster tree of still active projects in a 2-dimensional representation.

The cluster tree for the still active projects (see Figure 6 above) suggests a partitioning of the still active projects into five distinct clusters. Cross-checking with the corresponding biplot (Figure 2), both results are consistent in that the clusters identified in the cluster tree largely map the clusters identified in the biplot: The foot indexes of the cluster ids in Figure 6 indicate the biplot cluster(s) that map into it.

5 Commentary & next steps

The most obvious result of this landscape analysis is the confirmation of the hierarchical nature the Cyberwatching.eu two-tier taxonomy for research in cybersecurity and privacy, consistent across the two different analysis approaches.

However, one difference stands out when comparing the result across all 177 projects with the results for the still running projects is that there are differentiating degrees of freedom in recent projects when compared to all projects. We see two possible explanations for this:

a) projects may in the past have attempted to cover as many aspects as possible, to be as attractive as possible for funding grants, or
b) The definition and semantics of the Cyberwatching taxonomy differs from that used in the past.

The landscape for more recent projects displays two significant degrees of freedom. Projects appear to have a more matured differentiation between the technical aspects of cybersecurity (secure systems, and privacy), and the other aspects that can largely be described as policy (Human Aspects, National and international governance) and procedural (Operational Risk and Analytics, and Verification and Assurance).

Privacy and secure technical systems are much less often combined into project proposals (correlation factor 40%), and in about half the time (correlation factor 61%) combined with either policy or procedural aspects of cybersecurity.

This indicates that projects are much more focused in their scope, picking only those topics that are really relevant to the problem they set out to solve.

The strong correlation of level-two terms of the taxonomy is directly reflected in the biplots for all 177 projects, and the still active projects. Rotating the biplot in Figure 2 by approximately 180 degree and comparing it with the biplot in Figure 3 shows the same fundamental layout of principal components and their orientation to each other. This means that over time, the intrinsic correlation of cybersecurity aspects remained the same. This is supported by a significantly larger cluster of projects at the centre of the biplot in Figure 2 than in Figure 3. This is not a problem as we expect there to always be cross-cutting projects covering a large number if not all cybersecurity and privacy research topics.

However, this suggests that conjecture (b) above appears untrue, and that indeed projects have increased their focus and overall sharper positioning – perhaps as a response to tighter project application rules deployed by the Commission over the time: All 177 projects span both FP7 and Horizon 2020, whereas the second analysis of still active projects naturally focuses on projects from the Horizon 2020 programme only.

5.1 Clustering projects

One outcome of this landscape analysis is to find ways to cluster still active projects with similar aims for their mutual benefit, and to support these with targeted support activities (webinars, deep dives, focus events, etc) in the future.

Figure 6 indicates five clusters that we have identified that warrant further focus and support. These clusters are:

Cluster I (6 members):
Strong focus on securing technology and IT systems. Very technical projects.

- 56 HIPS

- 58 KONFIDO
- 67 mF2C
- 126 SODA
- 143 VESSEDIA
- 155 CYBER-TRUST

Cluster II (14 members):
Largely driven by (inter-)national policy, certification and intergovernmental collaboration.

- 13 CANVAS
- 14 certMILS
- 29 CS-AWARE
- 42 e-Sides
- 46 EU-SEC
- 102 PROTECTIVE
- 105 REASSURE
- 127 SPECIAL
- 163 BPR4GDPR
- 167 SMOOTH
- 168 DEFEND
- 174 SPARTA
- 175 CyberSec4Europe
- 176 ECHO

Cluster III (11 members):
Largely cross-cutting projects covering many if not all aspects. Might be difficult to support with activities with a strong focus.

- 27 CROSSMINER
- 39 DITAS
- 41 DSSO
- 49 FORTIKA
- 66 MELODIC
- 76 OPENREQ
- 130 STAMP
- 154 DECODE
- 156 DOGANA
- 169 CE-IoT
- 173 OCRE

Cluster IV (13 members):
Strong focus on securing operations of existing systems (e.g. intrusion detection, forensics, etc.)

- 5 ANASTACIA
- 22 COEMS
- 36 DEFENDER
- 38 DiSIEM
- 113 SAINT
- 124 SMESEC
- 131 STOP-IT
- 148 FENTEC
- 151 REACT
- 152 SerIoT
- 153 YAKSHA
- 159 FUTURE TPM
- 162 ASTRID

Cluster V (12 members):
Strong focus on privacy. With the GDPR now in force a very popular topic.

- 45 ENCASE
- 68 MH-MD
- 112 SAFERtec
- 121 SHiELD
- 129 SPOOC
- 142 UNICORN
- 160 SealedGRID
- 161 SEMIoTICS
- 164 PAPAYA
- 165 POSEIDON
- 166 SPEAR
- 177 ENACT

Over the course of the Cyberwatching.eu project, we will work with our partners on how to support the projects in the future. Information on start and closure dates of projects are included in Appendix 1. Enagement with ongoing projects will be prioritized.

Now with the clusters identified, Cyberwatching.eu will work towards establishing light-weight synergies between the projects. We anticipate that this will be challenging and we are implementing a series of activities outlined below which are designed to build synergies between projects and build broad pictures of the different markets in those three different areas.

1. **Deep dive workshops:** These events, carried out both remotely and possibly physically will look to identify synergies between projects and also re-use of results around the topics of the clusters.
2. **Promotion of clusters through webinars and events:** Through workshops and webinars, cyberwatching.eu will provide dissemination opportunities for projects within the clusters. For example, Cluster V was used as a basis for the organization of a webinar on GDPR and emerging technologies[3] in July 2019 as well as input for D3.4 Cybersecurity, legal and policy aspects[4]. In addition, a webinar is planned for the end of M28 to disseminate the results of this report and to promote the clustering activity.
3. **Promotion on project website:** What is true for any commercial operator in that it is crucial to clearly position themselves in the market, and targeting the right customer group for their products and services, should equally be of concern for the projects in the "market of EC funded projects". The cluster solution found in Figure 6 will help us to better tailor messages to the right groups of projects and involved organisations.

The clusters will be highlighted on the project hub through news pieces and regular newsletters sent to registered users. With cluster V project pages on the hub, related content featured highlights content related to GDPR.

In addition, for projects that are nearing the end of their lifetime or have finished, the clustering activity is useful in terms of promoting their results through the marketplace.

An example of the promotion of a cluster of cybersecurity is seen with the services provided by the TRUSTEE cluster[5], a cluster of cloud-related cybersecurity projects

[3] https://www.cyberwatching.eu/gdpr-compliance-age-emerging-technologies
[4] https://www.cyberwatching.eu/d34-eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead
[5] https://credential.eu/trustee/trustee-ready-platforms/

that have been working together for the last 3 years. Here, common branding has been used to promote their results.

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	AARC2	EINFRA-22-2016	RIA	May 2017	Apr 2019
2	ABC4Trust	ICT-2009.1.4	CP	Nov 2010	Feb 2015
3	ADDPRIV (F)	SEC-2010.6.5-2	CP	Feb 2011	Mar 2014
4	AEGIS	DS-05-2016	CSA	May 2017	Apr 2019
5	ANASTACIA	DS-01-2016	RIA	Jan 2017	Dec 2019
6	ARIES	FCT-09-2015	RIA	Sep 2016	Feb 2019
7	ARMOUR (F)	ICT-12-2015	RIA	Feb 2016	Jan 2018
8	ASAP (F)	ERC-AG-PE6	ERC-AG	Oct 2012	Sep 2018
9	ATENA	DS-03-2015	IA	May 2016	Apr 2019
10	BEACON (F)	ICT-07-2014	RIA	Feb 2015	Jul 2017
11	BIOSEC (F)	FP7-PEOPLE-IOF-2008	MC-IOF	Mar 2009	Feb 2012
12	C3ISP	DS-04-2015	IA	Oct 2016	Sep 2019
13	CANVAS	DS-07-2015	CSA	Sep 2016	Aug 2019
14	certMILS	DS-01-2016	IA	Jan 2017	Dec 2020
15	CHOReVOLUTION (F)	ICT-09-2014	RIA	Jan 2015	Dec 2017
16	CIPSEC	DS-03-2015	IA	May 2016	Apr 2019
17	CITADEL	DS-03-2015	IA	Jun 2016	May 2019
18	CLARUS (F)	ICT-07-2014	RIA	Jan 2015	Dec 2017
19	CloudSocket (F)	ICT-07-2014	RIA	Jan 2015	Dec 2017
20	CloudTeams (F)	ICT-07-2014	IA	Mar 2015	Feb 2017
21	COCKPITCI (F)	SEC-2011.2.5-1	CP-FP	Jan 2012	Dec 2014
22	COEMS	ICT-10-2016	RIA	Nov 2016	Oct 2019
23	COLA	ICT-06-2016	IA	Jan 2017	Jun 2019
24	COMPACT	DS-02-2016	IA	May 2017	Oct 2019
25	CONSENT (F)	SSH-2009-3.2.1.	CP-FP	May 2010	Apr 2013
26	CREDENTIAL (F)	DS-02-2014	IA	Oct 2015	Sep 2018
27	CROSSMINER	ICT-10-2016	RIA	Jan 2017	Dec 2019
28	CryptoCloud	ERC-AG-PE6	ERC-AG	Jun 2014	May 2019
29	CS-AWARE	DS-02-2016	IA	Sep 2017	Aug 2020
30	CYBECO	DS-04-2016	RIA	May 2017	Apr 2019

#	Project	Call	Type	Start	End
31	CyberWiz (F)	DRS-17-2014	SME-2	Sep 2015	Aug 2017
32	CYCLONE (F)	ICT-07-2014	IA	Jan 2015	Dec 2017
33	CYRail (F)	S2R-OC-IP2-01-2015	Shift2Rail-RIA	Oct 2016	Sep 2018
34	DAPPER (F)	FP7-PEOPLE-2013-CIG	MC-CIG	Apr 2014	Mar 2018
35	DECODE	ICT-12-2016	RIA	Dec 2016	Nov 2019
36	DEFENDER	CIP-01-2016-2017	IA	May 2017	Apr 2020
37	DISCOVERY (F)	ICT-38-2015	CSA	Jan 2016	Dec 2017
38	DiSIEM	DS-04-2015	IA	Sep 2016	Aug 2019
39	DITAS	ICT-06-2016	RIA	Jan 2017	Dec 2019
40	DOGANA (F)	DS-06-2014	IA	Sep 2015	Aug 2018
41	DSSC	MSCA-COFUND-2016	MSCA-COFUND-DP	May 2017	Apr 2022
42	e-Sides	ICT-18-2016	CSA	Jan 2017	Dec 2019
43	ECRYPT-CSA (F)	ICT-32-2014	CSA	Mar 2015	Feb 2018
44	ECRYPT-NET	MSCA-ITN-2014-ETN	MSCA-ITN-ETN	Mar 2015	Feb 2019
45	ENCASE	MSCA-RISE-2015	MSCA-RISE	Jan 2016	Dec 2019
46	EU-SEC	DS-01-2016	IA	Jan 2017	Dec 2019
47	EUNITY	DS-05-2016	CSA	Jun 2017	May 2019
48	FIDELITY (F)	SEC-2011.3.4-1	CP-IP	Feb 2012	Jan 2016
49	FORTIKA	DS-02-2016	IA	Jun 2017	May 2020
50	FutureTrust	DS-05-2015	IA	Jun 2016	May 2019
51	GenoPri (F)	MSCA-IF-2015-EF	MSCA-IF-EF-ST	May 2016	Apr 2018
52	GHOST	DS-02-2016	IA	May 2017	Apr 2020
53	HEAT (F)	ICT-32-2014	RIA	Jan 2015	Dec 2017
54	HECTOR (F)	ICT-32-2014	RIA	Mar 2015	Feb 2018
55	HERMENEUT	DS-04-2016	RIA	May 2017	Apr 2019
56	HIPS	ERC-CG-2013-PE6	ERC-CG	Oct 2014	Sep 2019
57	IMPACT	ERC-2013-SyG	ERC-SyG	Feb 2015	Jan 2021
58	KONFIDO	DS-03-2016	RIA	Nov 2016	Oct 2019
59	LAST (F)	ERC-SG-PE6	ERC-SG	Oct 2009	Sep 2014
60	LIGHTest	DS-05-2015	IA	Sep 2016	Aug 2019
61	LV-Pri20 (F)	MSCA-IF-2014-EF	MSCA-IF-EF-CAR	Jun 2015	Jun 2017
62	MAMI (F)	ICT-12-2015	RIA	Jan 2016	Jun 2018
63	MAPPING (F)	SiS.2013.1.2-1	CSA-SA	Mar 2014	Feb 2018

#	Project	Call	Type	Start	End
64	MAS2TERING (F)	ICT-2013.6.1	CP	Sep 2014	Aug 2017
65	MATTHEW (F)	ICT-2013.1.5	CP	Nov 2013	Oct 2016
66	MELODIC	ICT-06-2016	RIA	Dec 2016	Nov 2019
67	mF2C	ICT-06-2016	RIA	Jan 2017	Dec 2019
68	MH-MD	ICT-18-2016	RIA	Nov 2016	Oct 2019
69	MIKELANGELO (F)	ICT-07-2014	RIA	Jan 2015	Dec 2017
70	MITIGATE (F)	DS-06-2014	IA	Sep 2015	Feb 2018
71	MUSA (F)	ICT-07-2014	RIA	Jan 2015	Dec 2017
72	NECOMA (F)	ICT-2013.10.1	CP	Jun 2013	Mar 2016
73	NeCS	MSCA-ITN-2015-ETN	MSCA-ITN-ETN	Sep 2015	Aug 2019
74	OCGN	MSCA-IF-2015-EF	MSCA-IF-EF-ST	May 2017	Nov 2018
75	OCTAVE (F)	DS-02-2014	IA	Jun 2015	Jul 2017
76	OPENREQ	ICT-10-2016	RIA	Jan 2017	Dec 2019
77	OPERANDO (F)	DS-01-2014	IA	May 2015	Apr 2018
78	P5 (F)	SEC-2012.2.3-1	CP-FP	Aug 2013	Oct 2016
79	PaaSword (F)	ICT-07-2014	RIA	Jan 2015	Dec 2017
80	PACT (F)	SEC-2011.6.5-2	CP-FP	Feb 2012	Jan 2015
81	PANORAMIX (F)	DS-01-2014	IA	Sep 2015	Aug 2018
82	PARIS (F)	SEC-2012.6.1-2	CP-FP	Jan 2013	Feb 2016
83	PASS (F)	PEOPLE-2007-4-3.IRG	MC-IRG	Dec 2008	Nov 2012
84	PATS (F)	SiS-2008-1.2.2.1	CSA-SA	Aug 2009	Mar 2012
85	PICOS (F)	ICT-2007.1.4	CP	Feb 2008	Jun 2011
86	PQCRYPTO (F)	ICT-32-2014	RIA	Mar 2015	Feb 2018
87	PRACTIS (F)	SiS-2009-1.1.2.1	CP-FP	Jan 2010	Mar 2013
88	PRECIOSA	ICT-2007.6.2	CP	Mar 2008	Aug 2010
89	PRESCIENT	SiS-2009-1.1.2.1	CP-FP	Jan 2010	Mar 2013
90	PreserviX	ICT-37-2014-1	SME-1	May 2015	Oct 2015
91	PrEstoCloud	ICT-06-2016	RIA	Jan 2017	Dec 2019
92	PrimeLife	ICT-2007.1.4	CP	Mar 2008	Jun 2011
93	PRIPARE	ICT-2013.1.5	CSA	Oct 2013	Sep 2015
94	PRISM	ICT-2007.1.4	CP	Mar 2008	May 2010
95	PRISM CODE	FP7-PEOPLE-2012-CIG	MC-CIG	Nov 2012	Oct 2016
96	PRISMACLOUD	ICT-32-2014	RIA	Feb 2015	Jul 2018

#	Project	Call	Type	Start	End
97	PRISMS	SEC-2011.6.5-2	CP-FP	Feb 2012	Jul 2015
98	PRIVACY FLAG	DS-01-2014	IA	May 2015	Apr 2018
99	Privacy.Us	MSCA-ITN-2015-ETN	MSCA-ITN-ETN	Dec 2015	Nov 2019
100	PRIVACY4FORENSICS	FP7-PEOPLE-2013-IIF	MC-IIF	Feb 2015	Mar 2018
101	ProBOS	SMEInst-13-2016-2017	SME-2	Oct 2016	Sep 2018
102	PROTECTIVE	DS-04-2015	IA	Sep 2016	Aug 2019
103	Ps2Share	ICT-35-2016	RIA	Jan 2017	Dec 2017
104	RAPID	ICT-07-2014	RIA	Jan 2015	Dec 2017
105	REASSURE	DS-01-2016	RIA	Jan 2017	Dec 2019
106	ReCRED	DS-02-2014	IA	May 2015	Apr 2018
107	REDSENTRY	H2020-SMEINST-1-2016-2017	SME-1	Jul 2017	Dec 2017
108	RESPECT	SEC-2011.6.1-5	CP-FP	Feb 2012	May 2015
109	REVEN-X1	ICT-37-2015-1	SME-1	Jul 2015	Dec 2015
110	SafeCloud	DS-01-2014	IA	Sep 2015	Aug 2018
111	SAFEcrypto	ICT-32-2014	RIA	Jan 2015	Dec 2018
112	SAFERtec	DS-01-2016	RIA	Jan 2017	Dec 2019
113	SAINT	DS-04-2016	RIA	Mar 2017	Feb 2021
114	SAURON	CIP-01-2016-2017	IA	May 2017	Apr 2019
115	SCISSOR	ICT-32-2014	RIA	Jan 2015	Dec 2017
116	SCOTT	ECSEL-2016-2-IA-two-stage	IA	May 2017	Jun 2020
117	SCR	SMEInst-13-2016-2017	SME-1	Jul 2016	Dec 2016
118	SecIoT	INNOSUP-02-2016	CSA	Sep 2017	Aug 2018
119	SERECA	ICT-07-2014	RIA	Mar 2015	Feb 2018
120	SHARCS	ICT-32-2014	RIA	Jan 2015	Dec 2017
121	SHiELD	DS-03-2016	RIA	Jan 2017	Dec 2019
122	SHIELD	DS-04-2015	IA	Sep 2016	Feb 2019
123	SISSDEN	DS-04-2015	IA	May 2016	Apr 2019
124	SMESEC	DS-02-2016	IA	Jun 2017	May 2020
125	SocialPrivacy	FP7-PEOPLE-2011-IOF	MC-IOF	Sep 2012	Aug 2015
126	SODA	ICT-18-2016	RIA	Jan 2017	Dec 2019
127	SPECIAL	ICT-18-2016	RIA	Jan 2017	Dec 2019
128	SpeechXRays	DS-02-2014	IA	May 2015	Apr 2018
129	SPOOC	ERC-CoG-2014	ERC-COG	Sep 2015	Aug 2020

#	Project	Call	Type	Start	End
130	STAMP	ICT-10-2016	RIA	Dec 2016	Nov 2019
131	STOP-IT	CIP-01-2016-2017	IA	Jun 2017	May 2021
132	STORM	EE-13-2014	RIA	Mar 2015	Aug 2018
133	SUNFISH	ICT-07-2014	RIA	Jan 2015	Dec 2017
134	SUPERCLOUD	ICT-07-2014	RIA	Feb 2015	Jan 2018
135	SurPRISE	SEC-2011.6.5-2	CP-FP	Feb 2012	Jan 2015
136	SysSec	ICT-2009.1.4	NoE	Sep 2010	Nov 2014
137	TOREADOR	ICT-16-2015	RIA	Jan 2016	Dec 2018
138	TREDISEC	ICT-32-2014	RIA	Apr 2015	Mar 2018
139	TRUESSEC.EU	DS-01-2016	CSA	Jan 2017	Dec 2018
140	TYPES	DS-01-2014	IA	May 2015	Oct 2017
141	U2PIA	SMEInst-13-2016-2017	SME-1	Nov 2016	Mar 2017
142	UNICORN	ICT-06-2016	IA	Jan 2017	Dec 2019
143	VESSEDIA	DS-01-2016	RIA	Jan 2017	Dec 2019
144	VIRT-EU	ICT-35-2016	RIA	Jan 2017	Dec 2019
145	VisiOn	DS-01-2014		Jul 2015	Jun 2017
146	WISER	DS-06-2014	IA	Jun 2015	Nov 2017
147	WITDOM	ICT-32-2014	RIA	Jan 2015	Dec 2017
148	FENTEC	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
149	SAWSOC	FP7-SEC-2012-1	CP-FP	Nov 2013	Apr 2016
150	PROMETHEUS	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2019
151	REACT	H2020-DS-SC7-2017	RIA	Jun 2018	May 2021
152	SerIoT	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
153	YAKSHA	H2020-ICT-2017-1	IA	Jan 2018	Jun 2020
154	DECODE	H2020-ICT-2016-1	RIA	Dec 2016	Dec 2019
155	CYBER-TRUST	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021
156	DOGANA II		IA	Jan 2017	Dec 2019
157	CYBECO II	H2020-DS-SC7-2016	RIA	May 2017	Apr 2019
158	PRIVILEDGE	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
159	FUTURE TPM	H2020-DS-LEIT-2017	RIA	Jan 2018	Dec 2020
160	SealedGRID	H2020-MSCA-RISE-2017	MSCA-RISE	Jan 2018	Dec 2021
161	SEMIoTICS	H2020-IOT-2017	RIA	Jan 2018	Dec 2020
162	ASTRID	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021

#	Project	Call	Type	Start	End
163	BPR4GDPR	H2020-DS-SC7-2017	IA	May 2018	Apr 2021
164	PAPAYA	H2020-DS-SC7-2017	IA	May 2018	Apr 2021
165	POSEIDON	H2020-DS-SC7-2017	IA	May 2018	Oct 2020
166	SPEAR	H2020-DS-SC7-2017	RIA	May 2018	Apr 2021
167	SMOOTH	H2020-DS-SC7-2017	IA	May 2018	Oct 2020
168	DEFEND	H2020-DS-SC7-2017	IA	Jun 2018	May 2021
169	CE-IoT	H2020-MSCA-RISE-2017	MSCA-RISE	Jul 2018	Jun 2022
170	OLYMPUS	H2020-DS-SC7-2017	IA	Sep 2018	Aug 2021
171	THREAT-ARREST	H2020-DS-SC7-2017	IA	Sep 2018	Aug 2021
172	CONCORDIA	H2020-SU-ICT-2018-2	RIA	Jan 2019	Dec 2022
173	OCRE	H2020-INFRAEOSC-2018-1	RIA	Jan 2019	Dec 2021
174	SPARTA	H2020-SU-ICT-2018-2	RIA	Feb 2019	Jan 2022
175	CyberSec4Europe	H2020-SU-ICT-2018-2	RIA	Mar 2019	Jul 2022
176	ECHO	H2020-SU-ICT-2018-2	RIA	Mar 2019	Feb 2023
177	ENACT	H2020-IOT-2017	RIA	Jan 2018	Dec 2020