cyberwatching.eu

The European watch on cybersecurity & privacy

Assessing Research Outputs within the Cybersecurity and Privacy Landscape

Funded by the European Commission
Horizon 2020 – Grant # 740129

Session Overview

TIMING	SESSION
15:45 - 16:10	**Cybersecurity Taxonomy & Technology Radar** ***David Wallom***, Associate Professor and Associate Director – Innovation of the Oxford e-Research Centre
16:10 - 16:30	**Understanding project output readiness** ***Michel Drescher***, Cloud Computing Standards Specialist of Oxford e-Research Centre at the University of Oxford
16:30 - 17:15	**Panel discussion on approaches to readiness for projects moving from proof of concept to realization** Chair: **Raul Amarelle Valera,** Project manager, AEI Ciberseguridad Aitor Couce, ICMAT & CYBECO John Davies, Co-founder and Chair of the South Wales Cyber Security Cluster Niccolo' Zazzeri, Trust-IT Services & WISER & CYBERWISER.eu Jose Ruiz, ATOS, SMESEC & CIPSEC

cyberwatching.eu

The European watch on cybersecurity & privacy

Cybersecurity Taxonomy and Technology Radar

Professor David Wallom

Funded by the European Commission
Horizon 2020 – Grant # 740129

Mapping & Clustering of R&I in EU National & Associated countries

- Create mechanism to enable EC and member state supported projects to come together to share outputs, methods and best practices
- Analyse project attributes to determine related activities
- Apply repeatable unsupervised machine learning techniques to these data as evidence-based characterisation of the cybersecurity landscape
- Use resampling of the dataset and replacement to enable bootstrapping analysis to validate taxonomy.
- Understand the current status of project outputs and publicise their suitability for exploitation outside the the developing project team.

Cybersecurity Research Taxonomy

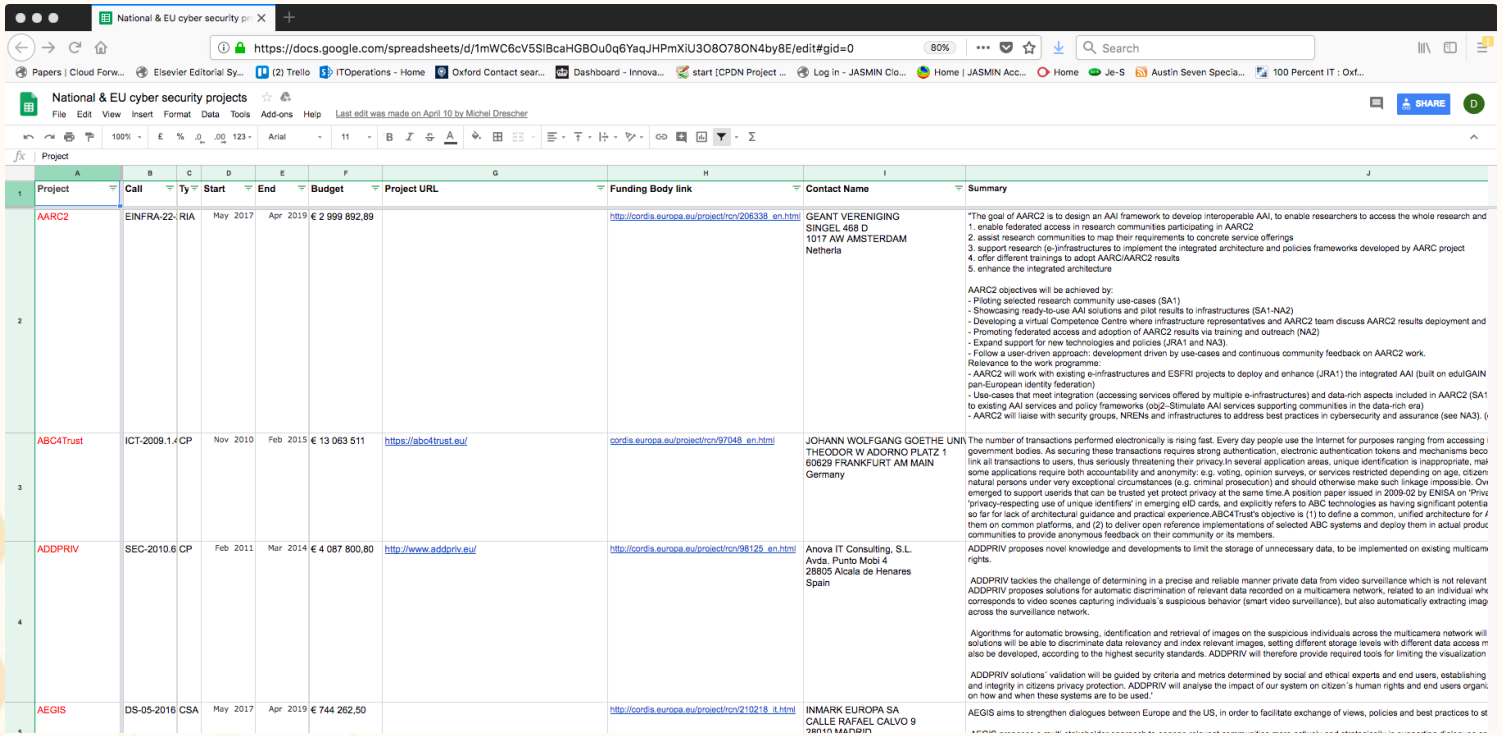
Foundational technical methods & risk management for trustworthy systems in cybersecurity & privacy

Applications and user-oriented services to support cybersecurity and privacy

Policy, governance, ethics, trust, and usability, human aspects of cybersecurity & privacy.

Mapping & Clustering of R&I in EU National & Associated countries

- Project Catalogue
  - A single catalogue of EU and national cybersecurity projects, showcasing technical developments and project foci
    - 148 projects listed (still running and completed)



Project	Call	Ty	Start	End	Budget	Project URL	Funding Body link	Contact Name	Summary
AARC2	EINFRA-22-	RIA	May 2017	Apr 2019	€ 2 999 892,89		http://cordis.europa.eu/project/rcn/206338_en.html	GEANT VERENIGING SINGEL 468 D 1017 AW AMSTERDAM Netherla	"The goal of AARC2 is to design an AAI framework to develop interoperable AAI, to enable researchers to access the whole research and 1. enable federated access in research communities participating in AARC2 2. assist research communities to map their requirements to concrete service offerings 3. support research (e-)infrastructures to implement the integrated architecture and policies frameworks developed by AARC project 4. offer different trainings to adopt AARC/AARC2 results 5. enhance the integrated architecture AARC2 objectives will be achieved by: - Piloting selected research community use-cases (SA1) - Showcasing ready-to-use AAI solutions and pilot results to infrastructures (SA1-NA2) - Developing a virtual Competence Centre where infrastructure representatives and AARC2 team discuss AARC2 results deployment and - Promoting federated access and adoption of AARC2 results via training and outreach (NA2) - Expand support for new technologies and policies (JRA1 and NA3). - Follow a user-driven approach: development driven by use-cases and continuous community feedback on AARC2 work. Relevance to the work programme: - AARC2 will work with existing e-infrastructures and ESFRI projects to deploy and enhance (JRA1) the integrated AAI (built on eduIGAIN pan-European identity federation) - Use-cases that meet integration (accessing services offered by multiple e-infrastructures) and data-rich aspects included in AARC2 (SA1 to existing AAI services and policy frameworks (obj2–Stimulate AAI services supporting communities in the data-rich era) - AARC2 will liaise with security groups, NRENs and infrastructures to address best practices in cybersecurity and assurance (see NA3). (
ABC4Trust	ICT-2009.1.4	CP	Nov 2010	Feb 2015	€ 13 063 511	https://abc4trust.eu/	cordis.europa.eu/project/rcn/97048_en.html	JOHANN WOLFGANG GOETHE UNI THEODOR W ADORNO PLATZ 1 60629 FRANKFURT AM MAIN Germany	The number of transactions performed electronically is rising fast. Every day people use the Internet for purposes ranging from accessing i government bodies. As securing these transactions requires strong authentication, electronic authentication tokens and mechanisms beco link all transactions to users, thus seriously threatening their privacy.In several application areas, unique identification is inappropriate, mak some applications require both accountability and anonymity: e.g. voting, opinion surveys, or services restricted depending on age, citizen natural persons under very exceptional circumstances (e.g. criminal prosecution) and should otherwise make such linkage impossible. Ove emerged to support userids that can be trusted yet protect privacy at the same time.A position paper issued in 2009-02 by ENISA on 'Priva 'privacy-respecting use of unique identifiers' in emerging eID cards, and explicitly refers to ABC technologies as having significant potentia so far for lack of architectural guidance and practical experience.ABC4Trust's objective is (1) to define a common, unified architecture for A them on common platforms, and (2) to deliver open reference implementations of selected ABC systems and deploy them in actual produc communities to provide anonymous feedback on their community or its members.
ADDPRIV	SEC-2010.6	CP	Feb 2011	Mar 2014	€ 4 087 800,80	http://www.addpriv.eu/	http://cordis.europa.eu/project/rcn/98125_en.html	Anova IT Consulting, S.L. Avda. Punto Mobi 4 28805 Alcala de Henares Spain	ADDPRIV proposes novel knowledge and developments to limit the storage of unnecessary data, to be implemented on existing multicame rights. ADDPRIV tackles the challenge of determining in a precise and reliable manner private data from video surveillance which is not relevant ADDPRIV proposes solutions for automatic discrimination of relevant data recorded on a multicamera network, related to an individual wh corresponds to video scenes capturing individuals's suspicious behavior (smart video surveillance), but also automatically extracting imag across the surveillance network. Algorithms for automatic browsing, identification and retrieval of images on the suspicious individuals across the multicamera network will solutions will be able to discriminate data relevancy and index relevant images, setting different storage levels with different data access m also be developed, according to the highest security standards. ADDPRIV will therefore provide required tools for limiting the visualization ADDPRIV solutions' validation will be guided by criteria and metrics determined by social and ethical experts and end users, establishing and integrity in citizens privacy protection. ADDPRIV will analyse the impact of our system on citizen's human rights and end users organi on how and when these systems are to be used.'
AEGIS	DS-05-2016	CSA	May 2017	Apr 2019	€ 744 262,50		http://cordis.europa.eu/project/rcn/210218_it.html	INMARK EUROPA SA CALLE RAFAEL CALVO 9 28010 MADRID	AEGIS aims to strengthen dialogues between Europe and the US, in order to facilitate exchange of views, policies and best practices to st

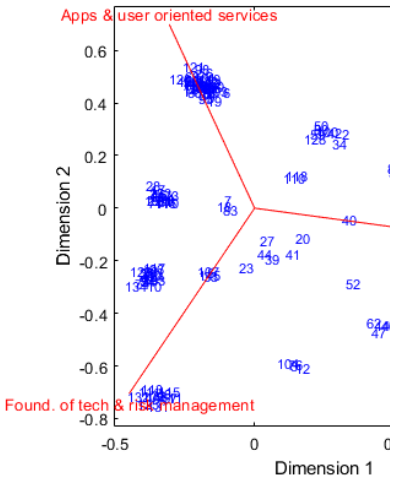
Mapping & Clustering of R&I in EU National & Associated countries

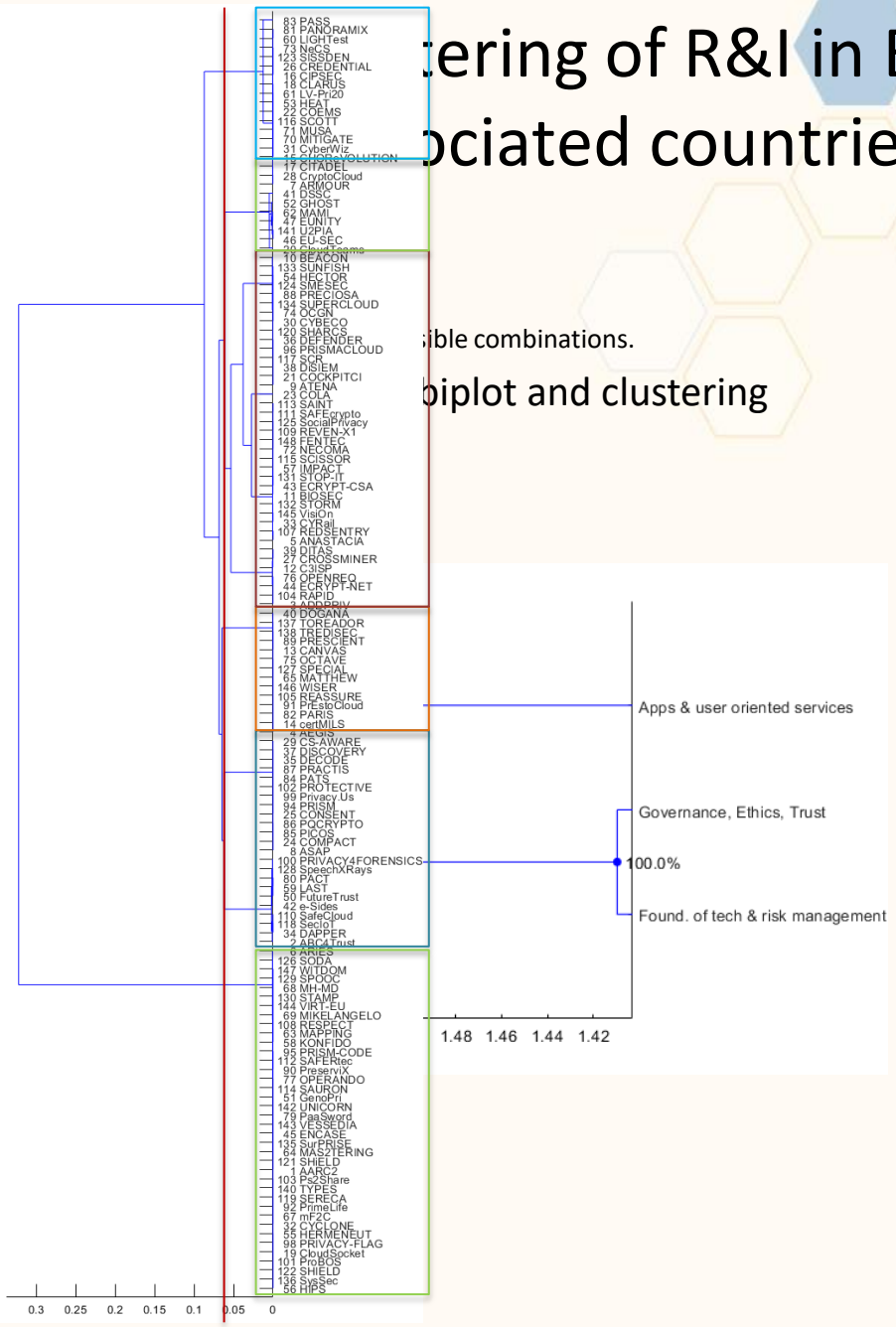
- First clustering using Level 1 taxonomy of all projects currently in the catalogue
- Initial scoring by Cyberwatching.eu partners from project details in catalogue.
  - The process of scoring is as follows:
    - Study the objectives of the project indicated in column A using the available material and references collected in the catalogue
    - Consider which of the three high-level categories in the Cyberwatching taxonomy is MOST IMPORTANT for this project, and select it in the column "Rank 1".
    - Now, consider the category that is SOMEWHAT IMPORTANT, and select it in "Rank 2".
    - The remaining category which is considered LEAST IMPORTANT then needs to be selected for Rank 3.
    - You must provide AT LEAST Rank 1; Rank 2 and Rank 3 are optional in case the remaining two (or one, respectively) category are out of scope of the project.

1		Classification - Cyberwatching		
2		Name:	Michel Drescher	
3		Partner:	UOXF	
4				
5	In bold - Projects from unit invited	Cyberwatching cluster ranking		
6	EC Project name	Rank 1	Rank 2	Rank 3
7	AARC2	Apps & user oriented services		
8	ABC4Trust	Apps & user oriented services	Governance, Ethics, Trust	
9	ADDPRIV	Found. of tech & risk management	Governance, Ethics, Trust	
10	**AEGIS**	Governance, Ethics, Trust		
11	**ANASTACIA**	Found. of tech & risk management	Apps & user oriented services	Governance, Ethics, Trust
12	ARIES	Apps & user oriented services		
13	ARMOUR	Apps & user oriented services	Found. of tech & risk management	Governance, Ethics, Trust
14	ASAP	Governance, Ethics, Trust	Apps & user oriented services	
15	**ATENA**	Found. of tech & risk management	Apps & user oriented services	
16	BEACON	Found. of tech & risk management	Apps & user oriented services	
17	BIOSEC	Found. of tech & risk management		
18	**C3ISP**	Found. of tech & risk management	Governance, Ethics, Trust	
19	**CANVAS**	Governance, Ethics, Trust		
20	**certMILS**	Governance, Ethics, Trust		
21	CHOReVOLUTION	Apps & user oriented services	Found. of tech & risk management	
22	**CIPSEC**	Apps & user oriented services	Found. of tech & risk management	
23	**CITADEL**	Apps & user oriented services	Found. of tech & risk management	
24	CLARUS	Apps & user oriented services	Found. of tech & risk management	Governance, Ethics, Trust
25	CloudSocket	Apps & user oriented services		
26	CloudTeams			
27	COCKPITCI	Found. of tech & risk management	Apps & user oriented services	
28	COEMS	Apps & user oriented services	Found. of tech & risk management	
29	COLA			
30	**COMPACT**	Governance, Ethics, Trust	Apps & user oriented services	
31	CONSENT	Governance, Ethics, Trust	Apps & user oriented services	
32	**CREDENTIAL**	Apps & user oriented services	Found. of tech & risk management	
33	CROSSMINER			
34	CryptoCloud	Apps & user oriented services	Found. of tech & risk management	
35	**CS-AWARE**	Governance, Ethics, Trust	Apps & user oriented services	
36	**CYBECO**	Found. of tech & risk management	Apps & user oriented services	
37	**CyberWiz**	Apps & user oriented services	Found. of tech & risk management	
38	CYCLONE	Apps & user oriented services		
39	CYRail	Found. of tech & risk management	Apps & user oriented services	Governance, Ethics, Trust
40	DAPPER	Apps & user oriented services	Governance, Ethics, Trust	
41	DECODE	Governance, Ethics, Trust	Apps & user oriented services	
42	DEFENDER	Found. of tech & risk management	Apps & user oriented services	
43	DISCOVERY (finished)	Governance, Ethics, Trust	Apps & user oriented services	
44	**DiSIEM**	Found. of tech & risk management	Apps & user oriented services	
45	DITAS			
46	**DOGANA**	Governance, Ethics, Trust	Apps & user oriented services	Found. of tech & risk management
47	DSSC			
48	e-Sides	Apps & user oriented services	Governance, Ethics, Trust	
49	ECRYPT-CSA	Found. of tech & risk management		
50	ECRYPT-NET			
51	ENCASE	Apps & user oriented services		
52	**EU-SEC**	Governance, Ethics, Trust	Found. of tech & risk management	
53	**EUNITY**	Governance, Ethics, Trust	Found. of tech & risk management	
54	FIDELITY			
55	FORTIKA			
56	FutureTrust	Apps & user oriented services	Governance, Ethics, Trust	
57	**GenoPri**	Apps & user oriented services		
58	**GHOST**	Governance, Ethics, Trust	Found. of tech & risk management	Apps & user oriented services
59	HEAT	Apps & user oriented services	Found. of tech & risk management	
60	**HECTOR**	Found. of tech & risk management	Apps & user oriented services	

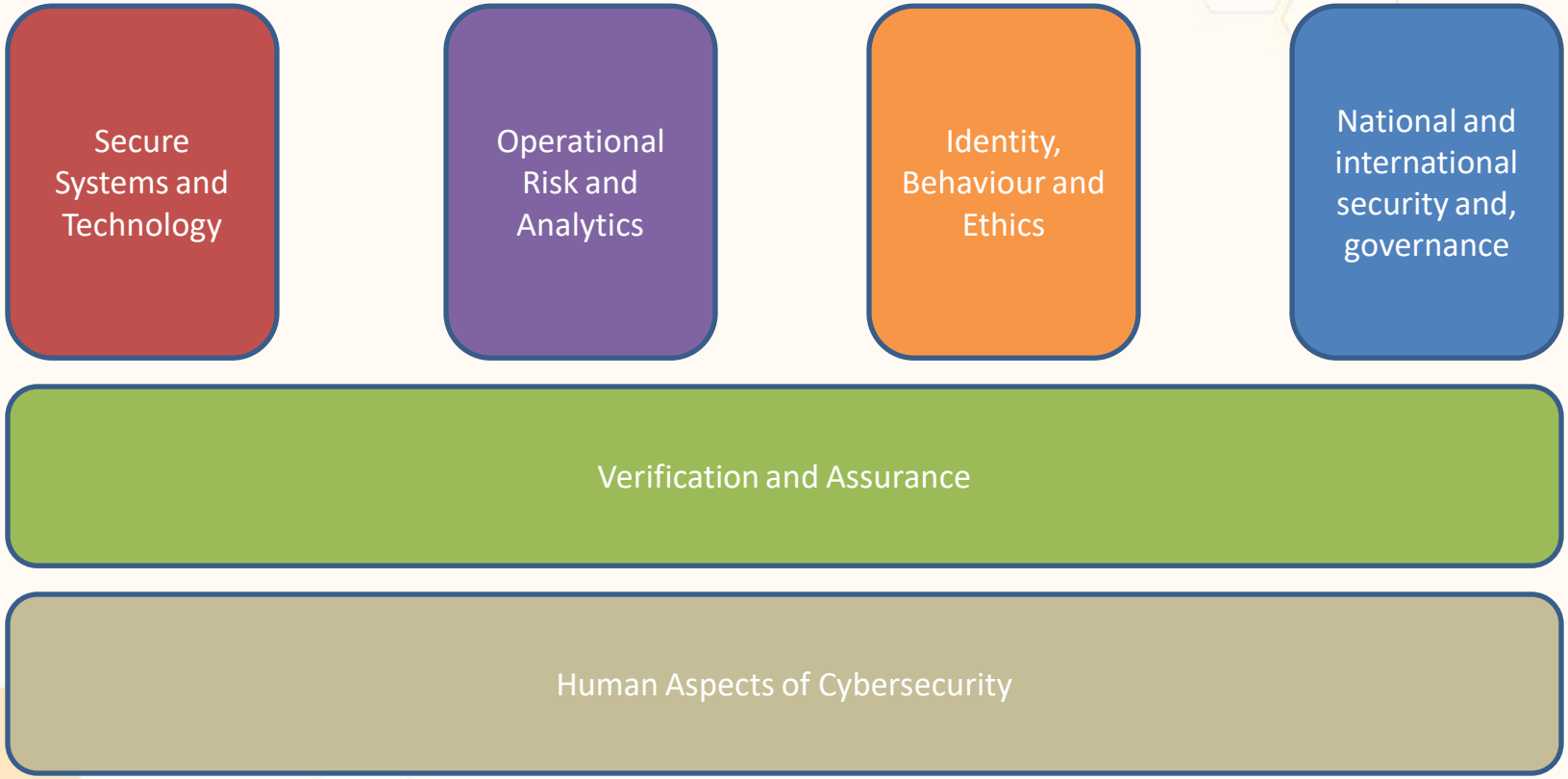
ering of R&I in EU
ociated countries

- Analysis and Clustering
  - Ranking with the possibility of null scores f ible combinations.
- Scores for project utilised to cre biplot and clustering
  - 66 'Apps & user oriented services' led
  - 35 'Found. of tech & risk management'
  - 32 'Governance, Ethics, Trust'





Cybersecurity Research Taxonomy



Secure Systems and Technology

- Building Security & privacy into technology from the design stage and technologies that are designed to deliver security capabilities, examples include;
  - Cryptography,
  - Trusted platforms,
  - Wireless & mobile security,
  - Cloud Computing security,
  - Secure software development/coding paradigms.

Operational Risk and Analytics

- Developing understanding of risk and harm resulting from cyberattack;
  - cyberattack propagation across and between organisations,
  - awareness of current understanding of scenario and risk management,
  - Metrics and models for security postures,
  - Analytics for predicting risk, prioritising responses and supporting security operations.

cyberwatching.eu
The European watch on cybersecurity & privacy

Identity, Behaviour, Ethics and Privacy

- Management of personal identity including different levels of assurance when used for online capabilities or services,
- How to understand common norms when applied in the online or digital realm,
- Diverse perspectives and interpretations to questions such as;
  - Who are you online with?
  - How do you communicate, and what can (or should) you do?
  - What expectations (personal and legally binding) are there? E.g. directives?
- What expectations of privacy can there be and should there be?

National and international security and, governance

- Development of Politics, international relations, defence, policy and governance issues
  - How do countries and communities interact with (and through) technology, and how might this change in different contexts?
  - How do national standards transcend borders or boundaries?
  - How should different threat persistence levels and domain cybersecurity understanding be shared?
  - At what point does something change from being a business problem to a national security problem?

Verification and Assurance

- Enabling the establishment of levels of confidence in a system in terms of security and privacy, primarily looking at other systems to either determine if they are secure or to assert they are;
  - Formal Verification seeks to build a mathematical model of a digital system and then try to prove whether it is ‘correct’, often helping to find subtle flaws,
  - Assurance focuses on managing risks related to the use, processing, storage, and transmission of information.

cyberwatching.eu
The European watch on cybersecurity & privacy

Human Aspects of Cybersecurity

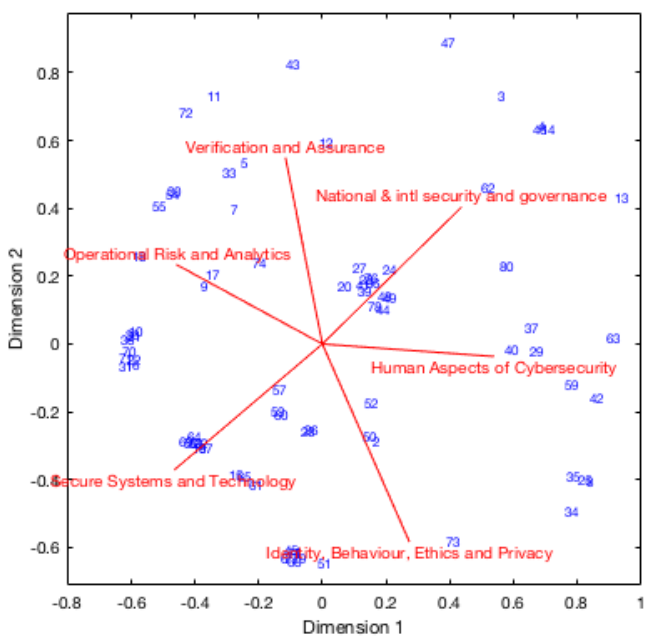
- Understanding humans interaction with, and through, digital systems;
  - whether to understand and design for target users,
  - understand how adversaries operate and can exploit the systems.
- Includes aspects like usability, trust, collaborative practices, social embeddedness, nationhood, cultural diversity and the relationship between microsocial interactions and global structures.

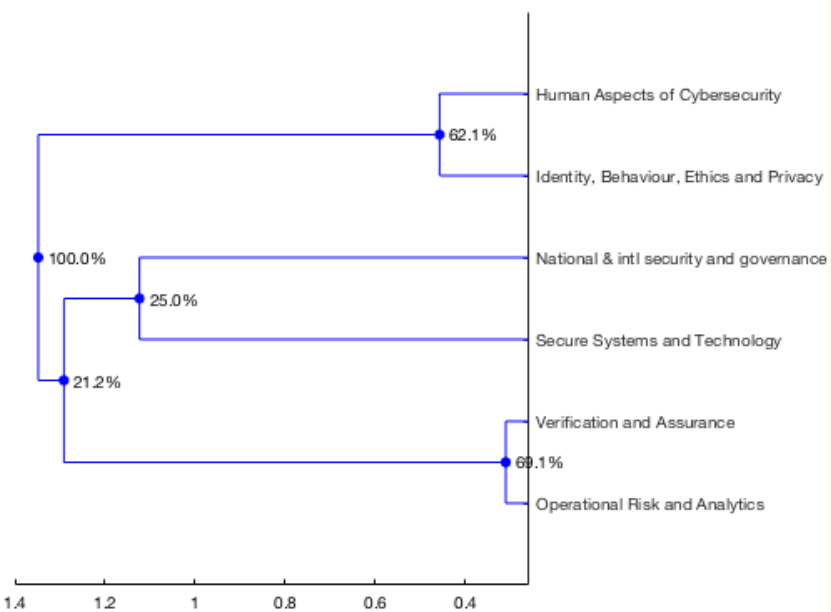
From clusters to understanding the R&I landscape

- Broad categories allow for projects to consider themselves how they understand a categories meaning
- Fewer simple categories generate clusters of projects with critical mass

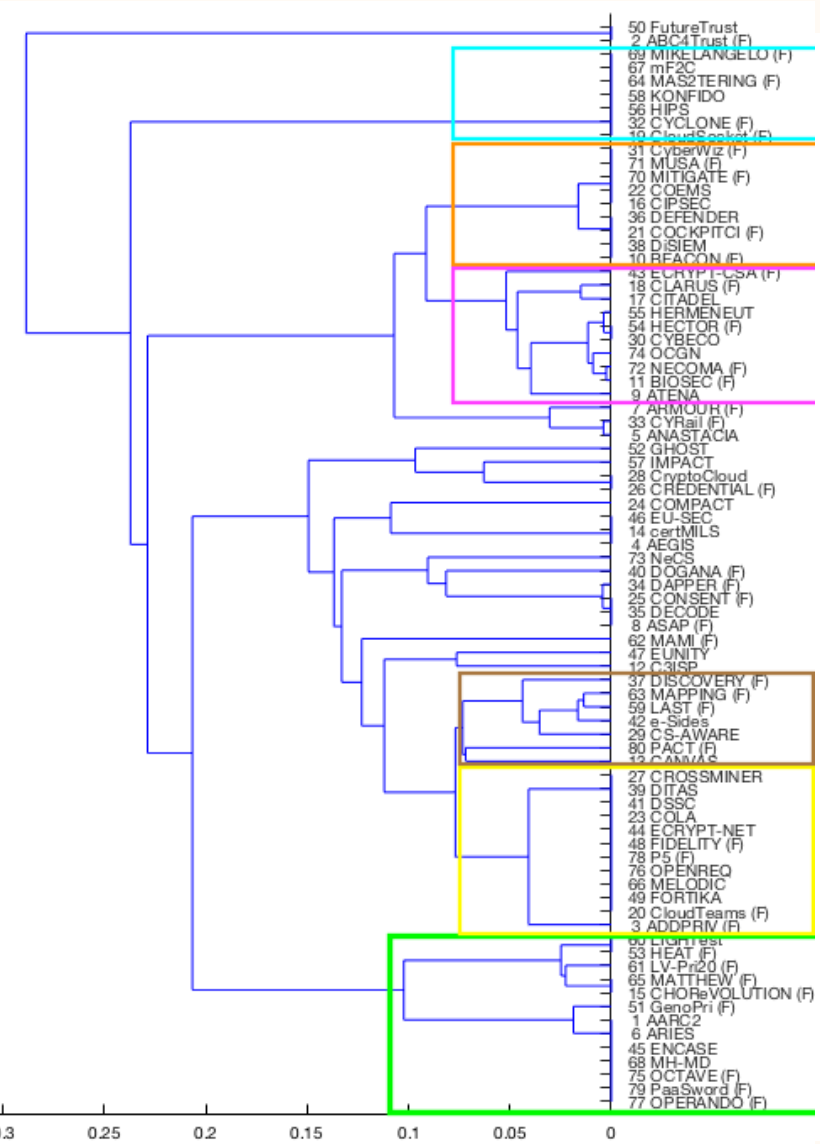
Mapping & Clustering of R&I in EU National & Associated countries

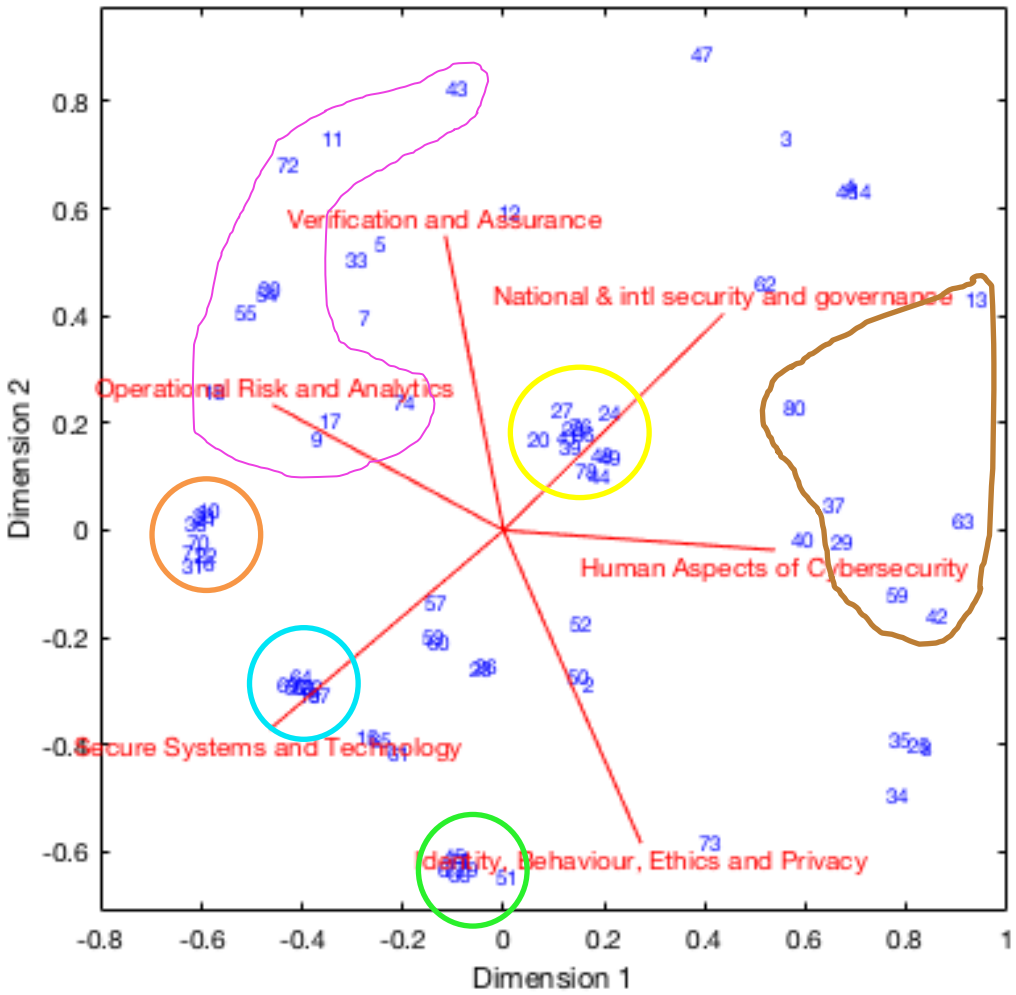
- Preliminary clustering has been performed with the first 80 EC projects within the catalogue.





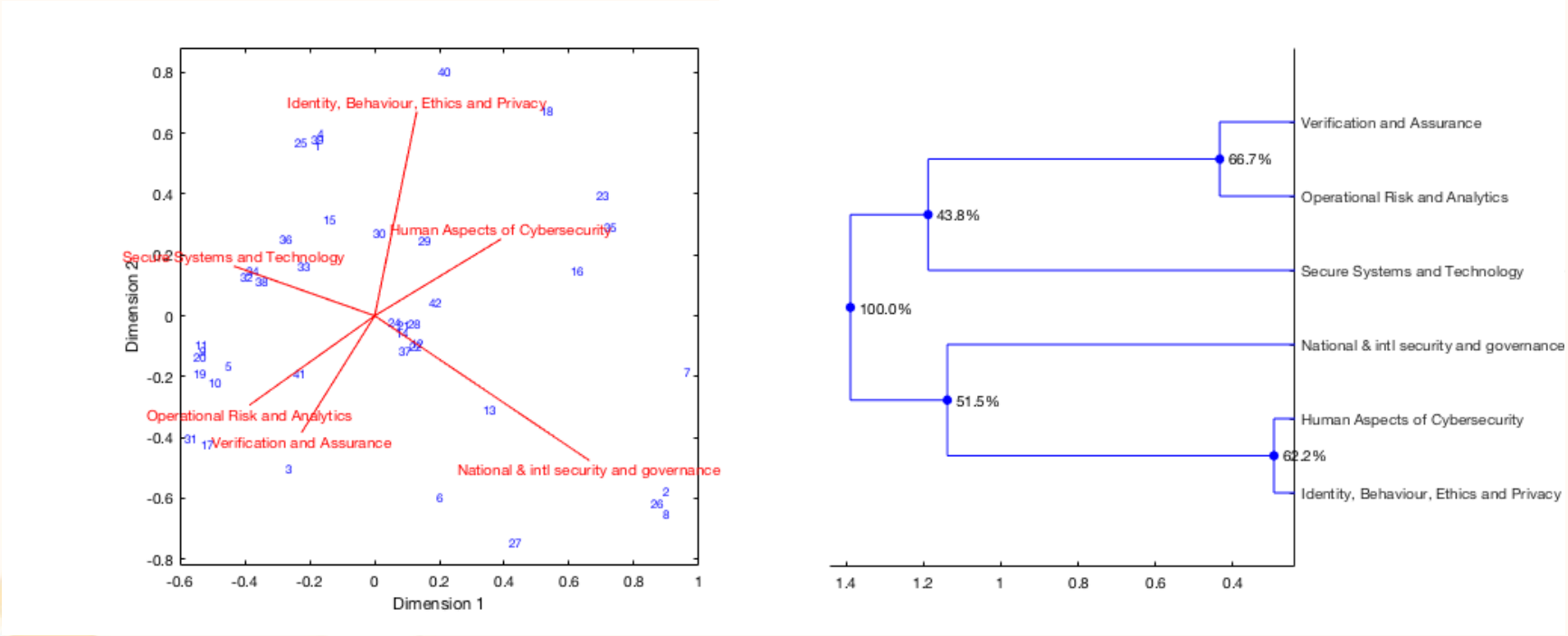
Mapping & Clustering of R&I in EU National & Associated countries





Mapping & Clustering of R&I in EU National & Associated countries

- Preliminary clustering has been performed with the first 80 EC projects within the catalogue.

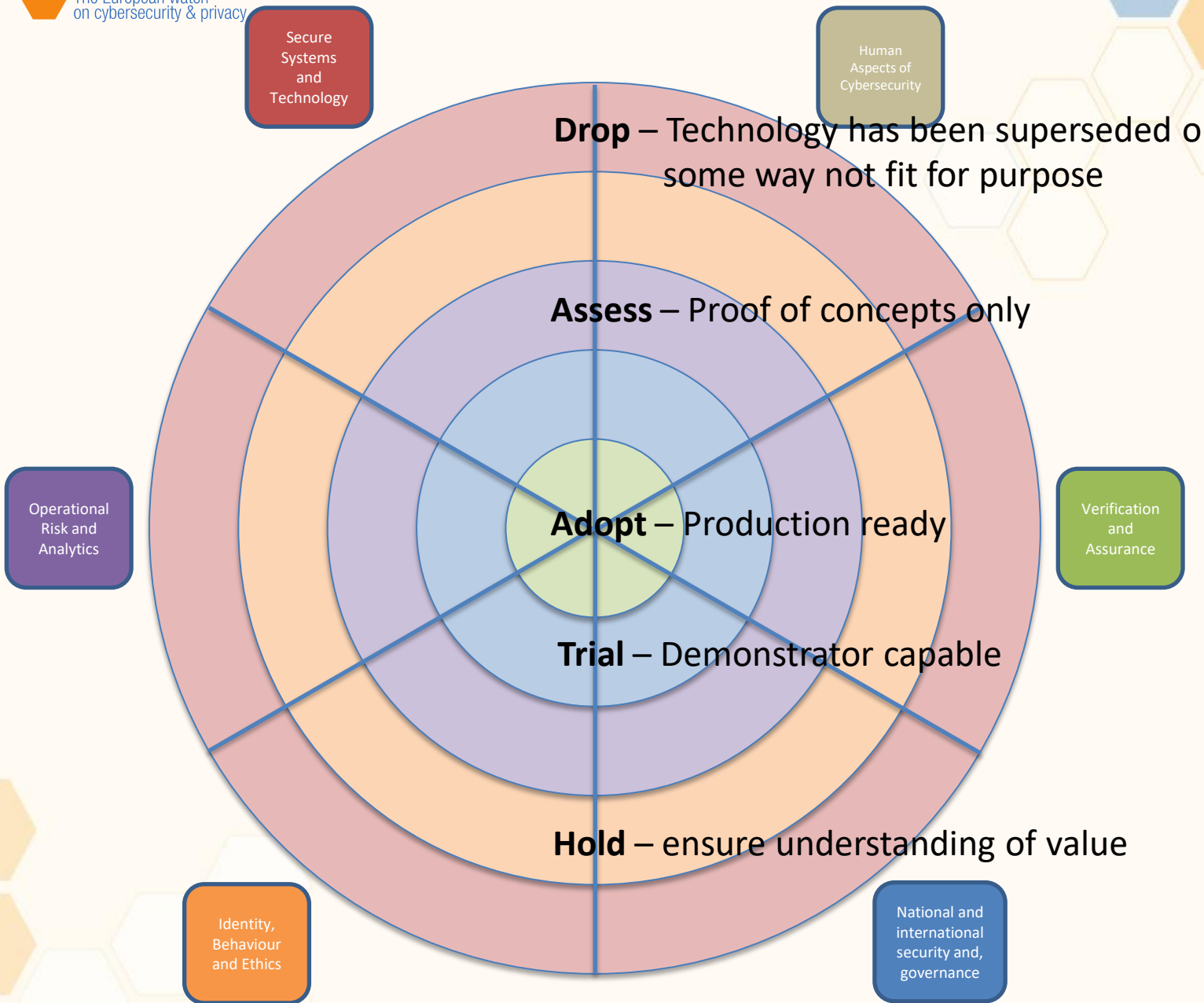


RUNNING PROJECTS ONLY

Cyberwatching Technology Radar

- Commonly used visualisation methodology to assess technology status.
- Independent sectors defined within a domain,
  - in Cyberwatching case this will be the L2 Taxonomy definitions
- Radial definitions applied across all sectors to give definition of in this case project output readiness;

Cyberwatching Technology Radar



Conclusions

- 1st Technology Radar to be published 31/10/18
- Commentary in additional documentation on rationale for product/project placement
- Living document with updates at a reasonable frequency to represent changing technology landscape.