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

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D10.1
Clustering results and SU-ICT-03 project CONCERTATION conference year 1

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	1.0

Related WP	WP10	Dissemination Level	CO
Lead Participant	CPT	Lead Authors	Mark Miller (CPT) Victoria Menezes Miller (CPT)
Contributing Beneficiaries	GUF, UPS-IRIT, FORTH, UMA	Related Deliverables	

Abstract:

This deliverable is intended to capture the key discussions and messages resulting from the first CyberSec4Europe Concertation Event held in Toulouse, France in November 2019. In addition, the document also includes a summary of collaboration activities undertaken by CyberSec4Europe project partners over the first one year of the project. In the original description of this deliverable a clustering task was included, however, this project clustering was actually first done at the CyberSec4Europe proposal stage (a summary of which is included as Figure 1, and furthermore, since another H2020 project (Cyberwatching.eu) has undertaken an extensive effort to address this specific task including more than 150 projects, rather than repeating the efforts, we have made the decision to place more work upon the key elements of the high level concertation event and the extensive collaboration work undertaken by the CyberSec4Europe partners. The concertation event included the active participation and discussions with top level European representatives from industry (e.g. Airbus), academia & research (e.g. IRIT and many other research and universities), the European Commission (e.g. DG CNECT), regional and national government (e.g. France and Occitanie Region), as well as a very significant and broad comprehensive set of stakeholders both from outside the consortium and as partners within CyberSec4Europe. The results, recommendations and conclusions are truly representative of the broadest set of inputs and feedback from the different communities and stakeholders, and as such can be used to form the basis for informed decision-making looking forward well into the future.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

CyberSec4Europe is a large-scale project funded by the European Union to pilot a number of the core building blocks of the upcoming regulation establishing the Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre.

With a focus upon the first CyberSec4Europe Concertation Event held in Toulouse, France, in November 2019, this deliverable represents the discussions of a comprehensive set of cybersecurity stakeholders across the private sector, the public sector, the research and academic community and society as a whole. Furthermore, this deliverable also presents the collaboration efforts of the partners during the first year of the CyberSec4Europe project.

The key recommendations resulting from this most significant CyberSec4Europe Concertation Event can be summarized in a concise way as follows:

1) Cooperation (including international cooperation) is a must in cybersecurity
2) Europe needs to take the leadership and continue to lead in the key area of privacy
3) Cybersecurity education of the private sector, the public sector and society as a whole must be made to be a key priority
4) A cybersecurity industrial policy is a key element that must be addressed by the European Institutions (European Commission, etc.)
5) Trust and cybersecurity certification are important, but certification must also be accessible and at a cost that is not burdensome for SMEs
6) Data sharing requires both trust and collaborative and secure structures for exchanging information and this should be a priority area on the European agenda
7) European focus on community building for the benefit of the users as well as the cybersecurity community
8) Regional hubs connecting directly into the European network and then the international community and networks should also be in the plan for the future (OcSSImore example as given in ANNEX 8)
9) A commitment to open and accessible cybersecurity standards for all is an important element
10) European investment in cybersecurity is necessary for the future – the European funding programmes must be re-adapted and made to be “fit for purpose” in this respect
11) The development of an “identity ecosystem” (discussions in Section 2.7) is an important step in addressing this issue, but this also requires European Institutions to support this approach

Document information

Contributors

Name	Partner
Victoria Menezes Miller (lead author/editor) Mark Miller (editor)	CPT
Kai Rannenberg Ahad Niknia Narges Arastouei Sebastian Pape	GUF
Antonio Skarmeta	UMU
Afonso Ferreira	CNR
Evangelos Markatos	FORTH
Vaclav Matyas	BRNO
Marco Crabu	ABI
Javier Lopez Carmen Fernandez	UMA
Aljosa Pasic	ATOS
Aida Omerovic	SINTEF
Alberto Lluch Lafuente	DTU
Marco Angelini	ENG
Lea Hemetsberger	OASC
Kimmo Halunen	VTT
Stephan Krenn	AIT
Pasquale Annicchino	ARCH
Liina Kamm	CYBER
David Goodman Romy Goodman	TDL
Dorien Surinx	TLEX
Davy Preuveneers	KUL
Pierantonia Sterlini	UNITN
Natalia Kadenko	TUD
Christos Douligeris	UPRC
Abdedelmalek Benzekri	IRIT

Reviewers

Name	Partner
Antonio Skarmeta	UMU
Evangelos Markatos	FORTH

History

0.01	2019-10-28	Lead author/editor	1st Draft
0.02	2019-12-10	Panel session contribution	2nd Draft
0.03	2019-12-30	Panel session contribution	3rd Draft
0.04	2019-12-31	Input to Chapter 1	4th Draft

0.05	2020-01-14	Additional input to Chapter 1	5th Draft
0.06	2020-01-14	Panel session contribution	6th Draft
0.07	2020-01-20	Panel session contribution	7th Draft
0.08	2020-01-21	Summaries of speeches	8th Draft
0.09	2020-01-23	GUF-High level Review	9th draft
0.10	2020-01-22	Input to Chapter 1	10th Draft
0.11	2020-01-24	Changes according to High Level Review (CPT)	11th Draft
0.12	2020-01-24	Additional input Chapter 1	12th Draft
0.13	2020-01-27	Changes according to High Level Review (FORTH, UMA, UMU, TDL) and contribution to Chapter 1 (TDL)	13th Draft
0.14	2020-01-27	Changes according to First Internal Review	14th Draft
0.15	2020-01-28	Changes according to First Internal Review (CNR)	15th Draft
0.16	2020-01-29	Changes according to Second Internal Review (UMU)	16th Draft
0.17	2020-01-30	Finalization last comments	17th Draft
1.0	2020-01-31	Additional input Chapter 1	18th Draft

List of Contents

List of Figures

List of Tables

List of acronyms of Consortium Partners

Acronym	Name of Consortium Partner
ABI	ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA
AIT	AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
ARCH	ARCHIMEDE SOLUTIONS SARL

Acronym	Name of Consortium Partner
ATOS	ATOS SPAIN SA
BBVA	BANCO BILBAO VIZCAYA ARGENTARIA SA*
BRNO	MASARYKOVA UNIVERZITA
C3P	UNIVERSIDADE DO PORTO
CNR	CONSIGLIO NAZIONALE DELLE RICERCHE
CONCEPT	CONCEPTIVITY SARL
CTI	INSTITOUTO TECHNOLOGIAS YPOLOGISTONKAI EKDOSEON DIOFANTOS
CYBER	CYBERNETICA AS
DAWEX	DAWEX SYSTEMS
DTU	DANMARKS TEKNISKE UNIVERSITET
ENG	ENGINEERING - INGEGNERIA INFORMATICA SPA
FORTH	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
GEN	COMUNE DI GENOVA
GUF	JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN
I-BP	INFORMATIQUE BANQUES POPULAIRES
ICITA	INTERNATIONAL CYBER INVESTIGATION TRAINING ACADEMY SDRUZHENIE
ISGS	INTESA SANPAOLO SPA
JAMK	JYVASKYLAN AMMATTIKORKEAKOULU
KAU	KARLSTADS UNIVERSITET
KUL	KATHOLIEKE UNIVERSITEIT LEUVEN
NEC	NEC LABORATORIES EUROPE GMBH
NTNU	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU
OASC	OPEN & AGILE SMART CITIES
POLITO	POLITECNICO DI TORINO
SIE	SIEMENS AKTIENGESELLSCHAFT
SINTEF	SINTEF AS
TDL	TRUST IN DIGITAL LIFE
TLEX	TIME.LEX
TUD	TECHNISCHE UNIVERSITEIT DELFT
UCD	UNIVERSITY COLLEGE DUBLIN, NATIONAL UNIVERSITY OF IRELAND, DUBLIN
UCY	UNIVERSITY OF CYPRUS
UM	UNIVERZA V MARIBORU
UMA	UNIVERSIDAD DE MALAGA
UMU	UNIVERSIDAD DE MURCIA

Acronym	Name of Consortium Partner
UNILU	UNIVERSITE DU LUXEMBOURG
UNITN	UNIVERSITÀ DEGLI STUDI DI TRENTO
UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER
UPS-IRIT	UNIVERSITE PAUL SABATIER TOULOUSE III
VAF	VaF, S. R. O.
VTT	TEKNOLOGIAN TUKIMUSKESKUS VTT Oy

List of Acronyms (other than Consortium partners listed above)

Acronym	Name
AI	Artificial Intelligence
AI HLG	High-Level Expert Group on Artificial Intelligence
AKE	Authentication and Key Establishment
C3ISP	Collaborative information sharing and analytics for cyber protection
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CHECK	Community Hub of Expertise and Cybersecurity Knowledge
CSSLP	Certified Information Systems Security Professional
CTI	Cyber Threat Incident
EBF	European Banking Federation
ECSO	European Cyber Security Organisation
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
EPC	European Payments Council
ETSI	European Telecommunications Standards Institute
EUROPOL	European Union Agency for Law Enforcement Cooperation
FDIS	Final Draft International Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPEN	Internet Privacy Engineering Network
ISO	International Organization for Standardization
ITU	International Telecommunications Union
JTC	Joint Technical Committee
LPWAN	Low-Power Wide-Area Network

Acronym	Name
NCP	National Contact Point
NeCS	EU Network on Cyber Security
NREN	National Research and Education Network
PSSG	Payment Security Support Group
SDO	Standards Development Organization
SEPA	Single Euro Payments Area
SIEM	Security Information and Event Management
SOC	Security Operations Center
TNC	Trusted Network Communications
TR	Technical Report
TS	Technical Specification
WG	Working Group

1 Introduction

As part of the original tasks in this deliverable, we had proposed a project clustering effort, however, as part of the proposal this was actually done since we identified all of the different projects where the CyberSec4Europe partners were addressing each and every topic area from the JRC taxonomy (see Figure 1 below). Furthermore, another project has actually undertaken this task of project clustering (Cyberwatching.eu) and rather than repeating the exercise within CyberSec4Europe it was decided that a better use of this smaller part of the funding was to add focus upon the CyberSec4Europe Concertation Event and partner collaboration activities with the key conclusions and recommendations resulting from these efforts which touch upon the broadest and most comprehensive set of stakeholders and the entire eco-system from the public sector, to the private sector, to research and academia as well as European society as a whole.

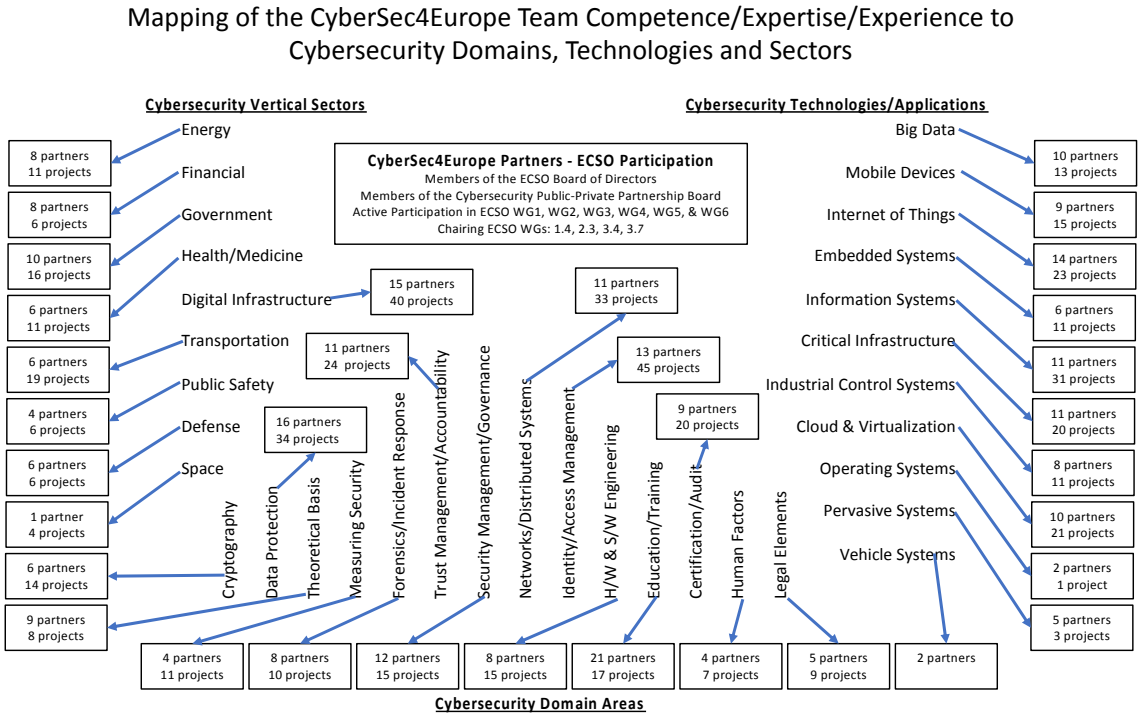


Figure 1: Mapping of CyberSec4Europe.eu Expertise to Cybersecurity Domains, Technologies and Sectors

1.1 Partner activities over the first year

The partner collaboration activities span a wide range of interactions within and external to the cybersecurity ecosystem. These interactions are with European Institutions, Standards Development Organizations (SDOs), Cybersecurity Communities (such as the European Cyber Security Organisation (ECSO)), and other organizations, stakeholders entities and institutions. A summary of the many CyberSec4Europe partner collaboration activities is contained in the tables which follow:

1.1.1 ENISA

Date & Venue	Title of Event	Partners	Comments /Remarks/Outcomes
February 2019 (and before) – January 2020	ENISA Advisory Group (previously Permanent Stakeholder Group)	GUF	Contributed to discussions, documents (e.g. the opinion on consumer IoT), and questionnairres
19.03.2019, (Brussels, Belgium)	Building cybersecurity bridges together: 15 years of ENISA	CPT	Contributed to the discussions
13-14.06.2019 (Rome, Italy)	ENISA Annual Privacy Fourm	GUF	Contributed as e.g. General Co-Chairs, also in several conference calls
August-September 2019	ENISA's Cyber Security Higher Education Map and CyberSec4Europe review of Cybersecurity Education in Europe (D6.2)	DTU	Discussed possible collaborations and content of the survey form
16.09.2019 (Heraklion, Greece)	6th ENISA-FORTH Summer School on Network & Information Security 2019, "Security Challenges of Emerging Technologies"	GUF	CyberSecurity 4 Europe Poster exhibition, Organized Tabletop Security Gaming Sessions
October – December 2019	The Certification of Cyber Security Degrees and ENISA's Cyber Security Higher Education Map Cybersecurity research directions for Digital Sovereignty in Europe	FORTH	Contributed to the documents Note: the documents are not public yet.
November 2019	Legal training	TLEX	Legal training for ENISA policy unit on e.g. EU cybersecurity law and Tallinn Manual 2.0
05.12.2019	ENISA Certification event	CPT	Participated in discussions, added ECSO WG1 information

Table 1: Participation/collaboration with ENISA

1.1.2 EDPS

Date & Venue	Committee	Title	Partners	Comments /Remarks/Outcomes
12.06.2019 (Rome, Italy)	Internet Privacy Engineering Network (IPEN)	Workshop	GUF	In connection with ENISA Annual Privacy Forum

Table 2: Participation in EDPS event

1.1.3 CEN/CENELEC

Date & Venue	Committee	Title	Partners	Comments /Remarks/Outcomes
06-07.06.2019 (Bucharest, Romania)	General Assembly	Security Workshop	GUF	
09-11.07.2019 (Paris, France) 19.-21.11.2019 (Bucharest, Romania)	JTC 13	Cyber-security and Data Protection	GUF	Also several conference calls
09-11.07.2019 (Paris, France) 19-21.11.2019 (Bucharest, Romania)	JTC 13/WG 1	Char Advisory Group	GUF	Also several conference calls
09-11.07.2019 (Paris, France) 19-21.11.2019 (Bucharest, Romania)	JTC 13/WG 5	Data Protection, Privacy and Identity Management	GUF	Also several conference calls
09-11.07.2019 (Paris, France) 19-21.11.2019 (Bucharest, Romania)	JTC 13/WG 6	Product Security	GUF	Also several conference calls
15.04.2019 (Berlin, Germany) 30.07.2019 (Frankfurt, Germany) 18.12.2019 (Berlin, Germany)	DIN BR-07 (German Mirror Committee to JTC 13)	Cyber-security and Data Protection	GUF	Also several conference calls
20-21.2. 2019 (Bonn, Germany) 26-27.8. 2019 (Berlin, Germany)	DIN NIA 27 AKs (German Mirror Committees to JTC 13 WGs)	Cybersecurity and Data Protection	GUF	

Table 3: Participation in CEN/CENELEC WGs

1.1.4 ISO/IEC

Date & Venue	Committee	Title	Partners	Comments /Remarks/Outcomes
All year 03-07.04.2019 (Ramat Gan, Israel) 14-18.10.2019 (Paris, France)	ISO/IEC JTC 1/SC 27 WGs	Information security, cybersecurity and privacy protection	AIT GUF CYBER ATOS	Category C liaisons with WG 2 (Cryptography and security mechanism) and WG 5 (Identity management and privacy technologies) were requested by AIT and CYBER, respectively. In WG 2, AIT, together with external partners, is editing ISO/IEC 23264-1, ISO/IEC

Date & Venue	Committee	Title	Partners	Comments /Remarks/Outcomes
				23264-2, and ISO/IEC 20009-3 in WG 2, and is currently preparing a new work item proposal on Secure Multiparty Computation, with support from internal and external partners. In WG 5, contributions, e.g., to ISO/IEC 27551 have been made. In WG 3 (Security evaluation, testing and specification), contributions, e.g., to ISO/IEC 29128 have been submitted
03-07.04.2019 (Ramat Gan, Israel) 14-18.10.2019 (Paris, France)	ISO/IEC JTC 1/SC 27/WG 5	Identity Management and Privacy Technologies	ATOS CYBER GUF	Participated in meeting. E.g. second UPDATED Terms of Reference for a Study Period "Use cases for identity assurance"
10-11.04.2019 (Ramat Gan, Israel) 17.10.2019 (Paris, France)	ISO/IEC JTC 1/SC 27 Plenary and Head if Delegations Meeting	Information security, cybersecurity and privacy protection	GUF	
20-21.2.2019 (Bonn, Germany) 26-27.8.2019 (Berlin, Germany)	DIN NIA 27 AA "IT-Sicherheitsver-fahren" (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	Information security, cybersecurity and privacy protection	GUF	
All year 06–08.02.2019 (Berlin, Germany) 21-23.5.2019 (Toronto, Canada) 19.10.2019 (Paris, France), together with ISO/IEC JTC 1/SC 27/WG 5) 21–23.10.2019	ISO/PC317 meetings of the PC itself, WG 1, AdHoc Groups and a workshop	Consumer protection: privacy by design for consumer goods and services	GUF	The project of ISO/PC317 is ISO/AWI 31700 "Consumer protection — Privacy by design for consumer goods and services". Technically this project could and should have been ecuted at ISO/IEC JTC 1/SC 27/WG 5, but the ISO TMB decided for its own Project Committee, after their had been concerns by consumer

Date & Venue	Committee	Title	Partners	Comments /Remarks/Outcomes
(St Denis, France)				representatives about the representation of ISO COPOLCO at ISO/IEC JTC 1. To enable as much collaboration as possible with JTC 1/SC 27/WG 5 a close liason is maintained and if possible back to back meeting dates are arranged. Especially consumer devices have a major lack of security, which is one reason for major privacy issues and often caused by poor development processes.

Table 4: Participation in ISO/IEC WGs

1.1.5 ECSO

Date & Venue	Working Group	Title	Partners	Comments /Remarks/Outcomes
All year (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	UMU VTT	Composition document - Contribution on the challenges of the composite certification document Participated in several Fora
06.06.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	CYBER CPT	Face-to-Face Meeting: Discussing the Meta-Scheme approach
15.10.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	UMU	Face-to-Face Meeting: Discussion about the composition document and the current activities of the WG1 regarding certification
11.10.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	UMU	Conference call to discuss about the composition document
27.10.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	UMU	Conference call to discuss about the composition document
17.10.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	UMU	Conference call to discuss about the composition document

Date & Venue	Working Group	Title	Partners	Comments /Remarks/Outcomes
05.12.2019 (Brussels, Belgium)	WG1	Standardisation, certification, labelling, supply chain management	CPT	Face-to-Face Meeting
All year (Brussels, Belgium)	WG2	Market deployment, investments and international collaboration	ENG	Participation in WG meetings/events
All year (Brussels, Belgium) 18.09.2019	WG4	Support to SMEs, coordination with countries and regions	VTT IRIT CPT	Participation in WG meetings/events
23.03.2019	WG4	Support to SMEs, coordination with countries and regions	CPT	SME Hub meeting
All year (Brussels, Belgium) 04.07.2019 19.06.2019 22.10.2019	WG5	Education, awareness, training, cyber ranges	SINTEF UNITN CPT CPT	Participation in WG meetings/events Updates on EHR4CYBER and collaboration with ECSO
All year (Brussels, Belgium)	WG6	SRIA and Cyber Security Technologies	ENG FORTH CPT FORTH SINTEFVTT ENG GUF IRIT UMA	Co-chair the SWG6.2 (Digital Transformation in Verticals) Co-chair the SWG6.3 (Data and Economy) Participation in the WG6 activities Co-chair the SWG6.4 (Basic and Disruptive Technologies)
10.04.2019	WG6	SRIA and Cyber Security Technologies	CPT	Presentation Cybersec4europe
17.04.2019	WG6	SRIA and Cyber Security Technologies	CPT	Participated in meeting
04-07.02.2019		ECSO High level Round Table	CPT GUF	Participated in meeting
20.03.2019, 17-18.6.2019 01.10.2019 (Helsinki, Finland) 04.12.2019		ESCO Board	CPT GUF	As Vice-Chairman of SMEs, participated in Board meetings As Member of the Board , participated in Board meetings

Date & Venue	Working Group	Title	Partners	Comments /Remarks/Outcomes
17.12.2019				Teleconference participation
18.06.2019		ECSO AGM	GUF	Participated in meeting
17.09.2019 03.12.2019 (Brussels, Belgium)		ECSO Strategy Committee	CPT	Participated in meeting
22.10.2019		ECSO Meeting with EU	CPT	Priorities for cybersecurity
21.11.2019 (Brussels, Belgium)		ECSO Scientific and Technical Committee	IRIT	Member. Participated in meeting
15.05.2019 (Brussels, Belgium)		cPPP	FORTH VTT CPT GUF	Member of the ECSO Partnership Board
All year (Brussels, Belgium)	Cyber Security Working Group		ENG	EOS Position Paper – EU Digital Autonomy: Challenges & Recommendations for the Future of European Digital Transformation

Table 5: Collaboration/Participation in ECSO WGs

1.1.6 EOS

Date & Venue	Title of Event	Partners	Comments/Discussions/ Outcomes
26.11.2019 (Brussels, Belgium)	Meeting with DG Move	CPT	Aviation cybersecurity

Table 6: Participation in EOS

1.1.7 IoT Forum

Date & Venue	Title of Event	Partners	Comments/Discussions/ Outcomes
02.06.2019	IoT Week	UMU	Panel on Cybersecurity and IoT where the CyberSec4Europe project was put in relation to the IoT aspects of certification and CTI aspects

Table 7: Participation in IoT Forum event

1.1.8 IETF

Date & Venue	Title of Event	Partners	Comments/Discussions/Outcomes
26.07.2019	Secure IoT Bootstrapping: A Survey	UMU	Standardization effort in the IETF. This work is expected to provide an overview of the current state of the art in the area of Bootstrapping in IoT. This would help understand where the current efforts are being done, and how are the characterized in terms of architecture, deployment and security properties
06.12.2019	Requirements for a Lightweight AKE for OSCORE	UMU	Work adopted as LAKE Working Group item This work will help establish the expected requirements of an Authentication and Key Establishment (AKE) for the recently standardized protocol OSCORE. Here it is analyzed the requirements accounting for the restrictions of IoT and different use cases such as 6tisch and LPWAN

Table 8: Collaboration with IETF

1.1.9 Summary of the four Pilots Joint Events

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
From 06.02.2019 about monthly (mostly Brussels, Belgium)	All four pilots	GUF	Pilots Meeting with DG CONNECT, JRC, ECSO
18.02.2019 (Paris, France)	SPARTA	CPT	SPARTA Kick-off
25.02.2019 (Paris, France)	ECHO	GUF	ECHO Launch event
13.03.2019 (Strasbourg, France)	All four pilots	GUF	Pilots Meeting with Commissioner Gabriel, DG CONNECT, JRC, ECSO
20.03.2019 (Brussels, Belgium)	All four pilots	TDL	Community of Users: Organiser: DG Home in collaboration with DG CNECT Panel Title: Building a cybersecurity ecosystem to secure European society

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
			Comment: TDL acted as speaker coordinator for and attended this panel. The moderator was Sebastiano Tofaletti, Secretary General European Digital SME Alliance and partner in Cyberwatching.eu. The speakers were Rafael Tesoro Carretero (DG CNECT), Lea Hemetsberger (CyberSec4Europe), Géraud Canet (SPARTA), Felicia Cutas (for Gabi Dreo) (CONCORDIA) and Douglas Wiemer (ECHO) Outcome: A well-edited video based on the four interviews was produced and published on the four pilots' website.
04.04.2019 (Brussels, Belgium)	All four pilots	CPT	Pilots Meeting with DG CONNECT
24.04.2019	SPARTA	BRNO	Joint event with 2 expert lectures on smartcard security
04.06.2019 (Brussels, Belgium)	All four pilots At a cyberwatching.eu event	TDL	Panel Title: Building a cybersecurity ecosystem to secure European society Comment: TDL represented CyberSec4Europe on a panel with representatives from the other three pilots, namely Gabi Dreo (CONCORDIA), Géraud Canet (SPARTA) and Wim Mees (ECHO). The session was moderated by Nick Ferguson. Each of the pilots were asked to discuss their own approaches to the following topics: • Cyber ranges • Threat intelligence • Certification • Cybersecurity skills • Collaboration between the projects Each of the panellists took part in ten-minute interviews after the session and were asked to respond to the following four prepared questions: 1. In order to pilot the Cybersecurity Competence Network: How will the operational & substantive cooperation be achieved among the 4 pilots and beyond? 2. How does your pilot interconnect with Europe's Cybersecurity capabilities? 3. Do you think it's possible to achieve Digital Sovereignty of Europe? What are the main challenges? 4. How do you imagine the Cybersecurity landscape in Europe in 5 years from now on?

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
			Outcome: The interviews were filmed and the material was collated and editted together to eventually be posted as a streaming video on the homepage of the common website (https://cybercompetencenetwork.eu/).
05.06.2019 (Brussels, Belgium)	CONCORDIA	CPT	Joint website kick off by the European Commission
13.06.2019 (Luxembourg City, Luxembourg)	All four pilots	TDL	Unit H1 Concertation Meeting: Organisers: ID2020/SEREN4 projects including the national contact points for cybersecurity TDL represented CyberSec4Europe together with representatives from the other three pilots, namely Matteo Merialdo (ECHO), Géraud Canet (SPARTA) and Olivier Festor (CONCORDIA). The pilots were asked to make a presentation different from the one we were usually doing in front of "usual" dissemination audiences and were asked to focus on the following points: What are the industrial verticals your pilot is covering? What is your pilot's view on what will be the outcome of the 4 pilots (a foundation, the EU research centre, a merging… what are your view on that)? How do you see the future of your pilot in the next 2 years and what related NCP activities can we help you with? Following the workshop, the pilot representatives were asked to participate in World Café sessions with the national contact points and discuss the following: Cooperation and synergy of the four projects – what has been done and what is planned for the future - How can we link better the NCP and the pilots? What new services to proposers/participants can the NCP/NCP projects offer with the support of the pilots (and vice-versa)? What future NCP services or national support can be foreseen at the end of the pilots? International collaboration: what are the planned actions in relation with Associated Countries and what international activities are foreseen, especially in terms of standards?
14.06.2019 (Ca' Foscari, Venice)	CyberSec4Europe	TDL OASC UNITN	Organiser: COMPACT project

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
			Event: COMPACT project workshop (in tandem with the Major Cities of Europe conference) Panel Title: Cybersecurity solutions for Local Public Administration' Comment: TDL represented CyberSec4Europe together with two other CyberSec4Europe partners, Davor Meersman (OASC) and Fabio Massacci (UNITN). Outcome: A representative of COMPACT (Marco Angelini) gave a presentation to the WP9 session during the CyberSec4Europe General Assembly on 4 July, which may lead to further collaboration in the context of T9.4.
19.06.2019 (Brussels, Belgium)	All four pilots	TDL	Event: CANVAS project workshop Organiser: CANVAS project Panel Title: Cybersecurity solutions for Local Public Administration Comment: TDL represented CyberSec4Europe together with representatives from the other three pilots, namely Thibaud Antignac (SPARTA), Wim Mees (ECHO) and Vassilis Prevelakis (CONCORDIA). Outcome: A representative of CANVAS gave a presentation session at the CyberSec4Europe General Assembly on 4 July
11.07.2019 (Munich, Germany)	All four pilots	TDL	Event: CODE 2019 conference Organiser: CANVAS project Comment: TDL represented CyberSec4Europe together with representatives from the other three pilots, namely Thibaud Antignac (SPARTA), Matteo Merialdo (ECHO) and AN Other (CONCORDIA). The moderator was Rafael Tesoro-Carretero (DG CNECT). After our individual presentations, Rafael posed the following questions: 1. Each pilot was asked to look at the other three projects and to tell about one good thing from (one/all three) of our peer pilots that might be somehow missing in or complement our own pilot. 2. The four pilots were asked to work together maximizing synergies and minimizing overlaps. a. What are the main challenges for 160+ partners working together? b. How do we plan to appeal and attract to the network others beyond the four pilot consortia?

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
			c. How do we envision the dynamics of the forthcoming Cybersecurity Competence Network, which is starting to be shaped by the four pilots? 3. What are the pilots' views about key technological and industrial priorities of cybersecurity in the EU? Can we name a few of these priorities? 4. In which concrete ways will the pilots contribute to the European strategic autonomy in the field of cybersecurity?
13-15.08.2019	CONCORDIA	BRNO	KYPO Summer School on Cybersecurity - joint event at KYPO cyber range platform
03-04.10.2019 (Sofia, Bulgaria)	ECHO	TUD	DIGILIENCE Conference. Participation in the conference and presenting the CyberSec4Europe approach to governance structure
18.10.2019 (Brussels, Belgium)	All four pilots	TDL	Event: 27th Meeting of the Horizon 2020 Programme Committee configuration for Secure Societies Organiser: DG CNECT Collaborative activities within the cluster of the four EU pilots on Cybersecurity competence network Comment: TDL represented CyberSec4Europe together with representatives from the other three pilots, namely Gabi Dreo (CONCORDIA), Florent Kirchner (SPARTA) and Wim Mees (ECHO). The meeting was chaired by Turo Mattila. The four pilots' session was introduced by Miguel Gonzalez-Sancho-Bodero, with CONCORDIA providing the four-pilot overview
15.11.2019 (Pisa, Italy)	All four pilots	TDL	Event: First cyberwiser.eu Open Pilots Workshop Organiser: Cyberwiser project Panel Title: EU Cybersecurity Network & Competence Centres: How your organisations will benefit? Comment: TDL represented CyberSec4Europe together with representatives from the other three pilots, namely Matteo Merialdo (ECHO), Fabio Martinelli (SPARTA) and Claudio Ardagna (CONCORDIA). Outcome: Nick Ferguson was invited to participate in 'Cybersecurity For Europe 2019' in Toulouse. CyberSec4Europe represented by

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
			T9.4 will share a stand with Cyberwiser at the FICO Conference on 28-29 January 2020.'
29.11.2019 (Brussels, Belgium)	All four pilots	GUF UMU UNITN CPT	1st Cyber Security Joint Project Workshop

Table 9: Summary of collaboration with other pilots

1.1.10 Four Pilots Communication Group

Date & Venue	Pilot	Partners	Comments/Discussions/Outcomes
26.02.2019 (Brussels, Belgium)	All four pilots	TDL	Action: Working in collaboration with DG CNECT and the other three pilot representatives, TDL published a press release concerning the commencement of CyberSec4Europe that was broadcast simultaneously with similar announcements made by DG CNECT and the other three pilots. Outcome: The impact and outreach of the communications activity by many of the partners is captured in Deliverable 9.1 'Website and Social Media 1'.
11.03.2019 (Brussels, Belgium)	All four pilots	TDL	TDL attended an all-day meeting at the invitation of CONCORDIA together with representatives from ECHO and SPARTA as well as three representatives of DG CNECT, including Konstantinos Ntantinos
February-May 2019	All four pilots	TDL	TDL participated in conference calls with representatives of the other three pilots and Konstantinos Ntantinos in formulating plans for the Communications Group, particularly the creation of a common brand and website.
6 June 2019	All four pilots	TDL	TDL was responsible for designing a logotype and branding for the activities of the four pilots, including the design for the common website (hosted by ECHO), as discussed in the communications group. The website was formally launched on stage by Despina Spadou and others at the evening social event of the CONCORDIA General Assembly with a 'red button' symbolically being pushed.

Table 10: Four Pilots Communication Group

1.1.11 International cooperation

Date & Venue	Title of Event	Partners	Comments/Discussions/Outcomes
17.01.2019	Connected Smart Cities Conference 2019	OASC	Organization of panel "Building Trust in a Connected World" at annual OASC conference "Connected Smart Cities Conference" to announce CyberSec4Europe (by Kai Rannenberg)
04-08.03.2019, (San Francisco, USA)	RSA International Conference	CPT KUL	Participated in Conference during which iinformal interventions referencing CS4E efforts and activities took place
26.03.2019 (Sao Paolo, Brazil)	Workshop of the Cybersecurity Group of the Brazilian IoT Forum	IRIT	Launch of the Cybersecurity Group of the Brazilian IoT Forum
26-28.03.2019 (Bucharest, Romania)	CIP Forum Bucharest	OASC	Presenting CyberSec4Europe in Panel on Digital Transformation of cities and implications for critical infrastructure protection
10-11.04.2019 (Chania, Crete)	3rd Cyber Security Conference of NATO Maritime Interdiction Operational Training Centre (NMIOTC)	UPRC	Disseminating CS4EU project concept and objectives via face-to-face communication with security experts from major international think tanks, lobbyists and cyber defense contractors
March–August 2019	Hosting of PhD-student intern from North Carolina State University	AIT	Submission on ring signatures to EUROCRYPT (acceptance notification pending), and planned submission on chameleon hashes
04-6.09.2019 (Chania, Crete)	10th NMIOTC Annual Conference "Countering Hybrid Threats: An Emerging Maritime Security Challenge"	UPRC	Presenting CS4EU maritime transport use cases in panel discussion on current and future maritime security challenges
12-14.06.2019 (Bucharest, Romania)	EU Digital Assembly	CPT	Participated in conference and informal interventions referencing CS4E efforts and activities
25.06.2019 (London, UK)	4th Maritime Cyber Risk Management Forum, Norton Rose Fulbright,	UPRC	Presented CyberSec4Europe in the maritime security interactive forum
July 2017-July 2019	ITU Focus Group on data processing	AS	Contribution to the technical report 'Framework for security, privacy, risk and

	and management to support IoT and smart cities and commnities		governance in data processing and management'
26–29.08.2019 (Canterbury, UK)	ARES: 14th International Conference on Availability, Reliability and Security, University of Kent	UPRC	Presentation of CyberSec4Europe at the International Workshop on Physical and Cyber Security in Critical Port Infrastructures (PCSCP 2019) of the 14th ARES 2019 Conference.
20-22.09.2019 (Piraeus, Greece)	SEEDA-CECNSM Conference 2019: the 4th South-East Europe Design Automation, Computer Engineering, Computer Networks & Social Media Conference	UPRC	Presenting CyberSec4Europe in a session devoted to on-going research projects and considerations on topics of computer engineering , network and automation in the era of integration of IoT, Cloud Computing and Cyberphysical systems
14–18.9.2019 (Antananarivo, Madagascar)	Summer School IT Security	GUF	Presentation and discussion on CyberSec4Europe and several of its topics
17-18.09.2019 (Sao Paolo, Brazil)	Brazilian IoT Forum Annual Symposium	IRIT	Organised and chaired a panel on cybersecurity and privacy
17-18.09.2019 (Sao Paolo, Brazil)	Brazilian IoT Forum Annual Symposium	IRIT	Presentation of CyberSec4Europe and Community Hub of Expertise and Cybersecurity Knowledge (CHECK) Toulouse
02.10.2019	SynchroniCity Scale-Up Meeting	OASC	Presentation of CyberSec4Europe at meeting of IoT Large-Scale Pilot "SynchroniCity"
09.10.2019	Asia Smart Cities Week, Yokohama	OASC	Presenting CyberSec4Europe in panel discussion and presentation
11.10.2019	Poznan Development Forum	OASC	Presenting CyberSec4Europe in keynote speech at Poznan Smart City Event
November 2019	Visit to Prof. Luca Viganò (Kings College)	DTU	Research on privacy models
11.11.2019	The Cybersecurity challenges in the IoT era	AS	Contribution to the webinar organized by Cyberwatching, available at: https://cyberwatching.eu/cyber-security-challenges-iot-era
20.11.2019	Global Digital Innovation Alliance Annual Meeting	OASC	Presenting CyberSec4Europe to international stakeholders of the Global Digital Innovation Alliance coordinated by Seoul Digital Foundation

December 2019	Hosting of Jorge Cuellar (Siemens)	DTU	Research on trust and supply chains
30.01.2020	Critical Infrastructure Security and Resilience (CISaR) research group;s workshop (NTNU)	GUF	Presentation of CyberSec4Europe

Table 11: Participation in International events

1.1.12 Other

Date & Venue	Title of Event/ Meeting/Standardization/ Focus Group/Board	Partners	Comments/Discussions/Outcomes
31.01.2019 (Athens, Greece)	Clustering Workshop	UPRC	Participated in privacy and security workshop
11.02.2019 (Pisa, Italy)	ITASEC	UNITN	Presenting CyberSec4Europe in Panel on launching the four pilots
27.03.2019 (Brussels, Belgium)	Vulnerabilities and Global Security of the CNS/ATM systems - The Innaxis Foundation and Research Institute	UNITN	Informal interventions referencing CS4E efforts and activities
27-29.03.2019 (Brussels, Belgium)	DG Home Community of Users	CPT	Informal interventions referencing CS4E efforts and activities
11.06.2019 (Brussels, Belgium)	iCPS	CPT	Participated in event as Session Chair on Cybersecurity
13.04.2019 (Patrasσ, Greece)	6th Patras Innovation Quest Exhibition – PatrasIQ 2019	UPRC	Invited speaker on "Cybersecurity Policies and Technology" infoday, organized by Industrial Systems Institute in the framework of PatrasIQ 2019
04.06.2019	Rencontres Cybersécurité d'Occitanie	IRIT	Presentation of CyberSec4Europe and of Community Hub of Expertise and Cybersecurity Knowledge (CHECK) Toulouse
17.06.2019 (Brussels, Belgium)	EC Community of Users	CPT	Informal interventions referencing CS4E efforts and activities
30.03.2019 (Berne, Switzerland)	EURESEARCH	CPT	Speaker on cybersecurity and competence center pilots
19-23.08.2019 (Windisch, Switzerland)	14th IFIP Summer School on Privacy and Identity Management	AIT GUF KAU	CyberSec4Europe members contributed to the program committee, general chairs, and steering committee of the conference

		KUL	Joint organization with partners from SPARTA, who in particular offered one of the program chairs Participated in conference
02-03.10.2019 (Helsinki, Finland)	Nordic Cybersecurity Event	CPT	Informal interventions referencing CS4E efforts and activities
14.10.2019, (Brussels, Belgium)	Cybersecurity in the Rail sector	ENG	Information Technology and Operational technology NIS Directive application in the rail sector Ongoing initiatives (CEN-CENELEC, rail ISAC) Cyber awareness and cyber culture
11.10.2019 (Brussels, Belgium)	CDSL (VUB): European cybersec month workshop: EU cybersecurity law	TLEX	Presented on the NIS-directive, the GDPR and the similarities between both instruments and participated in a panel
15-16.11.2019 (Bolzano, Italy)	SFScon 2019	UNITN	Talk on the topic of securing software development lifecycle referencing to CyberSec4Europe research activities
19.11.2019	6th meeting of the European Security & Defence College (ESDC)	UPRC	Presented the UPRC's research and training activities including Cybersec4Europe
29.11.2019 (Brussels, Belgium)	EU-China symposium on data security and personal data protection	TLEX	Participated in conference, informal interventions referencing CS4E efforts and activities
03.12.2019 (Brussels, Belgium)	Noord Info Security Dialogue Belux	TLEX	Participated in conference, informal interventions referencing CS4E efforts and activities
05.12.2019	StandICT final event	CPT	Informal interventions referencing CS4E efforts and activities
16.12.2019	Meeting of Spanish standardization committee UNE CTN 320	ATOS UMA	Overview of contributions to Spanish standards and updates regarding CEN/CLC JTC13 and other international bodies Participated in meetings as SC5 president
21.01.2020 (Brussels, Belgium)	7th Annual QED Conference on Cybersecurity	TLEX	Participated in conference, informal interventions referencing CS4E efforts and activities
04-5.12.2019 (Lisbon, Portugal)	Kaspersky Academy Partner Summit 2019	UNITN	Informal intervention referencing CS4E efforts and activities
Regular discussions in 2019 (Estonia)	Standardization Working Group	CYBER	Participation in WG that is putting together the new Information Security Standard for Estonia (a substitution for our current information

			security standard ISKE). Compliance to this standard will be compulsory for all government institutions.
Periodic discussions 2019	EBF Cybersecurity Working Group	ABI	WG participated by national Banking Associations from EEA countries. Cybersecurity experts share their views on threats trends, awareness activities, and implementation of regulations. Outcome: Sharing of new versions of international best practices, consultations about new regulations, definition of a working table focused on cybersecurity certification according to the cybersecurity act.
Three meetings in 2019 (two in Brussels, Belgium, one in Bucharest)	CEF Cyber Governance Board (INEA – European Commission)	ABI	National Representatives from the EU CERT community, members of the CEF Telecom funded projects, EU Commission representatives, ENISA, EU CERT members meet to discuss the on-going projects and the evolution of any issue related to the cybersecurity topic. ABI Lab is one of the CERT members of the Governing Board. ABI Lab has participated in the 2019 to three dedicated High-Level Meetings where presented the EU activities. Outcome: Definition of a Cyber Threat Methodology for the Banking sector. Currently undergoing presentations in the EU Banking community.
Periodic discussions 2019	FI-ISAC	ABI	Financial Institutions Information Sharing and Analysis Centre promoted by ENISA International WG participated by LEAs, CERTs, Banking association. Discussions: Continuous info sharing among members, about cyber-attacks, new threats, new fraud models.
Three meetings in 2019 (Brussels, Belgium)	Payment Security Support Group and Card Fraud Prevention (EPC)	ABI	International WG with participants from national Banking Associations of EEA countries. Cybersecurity experts share their views on threats trends, awareness activities, and implementation of regulations with a special focus on SEPA schemes. ABI Lab is one of the members of the PSSG Working Group and it has participated in the 2019 to three dedicated meetings to discuss security flaws in payments systems and to work

			on the Payment Threats and Fraud Trends Report
Periodic discussions 2019	EBF Ad Hoc Task Force EU Regulatory Framework of Experimentation	ABI	Ad Hoc European Banking Federation (EBF) Task Force. Member of the European Banking Federation Ad Hoc Task Force to discuss the Regulatory Framework of Experimentation. Contribution to the regulatory proposal.
Periodic discussions 2019 with cross-border cyber exercises in June	G7 CEG	ABI	G7 Cyber Expert Group aims to identify and face new vulnerabilities for EU Financial Ecosystem. The bigger cross-border cyber exercises have been performed in June. An international great success.
Periodic discussions 2019	EUROPOL	ABI	The working table discusses, periodically, new events and new trends related to cyber-crime. Definition and dissemination about the awareness campaign: EMMA5
Periodic discussions 2019	European Commission High-Level Expert Group on AI	ABI	As the voice of the European banking sector, the EBF has been accepted as a member of the European Commission newly established High-Level Expert Group on Artificial Intelligence (AI HLG). The AI HLEG has the general objective to support the implementation of the European strategy on AI. It will notably produce draft AI Ethics Guidelines. It will also advise the Commission on next steps addressing AI-related mid to long-term challenges and opportunities through recommendations. The ABI Lab leading person of the ABI Lab Task Force on AI and Data Governance has participated on behalf of the EBF to some of the meetings and activities. Outcome: ABI Lab is also one of the major contributors of the topic representing the various and different applications of the AI in the EBF Working Groups. ABI Lab has recently promoted and created the AI Hub with a special section topic related also to security.
Periodic discussions 2019 and dedicated meetings	Other dedicated Meeting B2B and F2F	ABI	High Level Bilateral Meeting ABI Lab – European Banking Federation (EBF)

			Observatory on Cyber Knowledge and Security Awareness Meeting Discussions: High level Meeting to present the Project activities to the EBF High Level Meeting with the CERTFin constituency to update and present them the EU cyber security activities.

Table 12: Participation/Collaboration in other organizations

It is most relevant that CyberSec4Europe partners have been very active in all of the key activities related to European cybersecurity and with all of the key stakeholders.

Most importantly, CyberSec4Europe partners have achieved key successes in working with standards development organizations, European Commission bodies including but not limited to DG CNECT and ENISA, public administrations, academic and research organizations, the community of products and services providers, users, and society as a whole. The depth and breadth of this impact can be felt within the activities of organizations such as ECSO, CEN/CENELEC, ISO, ENISA, DG CNECT, TrustinDigitalLife and many others.

2 Concertation Event

2.1 Background

As part of its activities, CyberSec4Europe held its first concertation event entitled **Cybersecurity for Europe 2019**, which took place at the Hôtel de Région in Toulouse, from 13-15 November 2019. The event was organized locally by Université Paul Sabatier and the Institut de Recherche en Informatique de Toulouse (IRIT), and OcSSImore, and was hosted by the Occitanie Région at the seat of the regional council of Occitanie.

With more than 8000 research staff from over 100 research units, Toulouse is at the forefront of technological research, playing host to highly innovative companies like Airbus, Orange, Thales, Continental, and Banques Populaires Caisse d'Epargne, among others. In particular, there were more than 3000 cybersecurity professionals in the Occitanie Region, which partnered with *CyberSec4Europe* in the organization of this event.

The event attracted around 154 participants comprising a comprehensive representation from the cybersecurity ecosystem and the stakeholder community, including but not limited to: the public sector (the European Commission, the Occitanie Region, ENISA), the private sector (large companies and SMEs), the research and academic community (from all over Europe), and civil society (NGOs, citizens advocacy organizations).

This event – the first of three annual CyberSec4Europe consultation events - represented a unique opportunity to obtain a snapshot of the current state of play in policy, research, and innovation in European cybersecurity, while at the same time it provided an opportunity to listen to and meet high level political representatives discussing the challenges and opportunities in cybersecurity.

The annual CyberSec4Europe event coincided with the launch of the new CyberSec4Europe website (https://www.cybersec4europe.eu), which introduced interesting features such as blog/news posts from CyberSec4Europe partners primarily based on their work packages deliverables and outputs. The timeliness of the launch with the concertation event saw a significant push in social media outreach rising from 4,534 tweet impressions in October to 24,500 tweet impressions in November. The number of followers on the CyberSec4Europe Twitter account, @CyberSec4Europe, (479) doubled in November, as did the number of website profile visits. Participants at the conference expressed satisfaction in the more dynamic nature of the website and news portal.

2.2 Conference program

The detailed agenda of the concertation event is found in ANNEX 1.

In the first afternoon, speeches were given by the following high-level officials:

> **Miguel Gonzalez-Sancho, Head of Unit, Cybersecurity Technology and Capacity Building, DG CNECT** spoke about "The View from the European Commission".
>
> > In brief, in his reflections on the future of cybersecurity, Miguel Gonzalez-Sancho set the scene of cybersecurity today and mentioned the timeliness of the four pilots, the new Commission starting in December, and the need for Europe to assert itself internationally. Cybersecurity had changed over the previous five years and still remains high on the agenda. Security by design and privacy by design are becoming more than just words.

Challenges remained in national security and internal market innovation, translating research to market, difficulties for SMEs, shortage of skills, and large differences from member state to member state.

There are many challenges which require a joint action with with priorities to address, such as emergency management, sustainable resilience, capability building.

Today, cybersecurity is no longer a matter for "techies" – it affects everyone and touches on national and strategic issues.

Europe is good at rules. Many countries are following the GDPR example. In the first 100 days of the new commission, there will be potentially a draft directive about AI. However, whilst rules are necessary, there is also a need for research, skills and targetted investment. Strategic investment is important on key cybersecurity priorities. The pilots have a very important part to play.

Pierre Benaim and Caroline de Rubiana and Bénédicte Bejim, AD'OCC, presented "A regional perspective: How the Occitanie region is building capacity in cybersecurity":

In brief, at the origin of the CYBER'OCC project, there are two driving objectives :

- The need to help SME's in the face of threats of cyber-attacks,
- The richness of the cybersecurity resources on the territory of Occitanie.

The Occitanie Region has entrusted the economic development agency AD'OCC with the accomplishment of this mission which is to improve the level of safety, structure the cybersecurity sector and prepare the future. In order to address this issue in a concrete way, a the creation of a Cybersecurity Regional Center is important. The presentation on AD'OCC by Caroline de Rubiana is given in ANNEX 2.

Luigi Rebuffi, Secretary General, ECSO, presented "The European Cyber Security Organisation (ECSO)" (ANNEX 3)

In brief, ECSO is an EU association, composed of many members. Since its conception, there is much more investment into cybersecurity with industry investing five times more. ECSO goes beyond research and innovation. ECSO is one of the components in the big dialogue in the domain of cybersecurity.

Since the beginning, ECSO supports the pilots and, in fact, 40% of ECSO's members are key members in the pilots.

In the governance of ECSO, we bring together different stakeholders and we work together in six Working Groups:

- WG1: Standardisation, certification and supply chain management
- WG2: Market deployment, investments and international collaboration
- WG3: Sectoral Demand (Industry 4.0, Energy, Financial, Public Services / e-Government, Health, Transportation, Smart Cities, Telecom - Media & Content)
- WG4: Support to SMEs , coordination with countries and regions
- WG5: Education, awareness, training, cyber ranges
- WG6: SRIA and Cyber Security Technologies

Alliances with non-European countries is necessary. Regulations are needed in some areas which are taking on importance. But what we need most is investment. Europe has not invested enough into cybersecurity. Member States should invest, the private sector should invest but in a common strategy and this is the big challenge. We need investment for research and capacity building. ECSO is already delivering as covered in the above-mentioned Working Groups. The pilots are are now delivering. PPP needs to continue.

The following presentations of the four Cybersecurity Competence Centres were delivered by:

- Aljosa Pasic (ATOS) for CONCORDIA (ANNEX 4),
- Wim Mees (Royal Military Academy) for ECHO (ANNEX 5),
- Fabio Martinelli (CNR) for SPARTA (ANNEX 6),
- Kai Rannenberg (GUF) for CyberSec4Europe (ANNEX 7).

The Conference was opened in the early evening of 13 November 2019 by Kai Rannenberg from Goethe University Frankfurt who is the coordinator of CyberSec4Europe, and who introduced the following speakers:

Bertrand Monthubert, President of Occitanie Data:

Bertrand Monthubert extended a warm welcome to Toulouse. In his opening speech, he said that cybersecurity is a very strong pillar of the digital world on which focus should be placed so that confidence can be gained. "Confidence" might be one of the most important words when considering the digital economy. It was no surprise that this CyberSec4Europe conference was taking place in the Occitanie Region where there are some very large and important research teams (IRIT being one of them) with some companies which are fully engaged in cybersecurity and which have decided to create a cluster around this area, for example, OcSSImore.

A digital strategy was recently adopted with many elements of cybersecurity therein. An objective is for companies to be aware of cybersecurity, to find solutions, and to enhance training. The region of Occitanie, France, is very active in these areas because there is a need to be independent. This is a matter of sovereignity for Europe. Strong research laboratories are necessary. This is a crucial element.

Renaud Vedell from the French Ministry of the Interior:

In his speech, Renaud Vedel highlighted the volatile nature of cybersecurity and the increasing numbers and forms of threats. Concern was that democracy was also being attacked through data and across frontiers – in fact, in cybersecurity, the question arises where do we place those frontiers? There are more and more physical systems and numerous digital systems emerging. Increasingly, cities and regions are being digitalized. In smart cities, there are many grids, and through one grid, an attack can be made on other grids. There is a change in the way we work with new sources of threats. There are continuous developments in AI with new threats and possibilities of hacking. Machines will be able to kind of see and hear, which may be a very good development, but those developments need to be secure and they need to be secured in an ethical framework.

The industry of cybersecurity is quite large but this sector is not well organized and the French government has urged this industry to structure itself better. There is a need to focus

more on fast evolving areas, such as IoT which is spreading in many directions and poses many threats. This is a sector which needs security by design.

Then, there is the digital identity and the e-IDAS Regulation. France is not so advanced in this area and the French government is trying to catch up. There are still many gaps.

There is also a need for intelligence services. The national model will be layered by a national agency. There are 600 agents but this is not enough for the whole country. In July 2019, there was an initiative to establish a French national security campus. This initiative of Occitanie is welcomed.

A roadmap has to be set up and talents and skills at all levels are required. A curriculum has to be prepared and the work of the pilots will be used as inspiration tools.

The dark side needs to be further addressed. Knowledge and prosecution play an important role. We have to make it clear that all malware and such actors will be prosecuted. EUROPOL and such bodies help in this domaine. The issues of sovereignty have to be tackled at several levels, at institution and civil levels. Regulations could help for data brokers to collect data.

Recruitment needs to be diversified: We need more and more to have diverse teams with IT people. We need to build closer ties with academia and research. We have to recognize the work they perform. This is the scenario we are looking at in our strategic review. We have to be creative.

A **video** message from Mariya Gabriel, European Commissioner, Digital Economy and Society for the Conference was shown to the audience, as reproduced below.

"Dear Ladies and Gentlemen,

Welcome to you all. Let me to start by thanking the Organizers to allow me contribute to this Cyber for Europe conference in Toulouse.

Last year, the Commission proposed to step up investments into cybersecurity research and industrial and operational capabilities via a new cybersecurity competence centre and network.

This structure and the European competence centre in particular will enable co-investment, network and community building. Most importantly, it will be the start of much more strategic cooperation and joint priority setting between member states and industry on both the supply and demand sides. But our proposal also directly addresses the larger cybersecurity community and centres of excellence that already exist in all member states. With the new network of cybersecurity competence centres, we want to bring them closer, together and enable practical cooperation at all levels.

Ladies and Gentlemen, you know that things move fast in the area of cybersecurity. That is why we have started the work even before our proposal has completed the legislative process.

Today, we have four European pilot projects of cybersecurity competence networks. They aim to strength the EU cybersecurity capacity and tackle huger cybersecurity challenges for a safer European digital single market and to collect valuable experience for the implementation of the European-wide cybersecurity competence network in the near future.

These four pilots are: CONCORDIA, ECHO, SPARTA and, of course, CyberSec4Europe. We have already met last March in Strasbourg and you know that I support your work. So let me congratulate again the participants of the CyberSec4Europe project but also of the three other projects represented at this event for the work done so far. There are high expectations on you, both in terms of making concrete advances in research and in terms of building and mobilising a wider community and advising the commission in its policy and regulatory work. Altogether you are bringing together more than 160 partners including big companies, SMEs, universities and cybersecurity research institutes from 26 European member states. The overall European investment in these projects will be more than 63.5 Million EUR. Our policy and regulatory work in cybersecurity has completed several important milestones recently.

The European Union Cybersecurity Act has given to ENISA, our European agency for cybersecurity, a strengthened and permanent mandate. Together with ENISA, for which this is a brand new task, we are proceeding well in the implementation of the first European cybersecurity certification framework. There is also very good progress in the implementation of the Commission's recommendation on the cybersecurity of 5G which is a major and urgent priority.

First, each Member State has carried out a national risk assessment of 5G networks and at the European level a coordinated risk assessment was published in early October. To address the risk and security challenges identified, we are now working with member states and ENISA to agree on the necessary mitigating measures by the end of this year.

Last but not least, like every year, October was European cybersecurity month. A very large collection of events driven by ENISA. Its main focus this year was to promote good cyber hygiene and to inform about cybersecurity risks. I cannot insist on this point too much: awareness, knowledge and skills are key if you want to raise to the challenge. More digitization means more exposure to cyber threats and therefore it needs to be accompanied by more training and information at all levels.

Ladies and Gentlemen - In view of all the cybersecurity incidents and threats we are facing, we need a step change, we need to step up investments from both the public and the private sector, we need to equip ourselves with critical technological capabilities and we need to build a stronger community, running from academia and technology to policy and cybersecurity operations. Once again, this insight is the basis for our proposal to create the new European cybersecurity competence centre and network and to make cybersecurity a priority in the Digital Europe Programme and the Horizon Europe.

If we are serious about European technological sovereignty, we must not fail to deliver on cybersecurity and this is the way forward.

I count on all of you and your contributions. And I wish you fruitful discussions during the Conference.

Thank you very much! "

Médéric Collas, who replaced Antoine Derain, Groupe Banques Populaires et Caisses d'Epargne due to a personal family circumstance presented "A regional cybersecurity competence community in the making: the local picture" (ANNEX 8).

In brief, Médéric Collas explained that it was three years ago that they realized that they could not work alone in the field of cybersecurity. They needed to be able to deal with global threats and to do so, it was necessary to source the right innovations and develop a cybersecurity concept which could be shared with their partners. Cooperating with a large pool of expertise was found to be the best way to address the many cybersecurity problems we are facing. For this reason, the OcSSImore Association was created.

The Internal Governance Model consists of:

- Stakeholder security hub
- Technology center
- Industry task force
- Economic development accelerator to foster innovation

They have started to implement this internal governance model and working at the EU level is the way forward. For this reason, they are cooperating with CyberSec4Europe.

The main objective is to create a community and their expectations are to:

- Share the OcSSImore vision on cybersecurity
- Share information to be better informed
- Share expertise with EU partners
- Leverage cybersecurity to improve business

Pascal Andrei, Chief Security Officer, Airbus, delivered the **Keynote speech** on "Cybersecurity at Airbus, bringing a risk-based approach for a better resilience".

The main points covered was Airbus' Corporate Security strategy for the years to come:

a. **Vision**:

- 100% of Airbus products, across all divisions, are secured from design to operations, until disposal
- Airbus is resilient to all security attacks and crisis are managed in a timely manner with controlled impacts
- Security embraces the future to enable business in a fast transforming and threatening environment
- Airbus is compliant with regulations and leverage associated security standards

b. **Top Priorities**:

- Implement global risk based security approach
- Protect supply chain and affiliates
- Protect industrial environment
- Reinforce detection and fast response to incidents

The goal is to have the highest security of Airbus' products and company.

There are 4 typical scenarios on cybersecurity threats linked to the supply chain:

- Malicious infection through supplier connection leading to give access to Airbus systems and networks
- Corrupted hardware or software delivered by supplier leading to corrupt Airbus Systems and Products
- Delivery stopped by supplier leading to postpone Airbus production / maintenance / operation
- Use of suppliers privileges accounts to hack into Airbus systems leading to data leaks

There are **many opportunities for collaboration** with us, such as through:

a. Universities:

- Partnerships on Research and innovations
- Job fairs have inherent limits
- More internships and apprenticeships
- Exchanges experts from industries → Universities

b. Regulators:

- Joint efforts to rationalize the regulations between national and European bodies (subsidiarity)
- Limit duplication of efforts
- Authorities of control and certification must work together
- Regulators are enablers to work on core future projects
- Support the emergence of "European Champions"

c. Threat Scape & Intelligence Services:

- Sharing "Good practices" is not enough
- Interest in having an international coordination to collect exploitable and useful information for companies

d. **Industries**:

- A concerted effort for the whole aerospace / transportation / defense ecosystem is necessary
- Protect the full continuum of assets with the involvement of all the actors
- Push for the market of efficient technical solutions to real technical issues
- Ability to attract and retain talents worldwide

Conclusion:

a. Our philosophy: Moving from IT security to Proactive Cybersecurity
b. Airbus has created a DSO (Digital Security Officer) instead of a traditional CISO
c. Data governance will be your best allied to embrace company's digital transformation
d. Security Risk Based approach must lead to Proactive Cybersecurity by design for efficient holistic resilience (transform processes and adoption of next generations technologies (advance analytics and machine learning) applying the right level of control to the relevant areas of identified risks

During the Conference, the following panels took place and were clustered around key (current and future) cybersecurity topics:

- Panel 1 – Cybersecurity Policy & Capacity Building

- Panel 2 – Recommendations for Cybersecurity Research and Innovation
- Panel 3 – European Cybersecurity Governance
- Panel 4 – Good practices in data sharing for incident handling
- Panel 5 - Who's calling? Managing identities in the cyber world
- Panel 6 – The future of European Cybersecurity
- Panel 7 - The upcoming European Cybersecurity Competence Network: a conversation with the four pilots

Short biographies of the speakers are available in ANNEX 14.

2.3 Panel 1 – Cybersecurity Policy & Capacity Building

Moderator: Kai Rannenberg, Coordinator CyberSec4Europe, GUF

2.3.1 Summary

This panel covered cybersecurity policy issues and capacity building. The invited experts were:

- Miguel González-Sancho, Head of Unit H.1 in DG CONNECT,
- Bertrand Monthubert from the Occitanie Region in France and
- Renaud Vedel, Préfet in the Ministry of Interior in France.

Together they represented three policy levels: the regional, the national, and the European level. The discussion was moderated by Kai Rannenberg, coordinator of CyberSec4Europe. Foci of the discussion were the difficulty of balancing interests of stakeholders from different policy levels, uniting the efforts against cybercrime, and the opportunities and challenges arising from a cybersecurity certification. Short biographies of the speakers are available in ANNEX 14.

2.3.2 Challenges

Challenge 1: Country Boundaries

The risks related to the cyberworld do not know any boundaries, while the public policy tools to fight them do have boundaries. There are national security and cyber intelligence organizations, however, the efforts need to be scaled up to a European level. The problem here is that the member states need to feel comfortable with it.

Challenge 2: Different Interests

It is difficult to bring together regional, national, and European interests and to effectively organize these three levels in an efficient way.

Challenge 3: Cybersecurity and sustainability

Some ICT systems, especially when using algorithms for cryptography and/or artificial intelligence, consume a lot of energy and therefore do not support sustainability. In the light of the environmental changes, this needs to be addressed.

Challenge 4: Security certification

A bit more than 15 years ago, when ENISA was set up, it was decided to not mandate ENISA with certification[1] because the assumption was that the market should deal with it on its own. This did not happen, at least not sufficiently, so now ICT certification is on the European agenda. One difficulty with certification is that it comes at a cost for the involved organizations. Another challenge is to manage the evaluation and accreditation measures that certification is built upon.

Challenge 5: Security often does not consider the perspective of the ordinary user

In most cases, security measures and processes are designed to protect assets. The impact on users' activities and routines is often not considered. So security measures often interrupt the flow of work and life, both in the professional and the private use of ICT: Users are often treated as potential attackers or people, who have no other task than to handle security mechanisms. Security measures often interrupt the flow of work and life, both in the professional and the private use of ICT. At the same time a lack of security can often go unnoticed by users (and often even by experts). This combination of issues does not motivate users to follow tedious security procedures.

2.3.3 Recommendations

Recommendation 1: Cooperation

Cooperation is key to succeed with policy challenges. It is crucial for member states to cooperate, as well as for the organizations and stakeholders at regional, national and European level. For that it is most important to have a common or at least a coordinated strategy. It is necessary that initiatives at the local level are visible. This is also their local responsibility. At the same time, they need to think big and consider how best practices on a local level can be transferred to national or EU level and what effect local best practices can have on larger ecosystems. Policy makers and managers at EU and national levels need to sense avidly the effect of their policy decisions.

Recommendation 2: An Interdisciplinary Approach with Diversity is a Must

It is essential to team up with people form academia, industry and policy to address the arising issues with people who have different expertise. To really understand all kind of threats, people from all different backgrounds are needed. This also includes gender diversity.

Recommendation 3: Enhancing European Competitiveness

In Europe, the European civilizational values and the welfare of people are cherished. However, they cannot be taken for granted and need to be made sustainable. For this, it is necessary to be competitive, e.g. in 5G, data management, artificial intelligence, etc. For this, the responsible sharing of data – while respecting the GDPR and privacy regulations in general– needs to be facilitated. To design and implement sharing of data in a responsible manner, help from cybersecurity experts is needed.

Recommendation 4: Attainable Certification for All

[1] The EC proposal for Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML) included the following recital: "(15) Despite the need for reliable processes, it is often difficult to assess the trustworthiness of products and services. There are publicly and privately organised evaluation and certification schemes. However, evaluation and certification processes tend to be cumbersome, expensive, and slow. All actors, including public authorities would benefit from better technical guidance in their efforts to promote efficient certification systems. A technically competent European body for objective advice on the quality of different standards would therefore improve the possibilities to promote reliable security standards, including where appropriate standards for privacy enhancing technologies, in Europe."[COM(2003) 63 final 2003/0032 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Network and Information Security Agency (presented by the Commission)]

As certification comes with costs, which might not be easy to cover for smaller players, such as SMEs, it is mandatory for its application needs to be well planned including financing models. Research can explore better solutions; however, it is time for decisions, at least for trials for a limited time. This needs to include a spectrum of mechanisms from liability provisions to simple self-declaration by providers.

Recommendation 5: Important to be Working from the Design Stage

In order to create solutions that are working for consumers and end users, it is important to collaborate with designers. They know how to incorporate end-user feedback throughout the whole development process.

2.4 Panel 2 – Recommendations for Cybersecurity Research & Innovation

Moderator: Mark Miller, CEO, CONCEPTIVITY s.à.r.l.

2.4.1 Summary

This panel focused on the realm of cybersecurity research and innovation and recommendations with respect to this topic. With the impending completion of the European Commission's Horizon 2020 Funding Programme and the implementation of the Cybersecurity Competence Centre Pilots, we are entering a new era for European funding of research and innovation. In this panel we have looked at the challenges, opportunities and recommendations for the future in some detail. The panelists, listed below, came from significantly different backgrounds in academia, research and industry sectors (including SMEs) and they have provided a quite lively discussion of the future and their expectations:

- Pierre-Henri Cros – IRIT
- Liina Kamm – Cybernetica
- Nicholas Ferguson – Cyberwatching.eu (Presentation available in ANNEX 9)
- Olivier Dellenbac – French Entrepreneur, ChapsVision & Founder of eFront SA, Paris
- Luigi Rebuffi – European Cyber Security Organisation

Short biographies of the speakers are available in ANNEX 14.

2.4.2 Challenges:

Each panelist was invited to present what they felt were the greatest challenges in the field of cybersecurity research and innovation.

Challenge 1: EU project solutions reaching the market

One of the big challenges encountered was getting the solutions, which emerge from cybersecurity research projects, to reach deployment in the real world. Very often, it was observed that the innovative solutions developed during the research projects do not go any further, especially where SMEs were involved. It was hoped that the pilots would make a difference.

On this subject, it was mentioned that one of the objectives of the EU-funded project "cyberwatching.eu" was to address the challenge of making EU project outcomes more visible. The project was addressing this issue by creating a market place with outputs from completed EU-funded research projects and products and services offered by providers across Europe. Cyberwatching.eu was developing a tool which includes about 180 projects, mapped in terms of taxonomy and their maturity level, with an aim to see how the projects could be exploited. The projects were analysed in terms of their technology readiness levels and MRTL combined with a self-assessment of the project. It is a useful landscaping tool for both EC and projects themselves. The Hub in Toulouse is also introducing a Technology Readiness Level in the maturity of proposed solutions to the market.

Challenge 2: Convincing governments to use EU project solutions

An observation was that governments might consider it easier to make a new law but find it much more difficult to use technology and apply it. For SMEs, it was found that it was a real challenge to use the solutions from research projects and convince others, in particular, governments, to use them.

Challenge 3: Creating cybersecurity giants in Europe

In Europe, there is a need for cybersecurity "giants" but the right strategy needs to be found to create these "giants" in EU. Large EU companies need to bet on smaller companies to push them forward. The issue of building giants is also about industrialization. For example, the number of patents in AI is huge but how many of these patents convert into a practical product. In order to succeed, the right strategy must be found to make global "European giants" emerge.

The industrial policy is coming up. In cybersecurity, national public administrations need to be involved, if Europe wants to put together, entrepreneurs etc., national support is necessary and only then, can we cross the borders. Public administrations are faced with this problem.

Challenge 4: National boundaries

On the question of Europe not being able to produce giants in Europe, the problem could be national. It is a challenge to help a champion go beyond his/her own border. For example, if a product is developed in France, it may be difficult to sell it in Germany simply because Germany will promote its own products. It is, therefore, difficult for a company to rise from a local to a European-based company. Today, in cybersecurity, there is a limitation of borders in Europe. For this reason, there is a need to build up a common market with common regulations.

Challenge 5: Working together with cultural influences and languages

In Europe, there are many different cultures and different languages to manage. Whilst Europe is rich in its cultural diversity, one of the challenges is this cultural influence and actually getting people to work together across Europe. With the pilots, the Commission is succeeding in getting a large number of researchers across Europe to come together. If compared with USA, Europe does not have the right mentality and this mentality is very much cultural and determined by boundaries.

There is yet another challenge. When things fall apart, they crumble. Therefore, more researchers are aiming at resilience. The adoption in Europe has been much more difficult whereas in USA, it is much more dynamic. The approach in Europe is "Yes, that's nice" but that's it. Prevention is okay but a move towards resilience is important. As Admiral Mike Roger said … the EU has to be attentive to this problem. There is a need to create this resilience in Europe.

Challenge 6: Need for investment in cybersecurity

There are different approaches as to how cybersecurity is addressed across the globe. An example given during the panel was that China was perceived as seeing cybersecurity as the state being in full control of the citizen whereas the USA, on the other hand, was leveraging funds to build an ecosystem. The current problem we face is where does the EU stand? Europe needs to invest in cybersecurity. Large companies need to spend money to invest in cybersecurity. The EU can provide some funding but governments, too, need to play their role. The concern expressed was that if Europe did not invest in cybersecurity, the European market and its intellectual property would be transferred to USA. Furthermore, the question arose as to whether Europe wanted its intelligence services to purchase American products to secure their most valuable assets.

Challenge 7: Future EU organization funding strategy in cybersecurity

A key question is "what kind of organization will be developed in the European Union in the future". How will this organization spend the money? There may be some 10-20 topics on which we need to focus EU

investment and attention. If money is invested in the traditional EU approach, then a second step should be considered, the EU defense approach.

Challenge 8: Vision for cybersecurity

Today a real and global vision in cybersecurity for the European Union is necessary. One of the buzz words is sovereignty. For increased sovereignty for the European Union, the digital autonomy should be increased. For this, what are the systems, services we need to provide, the security of the state, privacy of the citizens. There are maybe 10-20 topics on which we need to focus our investment and attention. If we invest money in the traditional EU approach, then we have to consider a second step, the EU defence approach.

Challenge 9: Capacity Building

There is a continued need to strengthen capacity building with respect to the infrastructure, and then, provide the short-term needs for operational capacity.

The Moderator asked the Panelists if there should be a cybersecurity industrial policy that comes from EC? Or, should there be something like that from EU, i.e. how to approach cybersecurity and keeping the IP within EU?

2.4.3 Recommendations

The Key recommendation of Panel 2 from each panellist for cybersecurity research and innovation are given below:

Recommendation 1: EU Regional ecosystems built into a European-scale ecosystem

In Toulouse, home of Airbus, an ecosystem has been set-up in order to be independent. A hope / recommendation is that through the pilot hubs, the set-up of such an ecosystem is being built-up to address and contribute to an independent Europe

Recommendation 2: EU leadership in privacy by design

USA has been very successful in its strategy for cybersecurity. There is an opportunity for Europe to also be successful by respecting the privacy of the individual.

Recommendation 3: Cybersecurity must be considered as an important component in all projects in all of the European funding programs

Cybersecurity should be considered as part of every call, not just specific cybersecurity calls. All projects should have cybersecurity included and should be included within a vertical. European funding programs (such as H2020, DEP and other funding programmes) must ensure that cybersecurity is a component of all projects, e.g. health, financial, transport, critical infrastructure, etc.

Recommendation 4: Investment in cybersecurity

Investment in cybersecurity in Europe is crucial. Europe is far (by a factor of 10) from what countries like USA and China are investing in cybersecurity. Europe needs to invest more in cybersecurity. There is a need to identify the kind of investments and a need to define the real priorities. Maybe an approach is to build 10 smaller airbus-type models in different sectors, e.g. in AI. Second, we do need investment because we have today the issue of 5G security. We are discovering what could have been discovered before. In Europe, we have not recognized that it is now the time to invest in this sector, in AI, blockchain, quantum. We need to invest in research right up to reaching the market level.

Recommendation 5: Cybersecurity industrialization policy is necessary

If Europe wants to be serious in cybersecurity, it is not only about the investment. The dynamics, the driving force, and the appropriate objectives need to be created. There should be a specific program in Europe on envisaging how we can make sure that there are new companies that can emerge in Europe. Focussing on research is insufficient. Think about industrialization in this realm.

Recommendation 6: Cybersecurity education should be a priority

To have a perspective from outside the R&I bubble is extremely important. The best of Europe is in education. The threat of USA competition is there. We need to plan how to address this.

2.5 Panel 3 – European Cybersecurity Governance

Moderator: Afonso Ferreira, CNRS/IRIT

2.5.1 Summary

The panel concentrated on the Governance of the Cybersecurity Community included in the European Commission's Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

The panel had a fruitful combination of industry, academia, PPPs, service providers, and policy makers, allowing for a diversity of perspectives. The panellists were:

- Ana Ayerbe – Tecnalia, Spain,
- Abdelmalek (Malek) Benzekri – UPS, France,
- Médéric Collas – Informatique Banques Populaires, France,
- Miguel Gonzáles-Sancho – European Commission (DG CNECT), Belgium,
- Nicole Harris – GÉANT, The Netherlands, and
- Antonio Skarmeta – UMU, Spain.

The moderator started by setting the scene by outlining the contents of the Regulation Proposal and encouraged the panel participants to focus on the challenges and recommendations for establishing and implementing the governance structure of the regional hubs. He was followed by the initial statements from three panellists, highlighting challenges connected to the governance of the Cybersecurity Community. The floor was then opened to a first set of questions from the audience. The remaining panellists then gave their statements, also followed by open questions. To conclude the panel, the moderator requested recommendations for the governance of the Cybersecurity Community from each of the panellists.

For the sake of clarity in the conversations, the moderator stated that the Community level competence nodes would be addressed as 'Hubs', whereas the European and National levels would continue to be addressed as 'Centres'.

Presentations of this Panel are available in ANNEX 10. Short biographies of the speakers are available in ANNEX 14.

2.5.2 Challenges

The initial statements from the panellists were based on their hands-on experience and existing research on cybersecurity governance. They addressed challenges in **establishing and implementing Governance for the regional expertise hubs, including accreditation, composition, membership** (National / Non-National; EU / non-EU), **IPR, connections with other (cross-border) hubs, connections with the National Competence Centre** and their networks, activities, added-value, financing, etc.

Miguel Gonzáles-Sancho described the European Commission's vision and encouraged the pilots' participants not to be constrained by the Proposal, which is a document in development, while admitting to certain procedural difficulties. He stressed the need for strategic, targeted investments and the importance of creating conditions for all stakeholders to work together. According to him, the main challenge was that the process of governance design was started before identifying the priorities.

Ana Ayerbe gave an overview of the work that Tecnalia is doing as cybersecurity hub in Spain. According to her, the main challenges are the following:

- Trust
- Proximity to industry
- Need to provide funds for nationally and internationally connected local ecosystems
- The need to reconcile different priorities (EU- and national level)
- The need to reconcile top-down with the bottom-up approach
- The need to build up on the existing community and elements

Malek Benzekri stated that the goal of making the Toulouse hub a worldwide influencer was indeed ambitious, and identified the following challenges:

- The need to find a way to leverage the expertise that the local hubs can provide to the society
- The scattered nature of the community: the lack of structure and organisation of the existing capabilities
- The lack of the right level of influence for the lone hub
- The need to work on aspects with regard to industrialization and how to make innovation meet its public

Nicole Harris expanded on her experience at GÉANT in creating an easy, accessible and affordable way to collaborate between TF-CSIRTs through a number of mechanisms, such as listing, self-accreditation, and certification programs for CSIRT teams. Nicole named establishing trust and connections as a priority, which bring about the following challenges:

- The challenge of maintaining a trust-based meritocratic approach
- The possibility for the new teams to find their way in
- Scaling, i.e., maintaining trust in the growing/ broader community
- Lack of auditors in sufficient quantities
- International outreach.

Médéric Collas outlined the following challenges, based on his daily work as a cybersecurity expert who develops solutions:

- The questionable efficiency of extra investments as means to gain leadership for Europe
- The questionable character of the idea to "grow" European giants rather than focusing on Use Cases
- Possessing the right vision in order to inform decisions
- Being able to determine the best cybersecurity capabilities

Antonio Skarmeta drew from his extensive experience as a renowned cybersecurity researcher and stressed the following challenges:

- How to formalize the existing coordination of the community
- How to engage the members
- How to define an efficient funding model

Anders Pall Skött (DTU), from the audience, took the floor to share experiences obtained regarding the establishment of the Danish Competence Centre. He expressed the need for an agile organisation and expressed the following challenges to succeed in such an ecosystem.

- Trust: a framework is necessary to collaborate
- Defining and implementing governance models
- Lack of skilled personnel and the means to train them
- Lean on other initiatives. There are a lot of initiatives but how can they be used
- How to drive an agenda for people to meet so that they can be close to each other
- Make a link to the general digital hubs in Denmark and Europe. Find a way to collaborate.

2.5.3 Recommendations

The recommendations provided were specifically connected to Governance that avoided the pitfalls of vague statements that are not actionable. The panellists and the audience recommended the following in order to establish workable and efficient governance for community level hubs of cybersecurity expertise:

Recommendation 1: Governance has to be context related

To remain open-minded with respect to governance, as different governance templates will be needed for different contexts (e.g. health, financial, Member States, etc.), including membership and structuring mechanisms and procedures, not forgetting to involve unusual stakeholders, for example, civil society, NGO's, and open source communities.

Recommendation 2: Effective infrastructures for connection and cooperation

To establish effective infrastructures for connection and cooperation, including research groups, connections to the wider community, and the need to go beyond individual interests.

Recommendation 3: Common vision and mission promoting European values via hubs communities

To federate in the hubs communities with a common vision and mission that promote the European values. Furthermore, the hubs should remain open and engage with effective strategies to build trust with the involved communities.

Recommendation 4: Concentrate on innovative offers for demand driven services and capacity building offerings

To concentrate the innovation offer on services, use cases, and capability building, that are demand-driven and oriented to serve the citizens. In this respect the hubs should engage SMEs and find the champions which can grow.

2.6 Panel 4 – Good practices in data sharing for incident handling

Moderator: Antonio Skarmeta, University of Murcia (UMU)

2.6.1 Summary

An Introduction to the topic was provided by Antonio Skarmeta who highlighted the overall technical and operational challenges in data sharing for incident handling, namely:

Technical challenges:

- **Interoperability** between threat intelligence sharing platforms

Learning new threats, based on **advanced data analysis:**

- **Common data models**, for data sharing
- **Reputation** of the reporting party
- Adversaries can **exploit machine learning** techniques
- **New models** based on the application of AI

Operational challenges:

- **Protecting the privacy of citizens** in data sharing, but still empowering the user to share information
- Providing an adaptative **security loop** to cyber threats and new attack vectors
- **Facilitating non-expert** (SMEs, professionals) access to technology

The panel consisted of the following experts:

- Fabio di Franco, ENISA
- Aljosa Pasic, ATOS
- Liina Kam, CYBERNETICA
- Edgardo Montes de Oca, Montimage
- Valerio Senni, UTRC

Presentations of this Panel are available in ANNEX 11. Short biographies of the speakers are available in ANNEX 14.

2.6.2 Challenges

Challenge 1: Need of common models and tools

Several of the panelist argued about the tools and data models' harmonization that are required for incident reporting and highlighted some of the challenges faced in European society due to digitalization which impacts the life of citizens every day.

Some of the challenges mentioned were:

- The speed of emerging challenges and how to mitigate them effectively
- Standard operational procedures are difficult to manage
- There are challenges in testing and improving knowledge in this field

ENISA is working with CSIRTs on building trust between Member States. Currently, it is difficult to foster trust between Member States but they are working on building trust in technical ways and through an

exchange of information. ENISA is developing a CSIRT network[2], with capacity building with training the trainers, risk management training and by providing expertise to Member States.

ENISA has developed a taxonomy, a CSIRT by country interactive map[3] and a list of 40 CSIRTs operating in Europe. Taxonomy is important as it provides a baseline for incident handling, statistics and information exchange. Tools such as "The Hive" and "MISP" are being considered.

Challenge 2: Emerging threat intelligence

Examples of quick reaction to respond to incidents was described by ATOS in their presentation concerning Cyber Threat Incident (CTI) sharing in the Financial sector. Nowadays, there is a lot of overhead from incident detection to incident reporting. It is a common problem for all banking institutions. Banks Need to comply with different regulations and are faced with different constraints and rules; even for the same incident, there can be a different kind of reporting. CyberSec4Europe has defined a workflow for incident reporting and immediate reporting in D5.1 (Incident Reporting Demonstration Case) which allows more time for CTI analysis and data sharing. Different tools are available, as well as a comparison of the tools.

In other contexts such as SMEs, Montimage provides CTI services to this sector where several aspects need to be taken into consideration:

The problem:

- 58% malware targets small businesses
- Attacks are increasing
- There is a need to provide threat intelligence for SMEs in an easy way for the information to be usable

The Opportunity:

- Currently SOCS, SIEMs are for large companies (representing only 0.2% of the market)
- SMEs are most dependent on cloud usage
- 73% of attacks are aimed at web applications. Therefore, there is an urgent need to provide tools for SMEs!

The Pain points:

- Real-time CTI (in just seconds)
- Comprehensive threat indicators based on open standards (STIX/TAXII)
- Problem of trust of intelligence shared, combine different sources, dataset OSINTs and commercial blacklists)
- Removing complexity: There is a need for real time reaction, a need for more comprehensive threat indicators, a need to automate processing to remove complexity for use by SMEs
- Modular and scalable: to serve different categories of customers (SMEs and large enterprises)

Challenge 3: Data sharing and interoperability

There are many challenges with respect to data sharing, in particular:

[2] Link to CSIR network: https://csirtsnetwork.eu/
[3] Link to CSIRT Interactive map : https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

- Everyone, consumer and producer (bilateral), has different levels of trust depending on whether they are acting as producer or consumer, and this has impact on how GDPR is applied
- There are various sharing models and policies
- Data quality and credibility are crucial to incident analysis
- There is a need to speed up processing and analysis
- There is a need for more tools to support increasing processing and analysis in machine-readable format

Valerio Senni spoke about data sharing of CTI handling in Civil Aviation. More and more, the software in civil aviation is looking towards standardizing how cybersecurity can be assured and how to promote sharing and collaboration in cybersecurity in the sector, considering aspects like:

- Threat modelling, data flow modelling, characterization of systems and assets (safety, legal, economic)
- Common risk models
- Continuous airworthiness, post-EIS support and minimize re-certification efforts

Challenge 4: Accelerating the reaction and countermeasures

There is an urgency for timely response to incidents in the digital world due to their immediate impact. We are connected at all times. Our services are interconnected across borders. An attack against one service in Europe can hinder others across Member States. Even an Estonian news web site uses backend services in Poland, France, Germany and the United States of America.

Preventing, detecting, resisting and pushing back against a cyberattack requires collaboration across borders. Cybersecurity awareness requires sharing information and collaboration between CERTs.

Some additional aspects are:

- How to provide evidence to a non-technical audience?
- How to rebuild trust after an incident?

One important aspect to consider is how the current body of knowledge will react in a timely way to detect threats, will the tools be fast enough, because the adversary – not human – will use stealth and learn about the defences. The Panellists responded as follows:

- CTI needs to be timely, automated and able to adapt dynamically
- Aviation is a more complex system that can be handled in a different way. There is still a need (ongoing) to analyse how to tackle this effectively
- Predictive security. One of the challenges is that we are interconnected. We continuously need to work on automatic and diverse reactions to strengthen our defence before the attack happens. Continuous defence
- How can we prevent the attacker from benefitting from this: attack their business model behind data sharing

Challenge 5: Privacy and Security balance

However, better security has a privacy problem – sharing information about attacks shows one's vulnerabilities. If someone tries to use an attack against you, they might believe that you are vulnerable. Thus, combining multiple sources for cybersecurity data will require protecting all data owners.

Cybernetica's vision is to build machine-readable standards for cybersecurity information and then build privacy-preserving services for cross-border CTI data sharing.

Following a question on data sharing and losing some privacy, the panellists responded as follows:

- The data shared needs to be encrypted and rules needed to be agreed upon in advance, i.e. what to declassify and analyse. Research needs to be continued
- There are some sources for analysing that can be used in which the GDPR does not apply as do not have private information
- If personal information is removed, it can be shared
- An IP-mask can be used

2.6.3 Recommendations:

The Key recommendation of Panel 4 from each panellist for cybersecurity research and innovation are given below:

Recommendation 1: Real time reactive data sharing solutions

The impact of cybersecurity has immediate impact in the digital world hence it is important that we have real-time and reactive data sharing.

Recommendation 2: New tools for support data sharing and privacy

Data sharing shows vulnerabilities and that is why it is important to have tools for cross-border sharing with privacy support.

Recommendation 3: Machine-learning tools to improve data management

The increase in the size of shared data and transferred data need to be made more manageable. Using machine-learning, it is possible to find out which threats are more important and the order of sharing.

Recommendation 4: Prevention based on resilience of the systems and predictive intelligence

There is a need to work on automatic and diverse reactions to strengthen our defence before the attack happens. Work is needed on new domains like civil aviation for prevention by increasing the resilience in civil aviation and related stakeholders. Prevention needs to be covered in the entire system, including Air operation centers.

Recommendation 5: Advanced analytics tools and for threat intelligence

Research is needed in providing an adaptative security loop to cyber threats and new attack vectors. Solutions need to be timely, automated and able to adapt dynamically, and more tools to support increased processing and analysis in machine-readable format.

2.7 Panel 5 – Who's calling? Managing identities in the cyber world

Moderator: Javier Lopez, University of Malaga (UMA)

2.7.1 Summary

This panel covered the issues of Identity Management. The invited experts were:

- Fabio Martinelli (CNR, Italy): Identities in data usage control
- Stephan Krenn (AIT, Austria, as a representative of CyberSec4Europe): Offline privacy in an online world
- Simone Fischer-Hübner (KAU, Sweden, as a representative of CyberSec4Europe): Challenges of user-centric privacy preserving Identity Management
- Jesús Luna (Bosch, Germany): End-to-End Identity Management
- Henrich C. Pöhls (University of Passau, Germany): Identity is technically interdisciplinary

As for the other panels, five very well-known professionals and researchers both from outside the CyberSec4Europe consortium and from the consortium itself discussed the theme of "Identity Management". The moderator was Javier Lopez who introduced the panel and the main issues to be discussed on managing identities in the cyber world and the dark problems that come from the use of the Internet (a fundamental technology for society today). Javier Lopez highlighted that even though progress is evidently notable and useful, the problems are also evident and remain. Presentations of this Panel are available in ANNEX 12. Short biographies of the speakers are available in ANNEX 14.

2.7.2 Challenges

Challenge 1: Different ways for access control

The technical concept of "identity" (is defined in the RFC 4949), which links Identity with Authentication. To do this, there are many mechanisms such as the verification of MAC-address for networks, keys for cryptography, laws, unique IDs for users, etc.; but they all force us to look at privacy at the same time and that the "identity" must be consistently aligned and interoperable across all the stakeholders' views. Any user must be aware of the type of mechanism applied and how.

The concept of access control is key in order to preserve privacy. As part of the usage control model, the specification of "obligations" and related aspects such as subjects (identity, credits, etc.) and objects (value, role permissions, etc.) are fundamental to reduce privacy risks. Indeed, access control is one of the key mechanisms to protect the subject and guarantee data anonymization (as an "obligation"). In detail, these related aspects are:

- Obligations. They are considered compulsory actions that must be performed by subjects stating "pre/on-going/after"
- Identity corresponds to attributes that must be used as a parameter of security "policies" (e.g., UCON policies) to allow access to resources. The attributes are updated under security "policies"

However, the challenge is that this type of model is not easy to take to real world scenarios and to be implemented by companies.

Authentication of devices is a challenge too and it should be applied depending on the scenario. For example, in monitoring scenarios where it is required to monitor in real time, the authentication should be done depending on the context so as not to impact in the real-time.

Challenge 2: Privacy risks linked to Identity Management. Are there sufficient regulators?

Preserving identities where privacy is itself a security issue is a challenge. Diverse mechanisms have been proposed for Identity Management starting with the use of traditional certificates followed by Online Identity Providers (using certificates plus including extra information about attributes) to the user-centric and privacy-friendly Identity Management models (where users decide about their information). Many approaches exist (PRIME, PRIMELIFE, ABC4TRUST, …) and they are available in the literature; simply we have to raise awareness on them so that they are applied.

The challenges of the "classical model" of user-centric privacy enhancing Identity Management were pointed out. The models should be enough to exclude information to preserve its value if required (i.e., to have more control of the data and its value). An example of this is precisely the eHealth scenarios (as considered in the project PRISMACLOUD - Redactable Medical Documents) where there are clear tradeoffs between privacy and patient safety and utility. In this sense, many aspects related to key management and trust are relevant issues to be considered.

Key management is crucial to provide privacy, but other related mechanisms are necessary such as secure key backup and recovery, transparency, and the establishment of privacy default settings.

Concerning the question on regulators there were different answers:

- There are regulation frameworks, but there are insufficient policies to manage the consequences
- There are regulators, but it is necessary to split the issues between security policies and Identity Management because the Supply Chain ecosystem is very complex and it is necessary to protect the diverse types of identities from the different stakeholders
- Laws are useful and they do exist but it is necessary to understand them and to listen to others in order to establish more useful rules (accurate regulators and more precise security that people need)

Further, concerning privacy issues in the diverse social networks, in order to navigate into the Internet (specifically Google) brings on its own type of privacy issues, and more so when the user forces the use of different authentication mechanisms. It is very important to see privacy-by-default (different results depending on the application and person).

Challenge 3: New risks associated by the rise of new technologies such as blockchain

The importance of the current "digital transformation" and its related challenges was covered by the panelists. There are many technologies that are being adopted in a determined context (IoT, IA, blockchain, etc.) making digitalization a very complex undertaking, mainly because, in this convergence, the identity ecosystem itself is part of the digital transformation, i.e., the challenge is to provide a holistic Identity Management solution. Indeed, this type of scenario also affects other areas, such as Supply Chain where many technologies and actors interact.

Challenge 4: Certification and its continuous updating requirements.

A possible solution for certification could be to provide continued certification to make ensure a continuity in auditing in order to prove "valid identities".

2.7.3 Recommendations

Recommendation 1: Creation of an "identity ecosystem"

A complex ecosystem needs to be created forcing at the same time the creation of an "identity ecosystem". As part of the identity ecosystem, it is necessary to consider the level of cooperation between partners (risk management into IdM processes), the interactions and performance of operations (for example, in the Supply Chain scenario), and certification updates.

Recommendation 2: Provision of certification of attributes

This might help users to build trust on the mechanisms used.

Recommendation 3: Provision of Privacy default settings

This might include the provision of a dynamic consent form that the users can update according to their needs and the different privacy requirements of the applications.

Recommendation 4: Use of auditing mechanisms

This could help to ensure the appropriate use of identities by companies.

Recommendation 5: Transparency

It is essential that it is transparent to the users the Identity Management mechanisms that are being used in each specific stage.

2.8 Panel 6 – The future of European Cybersecurity

Moderator: Evangelos Markatos, FORTH

2.8.1 Summary

The main focus of Panel 6 was to explore "The Future of European Cybersecurity". To do so, it assembled a selected set of panelists consisting of:

- Afonso Ferreira, Research Director, CNRS
- Fabio Di Franco, ENISA
- Fabio Martinelli, Research Director CNR
- Bart Preneel, Professor, KU Leuven

Presentations of this Panel are available in ANNEX 13. Short biographies of the speakers are available in ANNEX 14.

2.8.2 Challenges

Afonso Ferreira suggested that main trends include: AI, blockchain, quantum, IoT, 5G, HPC, Cloud, Fake news, Deep fake, Games, Robots, Autonomous systems, Cyber-Physical systems, Drones, Augmented Reality / Virtual Reality. With respect to the attackers, the main actors will include: Rogue states, Organised Crime, and Hybrid threats. He also mentioned that we should expect "black elephants": something likely to happen that will have a devastating impact.

Fabio Di Franco presented his work at ENISA. The main challenges identified for a safer Europe are on

(i) Complexity and Supply Chain
(ii) Crypto Systems and Quantum Computing
(iii) Privacy in Big Data and Digital Identities
(iv) Detection, Mitigation, and Response to Cyberattacks
(v) Digital Transformation &AI
(vi) Education and capacity building
(vii) Awareness Raising

Fabio Martinelli presented his work at CNR and ECSO. From the research areas mentioned, he focused on

(i) Blockchain
(ii) Artificial Intelligence
(iii) IoT, and
(iv) 5G

He emphasized that it is better to prevent than to cure. Thus, preventing security problems is the best approach.

Bart Preneel talked about the risks in supply chain, the mass surveillance, and the continuous data breaches. He said that European fragmentation is an issue that needs to be addressed. He talked about the changing role of cryptography and the use of multi-party computation as a safe and secure alternative to central collection of big data. With a stunning drawing of the Palace of Knossos in Crete he underlined that architecture is the key point: a single point of trust may eventually become a single point of failure and suggested that open source is a viable option.

2.8.3 Recommendations

After the presentations the panelists were asked a sequence of questions.

2.8.3.1 How has the field of cybersecurity changed in the last 5 years?

The panelists suggest that the topic is being discussed in EU continuously these days. It has become part of our everyday lives. New applications, such as autonomous vehicles, bring it to the forefront. There are daily articles in the press regarding incidents. Many more people have started working in cybersecurity. There is an understanding that national security agencies – especially after Snowden's revelations – collect and analyze a variety of data.

The panel also suggested that the digital transformation is already here. Applications like Robotics (including autonomous vehicles) have a clear impact on cybersecurity. It is understood that cybersecurity is a means of protecting the Digital lives of everyone – and Digital is everywhere now.

2.8.3.2 What is the biggest challenge that Europe faces in the area of cybersecurity?

It was suggested that there is a definite and profound collision between market perspectives and national security. Thus, there is a need to define the limits on what to control. A major challenge to be confronted is whether we will be able to protect what we develop while keeping separately the nations' cyber wars.

Another challenge is that Europe's competitors, such as the USA, are one country. On the contrary, the European fragmentation is obvious, since every country sees cybersecurity under its own national security paradigm. An example is the removal from the ENISA yearly updates the status on Crypto protocols. At the moment, there is no funding for such a project. Many countries have shown reluctance to support such efforts and provide data.

Also, whilst there is a lot of good research in Europe, the problem arises how to move from research to market exploitation. Moreover, there is a cultural difference between Europe and the US. In Europe, people do not want to fail.

Finally, there is a definite lack of venture capital in the EU. In the USA, billions of dollars are spent on Blockchain etc. whereas in Europe, investing in cybersecurity is insufficient.

2.8.3.3 What will be the biggest problem in European Cybersecurity five years from now?

Three were the main issues identified as:

(i) Overcoming fragmentation
(ii) The "war" of Artificial Intelligence and losing control
(iii) The IoT/5G scene will increase the surface of attacks

2.8.3.4 What do we need to do so that Europe will make a difference ten years from today?

Open source solutions: The panel suggested that open solutions will be an enabler, since they will increase the chances of verification.

Fund larger projects: There is also a need for larger project funding with a duration of more than 5 years. This will result in longer term capability building activities. There is a need to define "Grand Challenges" – such as the ones set by the CERN model.

FET Open in different areas: It was also suggested that we should look at FET Open and be collaborative with ERC, where excellent research is performed but the market is missing. The best ideas should flourish.

The DARPA model provides a good example of ideas moving to market and project ending if they do not perform in a short time period.

Restructure Funding: A good architecture of European funding would therefore consist of blue-sky individual projects under ERC, plus a large number of collaborative FET Open projects in strategic areas that could also network the results stemming from ERC, complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

Move from "National" to "European": There is a need for EU solidarity (the EU budget should take into account the digital market along with the welfare of its citizens). We should get rid of the national security approaches and move on to an EU security approach.

Possibly, also we need **better communication**: a better way to communicate our ideas to decision makers, including the European Commission, the European Parliament, and the European Council.

2.9 Panel 7 – The upcoming European Cybersecurity Competence Network: a conversation with the four pilots

Moderator: David Goodman, Trust in Digital Life (TDL)

2.9.1 Summary

The intention of this, the final session on the last day of the Cybersecurity for Europe 2019 event, was to review the proceedings of the previous two days and what it held in store for the future of the proposed European Cybersecurity Competence Network. To help guide the discussion, moderator, David Goodman (Trust in Digital Life), introduced representatives of the four pilots:

- Kai Rannenberg, Goethe University Frankfurt (CyberSec4Europe)
- Fabio Martinelli. Consiglio Nazionale delle Recherche (SPARTA)
- Wim Mees, Royal Military Academy of Belgium (ECHO)
- Aljosa Pasic, Atos Spain (CONCORDIA)

Short biographies of the speakers are available in ANNEX 14.

2.9.2 Challenges

Challenge 1: How Are We Doing?

The main question addressed to the panel underlying the subsequent conversation was: are we working well enough and, more to the point, are we working well enough together?

One question that is repeatedly asked of the four pilots whenever their representatives are assembled on a panel (such as this one!) is how they are going to work together, given that their objectives are so closely aligned. The coordinators have face-to-face meetings once a month, chaired by DG CNECT, and representatives of the respective dissemination and communications groups have been working as a team and have created a common brand and website.

One objective is to produce a common presentation showcasing the common tasks as well as the distinctive features and achievements of each pilot that any one of the pilots could present, thereby demonstrating tangible evidence of collaboration.

Challenge 2: Research Spending

One of the contentious assertions made in one of the previous sessions is that too much taxpayers' money is being spent on research that could be better deployed in other areas. Not surprisingly, all four representatives, while acknowledging the thrust of the argument fundamentally disagreed with the underlying premise.

We are not always united in diversity. In the case of the four pilots, our activities are aligned and overlapping and we should make sure that we are not doing the same thing over and over again. The coordinators have looked at introducing the possibility to have focus groups, which would help bring the pilots in. Activating this initiative would help bring more synergy, so that there is more direct interplay. Federated cyber ranges and an early warning system are two areas that could form the basis of one or more focus groups, possible as early as first quarter 2020.

Despite the breadth of coverage of the four pilots, very often the small players and some topics are left out e.g., payment areas, smart devices, etc..

Challenge 3: Mutual Admiration

Not surprisingly, as all four pilots responding to the same call for proposals in May 2018, there is a lot of similarities between them all. But there are differences and as we get familiar with each other in the spirit of collaboration rather than competition each pilot can afford to say what they particularly admire in each other.

Each of the pilots was asked in turn which feature of each of the other pilots they admired the most or even coveted. The value of this exercise formed a natural segue from the previous discussion, as one of the questions that is regularly posed to the four pilots is simply: why do we need four pilots, wouldn't one be enough? The often-observed response is that each pilot, whilst having addressed the same call for proposal, demonstrates the same eventual objectives but with different flavoured approaches. The differences are important – we wouldn't wish all four pilots to pursue the same approach to, say, research. Or, for that matter, targetting the same audiences. The Commission could have chosen just one pilot … but they didn't and wanted a more diverse approach.

Each panellist in turn considered the strengths of each of the other pilots. The standout features of each pilot were:

- CyberSec4Europe - openness including a commitment to open standards, and very clear vertical use cases and ambitions for citizens
- ECHO - an Early Warning System, federated cyber ranges
- CONCORDIA - community building including an eco-system for education, virtual labs as well as Women in Cybersecurity
- SPARTA - innovation approaches including the 'Moonshots' initiative

Challenge 4: Strategic Autonomy

There are two aspects to the question of strategic autonomy in Europe and, what is lacking to a large extent, is how can we build products, how can we build up European industry. Why do our young smart students not succeed and create success stories as they appear to do elsewhere? Strategic autonomy is not just technology driven.

Challenge 5: Future Concertation Events

The consensus was that the concertation event had provided considerable food for thought in relation to many of the key areas of research that are germane to a future network: but what about future events and, more specifically, what lessons could be learned from the event in Toulouse to inform preparations for the next two annual concertation events? One aspect was the regrettable paucity of representation from the other

three pilots, given that the primary purpose of this type of event, as acknowledged by each of the pilots and the Commission, is to bring together as many stakeholders as possible to achieve synergy and common purpose. In that respect, but only in that respect, the event was disappointing and a concerted effort has to be made, not only by the CyberSec4Europe organisers but the other pilots and the wider stakeholder community as well, to ensure that future events better fulfil expectations.

2.9.3 Recommendations

Recommendation 1: Increasing Stakeholder Participation At Future Events

A concerted effort has to be made, not only by the CyberSec4Europe organisers but the other pilots and the wider stakeholder community as well, to ensure that future events better fulfil expectations.

Recommendation 2: Meeting Expectations On Collaboration

The four pilots are consistently and constantly being made aware of the importance of both creating real synergies on project work and also being seen to collaborating in areas where there is obvious overlap. It should be a target for early 2020 for the coordinators to demonstrate concrete collaborative initiatives, perhaps through the proposed focus groups.

Recommendation 3: Pooling Presentation Material and Representation

Whilst it has been important during the first 12 months of the four pilots to have representatives from each participate at stakeholder events in Brussels and elsewhere, it is time-consuming and expensive. The four pilots' communications group working closely with the coordinators should come up with a series of presentations that a single appropriate representative from any of the four pilots is able to present. The presentation should contain an overview section ('chapeau') pertaining to all four pilots in addition to brief individual sections for each pilot.

Recommendation 4: Addressing Strategic Autonomy

One of the ever-present conundra is, despite the wealth of talent and experience, the lack of strategic autonomy for cybersecurity in European industry. There is a degree of urgency for the pilots individually and collectively to provide recommendations to the stakeholder community.

Recommendation 5: Minding The Gaps

Despite the broad range of technical and business issues covered by the pilots, there are many broad areas not covered as demonstrated by the taxonomy mappings. There are even more areas that require attention that need to be identified with recommendations as to how they should be addressed.

3 Conclusions and Recommendations

When gathering a high level participants from a comprehensive group of the cybersecurity eco-system it is evident that their conclusions and recommendations are relevant and important for the European Instititions and decision-makers to take notice. As such, we have summarized the key recommendations from all of the CyberSec4Europe Toulouse Concertation panel sessions in the section below. In many ways, to those in the cybersecurity community these conclusions and recommendations are not a surprise. However, what is required is action mainly on the part of the European Insititutions and the public sector in general and this is an important conclusion that must be taken into account.

Recommendations of Panel 1: Cybersecurity Policy & Capacity Building

Recommendation 1: Cooperation

Cooperation is key to succeed with policy challenges. It is crucial for member states to cooperate, as well as for the organizations and stakeholders at regional, national and European level. For that it is most important to have a common or at least a common strategy. If different strategies exist they should be coordinated. It is necessary that initiatives at the local level are visible. This is also their local responsibility. At the same time, they need to think big and consider how best practices on a local level can be transferred to national or EU level and what effect local best practices can have on larger ecosystems. Policy makers and managers at EU and national levels need to sense avidly the effect of their policy decisions.

Recommendation 2: An Interdisciplinary Approach with Diversity is a must

It is essential to team up with people form academia, industry and policy to address the arising issues with people who have different expertise. To really understand all kind of threats, people from all different backgrounds are needed. This also includes gender diversity.

Recommendation 3: Enhancing European Competitiveness

In Europe, the European civilizational values and the welfare of people are cherished. However, they cannot be taken for granted and need to be made sustainable. For this, it is is necessary to be competitive, i.e. in 5G, data management, artificial intelligence, etc. For this, the responsible sharing of data – while respecting the GDPR and privacy regulations in general– needs to be facilitated. To design and implement sharing of data in a responsible manner, help from cybersecurity experts is needed.

Recommendation 4: Attainable Certification for All

As certification comes with costs, which might not be easy to cover for smaller players, such as SMEs, it is mandatory for its application needs to be well planned including financing models. Research can explore better solutions, however it is time for decisions, at least for trials for a limited time. This needs to include a spectrum of mechanisms from liability provisions to simple self-declaration by providers.

Recommendation 5: Important to be Working from the Design Stage

In order to create solutions that are working for consumers and end users, it is important to consider perspective. Therefore it is useful to collaborate with designers, as designers know how to gather and incorporate end-user feedback throughout the whole development process.

Recommendations of Panel 2: Recommendations for Cybersecurity Research & Innovation

Recommendation 1: EU Regional ecosystems built into a European-scale ecosystem

In Toulouse, home of Airbus, an ecosystem has been set-up in order to be independent. A hope / recommendation is that through the pilot hubs, the set-up of such an ecosystem is being built-up to address and contribute to an independent Europe.

Recommendation 2: EU leadership in privacy-by-design

USA has been very successful in its strategy for cysbersecurity. There is an opportunity for Europe to also be successful by respecting the privacy of the individual.

Recommendation 3: Cybersecurity must be considered as an important component in all projects in all of the European funding programs

Cybersecurity should be considered as part of every call, not just specific cybersecurity calls. All projects should have cybersecurity included and should be included within a vertical. European funding programs (such as H2020, DEP and other funding programmes) must ensure that cybersecurity is a component of all projects, e.g. health, financial, transport, critical infrastructure, etc.

Recommendation 4: Investment in cybersecurity

Investment in cybersecurity in Europe is crucial. Europe is far (by a factor of 10) from what countries like USA and China are investing in cybersecurity. Europe needs to invest more in cybersecurity. There is a need to identify the kind of investments and a need to define the real priorities. Maybe an approach is to build 10 smaller airbus-type models in different sectors, e.g. in AI. Second, we do need investment because we have today the issue of 5G security. We are discovering what could have been discovered before. In Europe, we have not recognized that it is now the time to invest in this sector, in AI, blockchain, quantum. We need to invest in research right up to reaching the market level.

Recommendation 5: Cybersecurity industrial policy is necessary

If Europe wants to be serious in cybersecurity, it is not only about the investment. The dynamics, the driving force, and the appropriate objectives need to be created. There should be a specific program in Europe on envisaging how we can make sure that there are new companies that can emerge in Europe. Focussing on research is insufficient. Think about industrialization in this realm.

Recommendation 6: Cybersecurity education should be a priority

To have an outside perspective from the R&I bubble is extremely important. The best of EU is in education. The threat of USA is there. We need to plan on how to address this.

Recommendations of Panel 3: European Cybersecurity Governance

Recommendation 1: Governance has to be context related

To remain open-minded with respect to governance, as different governance templates will be needed for different contexts (e.g. health, financial, Member States, etc.), including membership and structuring mechanisms and procedures, not forgetting to involve unusual stakeholders, for example, civil society, NGO's, and open source communities.

Recommendation 2: Effective infrastructures for connection and cooperation

To establish effective infrastructures for connection and cooperation, including research groups, connections to the wider community, and the need to go beyond individual interests.

Recommendation 3: Common vision and mission promoting European values via hubs communities

To federate in the hubs communities with a common vision and mission that promote the European values. Furthermore, the hubs should remain open and engage with effective strategies to build trust with the involved communities.

Recommendation 4: Concentrate on innovative offers for demand driven services and capacity building offerings

To concentrate the innovation offer on services, use cases, and capability building, that are demand-driven and oriented to serve the citizens. In this respect the hubs should engage SMEs and find the champions which can grow.

Recommendations of Panel 4: Good practices in data sharing for incident handling

Recommendation 1: Real time reactive data sharing solutions

The impact of cybersecurity has immediate impact in the digital world hence it is important that we have real-time and reactive data sharing.

Recommendation 2: New tools for support data sharing and privacy

Data sharing shows vulnerabilities and that is why it is important to have tools for cross-border sharing with privacy support.

Recommendation 3: Machine learning tools to improve data management

The increase in the size of shared data and transfered data, need to be made more manageable. Using machine-learning, it is possible to find out which threats are more important and the order of sharing.

Recommendation 4: Prevention based on resilience of the systems and predictive intelligence

There is a need to work on automatic and diverse reactions to strengthen our defence before the attack happens. Work is needed on new domains like civil aviation for prevention by increasing the resilience in civil aviation and related stakeholders. Prevention needs to be covered in the entire system, including Air operation centers.

Recommendation 5: Advanced analytics tools and for threat intelligence

Research is needed in providing an adaptative security loop to cyber threats and new attack vectors. Solutions need to be timely, automated and able to adapt dynamically, and more tools to support increased processing and analysis in machine-readable format.

Recommendations of Panel 5: Who's calling? Managing identities in the cyber world

Recommendation 1: Creation of an "identity ecosystem"

A complex ecosystem needs to be created forcing at the same time the creation of an "identity ecosystem". As part of the identity ecosystem, it is necessary to consider the level of cooperation between partners (risk management into IdM processes), the interactions and performance of operations (for example, in the Supply Chain scenario), and certification updates.

Recommendation 2: Provision of certification of attributes

This might help users to build trust on the mechanisms used.

Recommendation 3: Provision of Privacy default settings

This might include the provision of a dynamic consent form that the users can update according to their needs and the different privacy requirements of the applications.

Recommendation 4: Use of auditing mechanisms

This could help to ensure the appropriate use of identities by companies.

Recommendation 5: Transparency

It is essential that it is transparent to the users the Identity Management mechanisms that are being used in each specific stage.

Recommendations of Panel 6: The future of European Cybersecurity

Recommendation 1: Open source solutions

Open- source solutions can potentially lead to better cybersecurity approaches.

Recommendation 2: Fund larger projects

Short-term projects (two to three years long) do not provide the sustainability needed to start from research and go all the way to the market. Projects longer than five years, possibly in the form of "Grand Challenges", such as the ones set by the CERN model, can completely transform the projects and their results

Recommendation 3: Create a FET Open for Cyber Security

It was also suggested that we should look at FET Open and be collaborative with ERC, where excellent research is performed but the market is missing. The best ideas should flourish. The DARPA model provides a good example of ideas moving to market and project ending if they do not perform in a short time period.

Recommendation 4: Restructure Funding:

A good architecture of European funding would therefore consist of blue-sky individual projects under ERC, plus a large number of collaborative FET Open projects in strategic areas – that could also network the results stemming from ERC –, complemented by DARPA-like technological projects that would bring close to the market the most promising ideas that have most impact potential.

Recommendation 5: Move from "National" to "European"

There is a need for EU solidarity (the EU budget should take into account the digital market along with the welfare of its citizens). We should move from the national security approaches to a pan European security approach.

Recommendation 6: Improve communication

Possibly, also we need better communication: the research community needs a better way to communicate their ideas to decision makers, including the European Commission, the European Parliament, and the European Council.

Recommendations of Panel 7: The upcoming European Cybersecurity Competence Network: a conversation with the four pilots

Recommendation 1: Increasing Stakeholder Participation At Future Events

A concerted effort has to be made, not only by the CyberSec4Europe organisers but the other pilots and the wider stakeholder community as well, to ensure that future events better fulfil expectations.

Recommendation 2: Meeting Expectations On Collaboration

The four pilots are consistently and constantly being made aware of the importance of both creating real synergies on project work and also being seen to collaborating in areas where there is obvious overlap. It should be a target for early 2020 for the coordinators to demonstrate concrete collaborative initiatives, perhaps through the proposed focus groups.

Recommendation 3: Pooling Presentation Material and Representation

Whilst it has been important during the first 12 months of the four pilots to have representatives from each participate at stakeholder events in Brussels and elsewhere, it is time-consuming and expensive. The four pilots' communications group working closely with the coordinators should come up with a series of presentations that a single appropriate representative from any of the four pilots is able to present. The presentation should contain an overview section ('chapeau') pertaining to all four pilots in addition to brief individual sections for each pilot.

Recommendation 4: Addressing Strategic Autonomy

One of the ever-present conundra is, despite the wealth of talent and experience, the lack of strategic autonomy for cybersecurity in European industry. There is a degree of urgency for the pilots individually and collectively to provide recommendations to the stakeholder community.

Recommendation 5: Minding The Gaps

Despite the broad range of technical and business issues covered by the pilots, there are many broad areas not covered as demonstrated by the taxonomy mappings. There are even more areas that require attention that need to be identified with recommendations as to how they should be addressed.

4 List of Annexes

Annex 1: Agenda of the Concertation Event 2019 in Toulouse
Annex 2: Presentation of CYBER'OCC Project
Annex 3: Presentation of ECSO
Annex 4: CONCORDIA Project
Annex 5: ECHO Project
Annex 6: SPARTA Project
Annex 7: CyberSec4Europe Project
Annex 8: Presentation of OcSSImore
Annex 9: Panel 2 presentations
Annex 10: Panel 3 presentations
Annex 11: Panel 4 presentations
Annex 12: Panel 5 presentations
Annex 13: Panel 6 presentations
Annex 14: Short Biographies of Speakers

Navigation
Accueil
Inscription
Comités
Programme
Hébergement
Informations pratiques
Plan d'accès
Dîner de Gala

SUPPORT
@ Contact

Programme

Wednesday 13 November	
12:30	Registration
13:00	Cocktail Lunch
	Session: The Pilot Projects for establishing and operating a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap Kai Rannenberg – Goethe University Frankfurt
14:00	The view from the European Commission Miguel González-Sancho – Head of Unit H1, DG CNECT
14:30	A regional perspective: How the Occitanie Region is building capacity in cybersecurity Pierre Benaim, Caroline de Rubiana and Bénédicte Bejm – AD'OCC, Toulouse -
14:45	The European Cyber Security Organisation Luigi Rebuffi – European Cyber Security Organisation, Brussels
15:00	CONCORDIA – Aljosa Pasic, Atos Spain
15:30	ECHO – Wim Mees, Royal Military Academy, Belgium
16:00	Coffee break
16:30	SPARTA – Fabio Martinelli, CNR, Pisa
17:00	CyberSec4Europe – Kai Rannenberg, Goethe University Frankfurt
17:30	Break
	Session: Launch of Cybersecurity For Europe 2019 Conference
18:00	Opening: Bertrand Monthubert – Occitanie Region, France Welcome addresses: Mariya Gabriel – Commissioner Digital Economy and Society, European Commission (by video) Renaud Vedel – Préfet, Ministry of Interior, France
18:30	Panel: Cybersecurity Policy Moderator: Kai Rannenberg – Coordinator, CyberSec4Europe, Goethe University Frankfurt Speakers Miguel González-Sancho – Head of Unit H1, DG CNECT Bertrand Monthubert – Occitanie Region, France Renaud Vedel – Préfet, Ministry of Interior, France
19:30	Cocktail reception

Thursday 14 November	
09:30	Opening Kai Rannenberg – Goethe University Frankfurt
09:40	A Regional Cybersecurity Competence Centre in the making: The local picture Antoine Derain – Groupe Banques Populaires et Caisses d'Épargne, Toulouse
10:00	Panel 2: Recommendations for Cybersecurity Research and Innovation Moderator: Mark Miller – CONCEPTIVITY, Geneva Speakers Pierre-Henri Cros – Institut de Recherche en Informatique de Toulouse (IRIT) Olivier Dellenbac – ChapsVision & Founder of eFront SA, Paris Nicholas Ferguson – Trust-IT Services and cyberwatching.eu, Pisa Luigi Rebuffi – European Cyber Security Organisation, Brussels Liina Kamm, Cybernetica, Tallinn, Estonia
11:15	Coffee break
11:45	Panel 3: European Cybersecurity Governance Moderator: Afonso Ferreira – CNRS-IRIT Speakers Ana Ayerbe – Tecnalia, Spain Abdelmalek Benzekri – Université Paul Sabatier, Toulouse Médéric Collas – Banques Populaires, Toulouse Miguel González-Sancho – Head of Unit H1, DG CNECT Nicole Harris – GÉANT, Amsterdam Antonio Skarmeta – University of Murcia
13:00	Lunch
14:30	Introduction to the afternoon panels Afonso Ferreira – CNRS-IRIT
14:50	Panel 4: Good practices in Data Sharing for Incident Handling Moderator: Antonio Skarmeta – University of Murcia Speakers Fabio di Franco – ENISA, Athens Liina Kamm – Cybernetica AS, Tallinn, Estonia Edgardo Montes De Oca – Montimage, Paris Aljosa Pasic – ATOS, Spain Valerio Senni – United Technologies Research Center, Rome
16:05	Coffee break
16:35	Panel 5: Who's calling? Managing identities in the cyber world Moderator: Javier Lopez – University of Malaga Speakers Simone Fischer-Hübner – Karlstad University Stephan Krenn – Austrian Institute of Technology, Vienna Jesus Luna – Bosch, Darmstadt Fabio Martinelli – CNR, Italy Henrich C. Pöhls – University of Passau
17:50	Recap of the Day and Open Conversation David Goodman – TDL, Brussels
18:30	End of meeting day
19:30	Conference Dinner

Friday 15 November	
09:25	Opening Abdelmalek Benzekri - Université Paul Sabatier, Toulouse
09:30	Keynote speech Pascal Andrei – Chief Security Officer, Airbus
10:30	Coffee break
11:00	Panel 6: The future of European Cybersecurity Moderator: Evangelos Markatos – FORTH, Heraklion Speakers Fabio Di Franco – ENISA, Athens Afonso Ferreira – CNRS-IRIT, Toulouse Fabio Martinelli – CNR, Pisa Bart Preneel – KU Leuven
12:15	Panel 7: The upcoming European Cybersecurity Competence Network: A conversation with the four Pilot Projects Moderator: David Goodman – TDL, Brussels Speakers CONCORDIA – Aljosa Pasic, Atos Spain ECHO – Wim Mees, Royal Military Academy, Belgium SPARTA – Fabio Martinelli, CNR, Pisa CyberSec4Europe – Kai Rannenberg, Goethe University Frankfurt
13:00	Conclusions Kai Rannenberg – Goethe University Frankfurt
13:30	Lunch
14:30	Conference ends

SUMMARY OF PRESENTATION ON CYBER'OCC PROJECT

At the CyberSec4Europe Concertation Event held from November 13-15, 2019, in Toulouse, France

Caroline de RUBIANA | *Chargé de mission Cybersécurité*
Direction de l'Innovation - Filière du futur
Agence régionale de développement économique AD'OCC

At the origin of the CYBER'OCC project, there are two driving objectives :

- The need for help for SME's in the face of the threat of cyber-attacks.
- The richness of the cybersecurity resources on the territory of Occitanie.

The Occitanie Region has entrusted the economic development agency AD'OCC with the accomplishment of this mission which is to improve the level of safety, structure the cybersecurity sector and prepare the future. In order to address this issue in a concrete way, we want to create a Cybersecurity Regional Center.

We have identified four axes of work :

- To Protect the most vulnerable economic actors
- To Promote Security by design
- To Respond to the recruitment issue
- To Support innovation for Cybersecurity

The **first pillar** is an emergency action : 98% of the economic fabric of the Occitanie Region is made up of companies with less than 10 employees, 70% of which are one-person companies. The trend continued in 2017, with a significant increase in the number of individual company start-ups in the business services and industry. VSEs/SMEs are the most vulnerable to attacks. We have to help them :

Our objective is to identify their security needs through a diagnosis and to identify providers who can meet these needs and also find financing. The aim is to include them in a long term approach to improve their level of security. We would like to extend this scheme to territorial communities and the health sector.

The **second pillar** concerns SecurityByDesign which should be integrated into any application project, and connected objects. SecurityByDesign should also apply to new companies.

We are studying with the partners the possibility of creating an offer that pools the solutions of several players to test the security of a connected object at a reasonable cost. We want to offer a solution to the many start-ups in the region that create connected objects but leave security aside due to a lack of knowledge and resources.

The **third pillar** concerns recruitment and training courses. Our cybersecurity companies have difficulty in recruiting knowledgeable people and experts in this field. We must encourage young people to find a future in this field, as well as people who want to reorient their careers and also those who are unemployed to gain expertise in this area.

We encourage girls and women to move into such professions. Thus, we need to identify the necessary training, increase the number of training courses and promote this sector widely.

Of a more general nature, everyone must be trained at a 1st level of Cybersecurity. To accomplish this, we must communicate on the subject matter, encourage companies to train all their staff, train the younger generations and disseminate good safety practices as widely as possible.

The last **fourth pillar**, concerns innovation. To promote partnerships between companies and research laboratories.

The Region and AD'OCC are a natural intermediary between stakeholders and partners since it offers financing mechanisms for innovation and research projects.

In the same way as Cybersec4Europe, we also need to think about needs and requirements for cybersecurity.

We have brought together public and private actors around the table who have chosen to pool their skills, experience and know-how around this project. For example, regional cybersecurity companies such as Scassi, Pradeo, IMS network are involved but also experts from large groups: Capgemini, Sopra Steria, Thales, Liebherr aerospace, Latécoère, schools and the universities of Toulouse and Montpellier, Research laboratories, IRIT, of course, (Research Institute of Computer Science of Toulouse), LAAS (Laboratory for Analysis and Architecture of Systems), LIRMM (Laboratory of Computer Science, Robotics and Microelectronics of Montpellier), CNES (National Centre for Space Studies), specialised government departments, the police, the army and ANSSI (National Information Systems Security Agency).

Our first achievement is the Cybersecurity Portal in Occitanie : CyberOcc.com

Communication, information, community animation are common elements to the different axes of the project and essential to the success of this ambitious goal. It meets the needs of Pillar 1 : online security assessment, list of regional cybersecurity providers. It is a one-stop shop.

Coming soon is a list of all regional cybersecurity trainings and entry requirements.

The Cybersecurity Regional center is expected to be officially established in the course of 2020.

The Cybersecurity centre project of the Occitanie Region

Cyber'OCC

UNION EUROPÉENNE

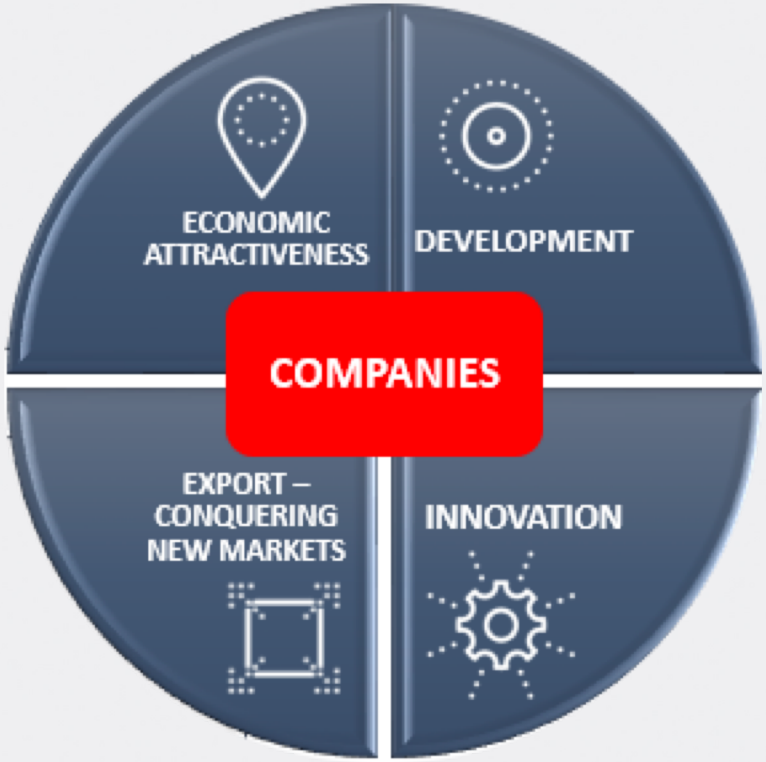
PRÉFET DE LA RÉGION OCCITANIE

AD'OCC Région Occitanie
Agence de Développement Économique

STRATÉGIE RÉGIONALE DE L'INNOVATION
Occitanie / Pyrénées - Méditerranée

A short presentation of AD'OCC

Our Task : to support businesses and create jobs in Occitanie



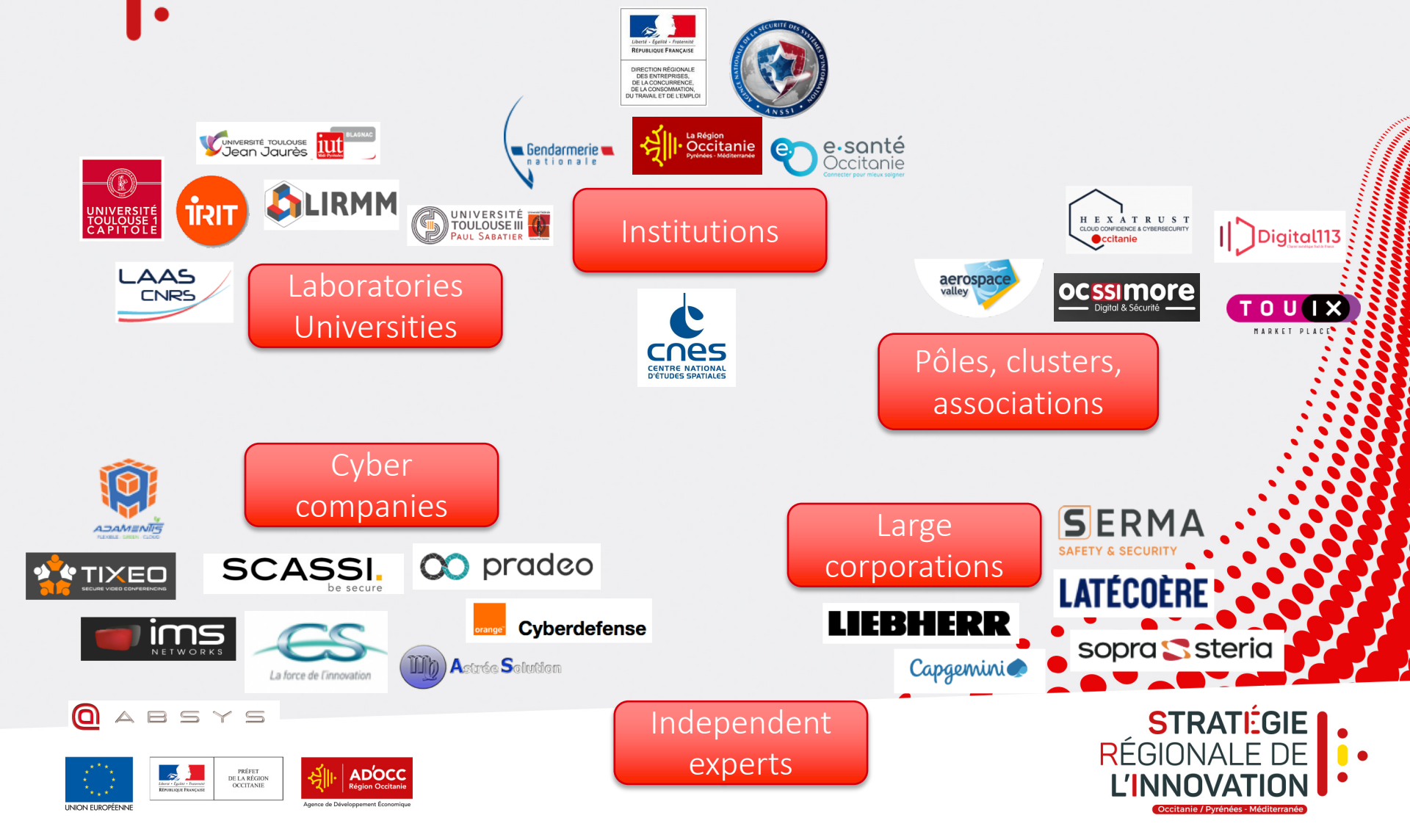
Cybersecurity centre project

Strengthen business protection
Make the regional offer visible

4 axes

- To Protect the most vulnerable economic actors
- To Promote Security by design
- To Respond to the recruitment issue
- To Support innovation for Cybersecurity

A few actors gathered around the project



A cybersecurity One-stop shop

https://www.cyberocc.com

To communicate, to inform, to advise,
to raise awareness, to evaluate oneself,
to find a service provider …

EUROPEAN CYBER SECURITY ORGANISATION

ECSO4CS4E
Working for a cyber resilient digital Europe

Toulouse 13 November 2019

Luigi REBUFFI – ECSO Secretary General
www.ecs-org.eu

ECSO: A NEW KIND OF PUBLIC PRIVATE PARTNERSHIP (https://ecs-org.eu/about)

ECSO is the European Commission's partner of the **cPPP on cybersecurity (signed at the European Parliament in Strasbourg in July 2016).**

Aim of the cPPP: Foster **cooperation between public and private actors at early stages of the research and innovation process** in order to allow people in Europe to access innovative and trustworthy European solutions
Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions

ECSO is the independent voice of the European cyber security stakeholder Community, representing **industry players**, national **public administrations, research centres, SME's, regions, and academia. Not a lobbying body but an independent advisor** to EU Institutions (presence of MS, different sectors and kind of stakeholders).

Main initial challenge: **Different sectors and different actors (suppliers / users) with different interests and different level of maturity** (it took more than a year to stabilise the governance (transparency and balanced) and start effective dialogue / cooperation, smoothening frictions and converge in positions, avoiding "low level compromises") ➔ **ECSO created an effective EU Community working together**

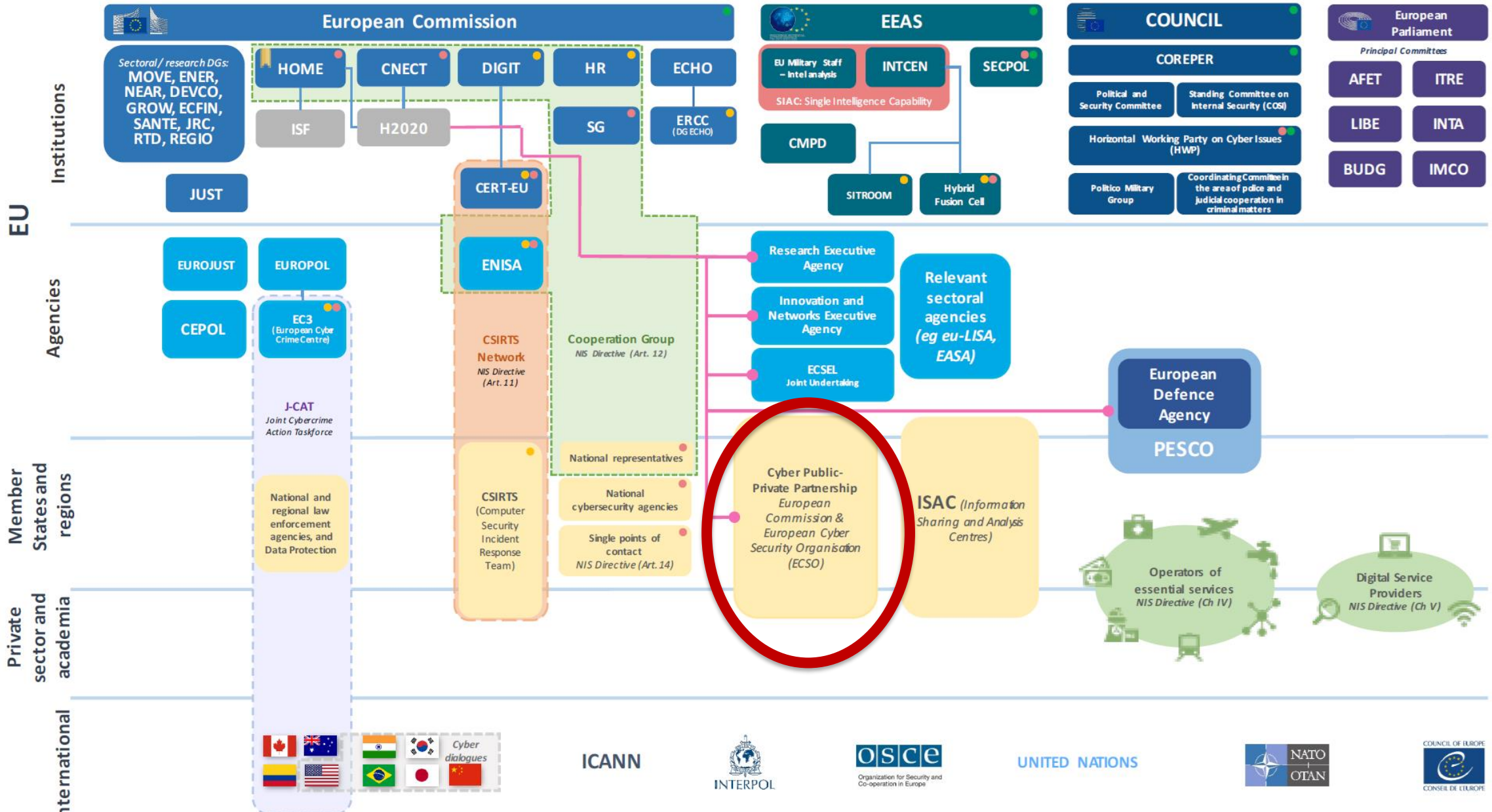
Our membership has grown **from 132 members in June 2016 to 263 members in November 2019** (reaching out to members of our 28 associations, i.e. **a Community of more than 2000 bodies**) and **almost 2000 experts** directly engaged in our working groups

Initial cPPP target: priorities for H2020 R&D on cybersecurity; foster private investments for at least 3 times the EC contribution (450mln€) – **actually we have reached a "leverage factor" of 5**

We go beyond Research & Innovation and industry needs: in our **6 working groups**, we deal with the different aspects of **cyber security industrial policy to support EU cyber ecosystem, EU Community and EU competitiveness growth**

CYBERSECURITY IN EU ORGANISATIONS: A COMPLEX PATCHWORK

Source: European Court of Auditors - Challenges to effective EU cybersecurity policy
https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf



ECSO coordination on cybersecurity activities in Europe (R&I and market issues) with the different main EU actors

- Dialogue with EU Institutions: EP (MEPs and Committees, Council of the EU, EC (DG CNECT, DG RTD, DG ENER, DG MOVE, DG JRC, DG DIGIT, ...)
- Cooperation with EU Agencies: ENISA, EUROPOL, EDA, ESA, EASA, EIT, EIB … and EEAS
- Coordination with other PPPs and JUs: EURobotics (Robotics), ECSEL (embedded electronics), BDVA (Big Data), AIOTI (IoT), EFFRA (Industry 4.0), 5G IA (5G), EUROHPC (HPC), INATBA (blockchain), A.SPIRE (process)
- Coordination with the 4 Pilots (/ cooperation: 40% members of ECSO): CONCORDIA, CYBERSEC4EUROPE, ECHO, SPARTA
- Cooperation with European sectoral associations: Finance, Energy, Transport, Telecom, Health, Defence & Space, Manufacturing
- Cooperation with National Bodies: national public admin (NAPAC representatives), national cybersecurity associations, …
- Coordination / cooperation with International Bodies: UN (ITU), WEF, OSCE, signed MoU with CEN/CENELEC and ETSI …
- Dialogue with non-EU public administrations and private sector in Japan (METI, MoI, …) and US (DHS, CISA)

ECSO membership growing (status as of 1 November 2019)

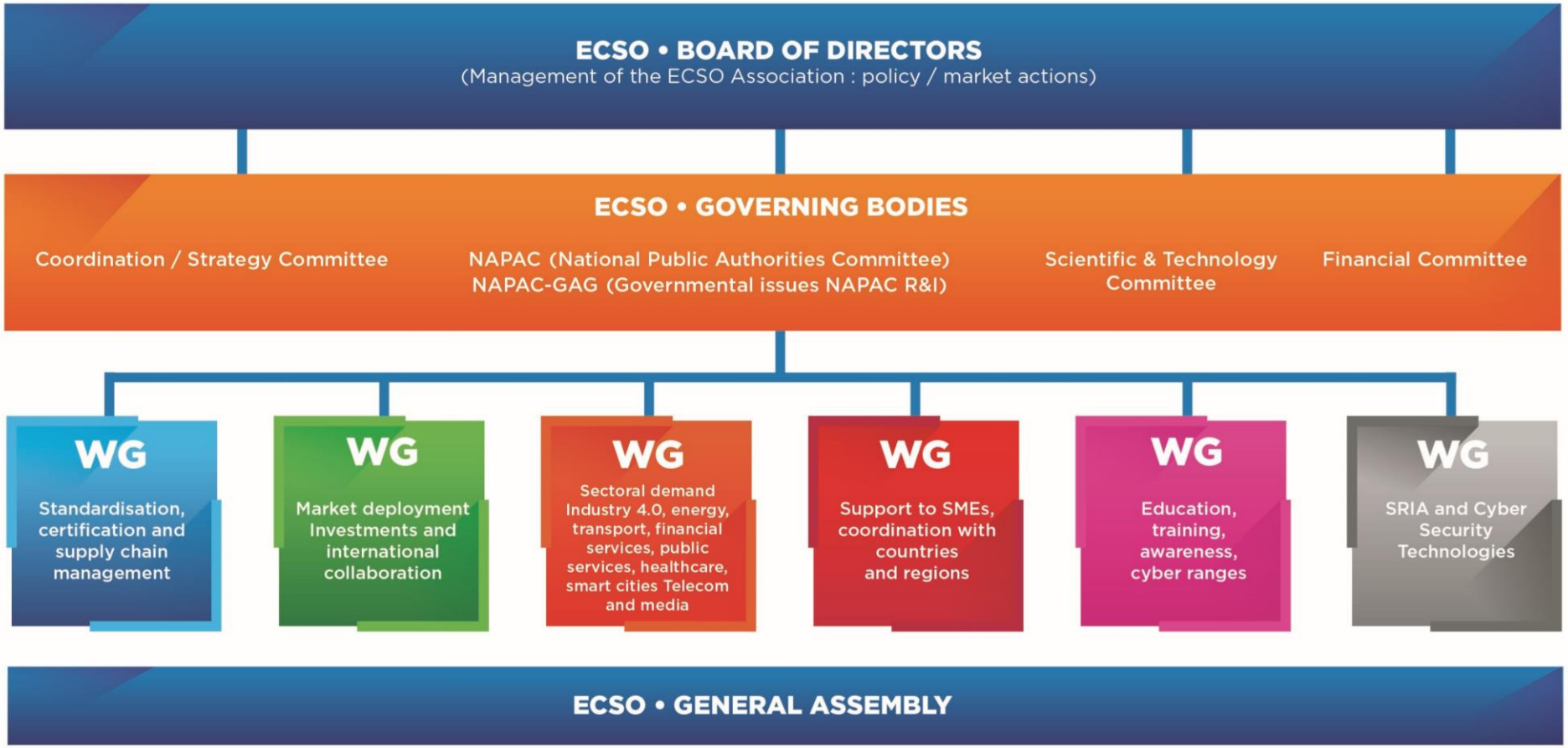
132 founding members: now we are **263 organisations** (including last requests - in brackets) **from 29 countries and counting ECSO is also reaching out to all the members of our 28 associations, i.e. a Community of more than 2000 bodies** and **almost 2000 experts** directly engaged in our working groups

AUSTRIA	7	LATVIA	1
BELGIUM	15 (+1)	LITHUANIA	1
EU ASSOCIATIONS	13	LUXEMBOURG	4
BULGARIA	2 (+1)	NORWAY	6
CYPRUS	6	POLAND	6
CZECH REP.	3	PORTUGAL	4
DENMARK	5	ROMANIA	2
ESTONIA	8	SLOVAKIA	1
FINLAND	9	SLOVENIA	1
FRANCE	29	SPAIN	34 (+1)
GERMANY	23	SWEDEN	3
GREECE	7	SWITZERLAND	5
HUNGARY	3	THE NETHERLANDS	14
IRELAND	5	TURKEY	4
ITALY	30	UNITED KINGDOM	9

- Associations : 26 (+2)
- Large companies: 55
- Users / Operators: 16
- Public Administrations: 21

  AT, BE (2), BG, CY, CZ (2), EE, FI, FR, GE, GR, IT, NL, NO, PL, RO, SE, SK, SP, UK

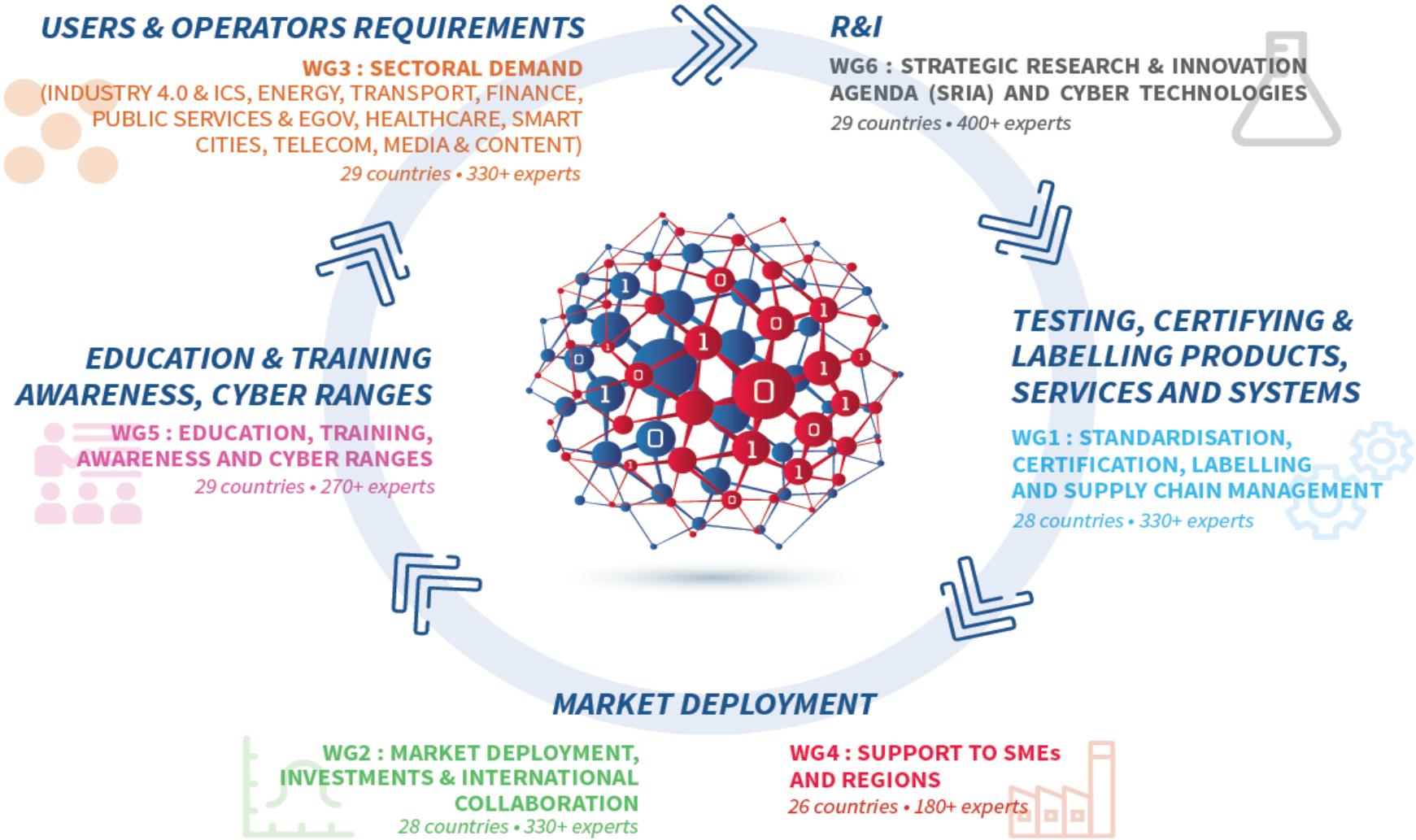
  Observers at NAPAC (DK, HU, IE, LT, LV, MT, PT, SI, …)
- Regions / clusters: 9
- RTO/Universities: 72
- SMEs: 61 (+1)



- SMEs solutions and services providers ; Local and regional SME clusters and associations; Start-ups, incubators and accelerators
- Large companies solutions and services providers / users
- National / European organisations or associations
- Regional / local administrations; Regional / local clusters for solutions and services providers or users
- Public or private operators of essential services
- National public administrations
- Research Centres ; Academia; Universities and their associations

ECSO: A NEW KIND OF PUBLIC PRIVATE PARTNERSHIP

6 WORKING GROUPS (https://ecs-org.eu/activities)



Main achievements in the first three years: from policy suggestions to concrete achievements

- ✓ **WG1 - Certification & Standardisation:** Input for the EU Certification Framework (meta-scheme methodology) and the Cybersecurity Act legislation; State of the art and industry needs for certification and standardisation; Security assessment and priorities for certification
- ✓ **WG2 – Market, Investments and International cooperation:** Cybersecurity market analysis; Taxonomy and Radar (identification of competences / products); Towards a EU Cybersecurity Investment Fund; International cooperation (e.g. Japan)
- ✓ **WG3 – Vertical sectors:** Identification of needs for the different vertical sectors (Industry 4.0, Energy, Financial, Public Services / eGov, Health, Transportation, Smart cities, Telecom – media & content); Trusted exchange of cyber threats among users
- ✓ **WG4 - Support to SMEs and Regions:** ECSO SME Hub – Registry and EU Cybersecurity Label; SMEs / Investors matchmaking; Network of Regions and their competence centres for smart cooperation in cybersecurity - European Cyber Valleys Project and inter-regional acceleration programme (services for SMEs)
- ✓ **WG5 – Education, Training, Awareness and Cyber Ranges:** EHR4CYBER: sharing of best practices for skills development and job creation); Women4Cyber for gender balance; Youth4Cyber (under development) for cyber-hygiene and carrier; Support to Cyber Ranges federation
- ✓ **WG6 - R&I priorities and innovative technologies:** SRIA (Strategic Research and Innovation Agenda) for H2020 priorities; Horizon Europe and DEP priorities; Support to coordination of cybersecurity activities across cPPPs, CCN Pilots and other EU Initiatives; Analysis of cyber security synergies for dual use
- ✓ **cPPP Monitoring:** delivering investment in the SRIA perimeter satisfying cPPP commitments

Main recommendations to the new EC and EP

1. **Digitalisation is only at the beginning**: cybersecurity issues are growing. Europe cannot undergo evolving threats without being prepared, cannot depend on non-EU solutions ➔ Europe needs a comprehensive approach in cybersecurity to protect its society, its democracy, its sovereignty, its economy

2. **Collaboration in Europe** is absolutely important between all stakeholders to develop our cybersecure digital ecosystem: public and private, citizens, professionals and decision makers (political and different economic sectors)

3. **Research and capability development** should be coordinated and supported, leveraging upon high level competence in Europe

4. **Market development and capacity building** should be supported to be consistent with EU values and for increased competitiveness of our industry

5. **Higher investments** are needed in a flexible approach, to follow the fast pace of digitalisation: do not leverage only on public investments but find synergies with private investments

6. **We are delivering:** ECSO is delivering (policy support and concrete actions) since more than 3 years. The 4 CC-Pilots have started effective contribution in different sectors ➔ **We have concrete results, we are preparing together the next steps**

7. These effective results and the already created **public – private dialogue and cooperation should be continued and well considered when envisaging the new EU approach on competence centres**.

Aljosa Pasic
Atos

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Vision: EU Leadership + Competitiveness + Growth

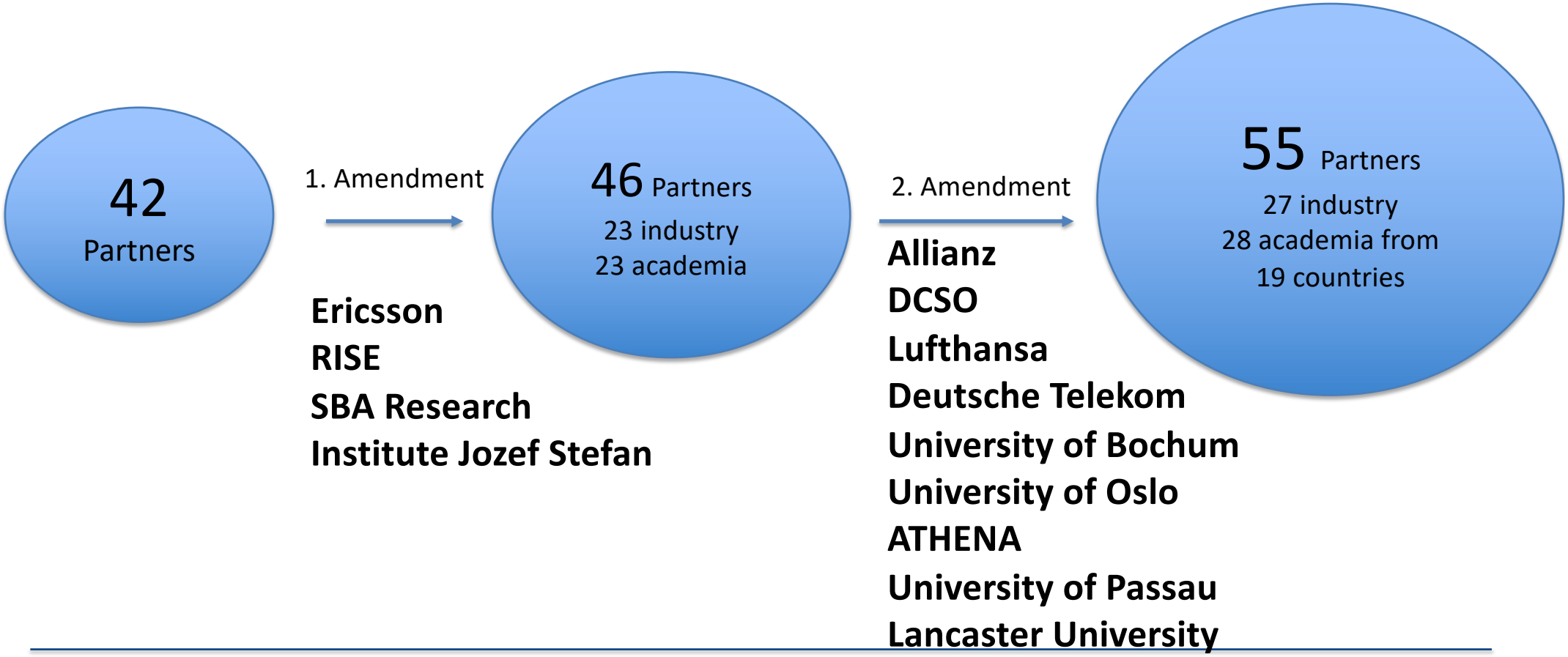
Technological, Business, Societal and Policy Innovation
Agile, Integrative & Inclusive Community Building

- Partners: 46 + (9)
  23 academia, 23 industry
  (28 academia, 27 industry)

- Countries: 19, 4 years

- Funding:
  16M from EU & 7M+ additionally from national authorities and industry

CONCORDIA is Growing



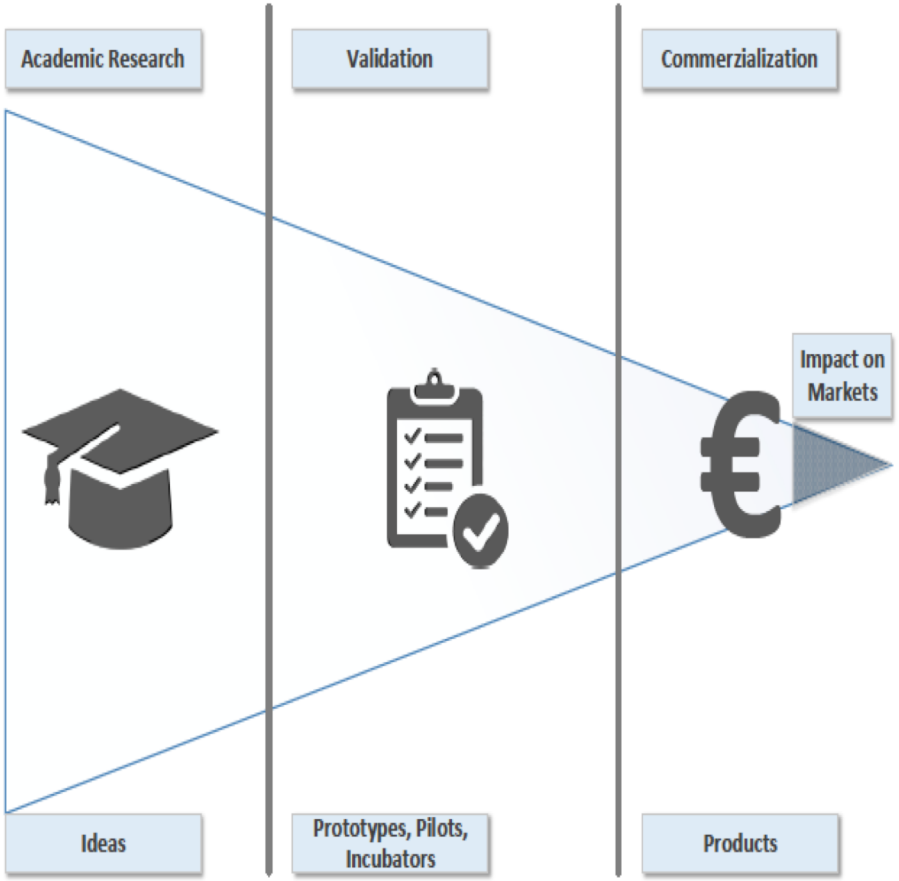
Objectives (1)

- O1: Position the **CONCORDIA ecosystem,** a Cybersecurity Competence Network with leading research, technology, industrial and public competences to build the **European Secure, Resilient and Trusted Ecosystem**, with the CODE research center as coordinator and hub, and ENISA as secretary.
- O2: Using an **open, agile and adaptive governance model** and processes
- O3: Devise a **cybersecurity roadmap** to identify powerful research paradigms, to do hands-on experimental validation, prototype and solution development in an agile way to quickly identify successful but also unsuccessful potential product development
- O4: Develop next-generation cybersecurity solutions by taking a **holistic end-to-end data-driven approach**
- O5: Scale up existing research and innovation with **CONCORDIA's virtual lab and services**

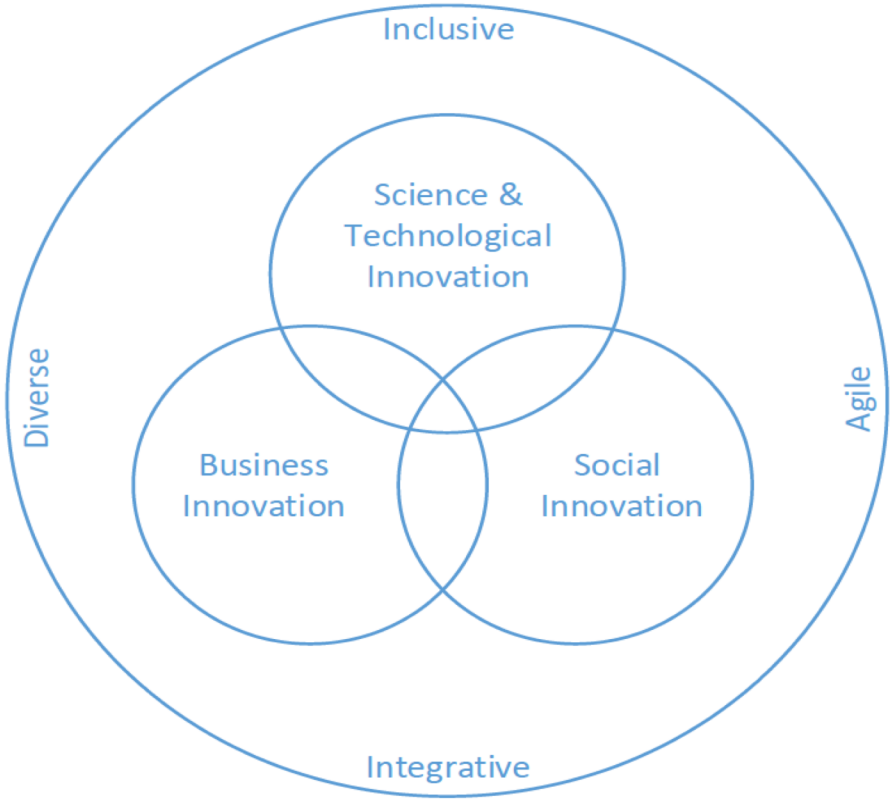
Objectives (2)

- O6: **Identify marketable solutions and grow pioneering techniques** towards fully developing their transformative potential
- O7: **Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators**
- O8: Launch **Open Calls** to allow entrepreneurs and individuals to stress their solutions with the development
- O9: Set up an Advisory Board
- O10: Mediate between multiple communities
- O11: Establish an **European Education Ecosystem for Cybersecurity**
- O12: Provide **expertise to European policy makers and industry**

Strengthening the competitiveness and growth



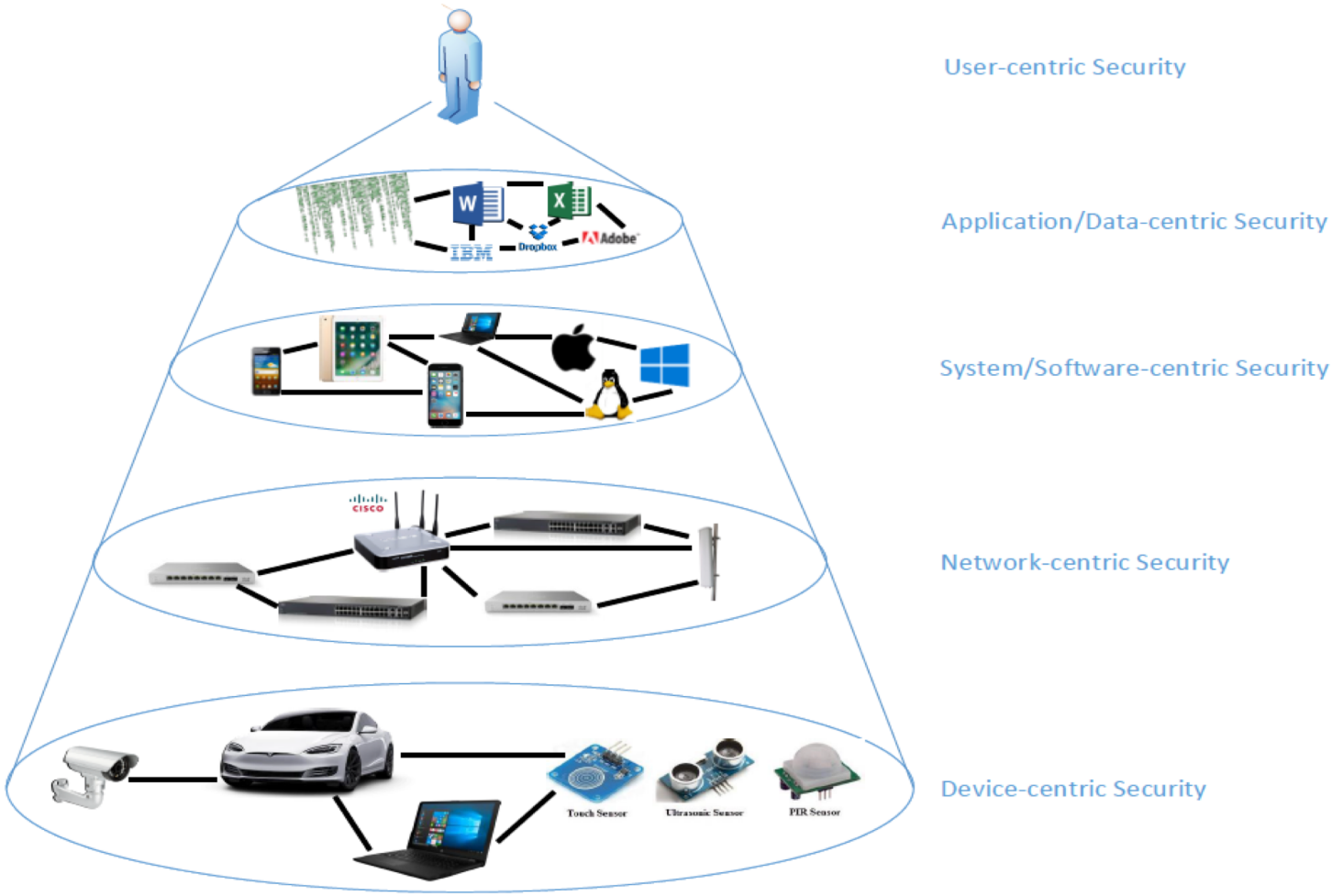
Innovation as key of success



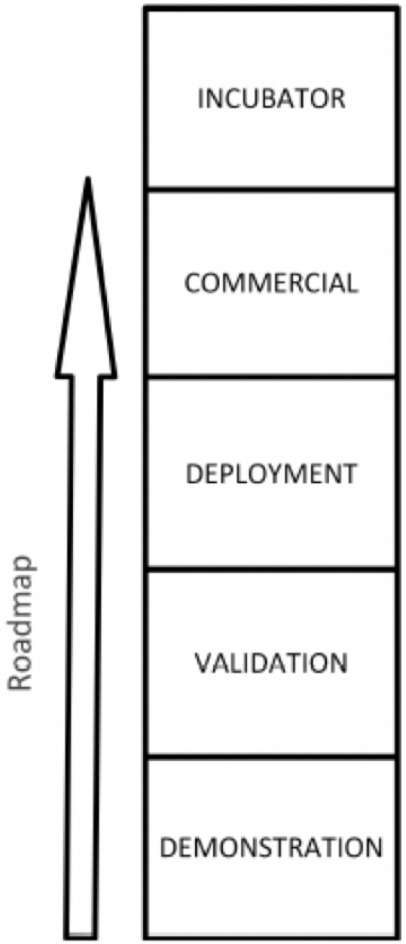
What CONCORDIA stands for?

Developing Competences, Tech Transfer, Tools, Solutions, Services, Repositories, Education, Policies → ***Community Building and Roadmap***

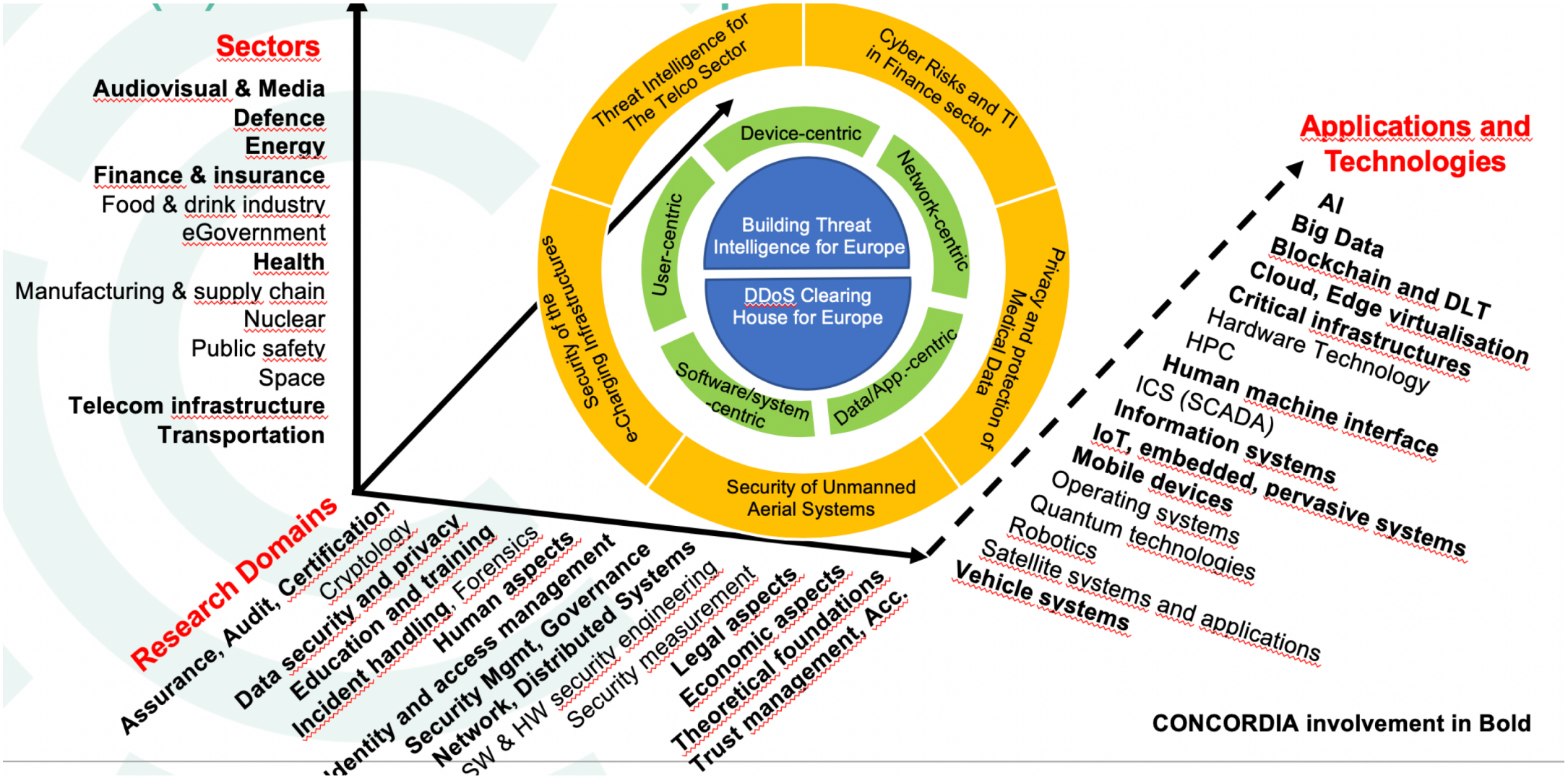
Research – Holistic Data-Centric Approach



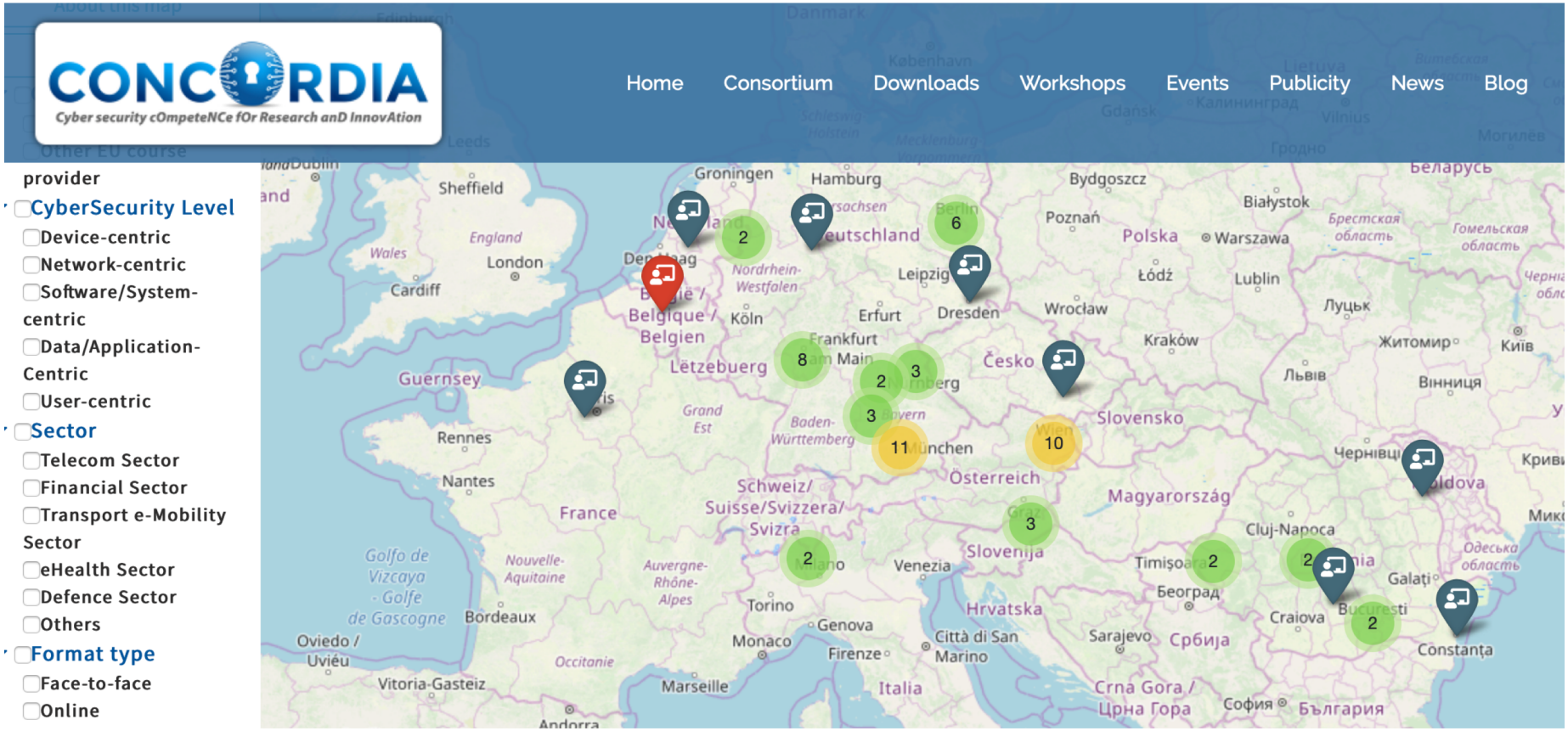
Pilots


INCUBATOR
COMMERCIAL
DEPLOYMENT
VALIDATION
DEMONSTRATION
Roadmap


Building Threat Intelligence for Europe
Piloting a DDOS Clearing House for Europe
Automated Processing of Threat Intelligence Information
Threat Intelligence for the Telco Sector
Handling Privacy and Anonymity with Machine Learning
Combining APTs and avoiding Flood Attacks from IoT devices
Plug & Charge
Load Management EV's
Security of The E-charging Infrastructure
Bidirectional charging management EV
Commericalization of flexibility of EV's batteries on Frequency Containment Reserves
Cyber Risks and Threat Intelligence in Finance and Insurance Sector
Physical or vitual impersonations
Knowledge Sharing
Privacy and Protection of Medical Data
Emergency data in e-Health services
Remote health services at home
Security of Unmanned Aerial Systems
telenor
Telefónica
efacec
DCSO
TELECOM
Bitdefender
ERICSSON
DFN-CERT
SIEMENS
Infineon
CaixaBank
Flowmon
Allianz
eesy INNOVATION
Atos
secunet
AIRBUS DEFENCE & SPACE
Together ahead.
RUAG


Sectors
Audiovisual & Media
Defence
Energy
Finance & insurance
Food & drink industry
eGovernment
Health
Manufacturing & supply chain
Nuclear
Public safety
Space
Telecom infrastructure
Transportation
Threat Intelligence for The Telco Sector
Cyber Risks and TI in Finance sector
Privacy and protection of Medical Data
Security of Unmanned Aerial Systems
e-Charging Infrastructures
Security of the
Device-centric
Network-centric
Data/App.-centric
Software/system -centric
User-centric
Building Threat Intelligence for Europe
DDoS Clearing House for Europe
Applications and Technologies
AI
Big Data
Blockchain and DLT
Cloud, Edge virtualisation
Critical infrastructures
Hardware Technology
HPC
Human machine interface
ICS (SCADA)
Information systems
IoT, embedded, pervasive systems
Mobile devices
Operating systems
Quantum technologies
Robotics
Satellite systems and applications
Vehicle systems
Research Domains
Assurance, Audit, Certification
Cryptology
Data security and privacy
Education and training
Incident handling, Forensics
Human aspects
Identity and access management
Security Mgmt, Governance
Network, Distributed Systems
SW & HW security engineering
Security measurement
Legal aspects
Economic aspects
Theoretical foundations
Trust management, Acc.
CONCORDIA involvement in Bold

Skills: Virtual Labs, Services, Training, Education



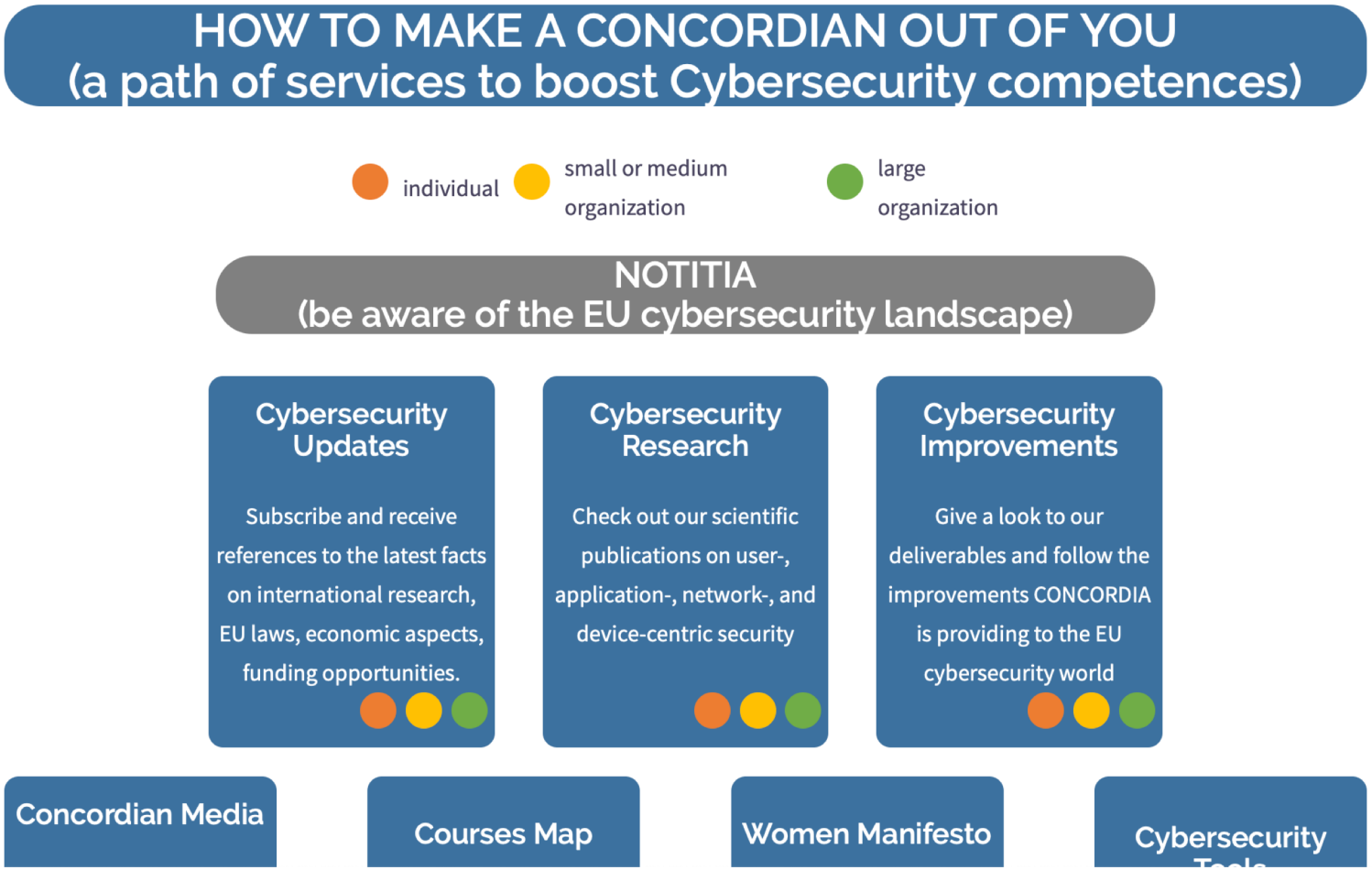
Women in Cyber

WOMEN IN CYBER

A MANIFESTO FOR TODAY


Stakeholder Groups e.g. National Cybersecurity Agencies
Liaison Groups e.g. ENISA, EDA, World Economic Forum
CONCORDIA
Service Catalogue
Observer Groups e.g. Standardisation, Certification
CONCORDIA
Community Building

CONCORDIA's Service Catalogue



... Much more ....

CONCORDIA is Boosting the Future of Cybersecurity in the EU!

Be Part of It!

www.concordia-h2020.eu

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.instagram.com/concordiah2020.eu

ECHO Project Overview

Matteo Merialdo
Project Implementation Coordinator

16 September 2019

RHEA Group

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement no 830943

Cybersecurity Challenges for EU

Cybersecurity challenges have been identified by the EC for the upcoming years

- Retain and develop essential capacities to secure its digital economy, infrastructures, society, and democracy
- Better align cybersecurity research, competences and investments
- Step up investment in technological advancements to make EU's digital single market more cybersecure and overcome fragmentation of research
- Master relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software
- Support industries and equip them with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks
- Contribute to the objective of European strategic autonomy

Cybersecurity Gaps for EU

ECHO consortium identified gaps in current cybersecurity technologies and operations in EU:

1. Lack of effective means to assess multi-sector technology requirements across security disciplines
2. Lack of effective means to assess dependencies between different industrial sectors
3. Lack of realistic simulation environments for technology research and development, or efficient security test and certification
4. Lack of an up-to-date cyberskills framework as a foundation for cybersecurity education and training
5. Lack of effective means to share knowledge and situational awareness in a secure way with trusted partners

These gaps **are particularly relevant for EU**

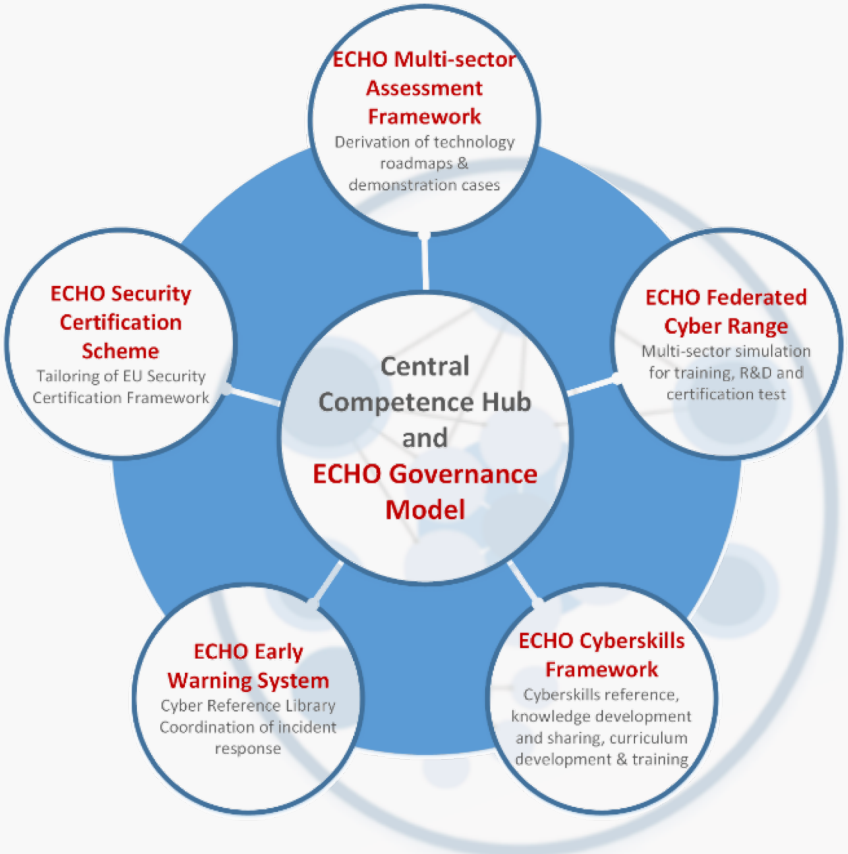
ECHO main objectives

- Network of cyber research and competence centres, with a central competence hub
  - Demonstrate a network of cyber research and competence centres, with a central competence hub, having a mandate for increasing participation through a new partner engagements model, including collaboration with other networks funded under the same call
  - Address all the aforementioned gaps, developing an adaptive model for information sharing and collaboration among the network of cybersecurity centres, supported by an early warning system and a framework for improved cyberskills development and technology roadmap delivery, in a multiple-sector context

ECHO

European network of Cybersecurity centres and competence Hub for innovation and Operations

- Project Coordinator: **Royal Military Academy of Belgium (Wim Mees)**
- Project Management: **RHEA System S.A. (Matteo Merialdo)**
- Main concepts:
  - ECHO Governance Model:
    - Management of direction and engagement of partners (current and future)
  - ECHO Multi-sector assessment framework:
    - Transverse and inter-sector needs assessment and technology R&D roadmaps
  - ECHO Cyberskills Framework and training curriculum
    - Cyberskills reference model and associated curriculum
  - ECHO Security Certification Scheme
    - Development of sector specific security certification needs within EU Cybersecurity Certification Framework
  - ECHO Federated Cyber Range
    - Advanced cyber simulation environment supporting training, R&D and certification
  - ECHO Early Warning System
    - Secured collaborative information sharing of cyber-relevant information



ECHO

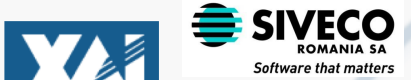
Partners

Key summary

- 30 partners
- 15 new partner engagements
- 13 existing competence centres
- 16 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios


guardtime


TAL TECH

VISIONSPACE


FINCANTIERI

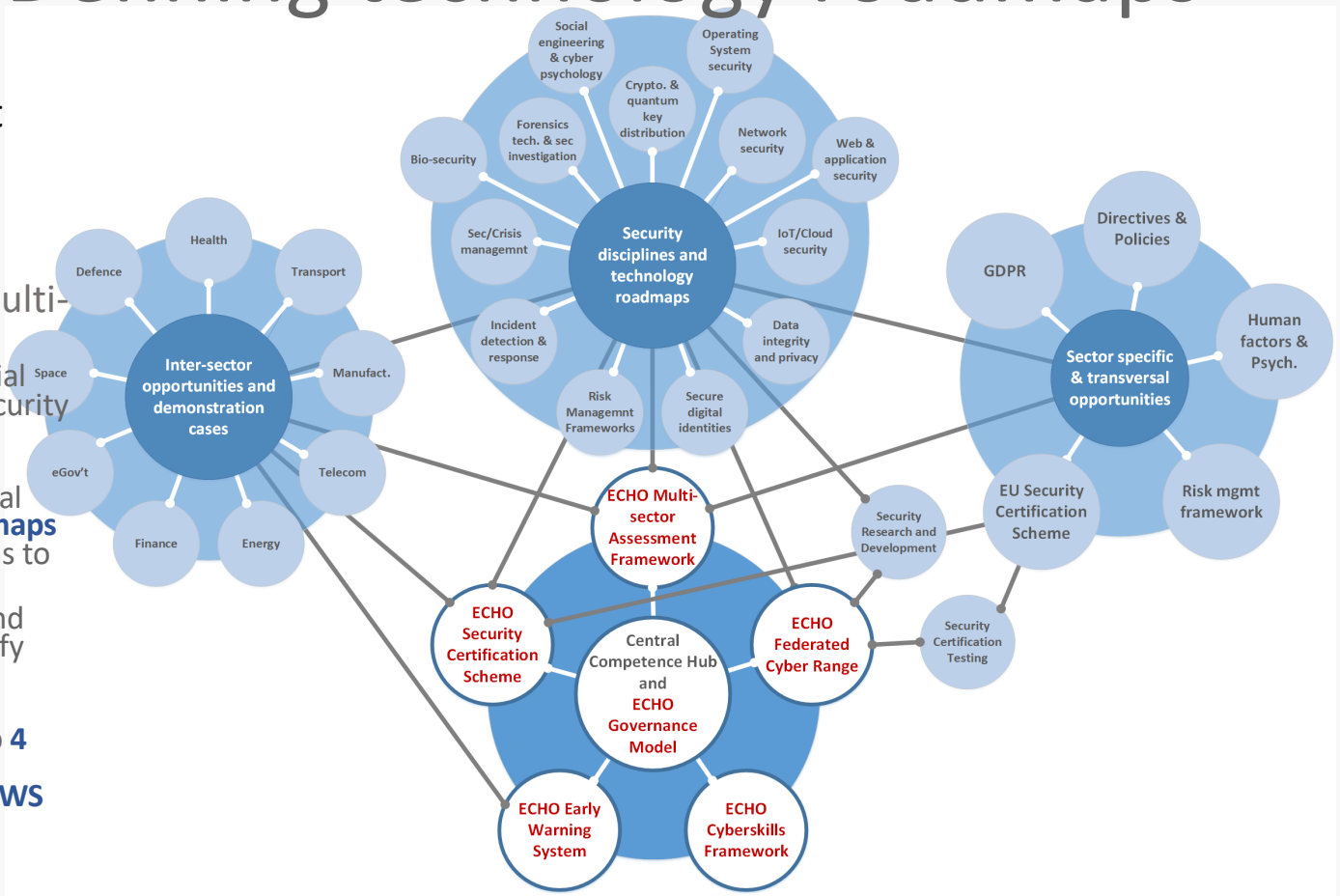
acea


Zanasi & Partners
Security Research and Advisory


NAVAL GROUP

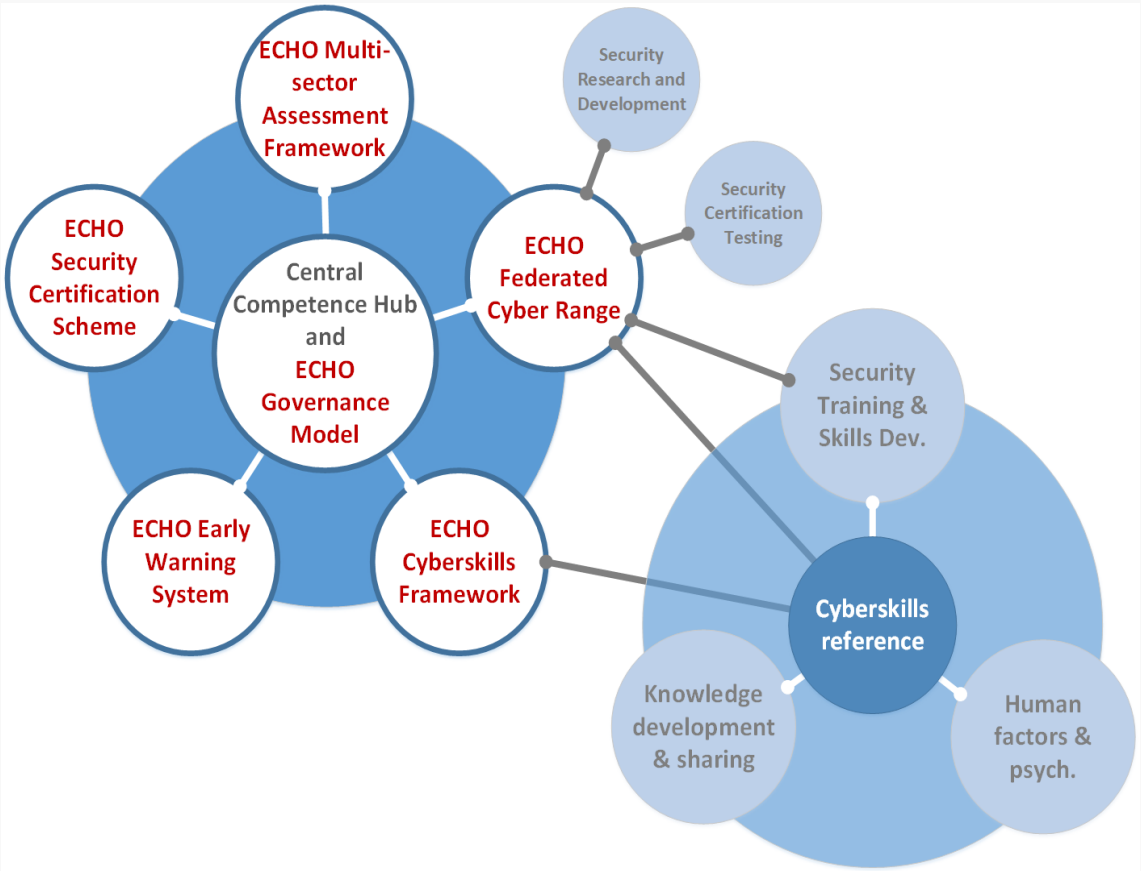

Defining technology roadmaps

- ECHO Multi-sector assessment framework
  - Mechanism to define and refine **technology roadmaps** and **demonstration cases**
- Risk based method to analyse multi-sector security needs including
  - **Inter-sector opportunities** (potential solutions) and **dependencies** to security challenges further analysed as **demonstration cases**
  - Comprehensive **analysis** of potential **contributions** to **technology roadmaps** across **security disciplines** as means to improve security posture
  - Analysis of **sector specific needs** and **transversal opportunities** to identify potential for improvement
  - ECHO targets to identify at least **6 technology roadmaps** and develop **4 technology innovations** on these roadmaps, including **E-FCR and E-EWS**



Innovations and Impact

- ECHO Cyberskills framework
  - Mechanism to improve the **human capacity** of cybersecurity across Europe
- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome based curricula**
- **Hands-on skills development** opportunities through realistic simulation (ECHO Federated Cyber Range)
- Lessons learned feed **knowledge sharing** (ECHO Early Warning System)

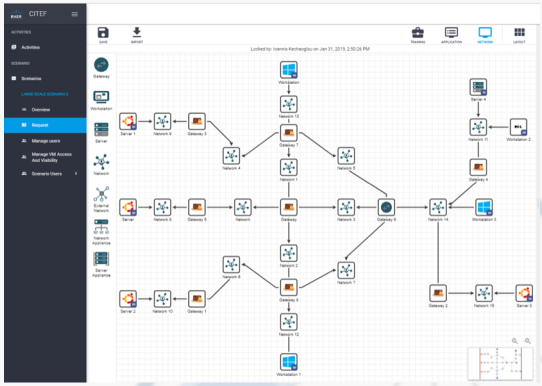


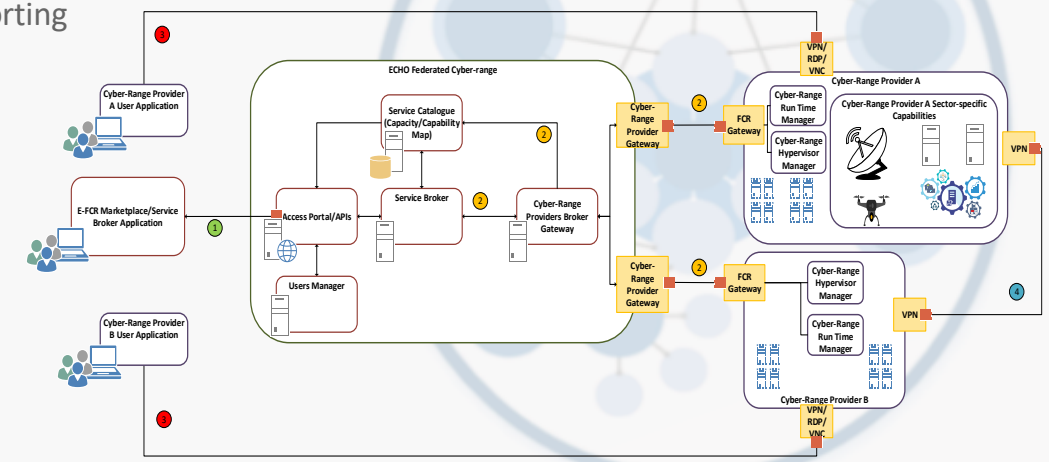
Innovations and Impact

- ECHO Cybersecurity Certification Scheme
  - Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
  - Provide **product oriented** cybersecurity certification schemes
    - Support sector specific and inter-sector security requirements
  - Support **delivery and acceptance of technologies** resulting from technology roadmaps
    - **Improved security assurance** through use of **certified products**
  - Support development of **Digital Single Market**
    - Limits duplication and fragmentation of the cybersecurity market
    - **Common** cybersecurity **evaluation methods, acceptance** throughout Europe
    - Applicability across **Information Technologies** (IT/ICT) and **Operations Technologies** (OT/SCADA)

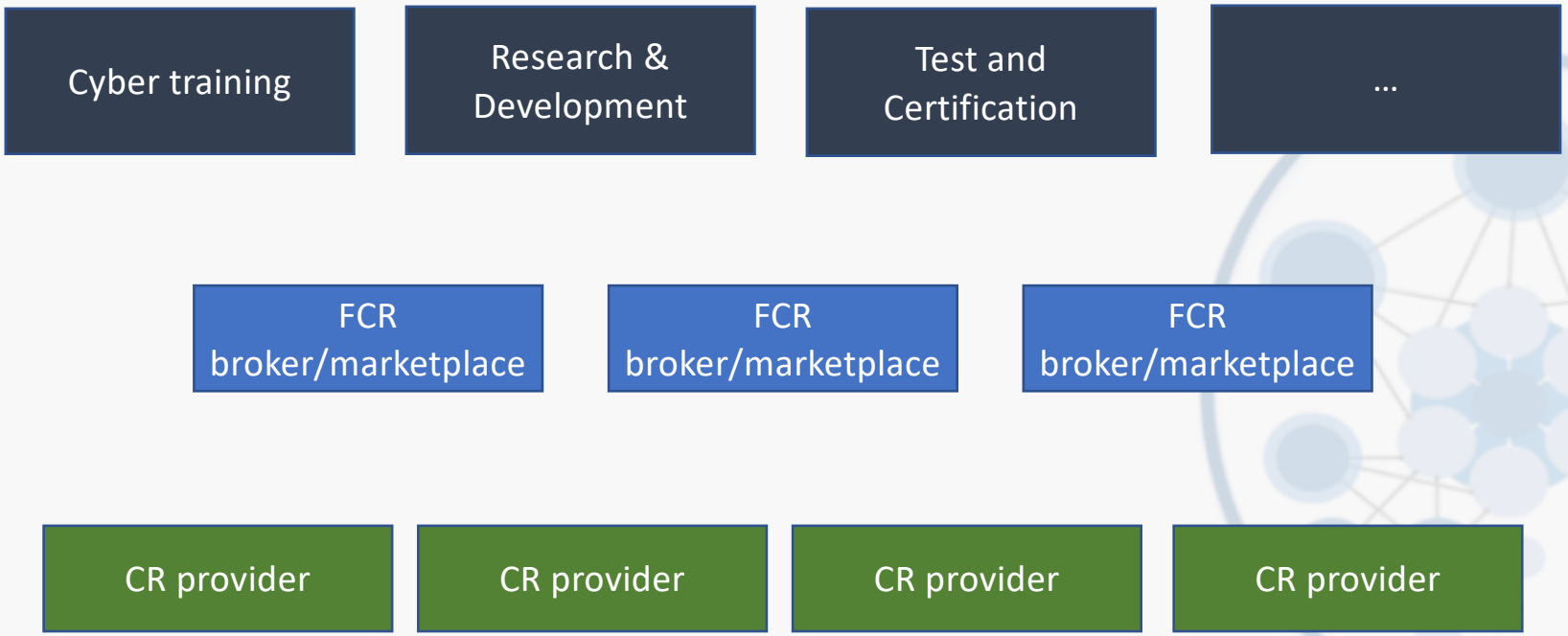
Technology roadmap: E-FCR

- ECHO Federated Cyber Range (FCR)
  - Interconnect existing and new cyber range capabilities through a convenient portal
  - Portal operates as a **broker** among cyber ranges
  - A **marketplace** enable content providers to sell cyber range contents to a wider market
  - Enables access to emulations of **sector specific and unique technologies**
  - Target **Technology Readiness Level: 8**
  - Governance Model in development
- Cyber Range is a multipurpose **virtualization environment** supporting **"security-by-design"** needs
  - Safe environment for **hands-on cyberskills** development
  - Realistic simulation for **improved system assurance** in development
  - Comprehensive means for **security test and certification** evaluation
- To be used as virtual environment for:
  - Development and demonstration of **technology roadmaps**
  - Delivery of specific instances of the **cyberskills training** curricula



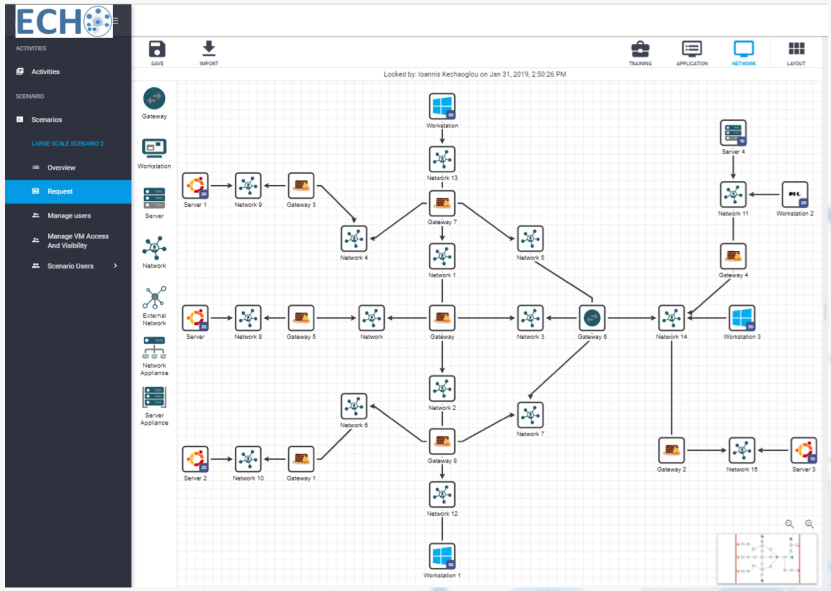


E-FCR concept



E-FCR concept

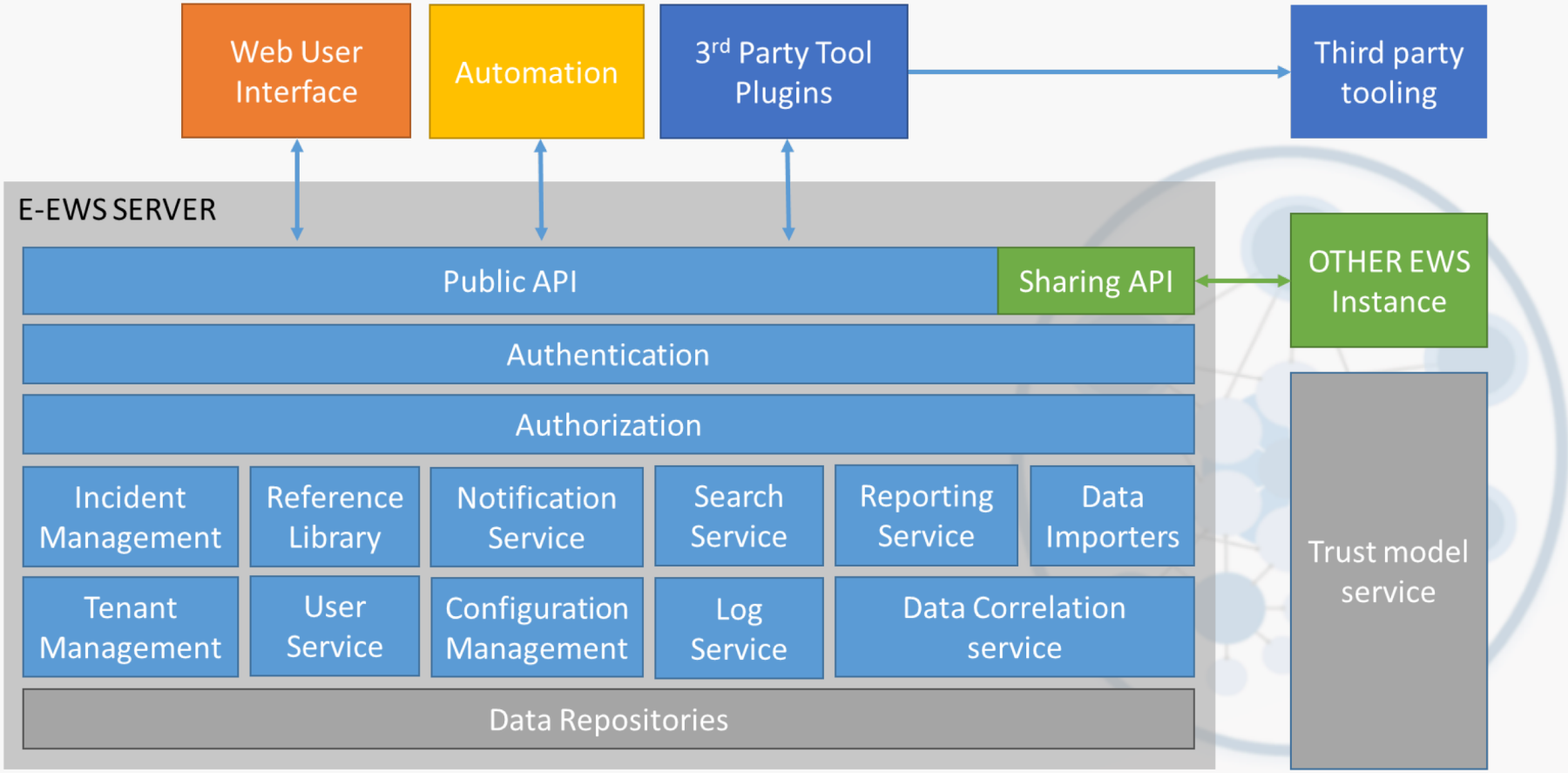
- Customers will have access to
  - Service Designer -> concept already in progress (develop new scenarios leveraging on single or multiple ranges)
  - Marketplace (content providers can upload contents/scenarios for a wider market)



Technology roadmap: E-EWS

- ECHO Early Warning System
  - **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
  - Secure information sharing **between organizations**; across organizational boundaries and national borders
  - Coordination of **incident management workflows**
  - Retain **independent management and control of cyber-sensitive** information
  - Account for **sector specific needs** and protection of **personal information protection** (GDPR compliant)
  - Includes sharing of **reference library** information and **incident management** coordination
  - Target **Technology Readiness Level: 8**
  - Governance and Sharing Models in development

E-EWS Concepts

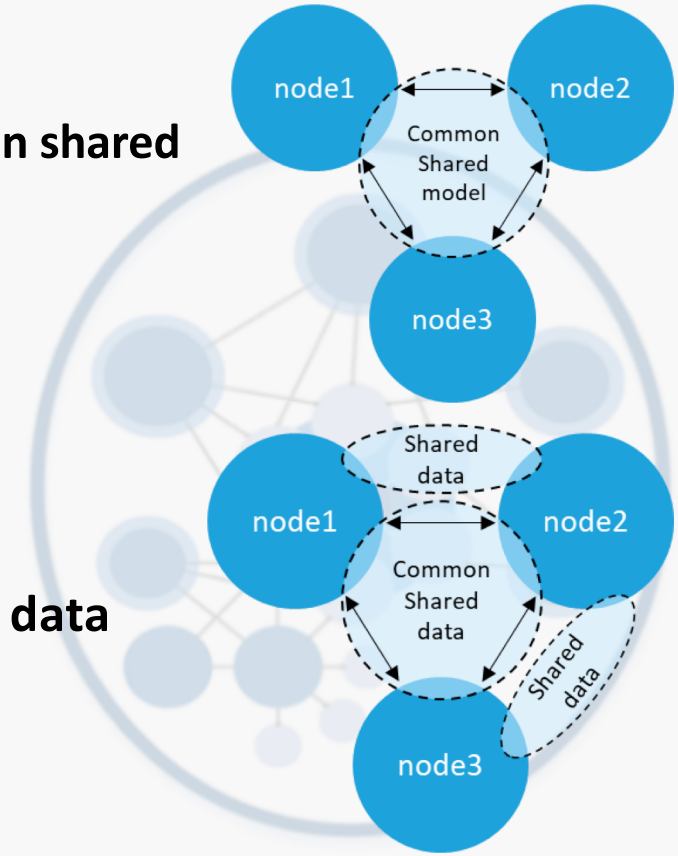


E-EWS Concepts

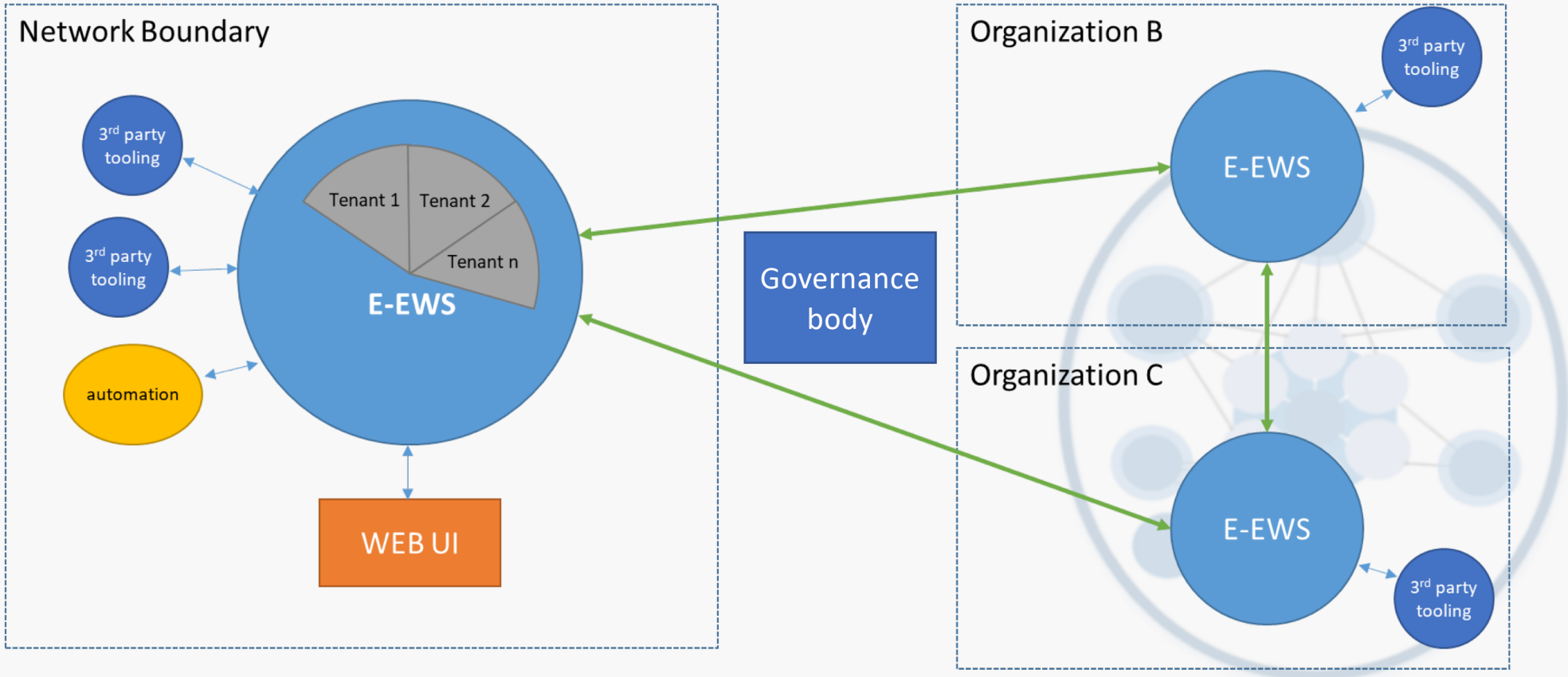
- E-EWS Server
  - The server installation or the E-EWS supports the main functionality of the system.
  - Exposes the APIs for public interaction
- Web User Interface
  - The main user interface in support of the E-EWS functionalities
  - Used by the EWS operators
  - Makes use of public API
- Automation
  - Allow tooling to be automated by E-EWS data
  - Makes use of public API
- 3rd Party Tool Plugins
  - Support 3rd party tooling to interact with E-EWS
  - Plugin architecture to allow independent development
  - Plugin acts as a bridge/mapping between the tooling API and the E-EWS
  - Makes if of public API
  - Trust Model

Common shared model

Shared data

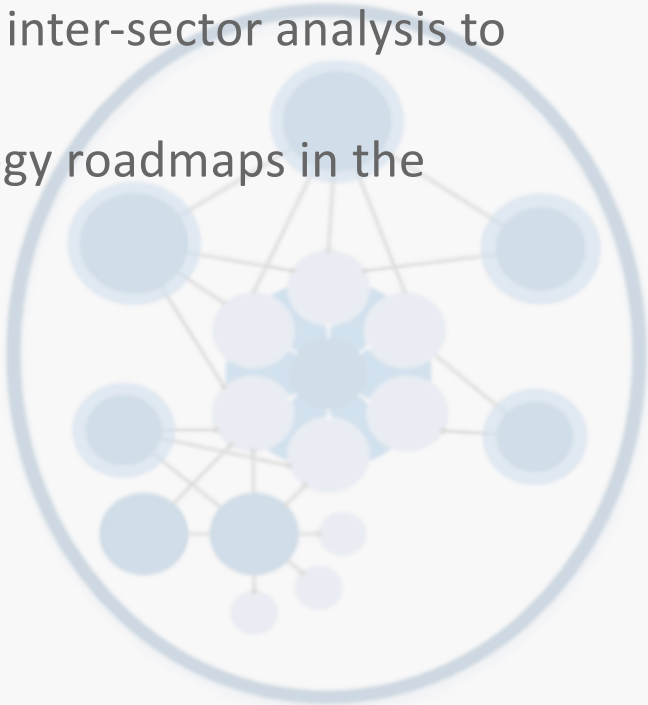


E-EWS concepts - distribution



Demonstration cases for validation

- Sector demonstration cases
  - Scenarios are subject to clarification and amendment based on the results of the project, in particular the results of the sector and inter-sector analysis to be conducted using the E-MSAF.
  - Technologies will be demonstrated from the technology roadmaps in the demonstrations.
  - Importance of inter-sector dependencies.
- Technology demonstration cases
  - E-EWS
  - E-FCR



Demonstration cases for validation

- Health sector
  - ICT becoming more and more pervasive in health care
    - Computerized systems for automation of diagnostic and collection of patient data;
    - Sensors and medical devices with IP addresses connected to the Internet (IOT);
    - Cloud-based health information management systems;
    - Multidisciplinary teams interact with patient and share sensitive data also through personal devices.
  - Cybersecurity lagging behind when compared to other industries
    - Evidence that healthcare is rapidly growing target for hackers;
    - Sensitivity of personal data that could be destroyed or leaked to unauthorized third parties in the event of an intrusion.

Demonstration cases for validation

- Marine sector scenario
  - Already very digitized
  - Major economic sector of strategic importance
  - Digital systems on vessels can be divided in two main categories:
    - Information Technology networks (IT), the hardware and software dedicated to manage and to exchange information; it belongs to IT networks.
    - Operational Technology networks (OT), the hardware and software dedicated to detecting or causing changes in physical processes through Industrial Control Systems.
  - Both networks highly integrated, raising specific challenges, cfr. the cyber kill chain for ICS
  - Risk Management must encompasses all digital systems on board, resulting in specific technical cyber security controls as well as procedural controls

Demonstration cases for validation

- Energy sector
  - Security of critical infrastructure is essential for the safety and security of citizens and the industrial capacity across the EU
  - Some use cases to be considered:
    - Attacks to the command and control systems of the critical infrastructure (unavailability, loss of serviceability, subversion of a C2 center)
    - Attacks to SCADA equipment/devices of the critical Infrastructure

The next two years

- ECHO schedule for the first 2 years is quite tight
  - **E-EWS** and **E-FCR TRL 6** prototypes to be developed for **mid 2021**
  - Governance Models (and related transition from the current model) for the network will be ready for **mid 2021**
  - Preliminary models for **sustainability** of the network, the E-EWS and the E-FCR
  - Goal is to immediately deploy E-EWS and E-FCR and start using them within the ECHO **enlarged partners** (beneficiaries + stakeholders) – **new tenants** for the E-EWS and **new cyber ranges** for the E-FCR
  - Training packages will be ready for **mid 2021** and in delivery, leveraging on E-EWS and E-FCR prototypes
  - **Healthcare**, **Maritime**, **Energy** sectors demonstrations in development (including dependencies with space and water sectors, likely)
  - Other 2 technology innovations (at least) from the technology roadmaps will be in development -> potential interest from NCPs

Outcomes

- ECHO targets practical use of outcomes to offer technologies and services having increased cyber-resilience by sector and among inter-dependent partners
  - Use of E-FCR for experimental simulation of cyber-attack scenarios, pre-production testing, product evaluations
  - Combined use of E-FCR and E-Cybersecurity Certification Scheme (E-CCS) for certified qualification testing of potential technologies required to meet customer specification
  - Use of E-CCS as benchmark of cybersecurity certification to be obtained as a market differentiator
  - Use of E-EWS to share early warning of cybersecurity related issues (e.g., vulnerabilities, malware, etc..)
  - Promotion of improved cyberskills through leveraging diverse education and training options made available by the E-Cybersecurity Skills Framework, particularly as it relates to security-by-design best practices
- Although not clear what will be the future of the 4 Pilot projects, it is expected the most relevant outcomes will be merged to create the **future EU cybersecurity competence centres network**

Engagement Opportunities

- ECHO is interested on enlarging the number of partners, when newcomers can bring an added value to the team
- Parties interested in ECHO will be mapped into the following categories:
  - Stakeholders
  - Potential new partners (R&D and Operational phases)
    - N.B. New partners are considered a subset of stakeholders.
  - Beneficiaries (of grant agreement)
    - N.B. Beneficiaries are currently fixed.
  - Project Advisory Committee Members
    - 15 members (5 identified)
    - Advise on strategic global trends, best and common practice, legal and ethical aspects, concept assessment, scenario definition and prioritization, analysis of operational environments, and test and validation;
    - Help strengthen the ECHO environment, leveraging on their network & experience.

Title	Definition
Stakeholders	Stakeholders are people or organisations who have an interest in the project and can either affect or be affected by the results. Such as users of the services, members of management boards, steering committees, regulatory or policy groups/bodies, lobby groups and suppliers etc.
Partners	Partners are stakeholders who wish to become more active in the project and become contracted parties, offering either funding, technical support or other services in exchange for collaborating in R&D activities.
Beneficiaries	Partners who wish to become active parties within the Consortium requiring a Grant Agreement amendment. Participate in R&D activities within scope of ECHO.

Passive & Active Parties

- Stakeholders & Partners to be considered as either passive or active
- Partners – opportunities for involvement
  - R&D phase 2019-2023 (participate in R&D activities and benefit of all or part of ECHO services (E-EWS, E-FCR, E-Cyberskills framework, E-Certification Framework, tech roadmaps, etc..), depending on their commitment)
  - Operational phase 2023+ (active involvement as service/content providers - TBD)

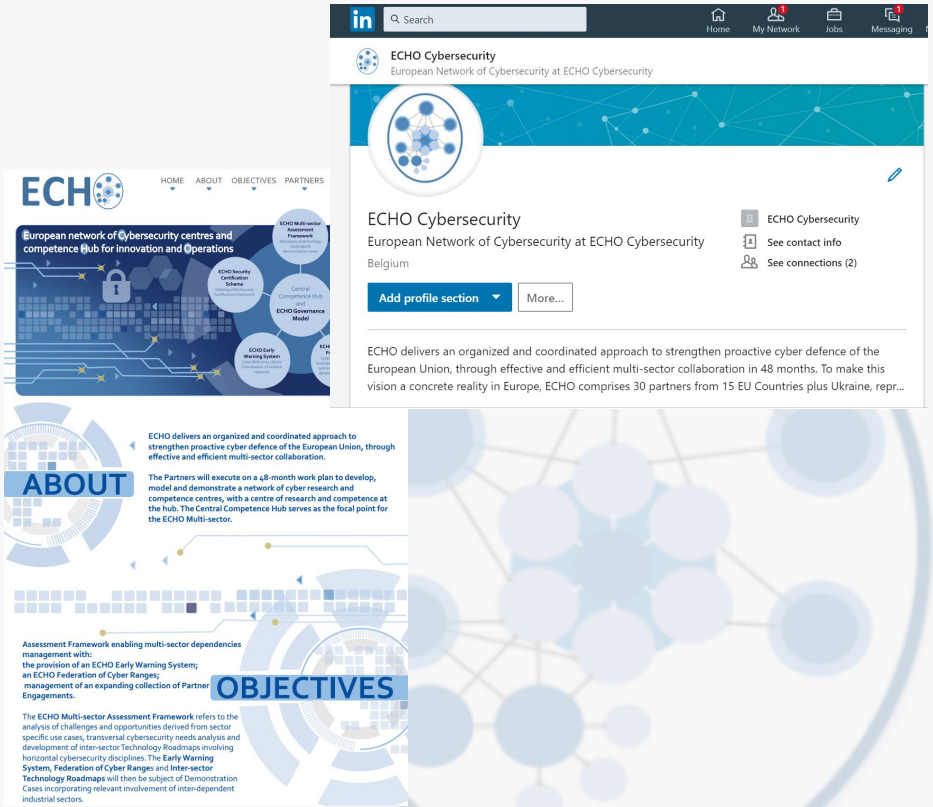
Type	Description
Passive	Passive stakeholders are interested in receiving outputs and results, but are not actively engaged in providing feedback.
Active	Active stakeholders are interested in receiving results and outputs of the project, but are also actively engaged in attending demonstrations, providing feedback and influencing the project direction.

Next steps

- ECHO Project (2019-2023) Governance established
- ECHO Group (2023+) Governance and Business models in development (M12-18) – aim is sustainability of the network after the end of the H2020
- Interested parties:
  - Multisector Innovation Exploitation Deputy Coordinator – a.butterworth@rheagroup.com
  - Project Implementation Coordinator m.merialdo@rheagroup.com
  - Identify key areas of interest
    - Matrix in preparation (October)
  - Legal documentation
    - Currently being drafted (October/November)

Social Media

- For information: info@echonetwork.eu
- ECHO website: www.echonetwork.eu
- Twitter: **@ECHOcybersec**
- Linkedin: ECHO cybersecurity



- Youtube: https://www.youtube.com/channel/UCDQBXrQhoLJ2lnf38x1X6Uw


SPARTA
RE-THINKING THE WAY CYBERSECURITY RESEARCH IS PERFORMED IN EUROPE (SPARTA)
Fabio Martinelli
National Research Council of Italy
@sparta_eu | sparta.eu

OVERVIEW

- The approach
- The structure
- SPARTA research programs
- SPARTA Roadmap
- SPARTA partnership
  - Joint Competence Centre Infrastructure (JCCI)
  - SPARTA associates
  - SPARTA monthly events
- Conclusion

Russians Win Race To Launch Earth Satellite

Man On Threshold Of Space Travel

By DANIEL F. GILMORE
United Press Staff Correspondent

LONDON (UP)—The pulsating radio "beep" of the first manmade earth satellite signalled today to the world that man had crossed the threshold into the age of travel through space.

The Soviet Union announced it had won the race into space by launching an earth satellite Friday, a 184-pound, 22-inch globe now orbiting the earth at 18,000 miles an hour, 560 miles up.

Millions of persons throughout the world heard the "beep...beep... beep..." rebroadcast today by local stations and realized that man

— WEATHER —

WEST VIRGINIA—Partly cloudy

How To Spot Satellite

By UNITED PRESS

Here's how to look for the Russian earth satellite which will be whizzing through the sky at 18,000 miles an hour.

The best time to spot it is at dawn or dusk when the sky is semi-dark. There is a chance that it could be seen if it travels across the face of the moon at night.

The best instruments to use are ordinary binoculars or telescopes. Powerful telescopes won't pick it up because of their narrow fields.

Through optical instruments, the satellite will look like the

U.S. May Sp Up Satellite Program

By JOSEPH L. M
United Press Staff Cor

WASHINGTON (UP)— scientists, caught flat Russia's epic launching man-made moon, indic the United States may its own earth satellite p

Leaders of the U.S. sa gram also said that Russia rocketed its pound satellite into a dling orbit with a roc


Russians Win Race To Launch Earth Satellite
STRATEGIC SURPRISE
Man On Threshold Of Space Travel
By DANIEL F. GILMORE
United Press Staff Correspondent
LONDON (UP)—The pulsating "beep" of the first manmade earth satellite signalled today to the world that man had crossed the threshold into the age of travel through space.
The Soviet Union announced it had won the race into space by launching an earth satellite Friday, a 184-pound, 22-inch globe now orbiting the earth at 18,000 miles an hour, 560 miles up.
Millions of persons throughout the world heard the "beep...beep... beep..." rebroadcast today by local stations and realized that man
Risky and complex developments
— WEATHER —
WEST VIRGINIA—Partly cloudy
How To Spot Satellite
By UNITED PRESS
Here's how to look for the Russian earth satellite which will be whizzing through the sky at 18,000 miles an hour.
The best time to spot it is at dawn or dusk when the sky is semi-dark. There is a chance that it could be seen if it travels across the face of the moon at night.
The best instruments to use are ordinary binoculars or telescopes. Powerful telescopes won't pick it up because of their narrow fields.
Through optical instruments, the satellite will look like the
Concrete and transformative results
U.S. May Sp Up Satellite Program
By JOSEPH L. M
United Press Staff Cor
WASHINGTON (UP)— scientists, caught flat Russia's epic launching man-made moon, indic the United States may its own earth satellite p
Leaders of the U.S. s gram also said that Russia rocketed its pound satellite into a dling orbit with a roc


THIS IS IT

Re-imagining the way cybersecurity research, innovation, and training are performed in Europe

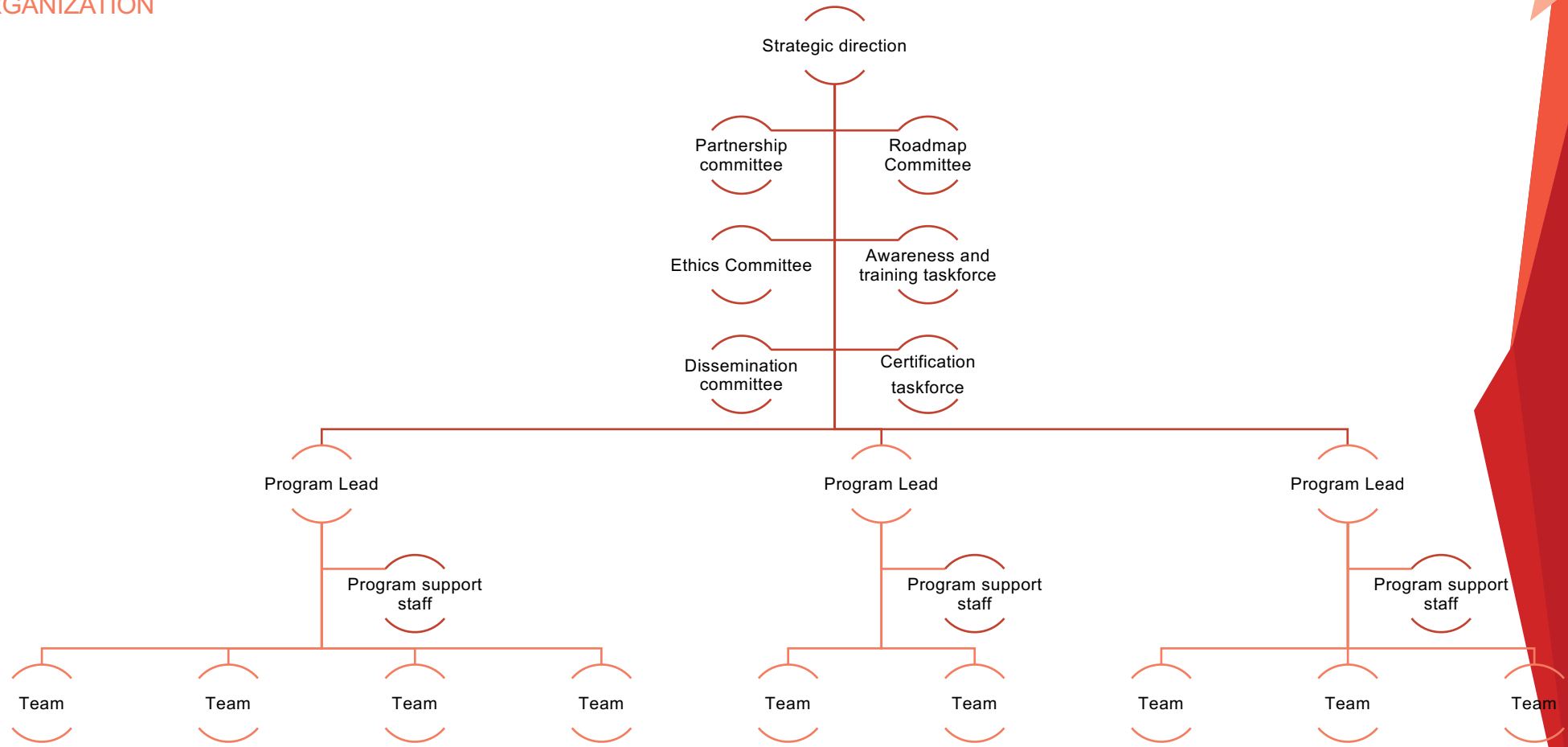
- **Develop unique but concrete innovation paths**
- **Setup shared and virtual spaces for collaborations**
- **Strenghten certification, outreach, and training capacities**
- **Pull together European, national, and regional ecosystems**

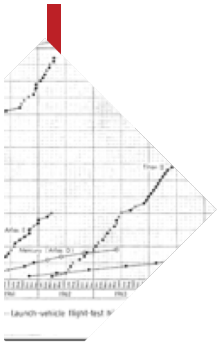
Contribute *inter alia* to the objective of European strategic autonomy

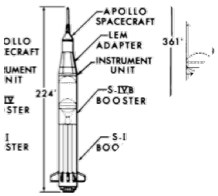
SPARTA
Structure

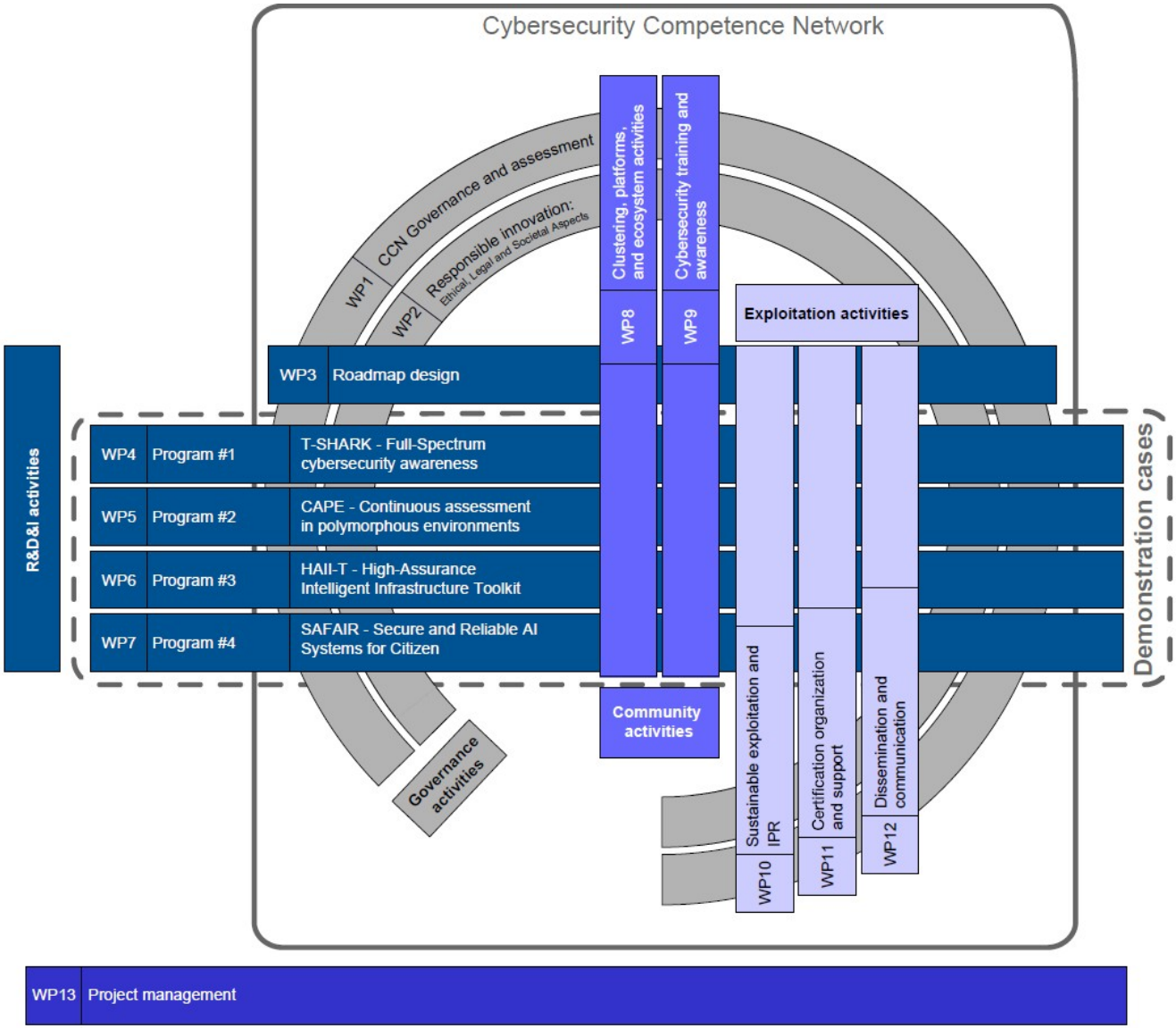
The performance of the defenders at the the Battle of Thermopylae is used as an example of the advantages of training, equipment, and good use of terrain as force multipliers and has become a symbol of courage against overwhelming odds

ORGANIZATION






APOLLO SPACECRAFT
LEM ADAPTER
INSTRUMENT UNIT
S-IVB BOOSTER
S-I
361'
224'


Cybersecurity Competence Network
WP1
CCN Governance and assessment
WP2
Responsible innovation:
Ethical, Legal and Societal Aspects
Clustering, platforms, and ecosystem activities
WP8
Cybersecurity training and awareness
WP9
Exploitation activities
WP3
Roadmap design
R&D&I activities
WP4
Program #1
T-SHARK - Full-Spectrum cybersecurity awareness
WP5
Program #2
CAPE - Continuous assessment in polymorphous environments
WP6
Program #3
HAII-T - High-Assurance Intelligent Infrastructure Toolkit
WP7
Program #4
SAFAIR - Secure and Reliable AI Systems for Citizen
Demonstration cases
Community activities
Governance activities
Sustainable exploitation and IPR
WP10
Certification organization and support
WP11
Dissemination and communication
WP12
WP13
Project management

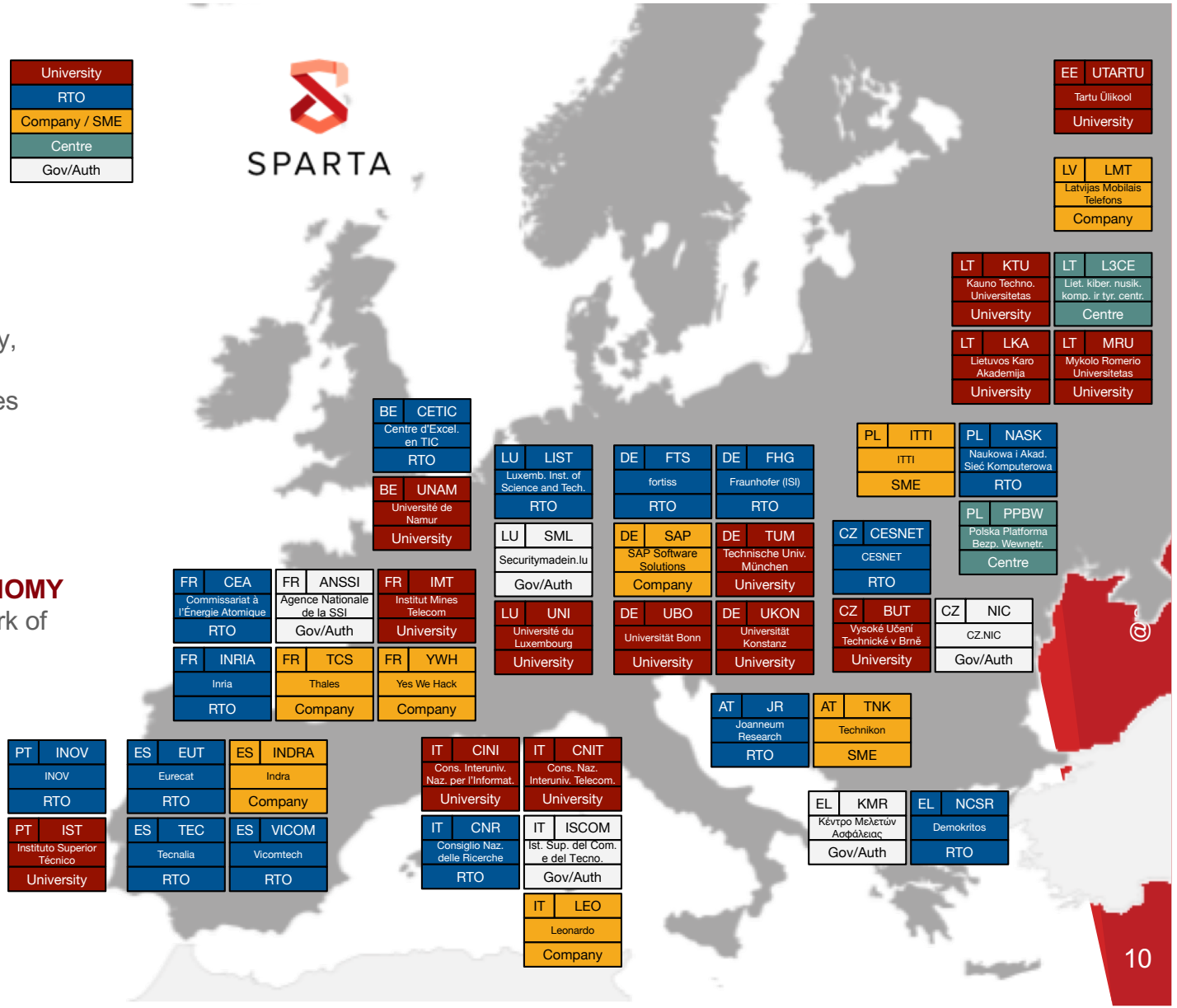
A STRONG BASIS OF EXCELLENCE

44 partners spanning academia, industry, institutions, grassroots
Pragmatically anchored in member states

STRATEGIC PROGRAMS

THE STAKES OF EUROPEAN AUTONOMY

Design a long-term roadmap and network of competence centers

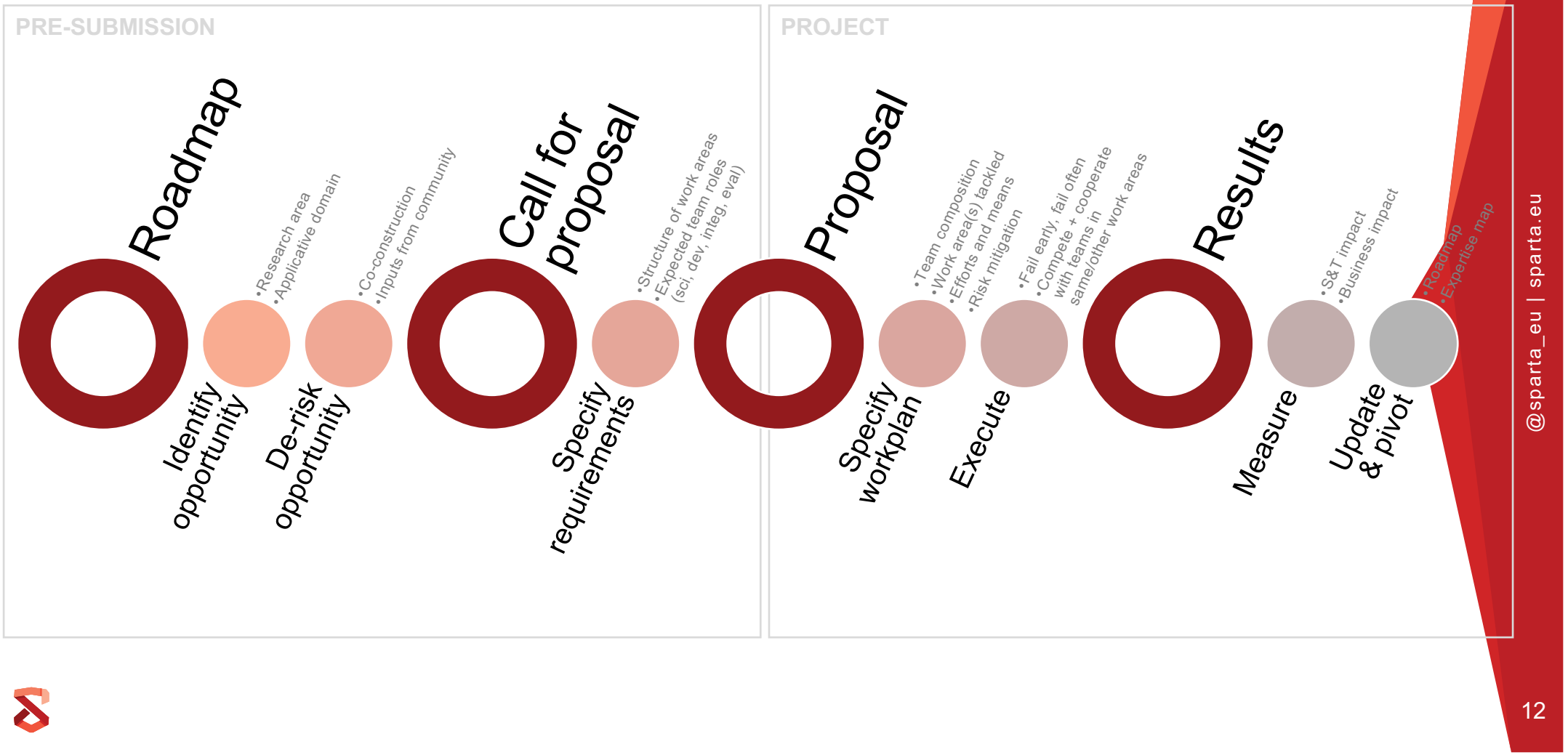


SPARTA

Current research Programs

The performance of the defenders at the the Battle of Thermopylae is used as an example of the advantages of training, equipment, and good use of terrain as force multipliers and has become a symbol of courage against overwhelming odds

PROGRAMS – SPARTA PROJECT



- T-SHARK Full-spectrum cybersecurity awareness
  - **objective** : expand the reach of threat understanding, from the current investigation-level definition, up to strategic considerations, and down to real-time events
  - **requires** : collection of heterogeneous data, models and predictions for multi-level security, AI and visualization
  - **strengths** : regulation encouraging information-sharing (NIS directive, French OIV law, ...), strong culture of data protection (GDPR, cryptography, ...)
  - **aims at** : providing decision-making tools, fostering a common cyber security culture, raising preparedness for possible disruptions and attacks
  - **capabilities** : thoroughly supervise critical systems including when they are not provided / integrated by EU actors, raise awareness and citizen involvement
- CAPE Continuous assessment in polymorphous environments
  - **objective** : enhance assessment processes to be able to perform continuously over HW/SW lifecycles, and under changing environments
  - **requires** : binary and code verification, scalable monitoring, network reaction, HW/SW roots of trust, dynamic assurance cases
  - **strengths** : one of the best evaluation ecosystem in the world (Common Criteria, smart cards, ...)
  - **aims at** : building tools for continuous trust in sovereign and foreign-sourced components, systems, and services
  - **capabilities** : drastically increase evaluation capabilities in a world where most of the components are developed outside of the EU, prepare future certification
- HAII-T High-Assurance Intelligent Infrastructure Toolkit
  - **objective** : manage the heterogeneity of the IoT by providing a secure-by-design infrastructure that can offer end-to-end security guarantees
  - **requires** : formal security models, application security, verification and validation, verified and scalable cryptography, secure OS
  - **strengths** : building on EU's lead position on formal methods for safety and security
  - **aims at** : providing a full verified software stack from applications down to the system software and SW/HW interface, which can serve in a variety of IoT devices
  - **capabilities** : simplify the the deployment of IoT applications ; facilitate their certification
- SAFAIR Secure and fair AI systems
  - **objective** : Evaluating security of AI systems, producing approaches to make systems using AI more robust to attackers' manipulation. Furthermore, the goal is to make AI systems more reliable and resilient through enhanced explainability and better understanding of threats
  - **requires** : adversarial machine learning, data from different AI application domains
  - **strengths** : increasing adoption of AI technology in various information systems within EU, recent strategy of EU member states to collaborate on Artificial Intelligence
  - **aims at** : providing methods and tools for analysis and assessment of security threats for AI systems, and solutions for protection
  - **capabilities** : exploratory

SPARTA
ROADMAP

The performance of the defenders at the the Battle of Thermopylae is used as an example of the advantages of training, equipment, and good use of terrain as force multipliers and has become a symbol of courage against overwhelming odds

SPARTA ROADMAP: MISSION

Mission: Establish a European cybersecurity research & innovation roadmap

That will

Strengthen the EU's cybersecurity capacity
Technology, Services, Applications and Products
Close cyber skill gaps and prepare for future challenges
Education, Life long learning,

Which is essential to

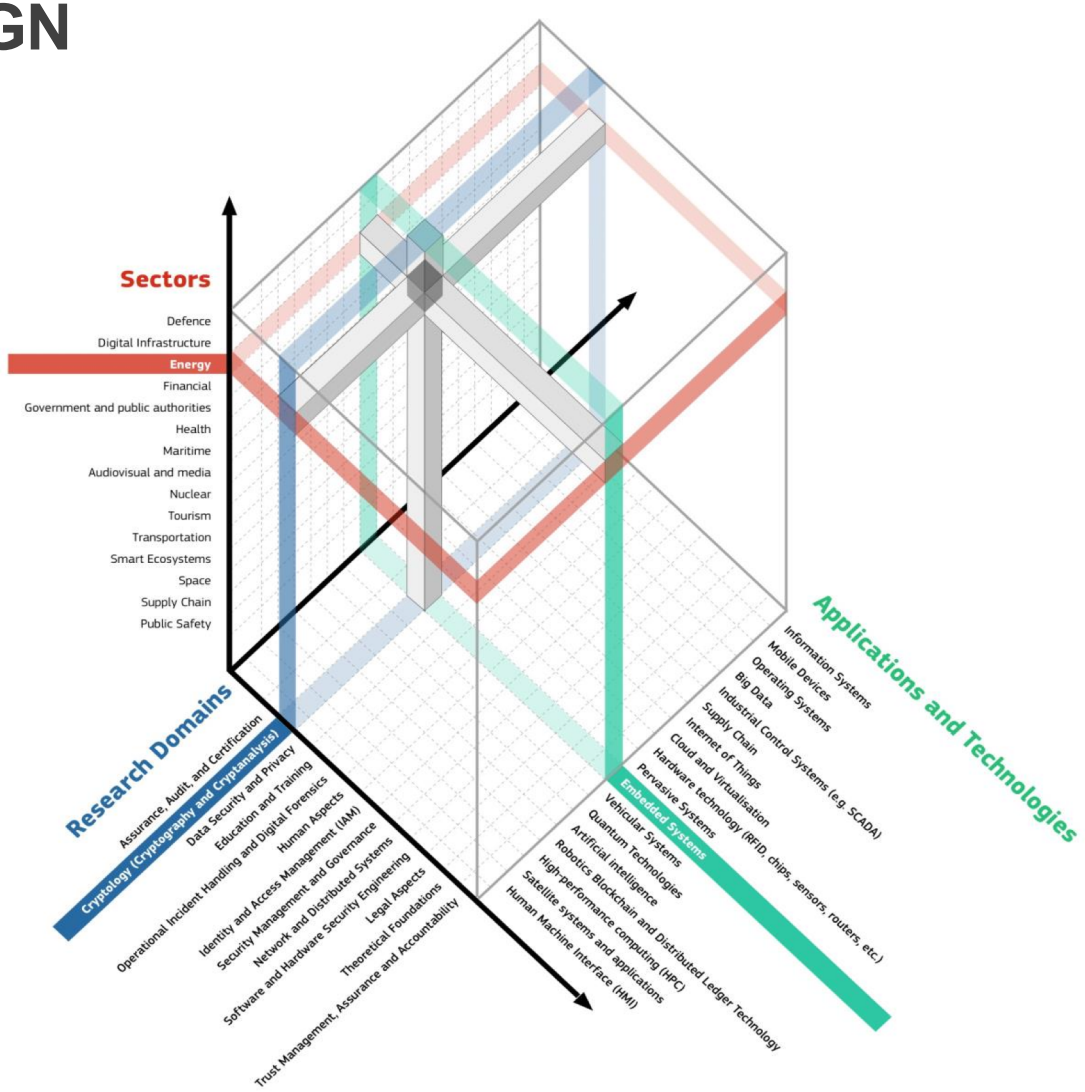
retain digital sovereignty and autonomy of the European industries and governments
increase trust in products, services and infrastructures

SPARTA ROADMAP DESIGN

Roadmap building blocks:

JRC Taxonomy

Roadmap Challenge Templates



4.1 Basis: JRC Taxonomy

- 3 planes for categorizing cybersecurity topics
  - Cybersecurity Research Domains
  - Application and Technologies
  - Sectors

SPARTA
Partnership

The performance of the defenders at the the Battle of Thermopylae is used as an example of the advantages of training, equipment, and good use of terrain as force multipliers and has become a symbol of courage against overwhelming odds

SPARTA Joint Competence Centre Infrastructure (JCCI)

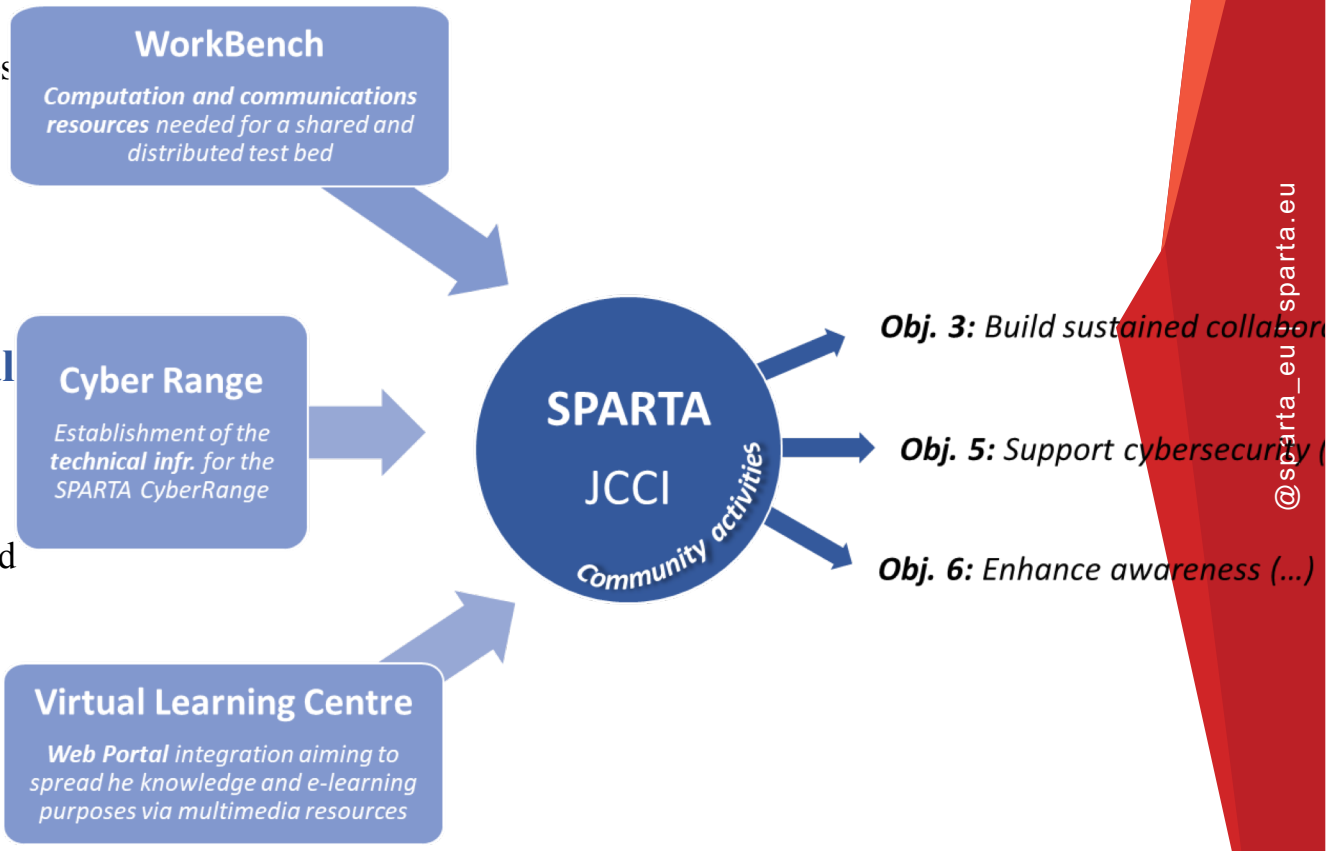
This task is specifically devoted to create a **common working environment** that enables the **sharing and collaboration among partners** also in a **remote way**.

This embodies both the **research and development aspects** as well as the **financial and administrative administration** of the network

Platforms developed in the SPARTA programs should be ideally integrated :

We need to consider:

- The minimal set of services
- The desired level of integration
- Terms of Use (business models)
- …



PARTNERSHIP AND ECOSYSTEM

14 European member states **44 partners** **more than 50 Associates**

SPARTA associates&friends

EC, JRC, Fellow ICT 03 Pilot Projects

And more !!!

Other EU projects for roadmapping as CyberWatching, AEGIS, EUNITY, Standard ICT, …

EU agencies as ENISA, EC3, EDA, ESA, …

Outside EU activities, international dimension (e.g. US/Japan)

EU organizations as ECSO, ERCIM, IFIP, …

ASSOCIATES&FRIENDS

- Access to SPARTA Infrastructures and platforms
- Contribution to the Roadmap
- Access to results of SPARTA programs
- Attending Bi-yearly SPARTA meetings
- …

SPARTA
FRIENDS

SPARTA
PARTNERSHIP

SPARTA
ROADMAP

SPARTA
PROGRAMS

SPARTA
ASSOCIATES

@sparta_eu | sparta.eu

		Large groups	SME	Clusters	Region authorities	Universities
Roadmap design and results		X				X
Early program results		X	X			
Networking		X	X	X	X	X
Capabilities maps	Training	X	X			X
	Certification	X				
	Industry	X	X	X		
Territorial animation			X	X	X	X
Incubators		X	X			X

ASSOCIATES

Include actors from

- Large groups and SME
- Local, National, European clusters
- Regional authorities
- Close academic and industrial entities

Access to

- Roadmap and early program results
- Networking with council and SPARTA members

Contributions to

- Training, certification, and industry capability maps
- Territorial animation
- Incubators

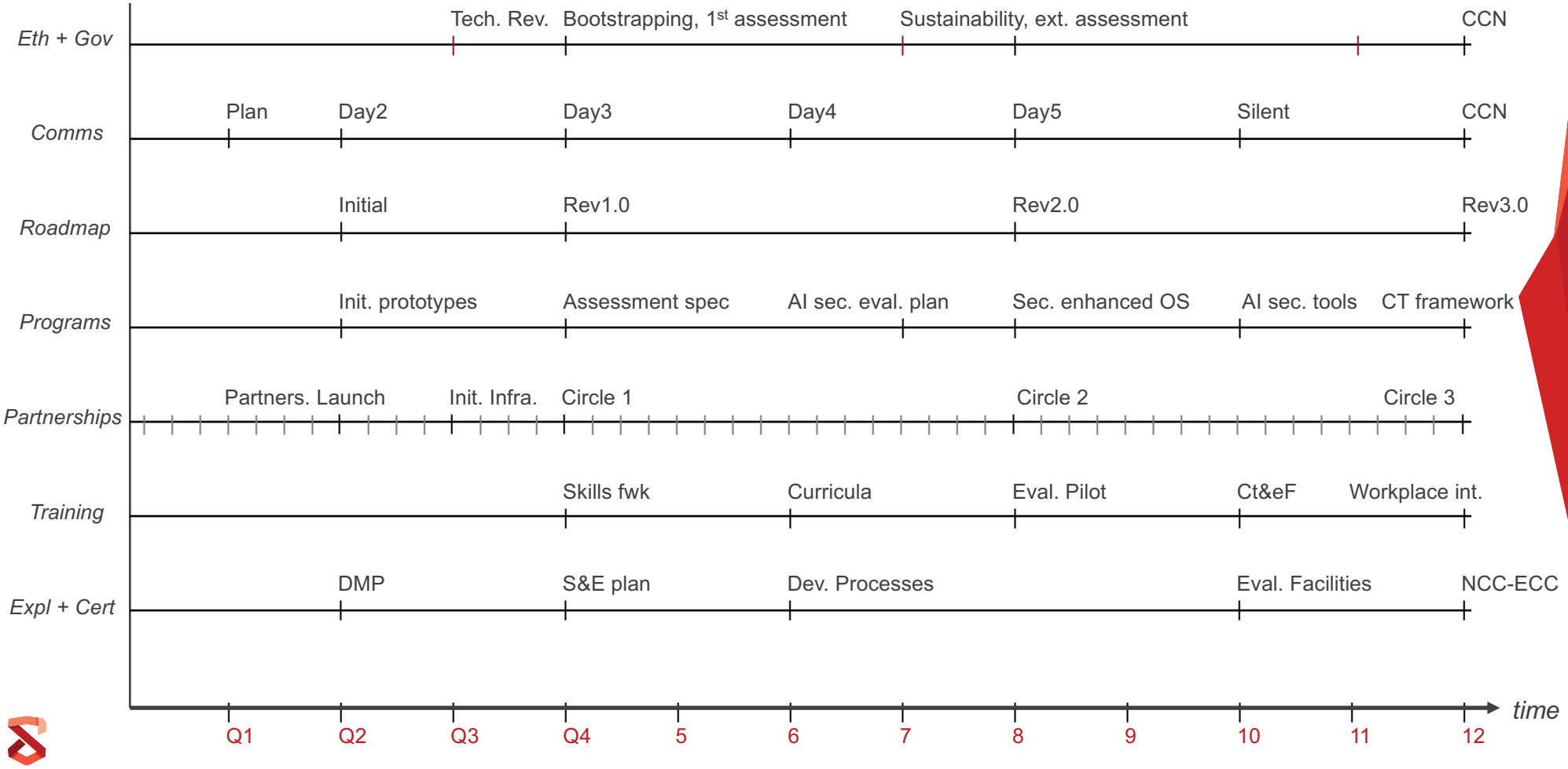
Eligible to complementary late-stage project funding

MONTHLY ASSOCIATE WORKSHOPS

- Each month at least one local SPARTA event involving the associates!
  - Comment on roadmap
  - Spread the SPARTA results
- A country represented in SPARTA is involved
- Opportunity to cluster and shape the local ecosystem and integrate it with the European one (SPARTA ecosystem).

- Btw, sparta means also “sow”/ “spread the seeds” in greek

OVERVIEW
FIRING ON ALL CYLINDERS




THIS IS IT


SPARTA
THANK YOU
FOR WATCHING!
sparta.eu
contact@sparta.eu
@sparta_eu
This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 830892

Cyber Security for Europe

CyberSec4Europe

Kai Rannenberg, Goethe University Frankfurt

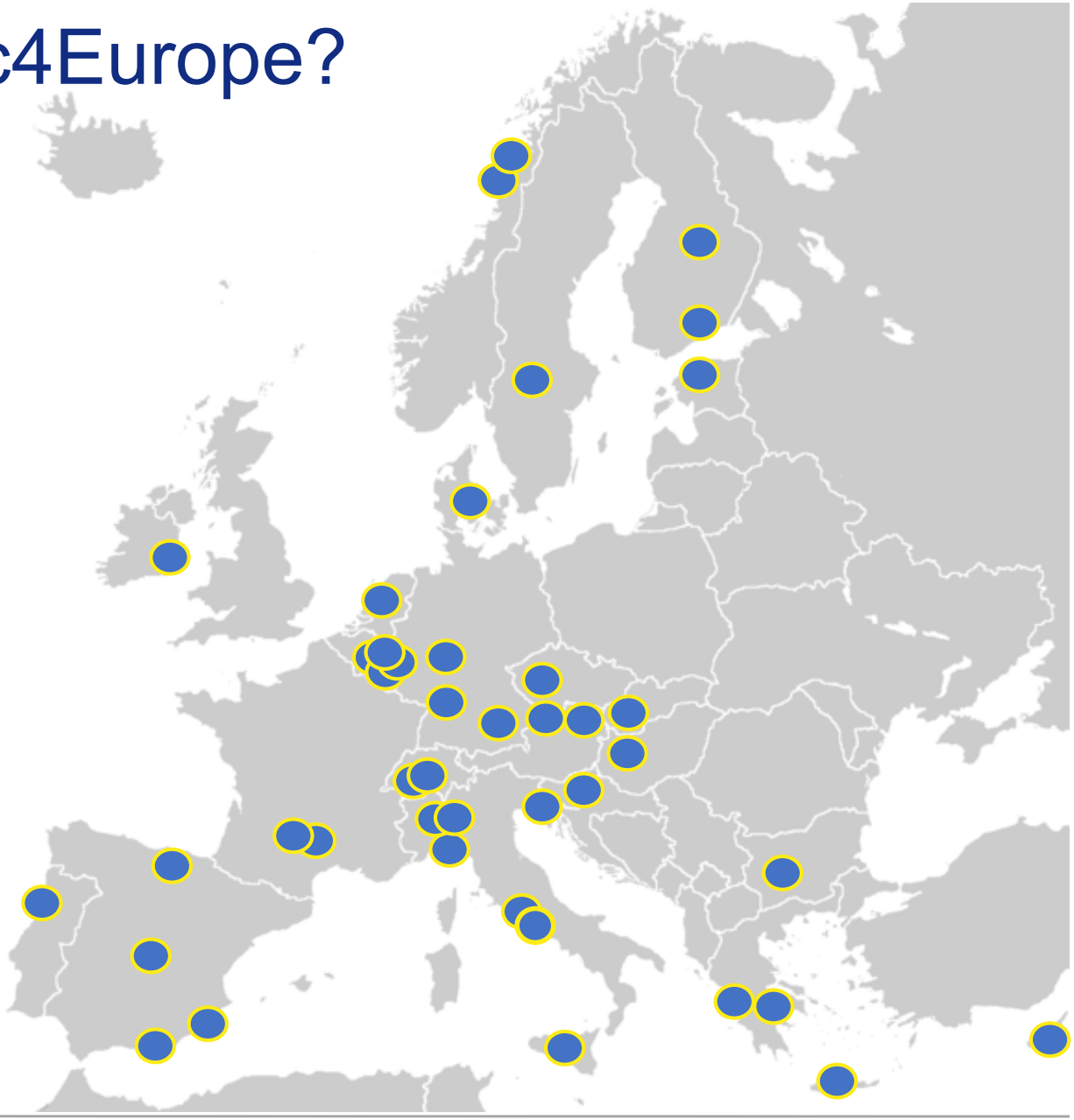
Cybersecurity for Europe 2019
2019-11-13/15
Toulouse, Hôtel de Région

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Who Are CyberSec4Europe?

- Centres of Excellence / Universities / Research Centres / SMEs
- 43 partners in 22 countries
- 26 ECSO members involved in 6 ECSO Working Groups
- Existing networks (ECSO, TDL, EOS, CEPIS)
- Experience from over 100 cybersecurity projects in 14 key cyber domains
- 11 technology/ application elements and coverage of nine vertical sectors
- Funding period: 02/2019 – 07/2022

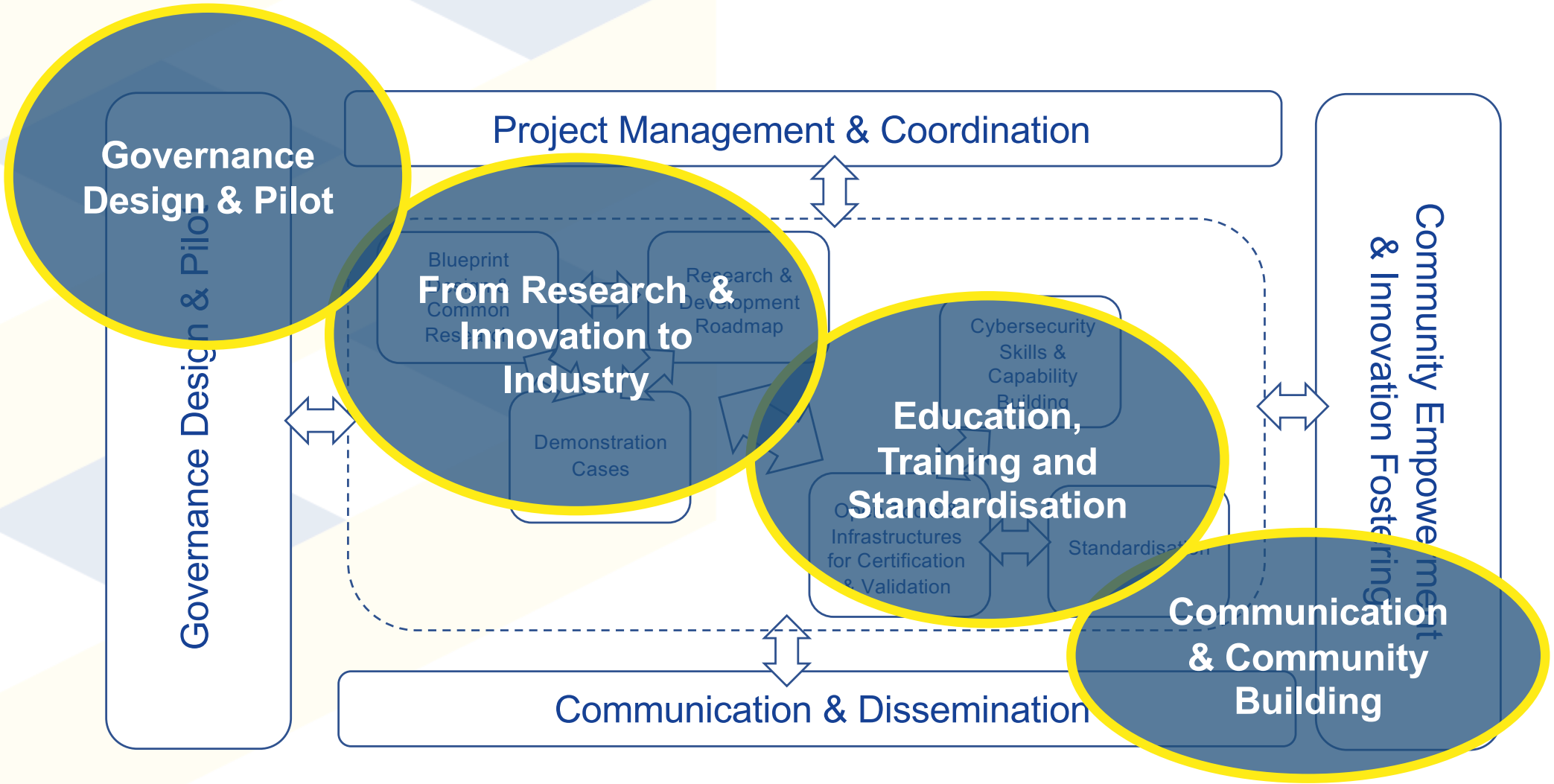


About CyberSec4Europe

CyberSec4Europe is a research-based consortium working across four different but inter-related areas with a strong focus on openness and citizen-centricity in order to:

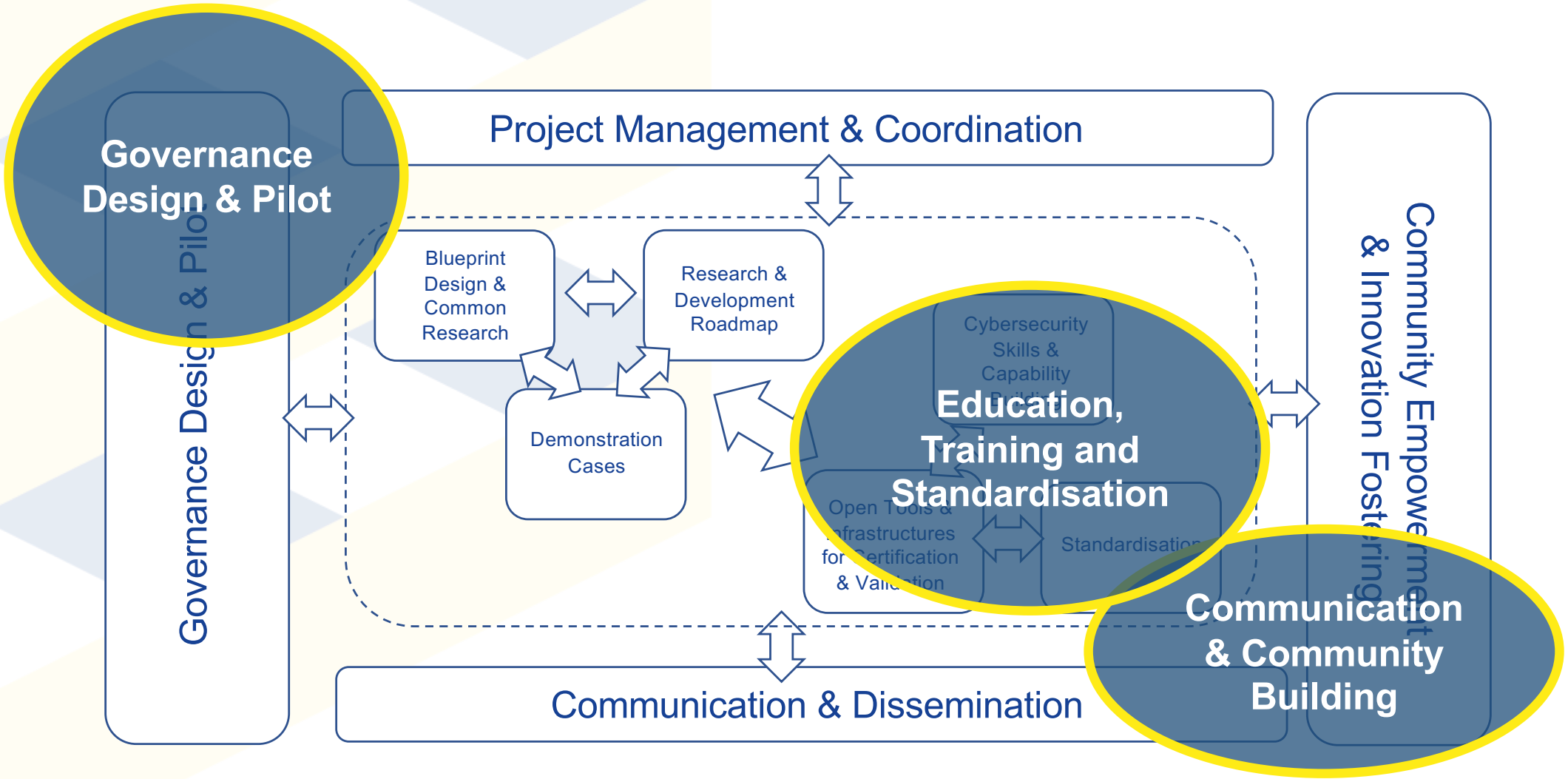
- Pilot a European Cybersecurity Competence Network
- Design, test and demonstrate potential governance structures for the network of competence centres
- Harmonise the journey from software componentry identified by a set of roadmaps leading to recommendations
- Ensure the adequacy and availability of cybersecurity education and training as well as common open standards
- Communicate widely and build communities

Piloting a Competence Network



From Research & Innovation to Industry

Cyber Security for Europe



Demonstration Cases by Industrial Sectors

Cyber Security for Europe

Finance

- Incident reporting
- PSD2 / GDPR issues

Health

- Medical data exchange

Smart Cities

- Citizen participation/e-Government
- Critical infrastructures
- Education

Transport

- Maritime (port critical infrastructure)
- Supply chain assurance

Boost the success of businesses and protect the rights of citizens in the EU.

Matching Industry Demonstrators with Blueprint Research

Cyber Security for Europe

Application Demonstrators

Finance
- Incident reporting
- PSD2 / GDPR issues

Health
- Medical data exchange

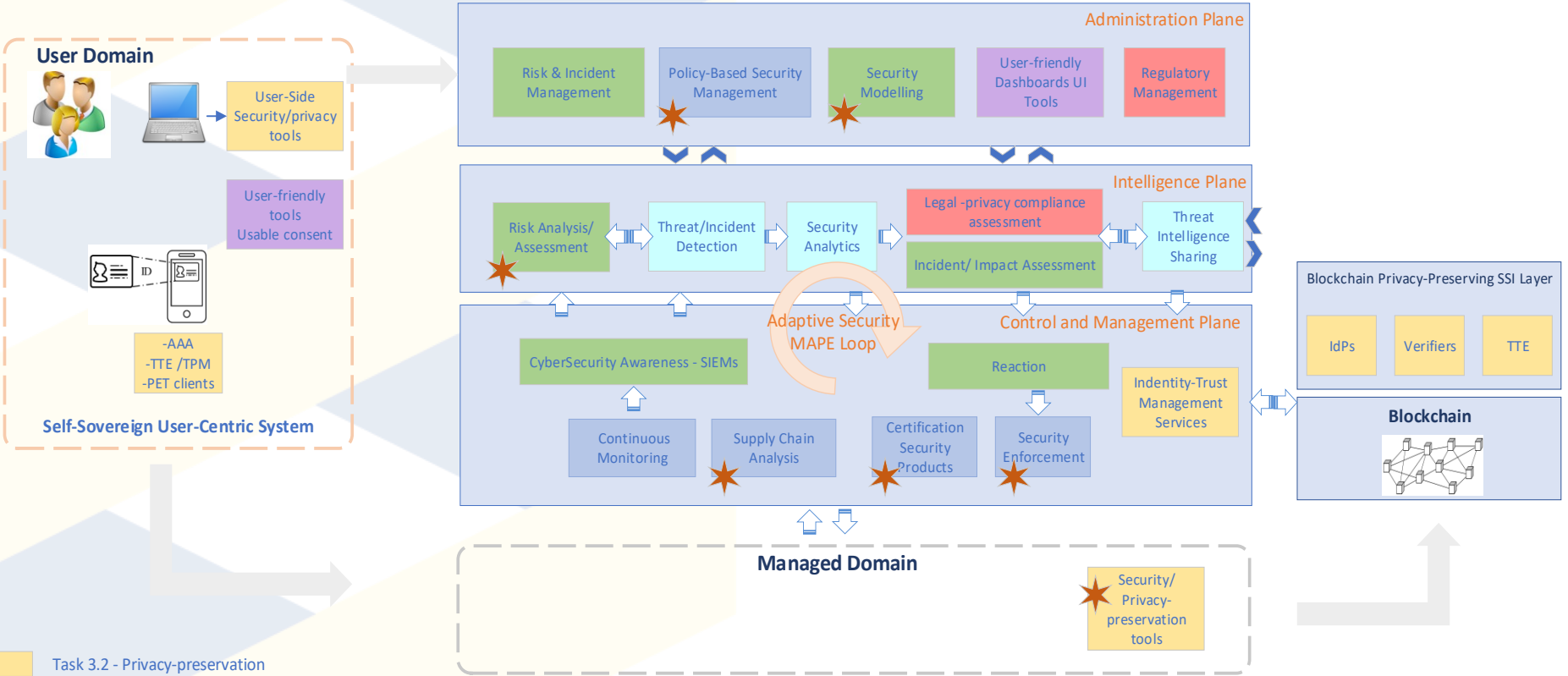
Smart Cities
- Citizen participation/e-Government
- Critical infrastructures
- Education

• Transport
- Maritime assurance
- Supply chain

Blueprint Research

- Research and integration on cybersecurity enablers and underlying technologies
- SDL - software development lifecycle
- Security intelligence
- Adaptive security
- Usable security
- Regulatory sources for citizen-friendly goals
- Conformity, validation and certification
- Continuous scouting
- Impact on society

WP3 Global Architecture and Tasks Block



Task 3.2 - Privacy-preservation

Task 3.3 - Software Development Lifecycle (SDL)

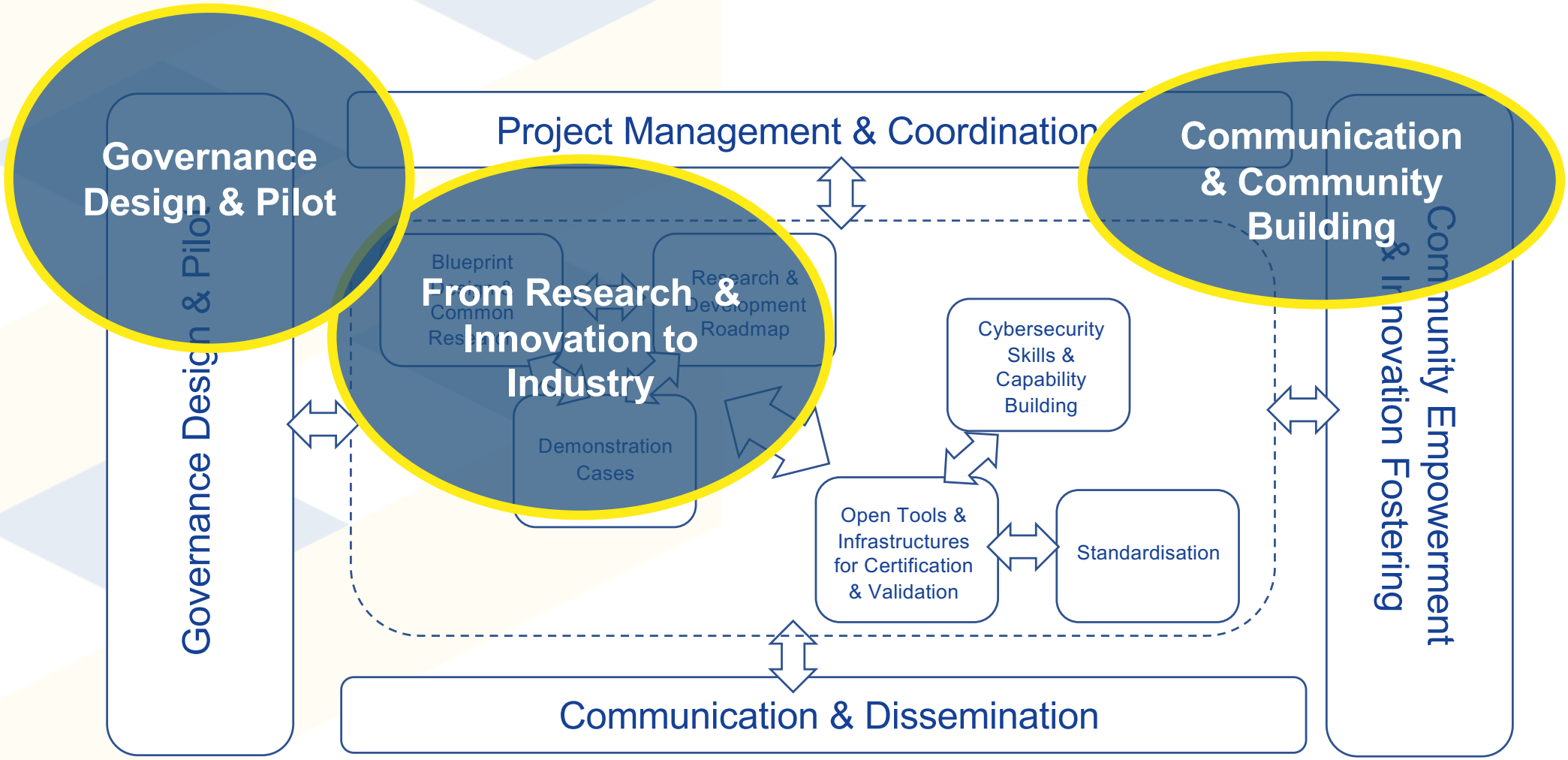
Task 3.4 -Security Intelligence

Task 3.5 - Adaptive Security

Task 3.6 - Usable Security

Task 3.7 - Regulatory Management

Education, Training & Standardisation



Cybersecurity Skills & Capability Building

Cyber Security for Europe

- Combines formal, professional and non-traditional skill building

- University education → Map education in Europe
- Professional training and workforce assessment
- Virtual education
  - Quality branding of MOOC education was the first pilot of governance delivered in the summer
- Cyber ranges as platform for education, training

Open Tools and Infrastructures for Certification and Validation

Cyber Security for Europe

- Open tools and common portable virtual lab
- Federated infrastructures for cyber range and testing
- Certification - methodologies, tools, and infrastructure

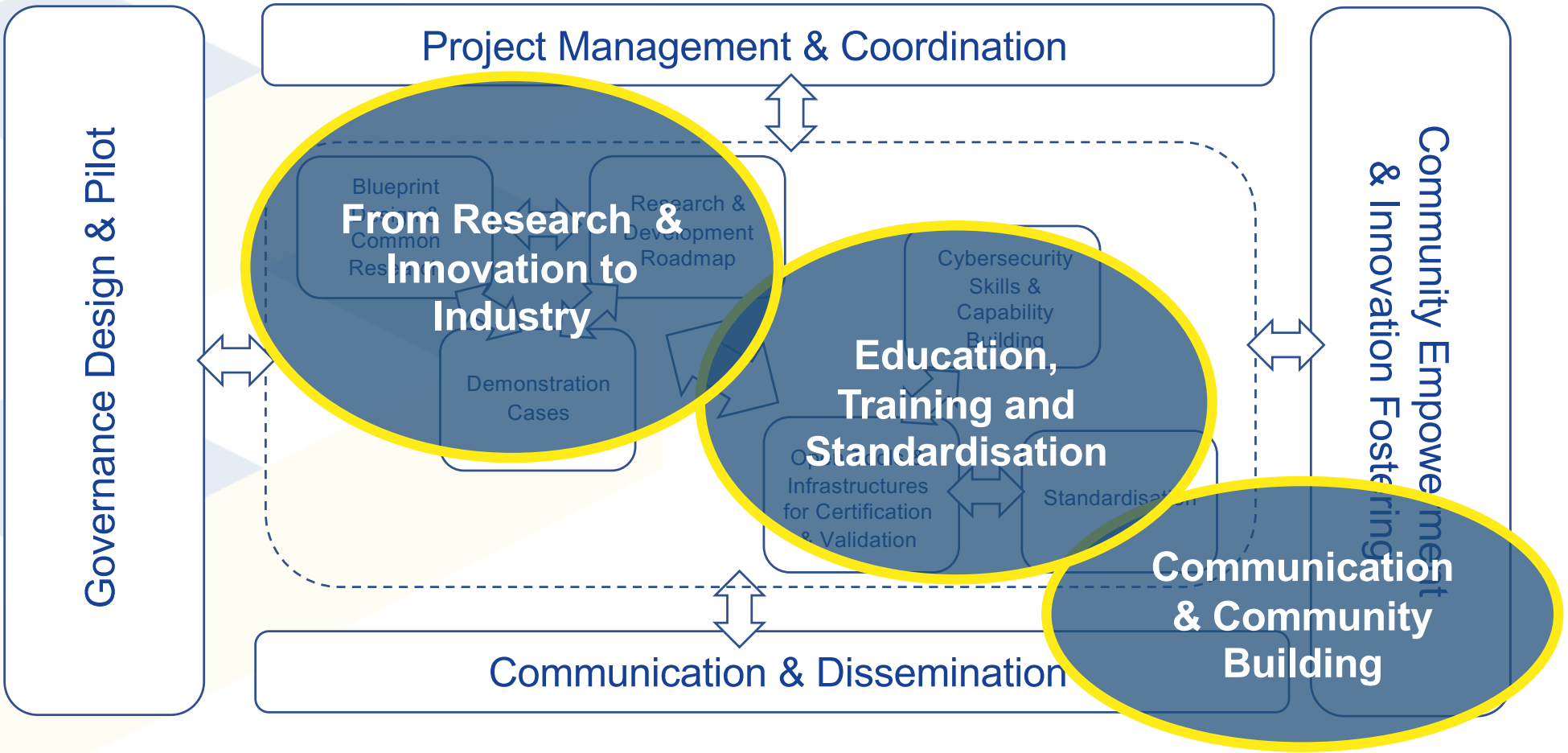
Standardisation

Cyber Security for Europe

- Increase economic impact of EU R&I → disseminating EU Tech into international standards

- Maintaining contacts with standardisation organisations
- Assessing existing procedures in the context of cybersecurity
- From technical work → standards
- Bring together standards projects and key cybersecurity experts

Governance Design & Pilot

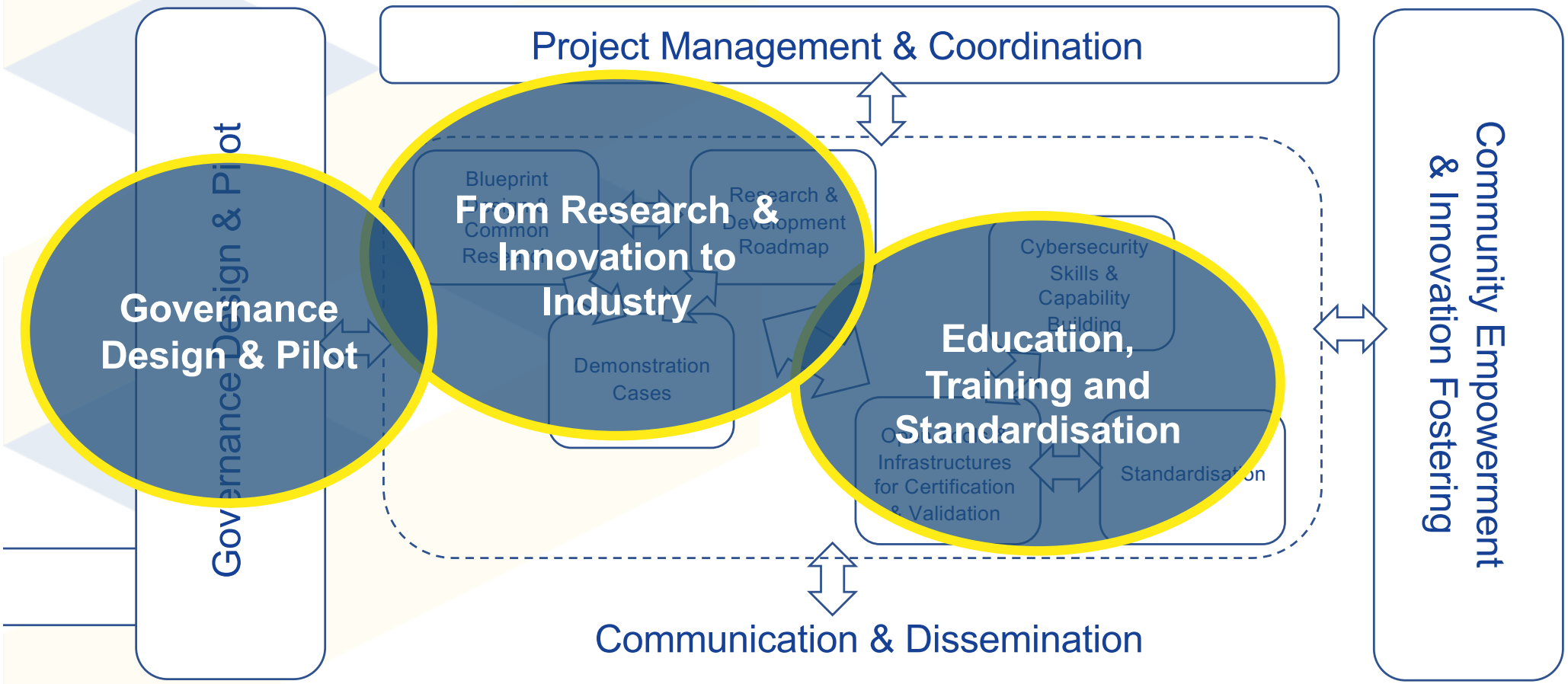


Governance Design & Tasks

Cyber Security for Europe

- Collecting Stakeholders' viewpoints
  - If you have strong opinions → UTrento likes to interview you
- Assessing best governance practices
  - Top-down vs. bottom up
  - Civil society (academia, NGOs, industry) involvement vs. government/admin (police, SIGINT, military) involvement
- Governance structure
  - Design: enable bottom-up advice
  - Operation and testing: MOOCs and regional hub in Toulouse
- Preparation for the implementation
  - Regional vs. national
    - Pilot regional competence hub in Toulouse
    - National hub candidate in Denmark

Communication & Community Building

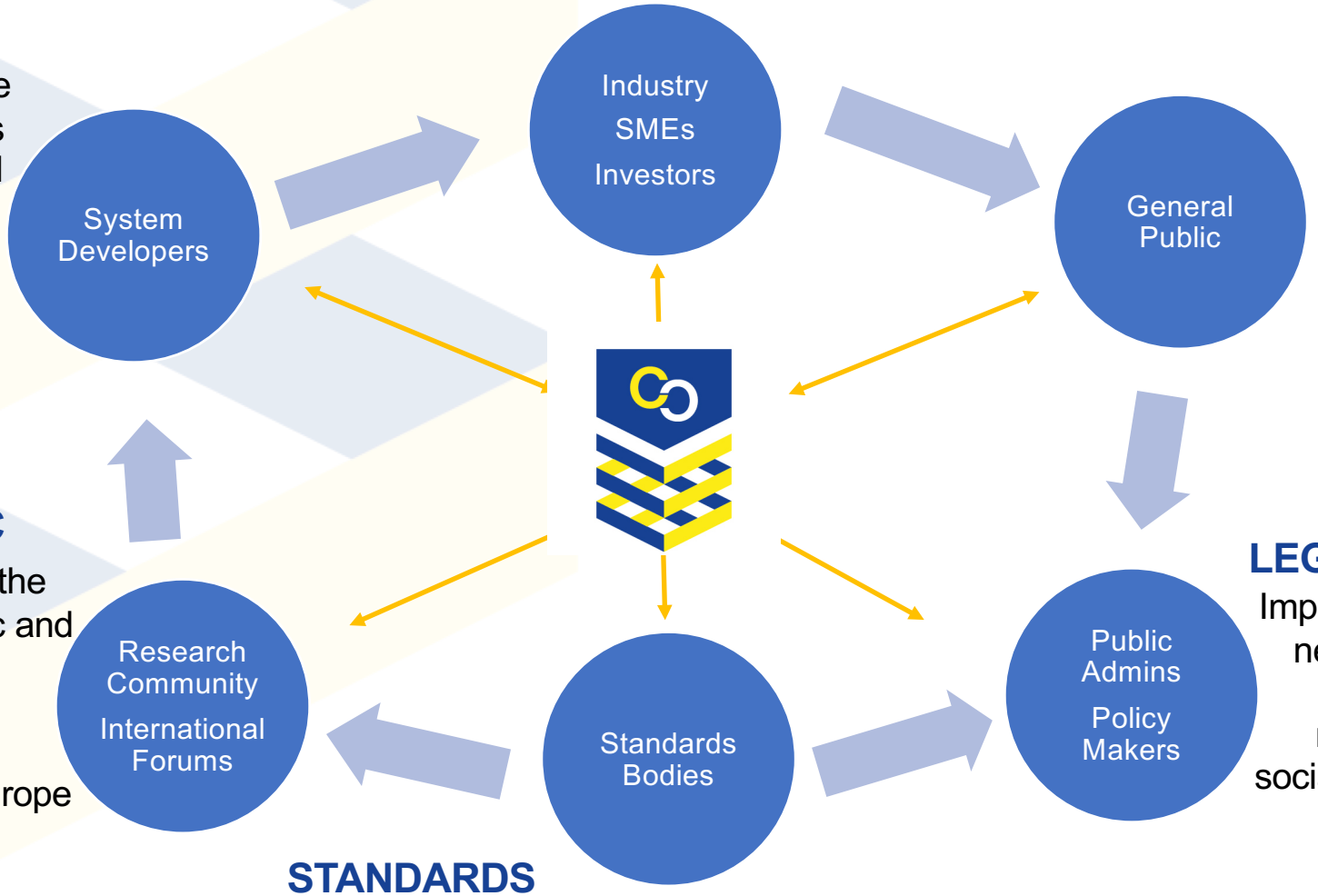


Cybersecurity Stakeholders

Cyber Security for Europe

BUSINESS Business opportunities and potential of technology and societal benefits

TECHNICAL
Understandable by ICT systems developers and system managers



SOCIAL
Understandable by a large public of non-specialists

SCIENTIFIC
High level on the main scientific and technical innovation addressed by CyberSec4Europe

LEGISLATIVE
Implementation of new EU privacy and security regulation and social implications

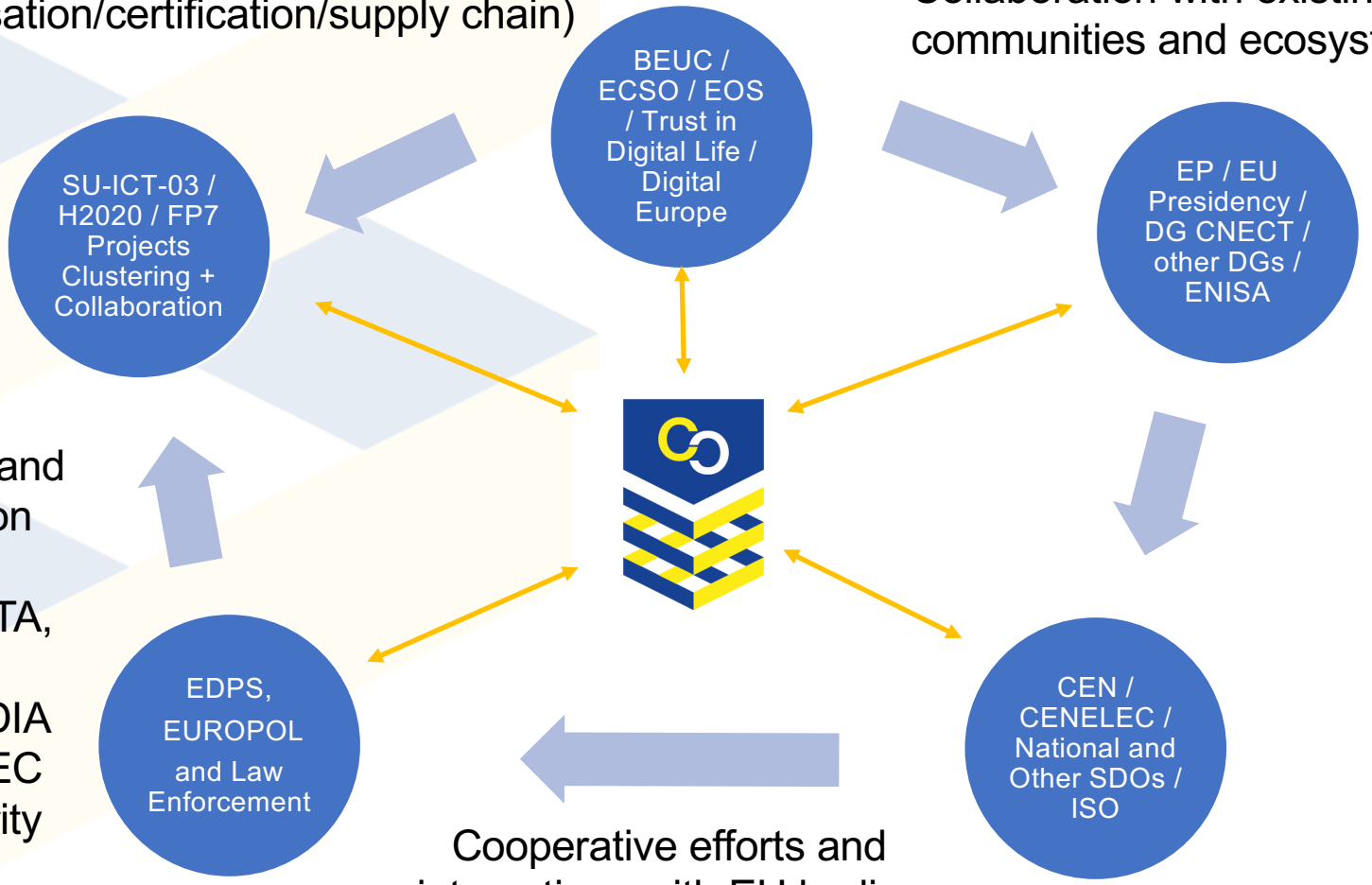
STANDARDS

Community Empowerment and Innovation Fostering

Cyber Security for Europe

Close working relationship with ECSO WG1 (standardisation/certification/supply chain)

Collaboration with existing cybersecurity communities and ecosystems innovation



Clustering and collaboration activities with SPARTA, ECHO and CONCORDIA and other EC cybersecurity projects

Cooperative efforts and interactions with EU bodies

Results So Far: Governance

Available at cybersec4europe.eu

Cyber Security for Europe

Governance Challenges for European Cybersecurity Policy: Stakeholder Views

- An outline of possible approaches to cybersecurity governance and a comparison against the recent cybersecurity policy initiative proposed by the EU to establish a European Centre and Network of Competence Centres which should be involved in, for example, European cybersecurity funding in the next decade.

Case Pilot for Governance (D6.1)

- A review of the offerings of cybersecurity MOOCs in Europe, consisting of academic, continuous learning and cyber range courses.
- A definition of the quality assurance process for branding CyberSec4Europe MOOCs based on a list of criteria, both generic and cybersecurity specific.

Results So Far: Industry Use Cases

Cyber Security for Europe

Available at cybersec4europe.eu

Requirements Analysis from **Vertical Stakeholders** (D4.1)

- Findings and recommendations from the engagement and consultation through a diverse set of approaches with vertical stakeholders (end users and industrial participants) to collect their requirements, to help define their important problems and to lay the foundation for the roadmap

Requirements Analysis of **Demonstration Cases** (D5.1)

- A comprehensive set of use cases and their requirements, covering the seven representative CyberSec4Europe demonstration cases.
- A thorough analysis with a rich set of functional and non-functional requirements (including security and privacy) that will guide research, technology development, and design, as well as the definition of the research roadmap.

Results So Far: Research

Cyber Security for Europe

Available at cybersec4europe.eu

Common Framework Handbook 1 (D3.1)

- First version of CyberSec4Europe common framework.
- Architecture to encompass all of the proposed CyberSec4Europe functional components
- Common asset template
- First set of assets identified in WP3
- Mapping between the pilots requirements in WP5 and the assets available in WP3

Results So Far: Standards

Cyber Security for Europe

Available at cybersec4europe.eu

Cybersecurity **Standardisation** Plan (D8.1)

- A snapshot of the activities that CyberSec4Europe partners are undertaking in the realm of standardisation and certification preparation.
- While some partners are clearly driving the efforts with SDOs and their committees, others are active participants in contributing content and feedback.

Cybersecurity

13-15 November 2019
Occitanie Regional Gc

3 days of collabc anels:
conversation & n cy

- With the EC, the C for cybersecurity
  French Governme vation
  academia as well a curity governance
  cybersecurity com data sharing for
- Opportunities to he
  explain their result naging identities in
  synergies with the
  other stakeholders pean cybersecurity
- Illustrations of prot
  actions

Cyber Security for Europe

—

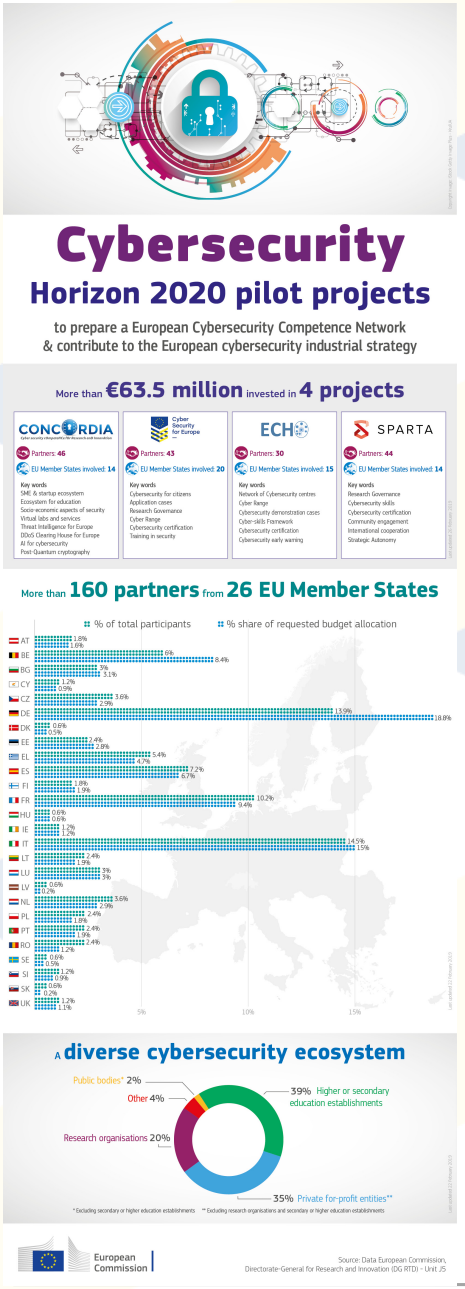
cybersec4europe.eu
@cybersec4Europe
Kai.Rannenberg@m-chair.de

Come and join us!

Cyber Security for Europe


Proposal for a European Cybersecurity Competence Network and Centre | Digital Single Market - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
Proposal for a European Cyber
https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-net
Suchen
Commission and its priorities
Policies, information and services
Log in
Search
European Commission > Strategy > Digital Single Market > Policies >
Digital Single Market
POLICY
Proposal for a European Cybersecurity Competence Network and Centre
Building on the ambitious cybersecurity initiatives announced in 2017, the European Commission proposes as a next step the creation of a Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre to invest in stronger and pioneering cybersecurity capacity in the EU.
About Cybersecurity
Policies
Blog posts
News
Events
Aims of this proposal
The mission of the proposal to establish a European Cybersecurity

Working Together Towards A Common Objective



Cyber Security for Europe

ECHO

CONCORDIA
Cyber security cOmpetenCe FOr Research anD innovAtion

SPARTA

Cyber Competence Network

Cyber Security for Europe

A European network of cybersecurity centres of excellence

Four pilot cybersecurity networks

Cyber Security for Europe

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners **55**
Member States **19**

Keywords
SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography

Cyber Security for Europe

Partners **43**
Member States **20**

Keywords
Cybersecurity for citizens
Application cases
Research governance
Cyber ranges
Cybersecurity certification
Training in security

ECHO

Partners **30**
Member States **15**

Keywords
Network of cybersecurity centers
Cyber range
Cybersecurity demonstration cases
Cyber-skills framework
Cybersecurity certification
Cybersecurity early warning

SPARTA

Partners **44**
Member States **14**

Keywords
Innovation governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic autonomy

Changing Europe' cybersecurity research and innovation landscape

Cyber Security for Europe

Diversity and ethics

Risk acceptance

Horizontal leverage

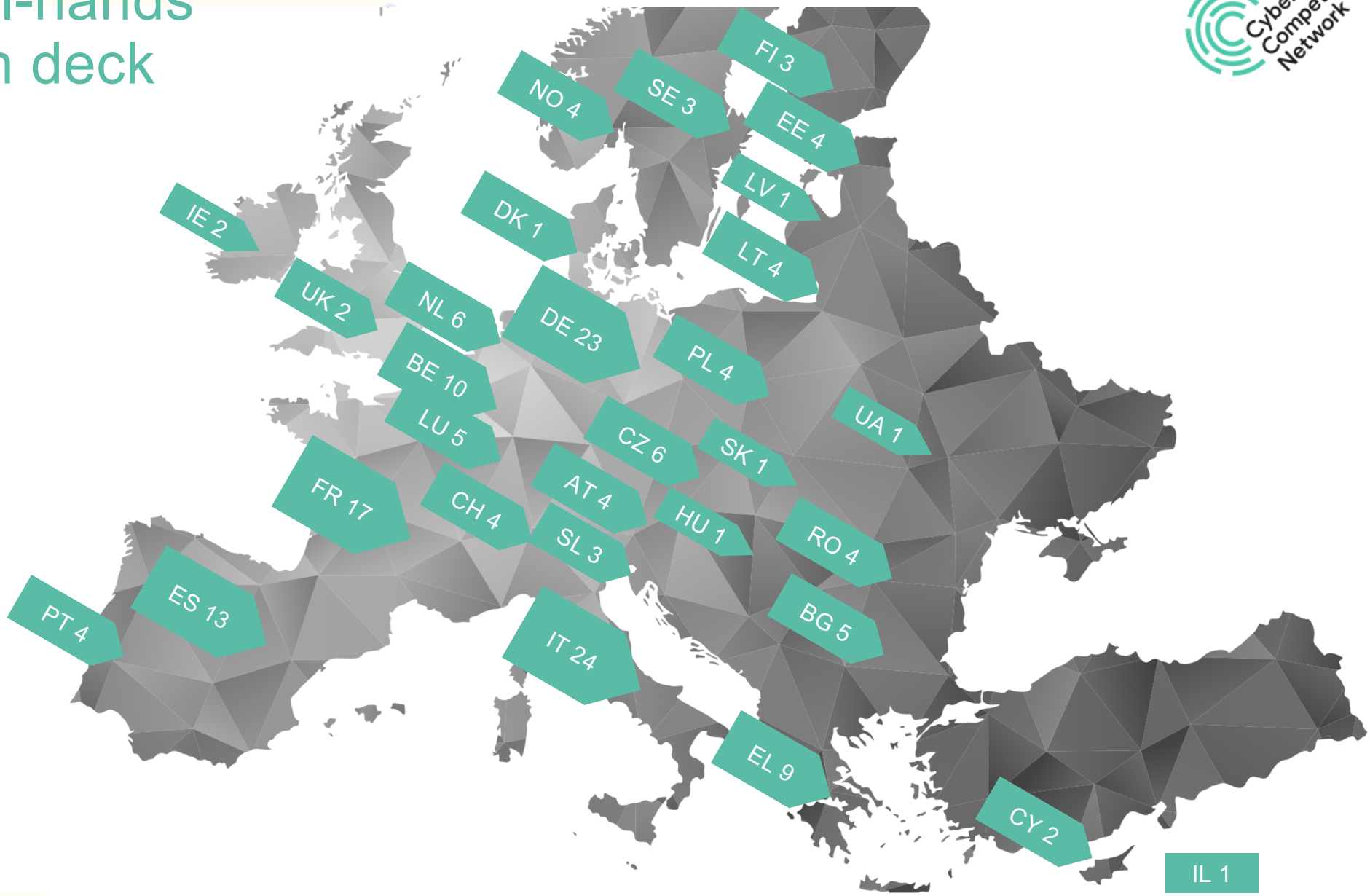
Open leadership

NETWORK OF COMPETENCE CENTRES

Strong academic performers
Insufficient critical mass

Intensified partnerships
World-leading capacities

All-hands on deck



Nurturing synergies

Cyber Security for Europe

Industry engagement

- SME and regional eco-systems
- Cross-domain collaborations

Research and innovation

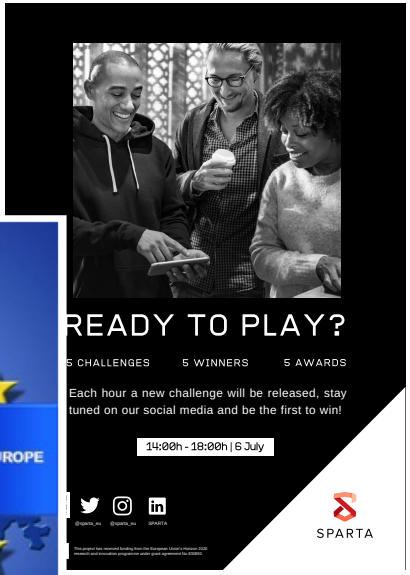
- Ties with ongoing calls and projects
- Consolidation with grassroots initiatives

Inclusive community-building

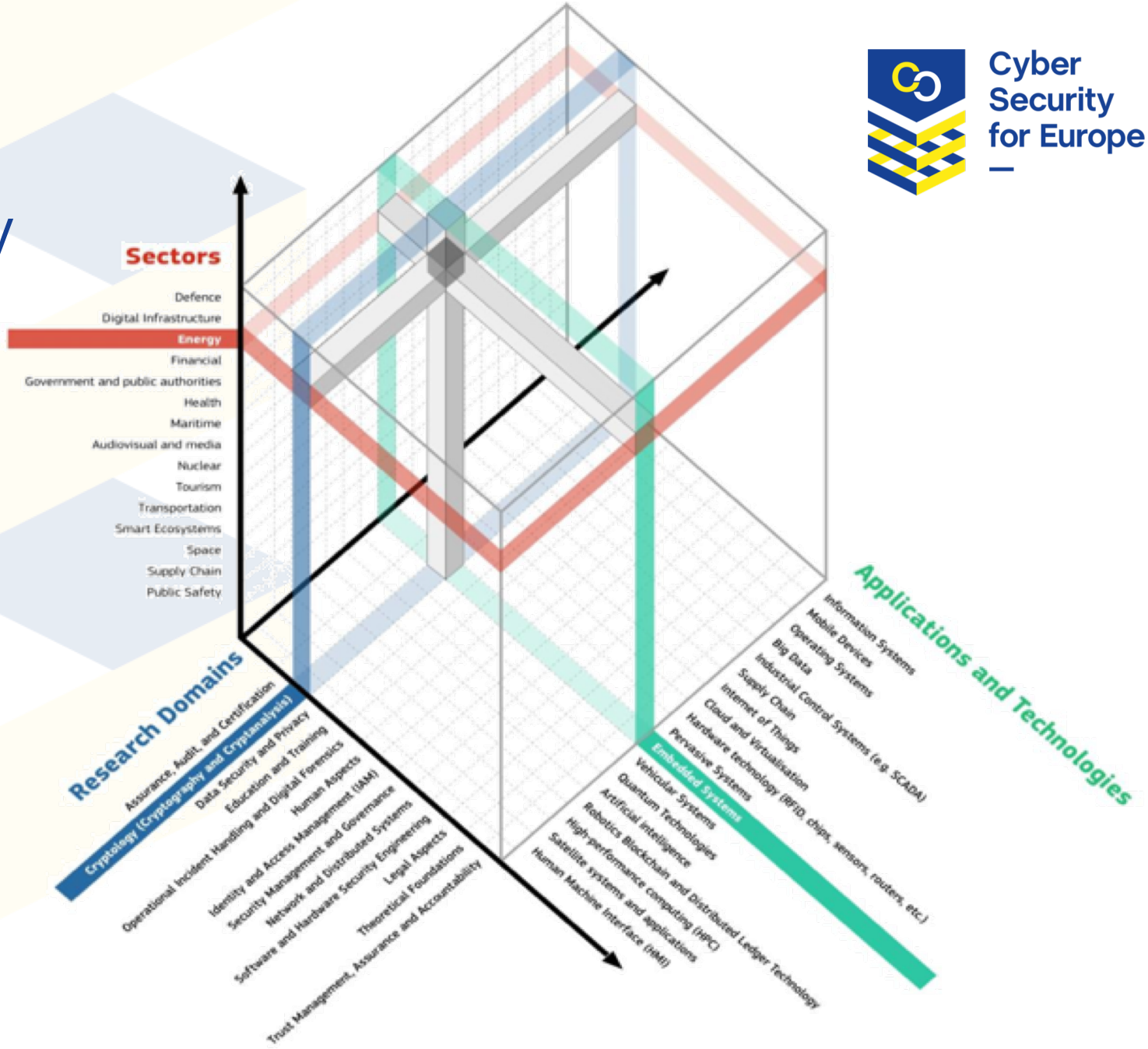
- End-users, pure players, academia, NGOs, hacker spaces, member states
- Service catalogue for various stakeholders
- Extension of network memberships

Capacity-building

- Skills, education, and training curricula
- Platforms: federated cyber ranges



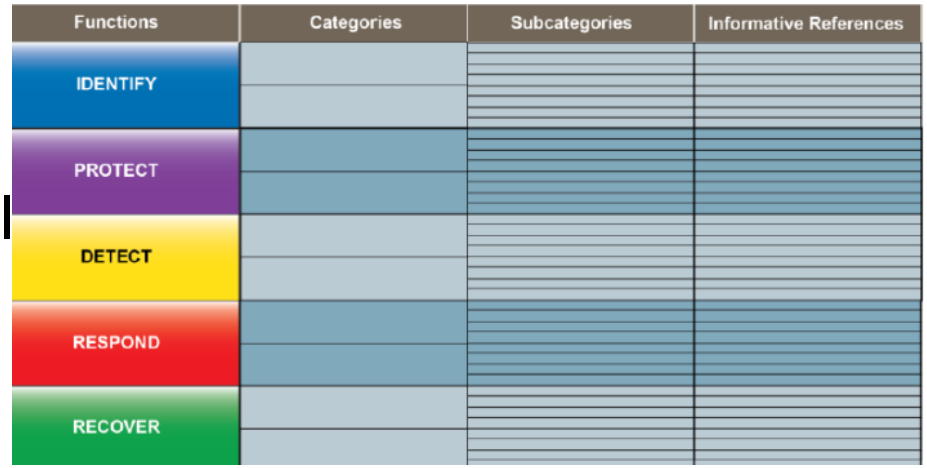
Alignment: testing the EC JRC Taxonomy and Atlas



Research Challenges

Task 3.1:
Common Framework Objective

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders about cybersecurity risk.
- Example NIST



Task 3.2: Research and Integration on Cybersecurity Enablers and underlying Technologies

Cyber Security for Europe

- identity management and authentication solutions over multiple non-federated providers,
- security and privacy services to deploy a basic Edge Computing platform,
- identify technologies to reduce the system attack surface,
- design security mechanisms based on Trusted Execution Environments (TEE) and design a framework for TEE-based cloud data processing,
- IoT Privacy Preserving Middleware Platform,
- improve integrated Security & Privacy by Design approaches,
- decentralized evidence-based authorization and distributed access control using blockchain, addressing applications in IoT
- and investigate approaches that achieve extreme privacy- and integrity-preserving storage and processing of critical data with long-term protection requirements.

T3.3: Software Development Lifecycle - Main challenge(s)

Cyber Security for Europe

Software and security today:

- Software is becoming more complex, more varied, and more heterogenous. Consider e.g. just the high variety of IoT technologies, (standards, protocols, languages).
- Security requirements are becoming more complex, more relative (e.g. quantitative), more dynamic. Consider e.g. the introduction of new regulations or security regulations that depend on “the available technology at the time…” (e.g. GDPR).
- Software considered to be secure today, maybe be not be so tomorrow.

Tackling such complexity, relativity, dynamicity and hetereogeneity demands for:

- Proactive, secure-by-design software development methodologies where security is part of the blueprint of software from day 1 and in all phases of the lifecycle (also after deployment).
- More and better automatization (e.g. tools) to validate, verify, measure, assess security properties, risks and vulnerabilities along the entire cycle of software.

Task 3.4: Security Intelligence Objectives

Cyber Security for Europe

- Define requirements and mechanisms to **share digital evidence** between expert systems
- **Interoperability** through unification of language, format, interface, or trusted intermediaries with respect for privacy, business requirements and national regulations
- Interact with **Threat Intelligence Information Services** for early malware activity detection
- Log/event management, threat detection and security analytics with **privacy-respecting** big data analytics
- Fortify underpinning **security intelligence** in defensive systems

Task 3.5: Adaptive Security

Cyber Security for Europe

- This task will explore the development of flexible security solutions that can adapt security controls in response to security relevant changes, such as new attacks or changes in security requirements.

Objectives

- Security modeling of dynamic systems:
  - we will provide tools and techniques to support elicitation and representation of assets, security requirements and threats, focusing on interconnected systems in various domains (e.g., cloud systems and Internet of Things)
- Scalable architectures for security situation computation and risk assessment
  - These architectures will also support selection and deployment of security controls that could satisfy security requirements and policies, also enabling awareness of the current system status
- Acceptance of adaptive systems:
  - techniques to provide explanations (assurances) about why certain security controls should be adapted

Task 3.6: Usable security

Cyber Security for Europe

- Objectives
  - Recommendations and guidelines on how to incorporate usability requirements in security design, as well as a tool-supported method for assessing the effectiveness factor of usability.
  - Test both usability and security requirements of biometric-based and multimodal user authentication mechanisms and we will design of new behavioural-based user authentication mechanisms including countermeasures and defences against attackers, validated through some of the demonstration cases.
  - The task will also provide users and administrators with awareness mechanisms to support visualisation of the system status and security risks, enabling effective and usable security controls.
- Key challenges include automation and AI to help users on their security and privacy decisions, secure and usable authentication, complexity assessment for new security policies, user informed consent on privacy policies and best ways to visualise security and privacy information

Task 3.7: Regulatory sources for citizen-friendly goals

- Challenges in application of GDPR legislation for users
  - How to provide a GDPR compliant solution, service and/or product?
  - Approach:
    - Check local recommendations and identify issues with implementation
    - Address the issues by developing guidelines with possible checklists
- Challenges in interoperability and cross-border compliance regarding specific regulation and/or legislation (e.g. eIDAS, PSD2)
  - What are the current cross-border compliance and interoperability issues?
  - Approach:
    - Report on interoperability and cross-border compliance issues

Task 3.8:
Conformity, Validation, and Certification

Cyber Security for Europe

- Analyse technologies, system designs and implementations to determine whether the desired security goals are achieved
- Design a security framework for
  - formally defining cyber-physical attack incidents
  - detecting an intrusion at different levels (physical or cyber)
- Provide a resiliency policy
- Generate a forensics analysis
- Based on the work of meta-schema for certification defined by ECSO, the ARMOUR project methodology and the NIST CPS.
- Testing and validation coordinated with WP7 to define a common strategy.

Task 3.9: Continuous Scouting

- monitor the trends to identify innovative approaches
  - the game-changing ones
  - those that could provide a competitive advantage to the early adopters
- impact on the roadmap in WP4
- provide to WP5 demonstration cases food for thoughts and for benchmarking
- will rely on the expertise of the participants, voluntary contributions from researchers all over the world, and cooperation with other cybersecurity competence centres (e.g. ENISA, EuroPol, national cybersecurity agencies, NIST)
- evaluate possibility of automatic text analysis to identify innovations

Task 3.10:
Impact on Society

- Developing a novel security awareness conceptual model, monitoring and enhancement methods with international applicability.

- This task will be devoted to analyze and identify efficient measures and methods for the continuous enhancement of societal security awareness regarding:
  - Up-to-date security solutions
  - Private usage of digital technologies
  - Human aspects of information security
  - Professional practice and competence-development
  - Governance
  - Management and achievement of results
  - Use of serious games for privacy and security awareness rising.

Task 5.1: Open Banking

Cyber Security for Europe

Objective

- To address security issues associated with PSD2 to resolve key inhibitors for service providers and users from moving forward with open banking with confidence.

Use Cases

Focus will be on security issues related to:

- Preventing social engineering and malware attacks
- Certificate verification
- Addressing both GDPR and PSD2
- Screen-scraping and API on-availability
- Security policy compatibility
- Authenticating in circles of trust

Expected Impact

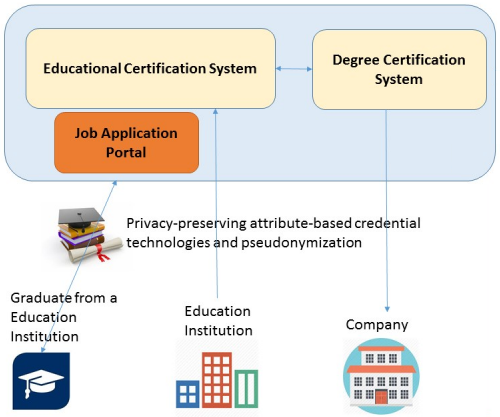
- Guaranteeing a high level of security will enable PSD2 to flourish as envisioned through innovative services, new market players, greater transparency and consumer choice.
- One of the best innovations comes from having third party providers in the payment chain able to access bank accounts and make payments on behalf of customers securely, enabling open banking.
- To securely communicate, third parties and ASPSPs will be able to rely on dedicated APIs, properly configured to reduce the risk of fraud and attack.

Task 5.2:
Supply chain security assurance

Cyber Security for Europe

- Definition of **processes and mechanisms** for the
  - identification of parts and products, including
  - information about their variants and attributes or configuration (**secure binding** of attributes to parts)
- Methods for detection of counterfeits
- Secure Monitoring and tracking for
  - supporting of real-time decision processes
- Tracing, monitoring and synchronization of manufacturing, storage and distribution steps
- Transparency of processes and routes in the production lines;
  - visibility and control over the enterprise partners, suppliers, and customers
- Automatic enforcement of specifications and business rules
- Assurance: Secure tests and compliancy checks for the parts and products
- Accountability: Resolution of conflicts, issues, and responsibilities

T5.3: Privacy Preserving Identity Management



Task Objectives

- Development of a privacy-preserving platform for sharing of personal data
- Enable self-sovereign identity management
- Ease legal compliance by enabling enabling data-minimization
- Secure transactions and counter frauds such as identity theft and impersonation

Challenges

- Guarantee interoperability of privacy-preserving solutions with industry standards
- Trade-off between usability and privacy, both for end-users and software developers
- Ensure legal compliance, in particular taking into account GDPR aspects
- Overcome efficiency limitations of anonymous credential systems
- Enable privacy-preserving identity management “as a service” without single point of failure

Task 5.4:
Incident Reporting Demonstrator

- Research challenges:
  - Technologies for Incident Reporting,
  - A common incident taxonomy taking into account all applicable regulatory requirements,
  - Tools & methodologies for the identification of the impact perimeter of an incident,
  - Tools and methods for the quantification of the potential or real impact of an incident to determine the overall severity of the critical event,
  - Trustworthy information sharing: secure and efficient protocols for information exchange (including Threat Intelligence Sharing),
  - Cybersecurity analytics: big data analysis of cybersecurity information,
  - Advanced Threat Intelligence: application of machine learning and AI to prevent attacks and threats, but also to assist in decision support and improve reaction to incidents,
  - Secure and privacy-preserving efficient information storage.

Task 5.5:
Maritime Transport

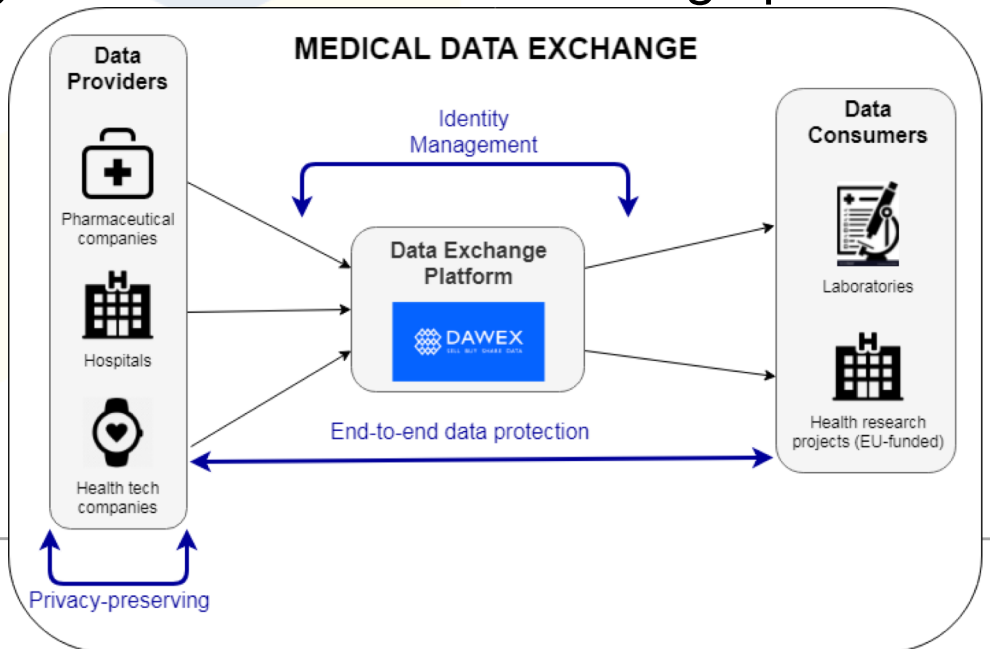
Cyber Security for Europe

Design a threat management system capable of **continuously managing cybersecurity threats against targeted critical cyber infrastructures at the maritime sector**

- Novel **threat modelling** techniques capturing non-obvious security threats
- Advanced **software-hardening** techniques for legacy/IoT systems
- **PKI services** for maritime systems
- Advanced **secure communications** for maritime systems

Task 5.6: Medical Data Exchange
Main challenges

- **To securely protect personal and medical data** avoiding leaks of sensitive information and ensure trustworthiness between the stakeholders (providers and consumers).
- **To guarantee privacy of users' data** by using privacy-preserving techniques, following the EU laws and regulations (e.g., GDPR), and **assuring the right data management**.
- **To improve the Identity Management system** for validating the stakeholders' identities accessing to the medical data exchange platform.



T5.7:
Smart City Demonstrator

Main Goals

- Setup a **consent-based infrastructure for personal data exchange and reuse** in public services, in compliance with GDPR
- Assess **cyber-security risk for public services, particularly with respect to the exposure of civil servants to social engineering techniques**
- Setup an **Open Innovation cycle** to drive city stakeholders from cyber security risks and needs assessment to the identification of the related solutions (i.e. cyber security services) to reduce costs for cyber security services and resources acquisition for PAs

Main Technical Challenge

- Safeguarding **data ownership and control** by allowing transparency about the “who, what, where, when, and why” for any data or information being collected;
- Forcing any personal data "processed" to require **signed consent** by the relevant parties covering its intended use;
- Giving **auditing capability** to monitor the access to any personal information

Novel business model

- Enabling "pooling" delivery model of cyber security services and resources

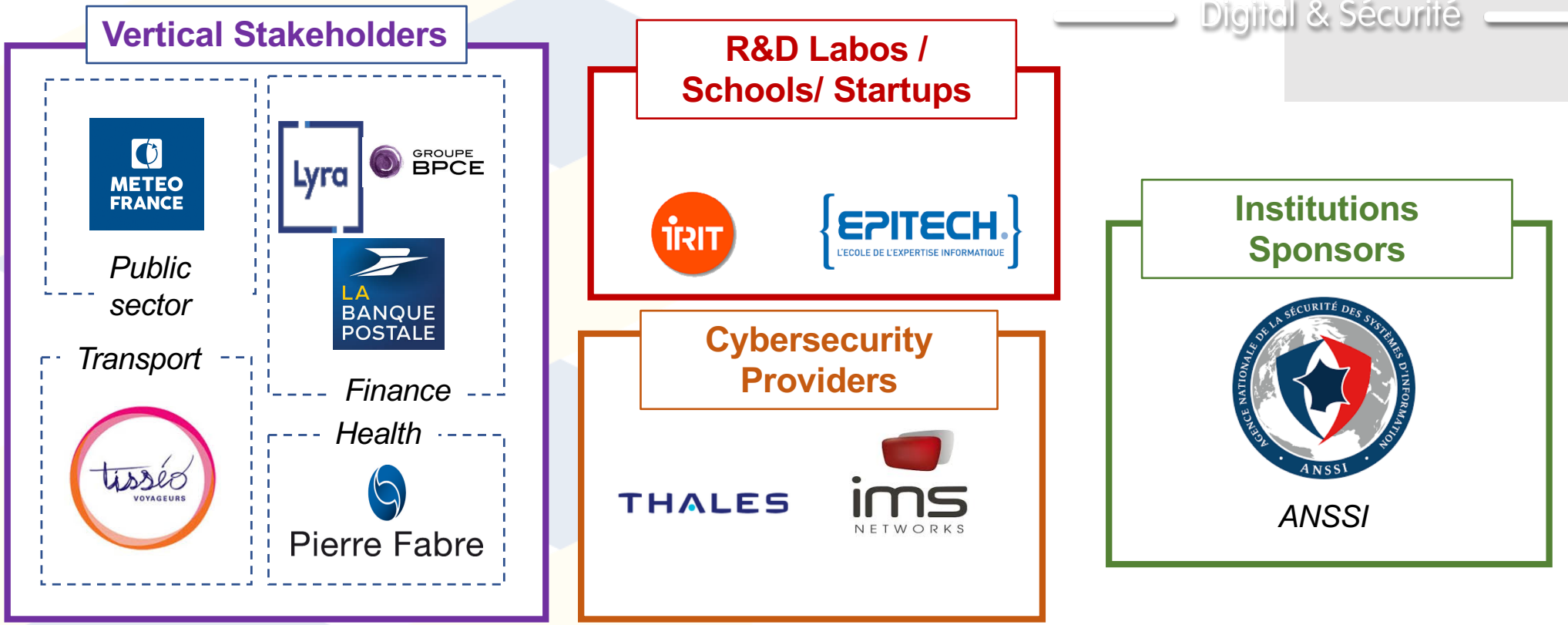
Cybersec4Europe

A regional cybersecurity hub in the making

2019/11/14

Médéric COLLAS, i-BP/BPCE

The Association



- An association **driven by the security vision of its vertical stakeholder members**
- A non-profit organization aiming at designing new innovations & businesses, but not running it
- A small and **agile structure** to **facilitate cooperation** (out of our strong and slow internal processes)
- A **dedicated brand** to ease **communication in the field of security**

Internal Governance Model

Regional Hub Draft Structure

Cyber Security for Europe

Stakeholder security Hub

- → Sharing security challenges in a **trust environment**
- → Identifying and formalizing **cross-sector needs** and **priorities**
- → Engaging innovation providers on **ROI guaranteed collaborations**
- → Providing community with **security4digital expertise** to develop **co-business** actions
- → Créating a dedicated and **common brand used to communicate** on the vision

Leadership: Cyber users
Main challenge: « Share! »

Technology center

- → **Sourcing** and **prototyping** innovative technologies
- → Ensuring **access** and promotion of **european expertises and capabilities**
- → Building and implementing the **training Road Map**
- → Monitoring european **R&I actions**

Leadership: R&D Labos
Main challenge: « think use case!»

Indus. task force

- → **Easing high-valued consortium building** to answer Europes R&I actions
- → Turning innovations into **fully supported solutions**
- → Creating innovative **business and intellectual property sharing models**

Leadership: Cyber providers
Main challenge: «short term is hell ! »

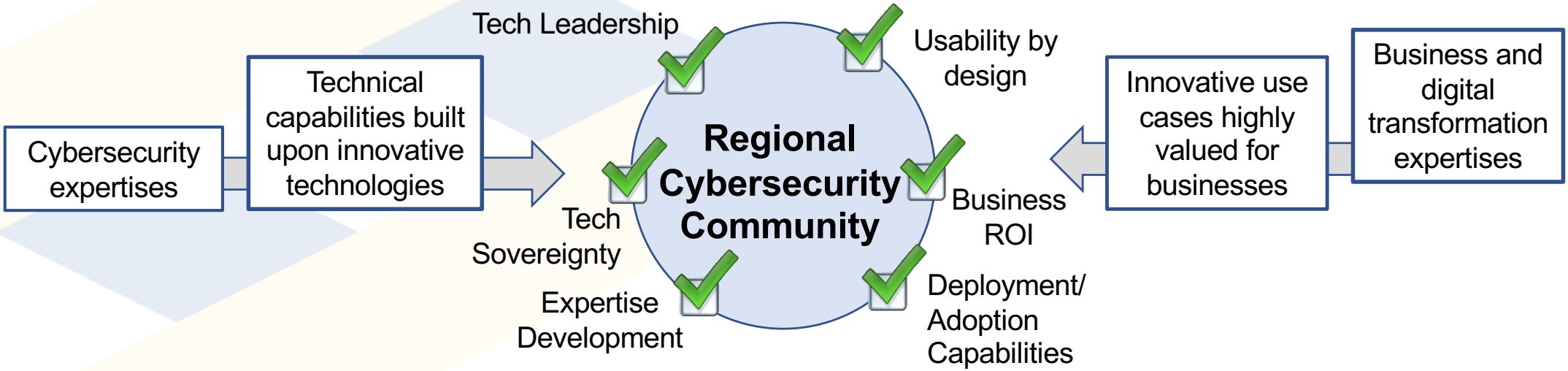
Economic Dev accelerator

- → Sourcing innovative SMEs
- → Providing deployment capabilities
- → Fostering final-user adoption
- → Making innovations usable and affordable for SMEs
- → Developing regional attractivity for talents

Leadership: Regional institution
Main challenge: « Growth and Jobs»

Our Regional Hub's Proposal

Creating a community providing a vision and the necessary expertise to create innovative trustworthy and trusted digital services



Our expectations

Cyber Security for Europe

Vision

Informations

Sharing

Business

Expertise

An Example

Cyber Security for Europe

OBSIDIAN

Open **B**anking **S**ensit**I**ve **D**ata and **I**nformation Sh**A**ring **N**etwork

The Starting Point

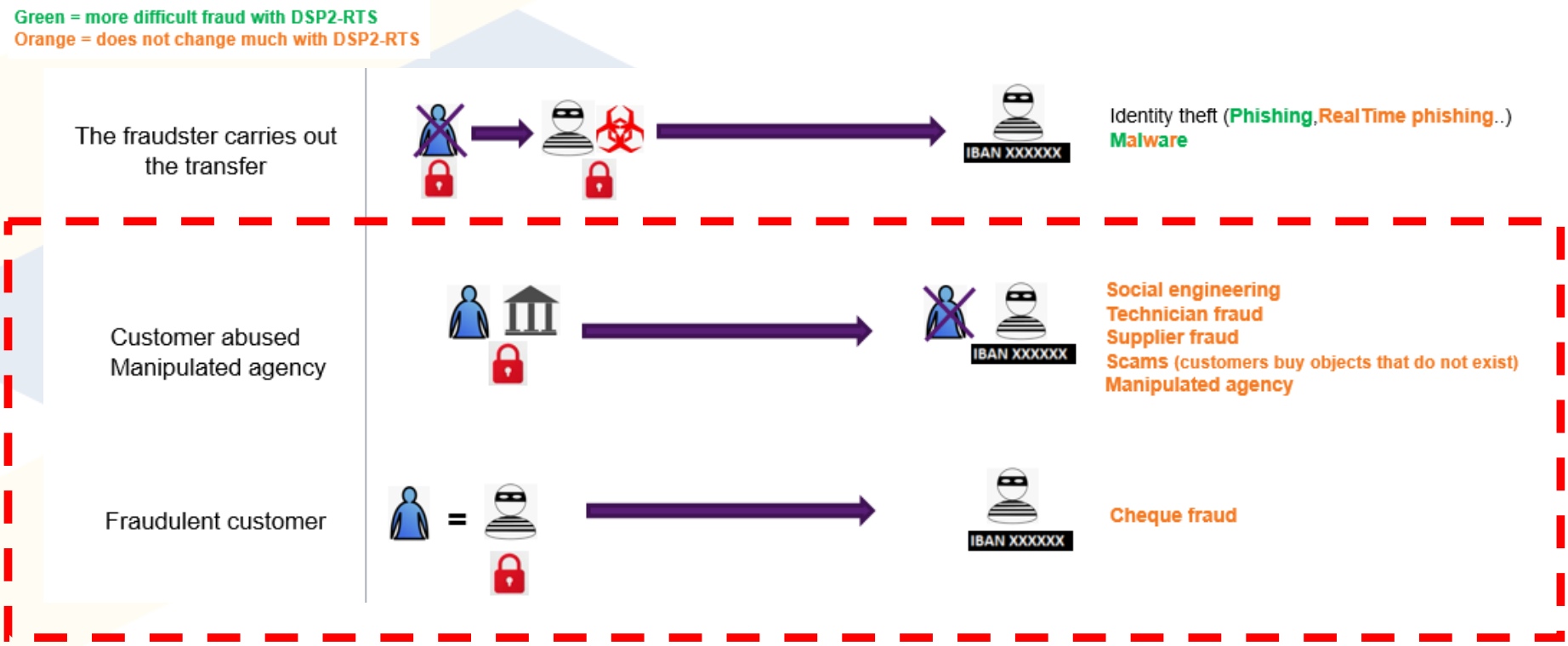
Cyber Security for Europe

37% : increase in cyber attacks in France in 2017

(Payment Services Directives 2 - Regulatory Technical Standards)
https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1555397475903&uri=CELEX:32018R0389

32%: increase in payment fraud in France in 2018 (1,045 milliard €) (*OMSP 07/2019)*
1,2 million de ménages ont été escroqués sur un an, soit une hausse de 144% depuis 2010 pour un Coût moyen de 860 euros par foyer victime

Fraud at the fake savings site is becoming an industrial phenomenon



What about the impact of the digital transformation ?

Cyber Security for Europe

- DSP2 / Open Banking
  - New actors in the payment/transfer chain (PISP)
- Digital-native banks
  - Opening a bank account online
- New usages
  - Instant Payment

The Idea

Cyber Security for Europe

01/02/2014 : The European Payment Council (EPC) validated SEPA regulation

Les 33 pays SEPA

Pays Union Européenne zone euro : Allemagne, Autriche, Belgique, Chypre (partie grecque), Espagne, Estonie, Finlande, France, Grèce, Irlande, Italie, Luxembourg, Malte, Pays-Bas, Portugal, Slovaquie, Slovénie, Croatie

Pays Union Européenne zone non euro : Bulgarie, Danemark, Hongrie, Lettonie, Lituanie, Pologne, République Tchèque, Roumanie, Royaume Uni, Suède

Pays de l'AELE (Association Européenne de Libre Echange) : Islande, Norvège, Liechtenstein et Suisse.

SEPA
SINGLE EURO PAYMENTS AREA

IBAN

How could we share informations about IBANs used in transfer frauds between open banking actors ? (#confidentiality / #anonimity)?

From the Idea to the building of the solution

Cyber Security for Europe

« We have the same fraud problem »
« If we don't find a solution to share these informations, I?M or ThreatM????X will find it for us (#sovereignity) »

« Sharing IBANs is possible, usefull to fight against fraud, we can share our experience and our fraud informations »

Sharing

« Do you need anonimity and confidentiality ? We are studying technologies that can fit your needs»

« such a network and/or their underlying technologies could help in other sectors (supply chain / Medical data exchange»

Next Step

Cyber Security for Europe

- Working with all our local/european partner to implement this network
- Turning this topic into a concrete opportunity to test and the CS4E deliverables, for exemple the WP2 deliverables
- Turning the future OBSIDIAN network into an european reusable asset for other sectors and other use cases

Thank You !

Mederic.collas@i-bp.fr

cyberwatching.eu
The European watch on cybersecurity & privacy

Visualising the EC H2020 Cybersecurity (Research) landscape

14 November 2019

Cybersec4Europe, Toulouse

cyberwatching.eu
The European watch on cybersecurity & privacy

The European watch on Cybersecurity and Privacy

Making sense of the landscape

ENGAGEMENT

+175 EU projects

Map, cluster and collaborate
EU Research & Innovation

EU Project Hub - Europe's only collaboration platform for EU-funded cybersecurity and privacy projects. Concertation and Cluster workshops to foster collaboration and market readiness of results.

+50 marketplace services

Promote EU innovation to the EU market

Marketplace - A curated Marketplace of R&I results and services offered by providers across Europe. Market readiness training for projects and SMEs. Free tools, guides and workshops for SMEs across the EU.

+5 resources for policy makers

Recommend policy and standards best practices

Policy, standards and certification - Recommendations reports: standards and certification, GDPR and emerging technologies. Technology radar including €560 million worth of funded projects.

Coordination & Support Action May 2017 – April 2021

Trust-IT Services Communicating ICT to markets · University of Oxford · ICT Legal Consulting Balboni Bolognini & Partners · Conceptivity 360 Security · European Digital SME Alliance · aeiciberseguridad · AON

cyberwatching.eu
The European watch on cybersecurity & privacy

EU H2020 Cybersecurity research

180 projects

Spanning 15 years
(Feb 2008 – Feb 2023)

€765M total budget

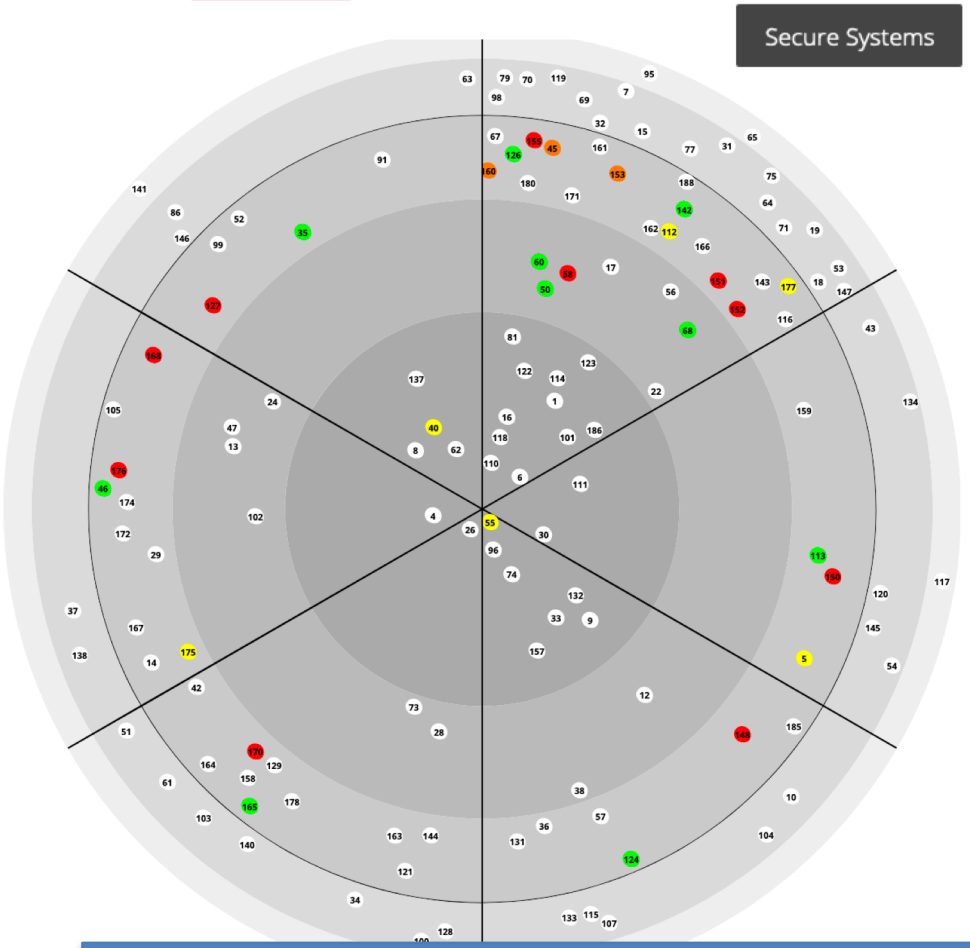
How can you get a bigger picture and then zoom in?
How can you get updated information?

CYBERWATCHING RADAR DATA - SPRING 2019

Secure Systems | Verification & Assurance | Operational Risk | Identity & Privacy | Cybersecurity Governance | Human Aspects

Choose a sheet to populate radar

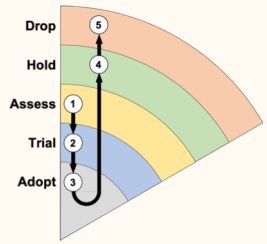
Spring 2019 Autumn 2018



6 CS&P R&I Taxonomy categories

177 project mapped

5 Rings
Project lifecycle
progress

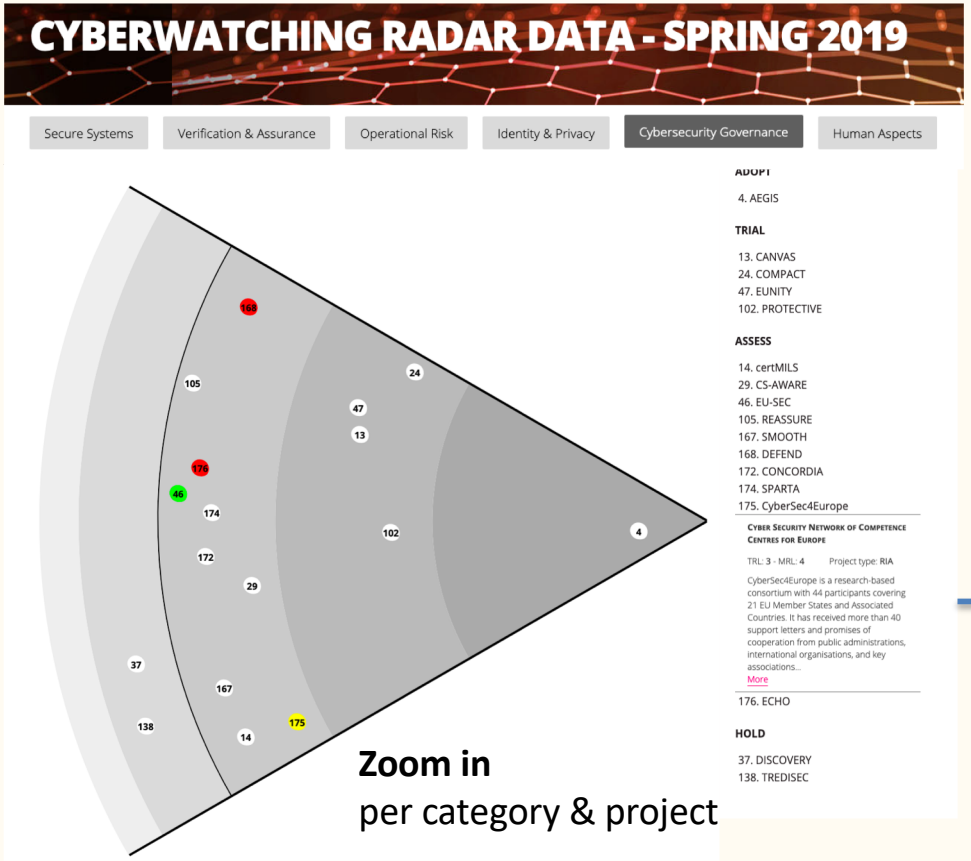


5-colour spectrum
Project outputs
maturity (MTRL)

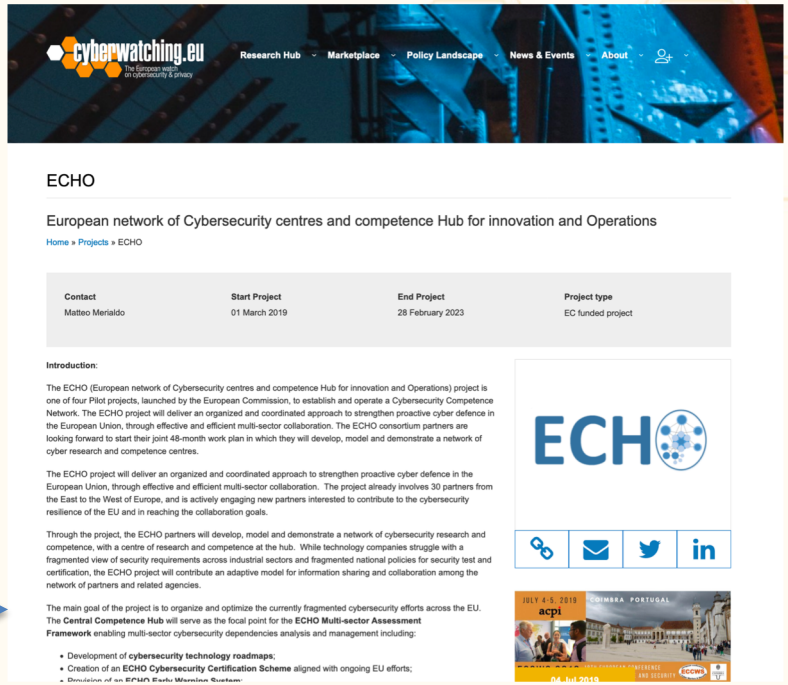
Red	indicates SLOWEST relative progress.
Orange	indicates SLOW relative progress.
Yellow	indicates MEDIAN relative progress.
Light-green	indicates FAST relative progress.
Lime	indicates FASTEST relative progress.
White	means no information available.

Useful landscaping tool for both EC and projects themselves

EU Project Radar



Zoom in
per category & project



Up-to-date info & RFI with projects
Up to the date information on the project via project hub – cyberwatching.eu

Projects manage their own profiles with updated info
Basis for future clustering and engagement activities with CS&P projects

cyberwatching.eu
The European watch on cybersecurity & privacy

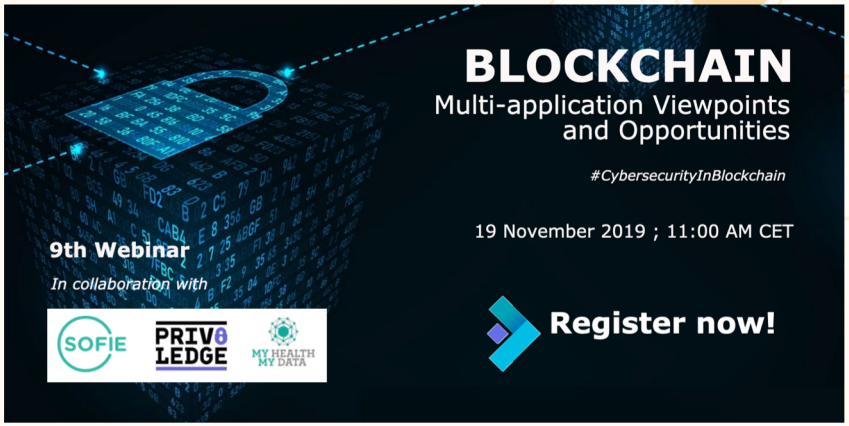
Looking ahead…

- 3rd radar iteration – April 2020
  - New visualisation options: Applications & technologies, Vertical sectors
  - New UI and improved UX
- Establish (light-weight) clusters of projects
  - (inter-)national policy, certification, inter-governmental collaboration
  - securing operations of existing systems (e.g. intrusion detection, forensics, etc.)
  - Privacy & GDPR
- Engage and support clusters
  - Cluster specific tech & synergies workshops
  - To promote practical guidance/training to improve MRL
  - To promote IPR best practices / guidance
  - To facilitate commercialization of partial results from projects

Thank-you

Nicholas Ferguson, Trust-IT Services

n.ferguson@trust-itservices.com



cyberwatching.eu
The European watch on cybersecurity & privacy

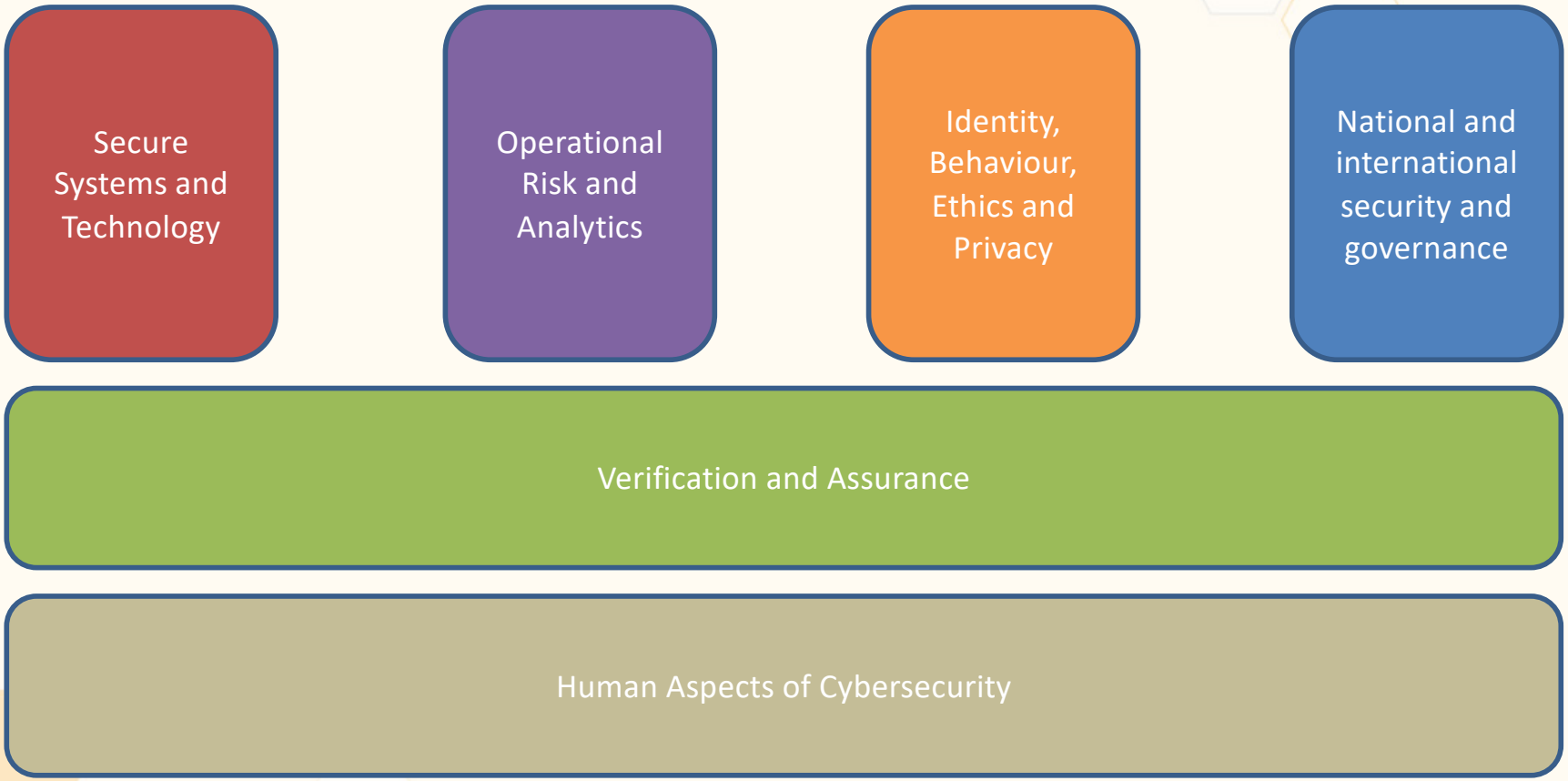
www.cyberwatching.eu
@cyberwatching.eu
info@cyberwatching.eu

Trust-IT Services Communicating ICT to markets
UNIVERSITY OF OXFORD
ICT LEGAL CONSULTING Balboni Bolognini & Partners
CONCEPTIVITY 360 SECURITY
European Digital SME Alliance
aeiciberseguridad
AON

EXTRAS

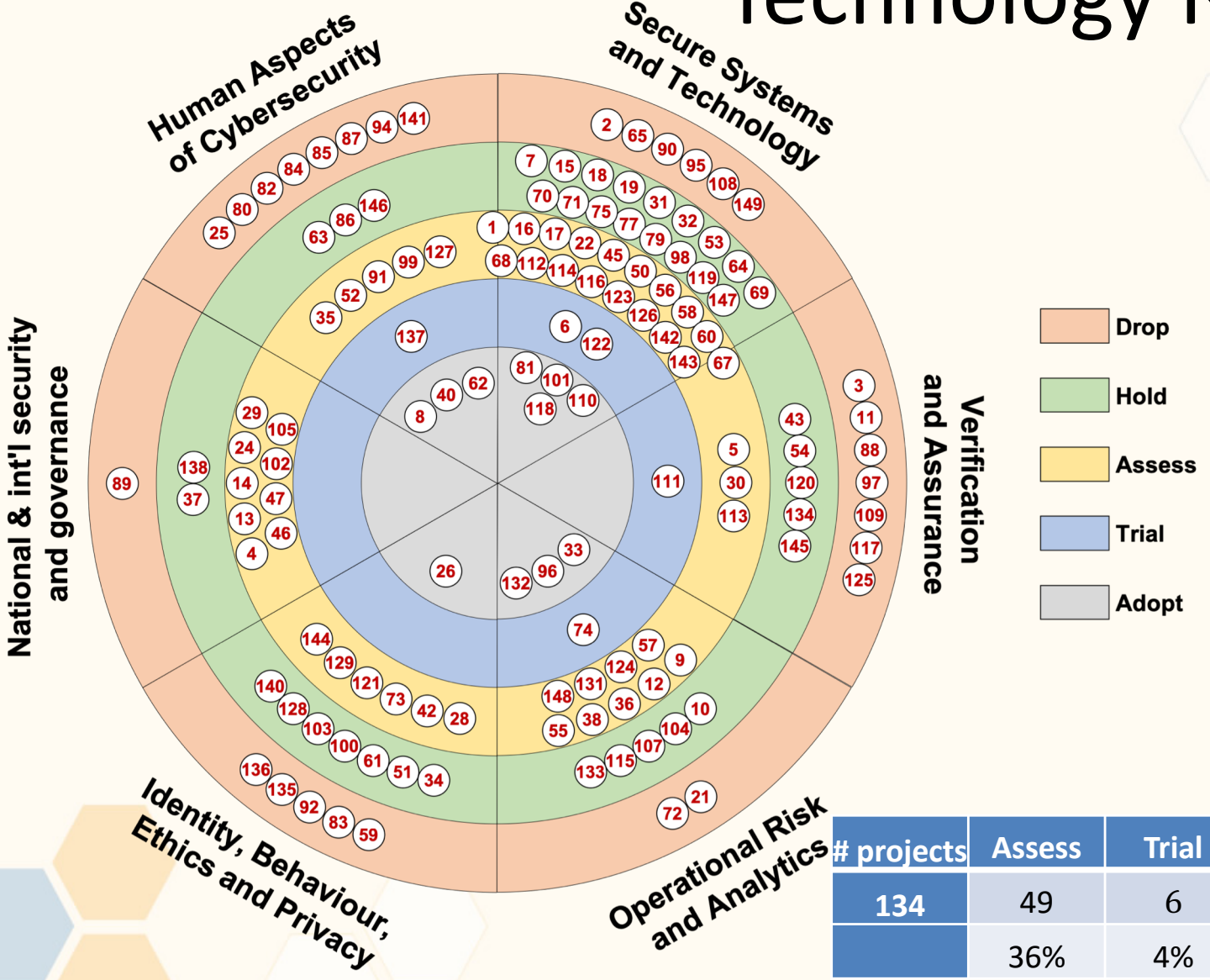
cyberwatching.eu
The European watch on cybersecurity & privacy

Cyberwatching.eu cybersecurity & privacy taxonomy



cyberwatching.eu
The European watch on cybersecurity & privacy

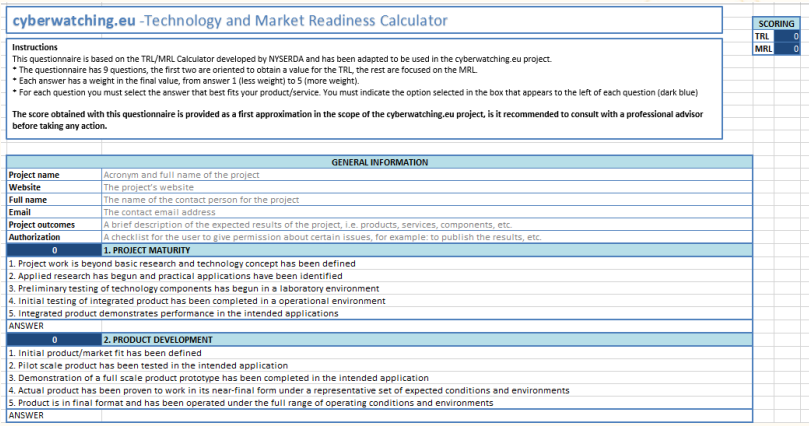
Autumn 2018 Technology Radar



# projects	Assess	Trial	Adopt	Hold	Drop
134	49	6	11	39	29
	36%	4%	8%	29%	21%

MTRL self-assessment

- Online self-assessment
- Results from 29 projects analysed



cyberwatching.eu -Technology and Market Readiness Calculator

SCORING
TRL 0
MRL 0

Instructions
This questionnaire is based on the TRL/MRL Calculator developed by NYSERDA and has been adapted to be used in the cyberwatching.eu project.
* The questionnaire has 9 questions, the first two are oriented to obtain a value for the TRL, the rest are focused on the MRL.
* Each answer has a weight in the final value, from answer 1 (less weight) to 5 (more weight).
* For each question you must select the answer that best fits your product/service. You must indicate the option selected in the box that appears to the left of each question (dark blue)

The score obtained with this questionnaire is provided as a first approximation in the scope of the cyberwatching.eu project, is it recommended to consult with a professional advisor before taking any action.

GENERAL INFORMATION	
Project name	Acronym and full name of the project
Website	The project's website
Full name	The name of the contact person for the project
Email	The contact email address
Project outcomes	A brief description of the expected results of the project, i.e. products, services, components, etc.
Authorization	A checklist for the user to give permission about certain issues, for example: to publish the results, etc.

0	1. PROJECT MATURITY
1. Project work is beyond basic research and technology concept has been defined	
2. Applied research has begun and practical applications have been identified	
3. Preliminary testing of technology components has begun in a laboratory environment	
4. Initial testing of integrated product has been completed in a operational environment	
5. Integrated product demonstrates performance in the intended applications	
ANSWER	

0	2. PRODUCT DEVELOPMENT
1. Initial product/market fit has been defined	
2. Pilot scale product has been tested in the intended application	
3. Demonstration of a full scale product prototype has been completed in the intended application	
4. Actual product has been proven to work in its near-final form under a representative set of expected conditions and environments	
5. Product is in final format and has been operated under the full range of operating conditions and environments	
ANSWER	

TRL questions

- Project Maturity
- Product Development

MRL questions

- Product definition/design
- Competitive landscape
- Team
- Documentation
- IPR management
- Go to market
- Manufacturing/supply chain

Main results

1. Most projects with TRL 6-7 have MRL 4-5, even when they are finishing
   → Clear need of improving **marketing capabilities**
2. Weakest point on marketing: Manufacturing / Supply chain
3. Strongest point on marketing: Team
4. Strong interest in support from cyberwatching.eu

Panel 3: European Cybersecurity Governance

Moderator: *Afonso Ferreira*

CNRS-IRIT

Toulouse, FR

Panel's subject

Proposal by the EC in Sept 2018 to establish a

Network of Cybersecurity Competence Centres

and a new

European Cybersecurity Industrial, Technology and Research Competence Centre

Basic Structures

- A European Cybersecurity Industrial, Technology and Research Competence Centre (in Brussels?)
- One National Cybersecurity Competence Centre per Member State
- A Network of such Centres, tightly connected to the central Centre
- A “Community”
  - ‘Regulated’ by its National Centre
  - All relevant stakeholders
  - May or may not decide to establish their own “centres of competence”

This Panel - Governance

- Of the “Community”
- In particular of Community competence centres
  - Let’s call them Cybersecurity Expertise Hubs for the sake of clarity

Topics include challenges and recommendations of establishing and implementing Governance for the community expertise hubs, eg:

- Accreditation
- Composition
- Membership (National / Non-National; EU / non-EU)
- IPR
- Connections with other (cross-border) hubs
- Connections with the National Competence Centre and their network
- Activities
- Added-value
- Financing
- Other

High Level Panellists

- Ana Ayerbe – Director of the IT Competitiveness area, Tecnalia, Spain
- Malek Benzekri – Professor, Université Paul Sabatier & IRIT, Toulouse & Leading efforts for Toulouse Cyber Hub for Regional Expertise
- Médéric Collas – Informatique Banques Populaires, Toulouse & Délégué Général of Ocssimore, incubator of the Toulouse Cyber Hub for Regional Expertise
- Miguel González-Sancho – Head of Unit Cybersecurity Technology & Capacity Building, DG CONNECT
- Nicole Harris – Head of Trust and Identity Operations, GÉANT, Amsterdam
- Antonio Skarmeta – Professor, University of Murcia & WP Leader at CyberSec4Europe pilot

Format

- Scene setting
- Opening statement by 3 panellists
- 5’ of Q&A with audience
- Opening statement by the remaining 3 panellists
- 5’ of Q&A with audience
- The case for Recommendations
- Main recommendations from the panellists
- More Q&A
- Final message from each of the panellists
- Closing

Cyber Security for Europe

CyberSec4Europe: Concertation Meeting Toulouse

Panel: European Cybersecurity Governance

Antonio Skarmeta
Universidad de Murcia

Ensuring the competitiveness of Europe
Enabling European economic growth
while protecting European society

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Challenges (no CS4E position)

Cyber Security for Europe

Implementation

- The top-down approach qute defined up to MS level, the issue it is what it is happening at the community level. **Need of a bottom-up approach from regional/sectorial competence centers.**
- **No one model** possible, there is a need to consider different possible approaches in the design of competence center;
- **Stakeholders need to be as diverse as possible**, we need to allow NGO, user community (i.e open source) and not just institutional;
- **Engage of SMEs**, there should be incentives, capacity building, user experience approach, **bootsting startups**
- **Regional hubs linked to national centers** and to the EU Centres within the network by a variety of tasks, advice and recommendations

Operational

- **Focus versus more broad vision** in some setting maybe difficult to maintain the interest if there is quiet diverse research challenges;
- Importance on a serious Involvement of **Users and civil society**
- Important to have procedures to define the membership, **reduce only observers partners**;
- Regional hubs of excellence as center of networks both regionally and **in combination with other regional hubs**

Open issues

- How **the link between the (accredited) community (network) and the EU Centre** on top or the national centers will happen
- How the **funding of the regional/sectorial could happen**.
- Interconnection on competence centers –> **community formalization;** possible federation of centers that could represent the community

Cyber
Security
for Europe

skarmeta@um.es

Panel 3: European Cybersecurity Governance

Ana Ayerbe

Manager of TECNALIA TRUSTECH Business Area where she works in trying to create trust in the digital and hyperconnected world developing technology to reinforce the digital immunological system of companies and society.

Enthusiastic of new technologies like the Internet of Things, Distributed Ledgers, HPC and Artificial Intelligence and the challenges and opportunities they offer related to Cybersecurity.

Member of the Board of Directors, Strategic Committee and Partnership Board of ECSO, member of the Strategic Board and Board of Director of EOS, RENIC Board of Directors and Permanent Committee of the Basque Cybersecurity Center (BCSC).

In 2019 she has also taken part in the Expert Committee for the elaboration of the Spanish Cybersecurity National Strategy.

Mentor of the INSPIRA STEAM project that tries to stimulate scientific and technological vocations among girls and member of the Council of the WOMEN4CYBER initiative.

tecnalia Inspiring Business

TECNALIA
RESEARCH AND TECHNOLOGICAL DEVELOPMENT

SINCE 2011
TECNALIA is a benchmark Research and Technological Development Centre in Europe

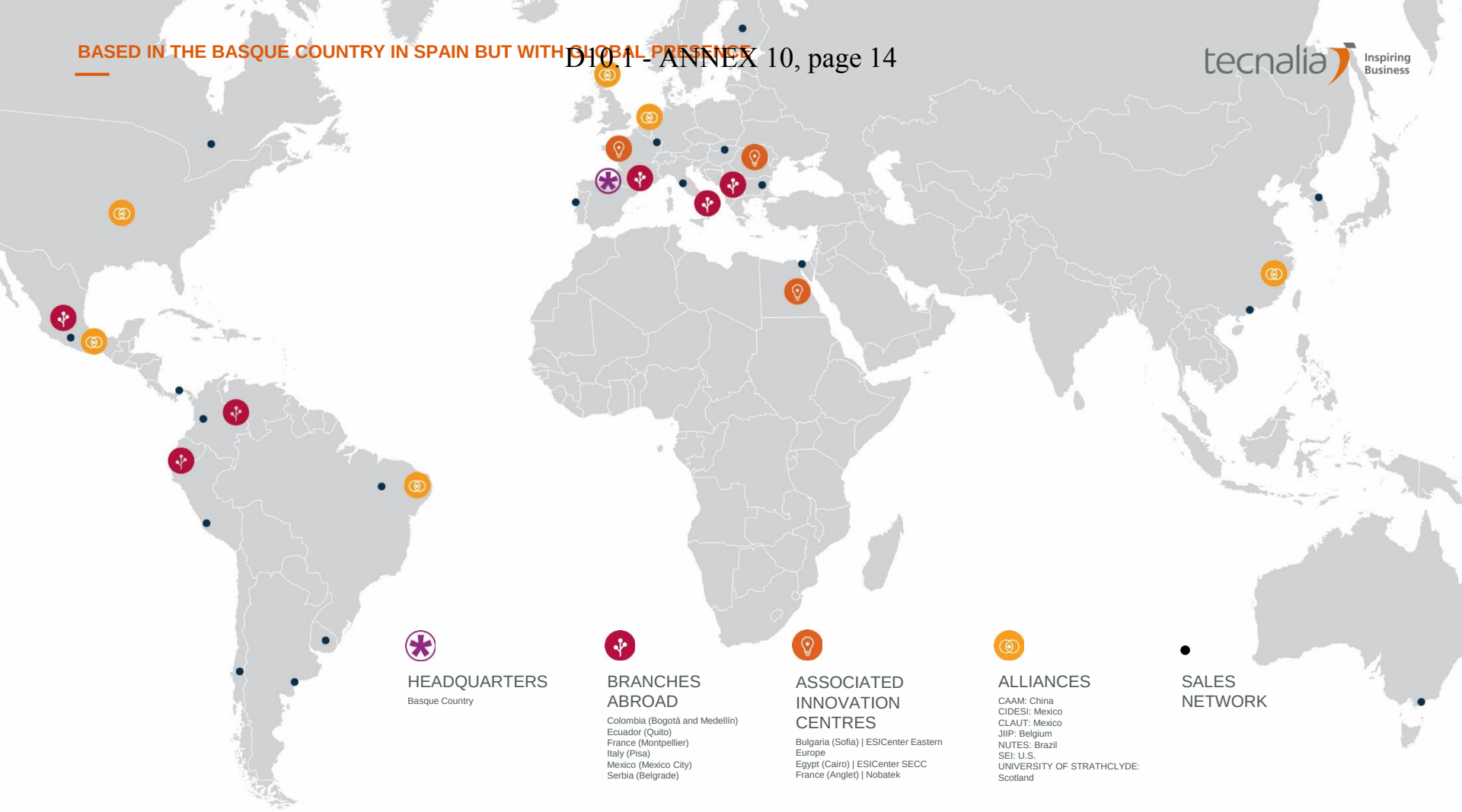
MULTISECTORAL
MULTI-TECHNOLOGY

A MODEL
ANTICIPATING THE FUTURE

A COMBINATION OF TECHNOLOGY, TENACITY, EFFICIENCY, COURAGE AND IMAGINATION

BASED IN THE BASQUE COUNTRY IN SPAIN BUT WITH GLOBAL PRESENCE

tecnalia Inspiring Business



HEADQUARTERS
Basque Country

BRANCHES ABROAD
Colombia (Bogotá and Medellín)
Ecuador (Quito)
France (Montpellier)
Italy (Pisa)
Mexico (Mexico City)
Serbia (Belgrade)

ASSOCIATED INNOVATION CENTRES
Bulgaria (Sofia) | ESICenter Eastern Europe
Egypt (Cairo) | ESICenter SECC
France (Anglet) | Nobatek

ALLIANCES
CAAM: China
CIDESI: Mexico
CLAUT: Mexico
JIIP: Belgium
NUTES: Brazil
SEI: U.S.
UNIVERSITY OF STRATHCLYDE: Scotland

SALES NETWORK

BASED IN THE BASQUE COUNTRY IN SPAIN BUT WITH GLOBAL PRESENCE

Very rich ecosystem with some characteristics:

- 2 million population
- Industry represents 24,1% GDP
- Own tax system
- High degree of autonomy in policy areas like education, industry, culture, health, law enforcement and social services.

Ecuador (Quito)
France (Montpellier)
Italy (Pisa)
Mexico (Mexico City)
Serbia (Belgrade)

Bulgaria (Sofia) | ESICenter Eastern Europe
Egypt (Cairo) | ESICenter SECC
France (Anglet) | Nobatek

ALLIANCES

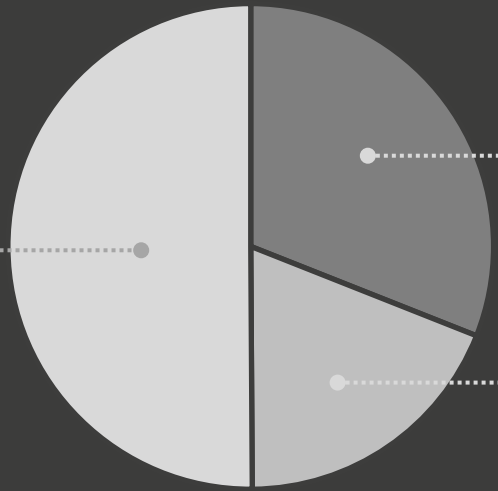
CAAM: China
CIDESI: Mexico
CLAUT: Mexico
JIIP: Belgium
NUTES: Brazil
SEI: U.S.
UNIVERSITY OF STRATHCLYDE: Scotland

SALES NETWORK

BALANCE OF ACTIVITIES AND THEIR FUNDING

INCOME

110 MILLION EUROS



32.3%
Competitive public funding

18.7%
Non-competitive public funding

49.1%
Private financing and others

BALANCE OF ACTIVITIES AND THEIR FUNDING

INCOME

h1. Publicaciones científicas indexadas – Indexed scientific publications

h2. Publicaciones científicas en primer cuartil (Q1) – Scientific publicaiton in the first quartil (Q1)

h3. Solicitud de patentes EPO y PCT – Patents enquiries EPO and PCT

h4. Ingresos por licencias y patentes (K€) – Incomes from licenses and patents (K€)

h6. Facturación procedente de NEBTs (k€) – Invoices coming from NEBTs (K€)

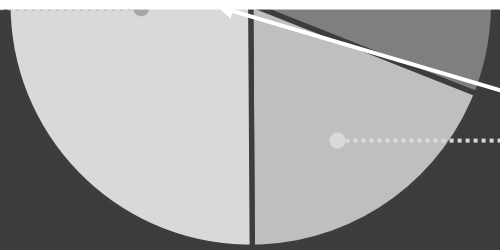
i1. % financiación privada en la CAPV - % private incomes in the Basque Country

i2. % financiación privada total - % total private incomes

I6. Co-invención de patentes – Patents co-invention

I7. % de financiación pública internacional - % of international public income

Private financing
and others



18.7%

Non-competitive
public funding

Scope: Functions

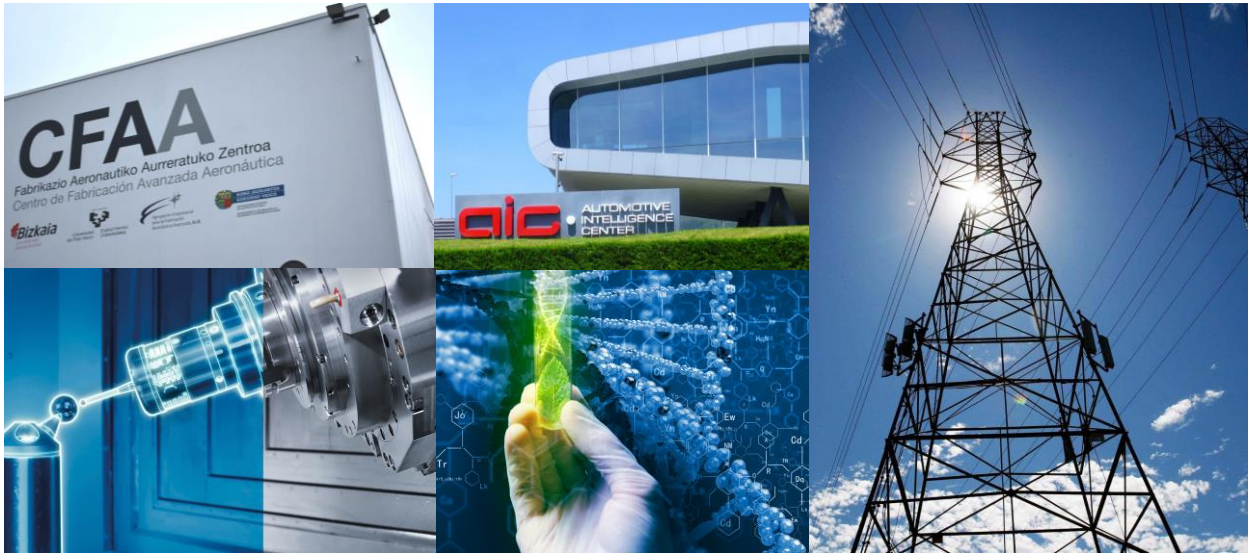
D10.1 - ANNEX 10, page 18

- Development
- Education
- Security / Police
- eGovernment
- Investment
- Research network
- Entrepreneurship

The Basque Cybersecurity Centre was created in October 2017 within the Basque Agency for Business Development (SPRI)

Aligned to the Regional Industry Strategy

- ✓ Research & Innovation
- ✓ Entrepreneurship
- ✓ Tractor companies
- ✓ Competitiveness
- ✓ Infrastructure



RIS3 - Our number one priority is the Basque industry.

Economic Development – Education X.0

Dual vocational training programmes adapted to the specificities of the local industry.

Post-degree Cybersecurity Programme.

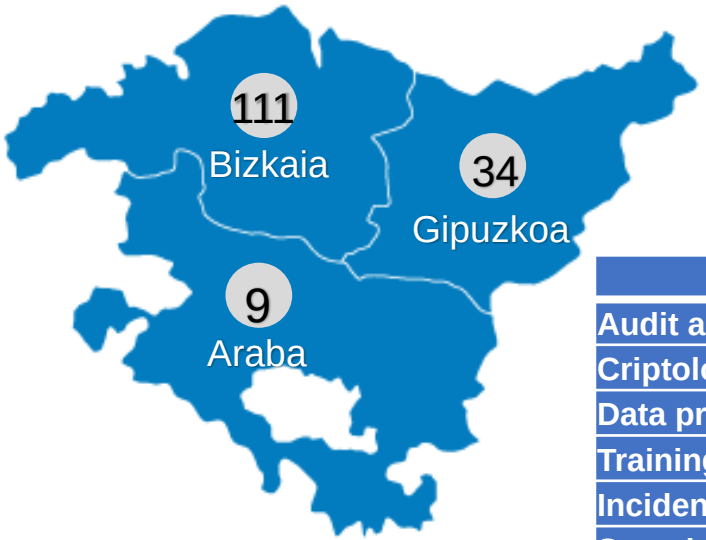
Recycling and reorienting

Awareness raising in the usage of digital devices.

Talent search and attraction.

Professionals of today and citizens of the future.

Economic Development – R&D&I



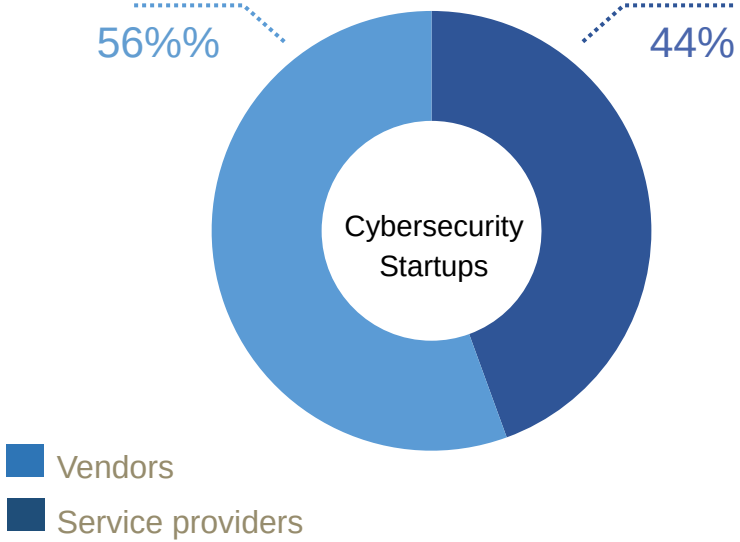
More than 150 researchers working in 125 R&D&I projects in Cybersecurity coordinated by the Basque Cybersecurity Centre.

More than 200 publications in the last 5 years.

Areas of expertise	Publications
Audit and certification	13
Criptology	11
Data protection and privacy	28
Training and education	5
Incident management and digital forensics	5
Security governance and management	11
Distributed networks and systems	89
Software and hardware security engineering	40
Security measures	2
Technology and legal aspects	2
Security analysis and design theoretical foundations	3

Technological transference is the real challenge.

Economic Development – Entrepreneurs profile



Entrepreneurship is a key innovation driver.

Economic Development – Business friendly

The Basque Country has been recognized – among 171 Agencies worldwide – in the **Strategy Awards 2018 by the Financial Times** (also attached "fDi Strategy Awards 2018") in different categories:

- First-Prize winner in "Aftercare" category. This category is about the relationship of the Government with companies (foreign capital) established in the Region.
- First-Prize winner in "Start-ups and SME support" category. Because of the Acceleration Program **Bind 4.0**
- Second-prize Winner in "Incentives" category. Incentives to Research, Development and Innovation have been the most remarkable.
- Second-prize Winner in "Project of major interest by an Agency of Investment Attraction". **VIRALGEN project.**

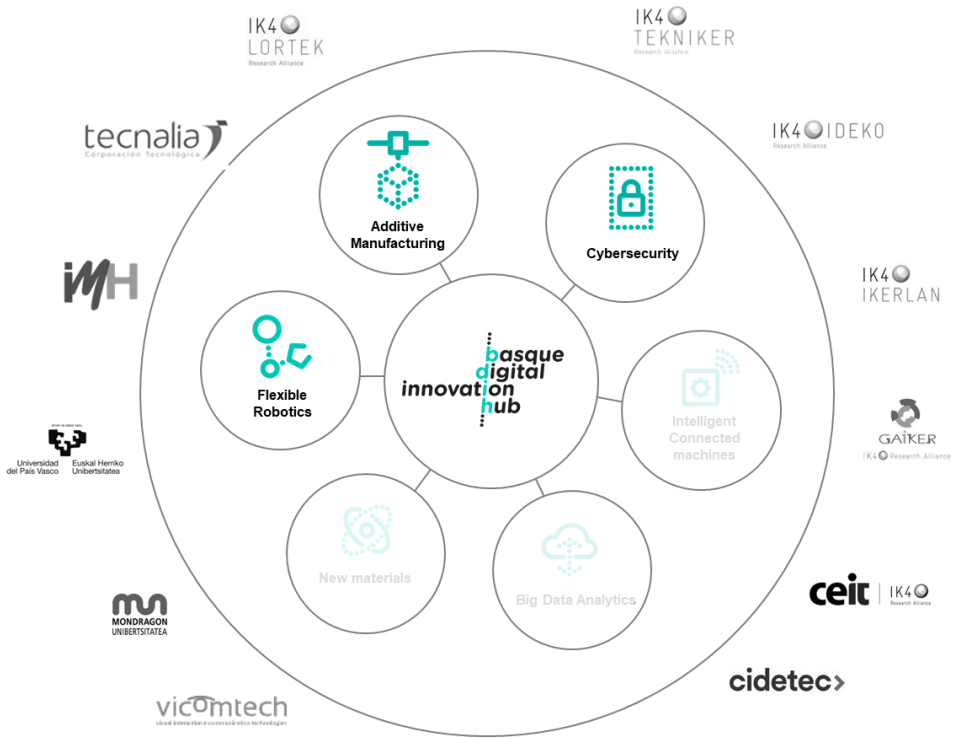
Ready for Innovation

BASQUE CYBERSECURITY CENTRE

- Basque Digital Innovation Hub
http://www.spri.eus/es/basque-industry/basque-digital-innovation-hub/

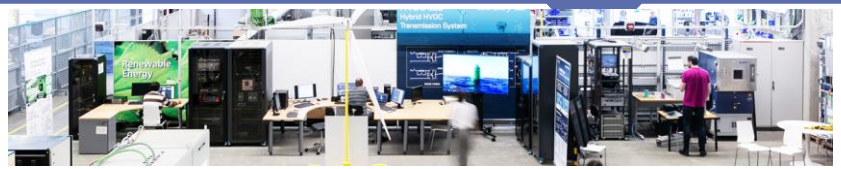
- Part of the Digital Innovation Hubs Catalog created by the EC
http://s3platform.jrc.ec.europa.eu/digital-innovation-hubs-catalogue

- An opportunity to foster interregional collaborative projects and to create an European network of DIHs.



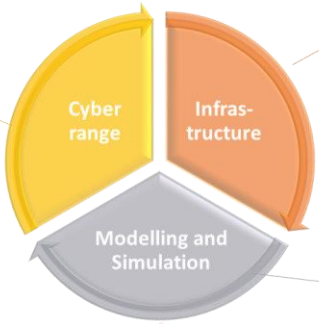
Focused

BASQUE CYBERSECURITY CENTRE



basque digital innovation hub

Node TECNALIA-PTA
Cyber range for training as well as for research



No vendor lock-in
Customizable network
VLANs
Virtualization

Modelling and simulation of different real-world scenarios (i.e., ICS)

rnli_
Red Nacional de Laboratorios Industriales

Node VICOMTECH
Focused on: Industry 4.0; Blockchain

Node TECNALIA-PTB
Focused on: Smart-Grid; Automotive; Industrial Blockchain

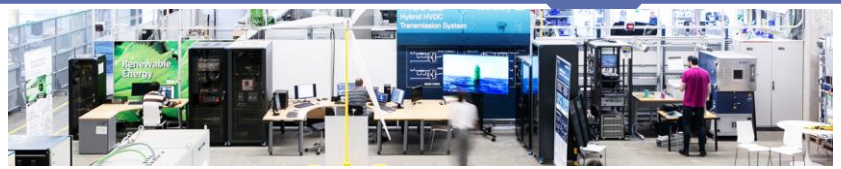
Node Ik4-IKERLAN
Focused on: Product Testing and Certification; Industry 4.0; Blockchain

Node BCAM: Focused on Mathematical models and computer simulation

5 Labs for Research and Innovation

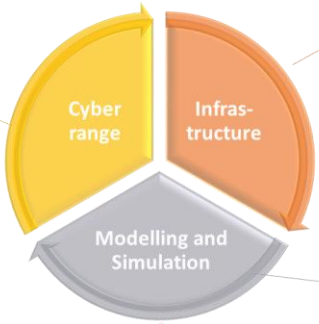
Focused

BASQUE CYBERSECURITY CENTRE



basque digital innovation hub

Node TECNALIA-PTA
Cyber range for training as well as for research



No vendor lock-in
Customizable network
VLANs
Virtualization

Modelling and simulation of different real-world scenarios (i.e., ICS)

rnli_
Red Nacional de Laboratorios Industriales

Node VICOMTECH
Focused on: Industry 4.0; Blockchain

Node TECNALIA-PTB
Focused on: Smart-Grid; Automotive; Industrial Blockchain

Node IK4-IKERLAN
Focused on: Product Testing and Certification; Industry 4.0; Blockchain

Node BCAM: Focused on Mathematical models and computer simulation

5 Labs for Research and Innovation

Challenges

- Last mile has proximitiy, knowledge and trust.
- Local ecosystems have a real value in itself if they have appropiate agents and funds.
- Regional, national and European can have different priorities that need to live and work together.
- Combining a top-down approach with a bottom-up approach. From the regional to the national, from the regional to the European, from the national to the European.
- Let´s build on the communities that already exists: ECSO, Cersecurity communitites in regions/nations, pilots.

Technological dependancy reduction, local capacities development, inter-regional cooperation.

ESKERRIK ASKO
GRACIAS
THANK YOU
MERCI

Cyber Security by tecnalia

tecnalia Inspiring Business

Cyber Security for Europe

D10.1 - ANNEX 11

CyberSec4Europe: Concertation Meeting Toulouse

Panel: Good Practice in Data Sharing for Incident Handling

Antonio Skarmeta
Universidad de Murcia

Ensuring the competitiveness of Europe
Enabling European economic growth
while protecting European society

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Challenges

Cyber Security for Europe

Technical

- **Interoperability** between threat intelligence sharing platform;
- Learning new threats, based on **advanced data analysis**;
- **Common data models**, for data sharing
- **Reputation** of the reporting party.
- Adversaries can **exploit machine learning** techniques
- **New models** based on the application of AI

Operational

- **protects the privacy of citizens** in the data sharing, empower the user on the sharing
- Adaptative **security loop** to cyber threats and new attack vectors
- **Facilitate non-expert** (SMEs, professionals) access to technology

Panelists

- Moderator: Antonio Skarmeta – UMU
- *Speakers*
- Fabio di Franco – ENISA
- Liina Kamm – CYBER
- Edgardo Montesdeoca – Montimage
- Aljosa Pasic – ATOS
- Valerio Senni – United Technologies Research Center

- Structure of the panel:
  - 5 min presentation by panelist of the position on challenges and best practices
  - First round on questions by the moderator linked to the topics
  - Open round of questions from the audience

Cyber
Security
for Europe

Thank you!

Antonio Skarmeta skarmeta@um.es
Universidad de Murcia

Mail: info@cybersec4europe.eu
Twitter: @CyberSec4Europe
Web: cybersec4europe.eu

THE EU CYBERSECURITY AGENCY

STRATEGIC RESEARCH PRIORITIES IN CYBERSECURITY

Fabio Di Franco, Ph.D.

CyberSec4Europe

14 | 11 | 2019

SECURING EUROPE'S INFORMATION SOCIETY

POSITIONING ENISA ACTIVITIES

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU
- ✓ Certification

COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

CSIRTS NETWORK SUPPORT

- Established by the NIS Directive "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation".
- Representatives of the Member States' CSIRTs and CERT-EU
  - cooperate
  - exchange information
  - build trust
  - improve the handling of cross-border incidents
  - discuss how to respond in a coordinated manner to specific incidents.
- ENISA provides the secretariat and actively supports the cooperation among members:
  - organizes meetings of the CSIRTs Network
  - provide infrastructure
  - provides its expertise and advice both to the EC and MS

https://csirtsnetwork.eu/

Active support and Secretariat

Leading tool development and maturity assessment

CSIRTs map

CSIRTs NETWORK
Powered by ENISA

CSIRTs self Assessment tool

Reference Taxonomy WG

Risk Management Training

Onsite

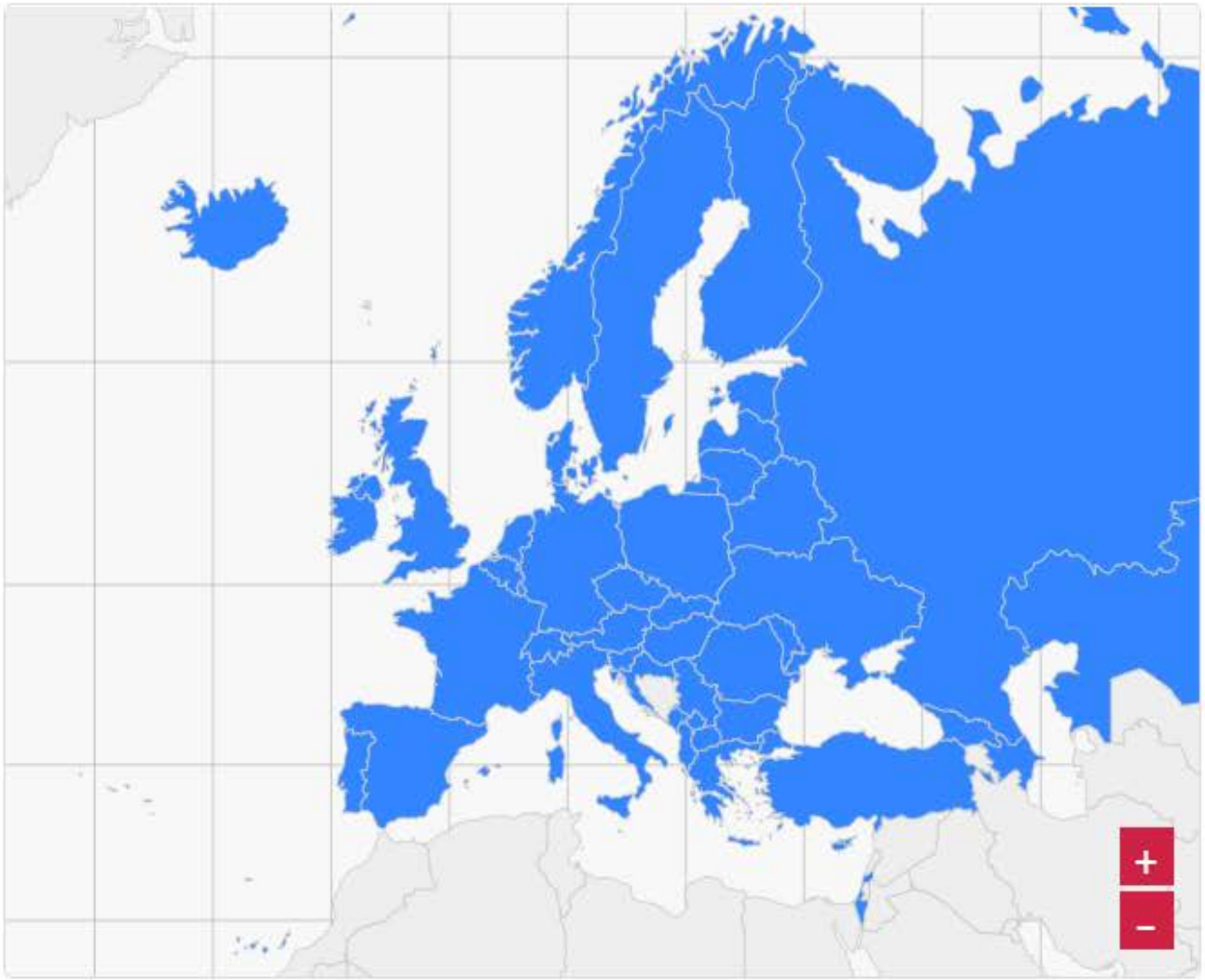
VMs, tutorials

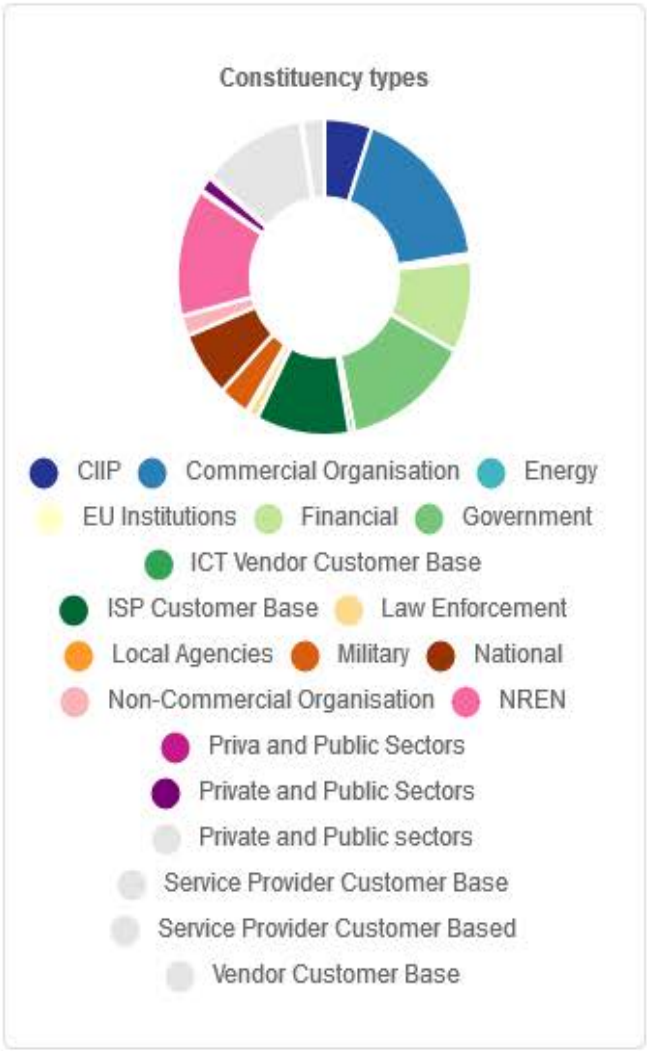
Train the trainers

Sectorial

enisa

CSIRTs by Country - Interactive Map





https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

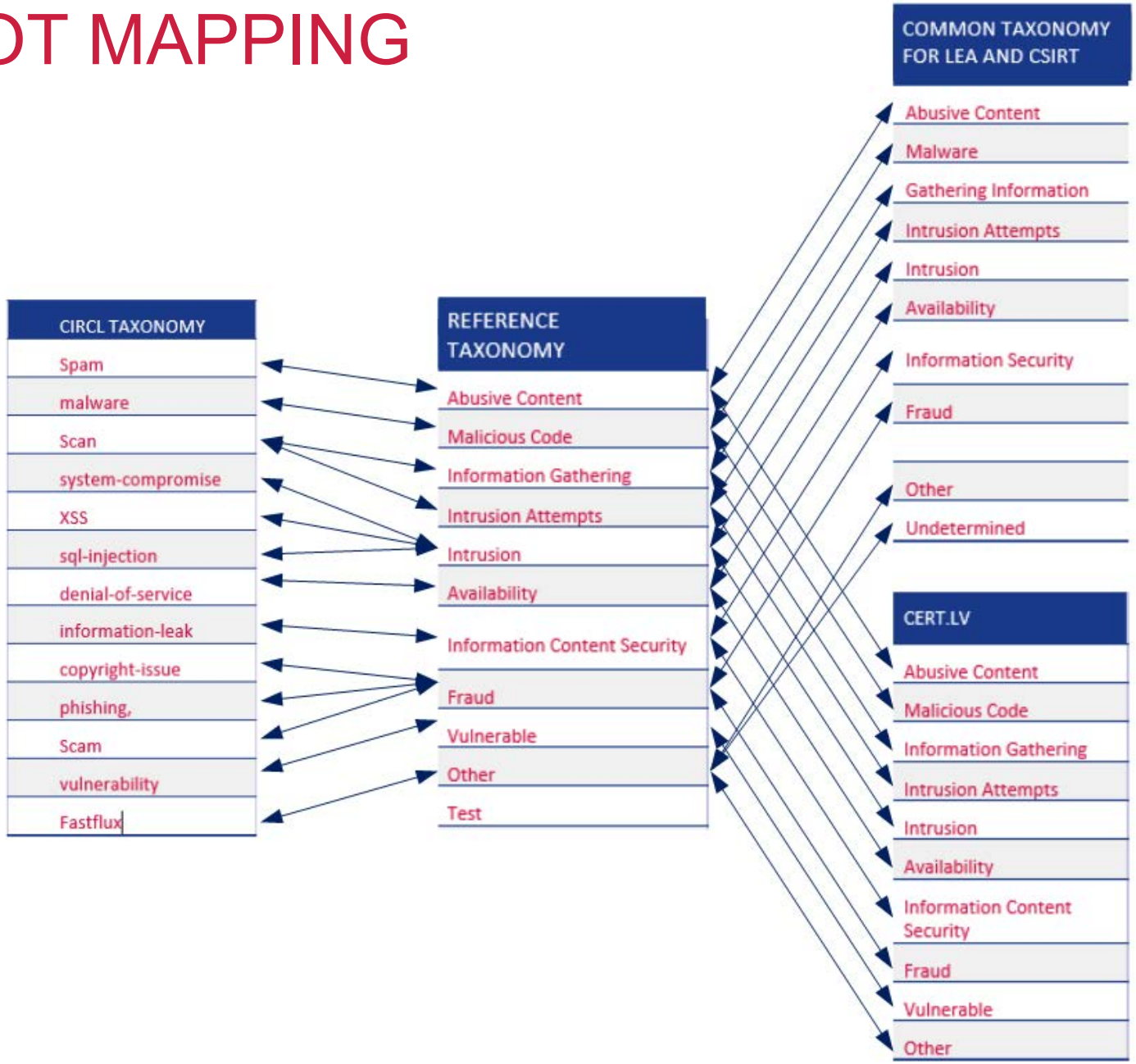
REFERENCE SECURITY INCIDENT TAXONOMY WORKING GROUP – RSIT WG

- ENISA introduces this idea in 2017 to the TF-CSIRT
- 54 participants from 17 MS within European CSIRT community
- Building a common language to face future incidents

Use Case:

- Incident handling
- Incident reporting
- Cross border incidents
- Statistics
- Performance and internal KPI
- Comparison with other entities
- Automation & Machine learning

PIVOT MAPPING



UPDATE AND VERSIONING MECHANISM

- Taxonomy text as a working copy on GitHub in MISP machine tag schema.
- Use GitHub 's "pull request" feature to transparently document change requests via a JSON file .
- Any WG member can add or change text and he/she is allowed to propose these changes on GitHub via pull requests.
- Latest version is automatically available in human and machine readable format on the GitHub repository.

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

TOOLS

https://thehive-project.org/

https://intelmq.readthedocs.io/en/latest/Developers-Guide/

https://github.com/MISP/misp-taxonomies

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 281 440 9665

fabio.difranco@enisa.europa.eu

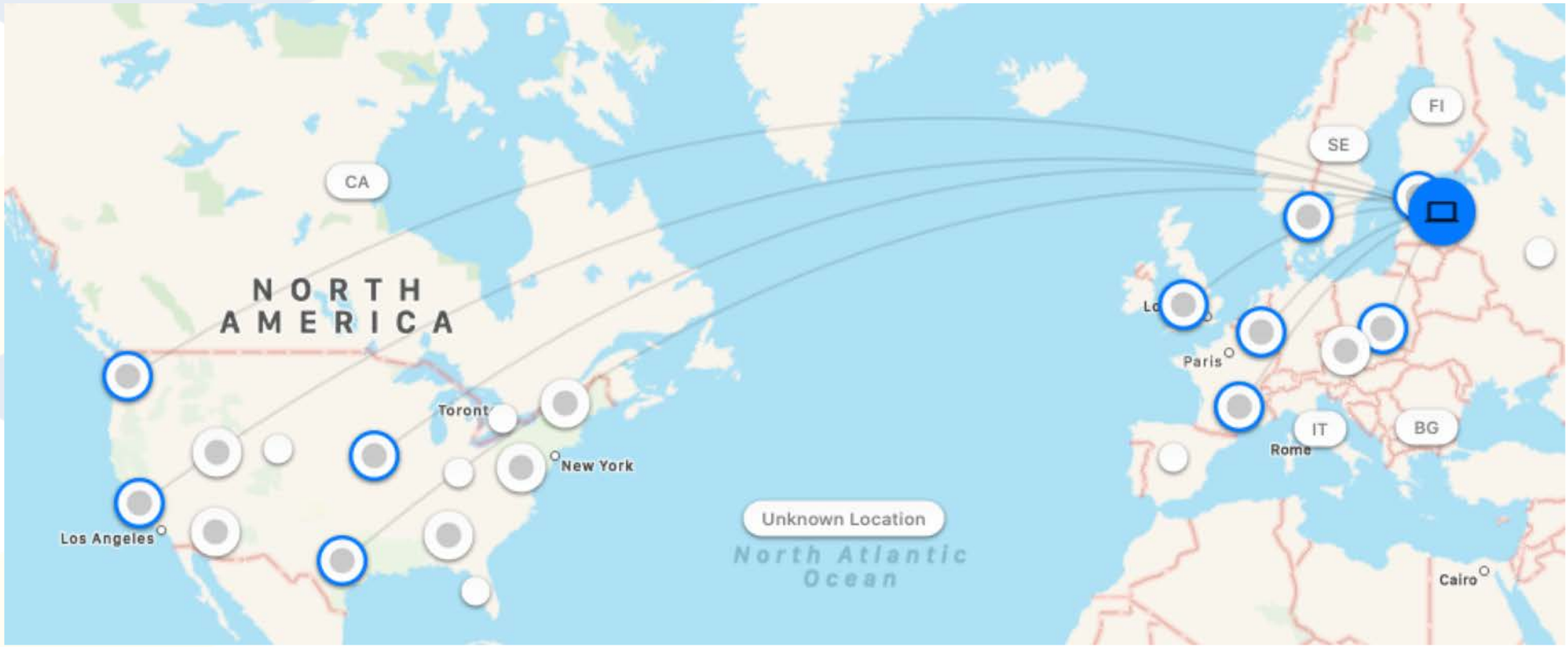
www.enisa.Europa.eu

Cyber
Security
for Europe

liina.kamm@cyber.ee

In the digital world, we are one

Attacks against cybersecurity and privacy have immediate global impact (compared to environmental).



Screenshot from the Little Snitch software while visiting delfi.ee
Little Snitch made by Objective Development Software (https://obdev.at)

Better security has a privacy problem!

Cyber Security for Europe

- Sharing information about attacks and defences shows ones vulnerabilities. This is a barrier to sharing.
- We have multiple sources for cybersecurity data
  - Governmental Cybersecurity Operations Centres – easier to share, good coverage
  - Corporate Cybersecurity Operations Centres – harder to convince to share, more targeted attacks,
  - Military Cybersecurity Operations Centres – very hard to get to share, can be very specific attacks
- In Cybernetica, we are building standards and networks for interorganisational **and** cross-border sharing of cybersecurity threat information, based on our work in privacy technologies.

Cyber Security for Europe

montimage

CYBERSEC4EUROPE: CONCERTATION MEETING TOULOUSE

CYBER THREAT INTELLIGENCE: OBTAIN AND EXPLOIT

EDGARDO MONTES DE OCA
CEO MONTIMAGE

ENSURING THE COMPETITIVENESS OF EUROPE
ENABLING EUROPEAN ECONOMIC GROWTH WHILE
PROTECTING EUROPEAN SOCIETY

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Brief presentation of Montimage

- Created in 2004; located in Paris (13ème)
- 100% independent, research oriented SME
- Team expert in Cybersecurity and Cyberdefence
- Recognized in Europe for its implication in ICT security research:

  H2020, CelticPlus, ITEA, ANR…

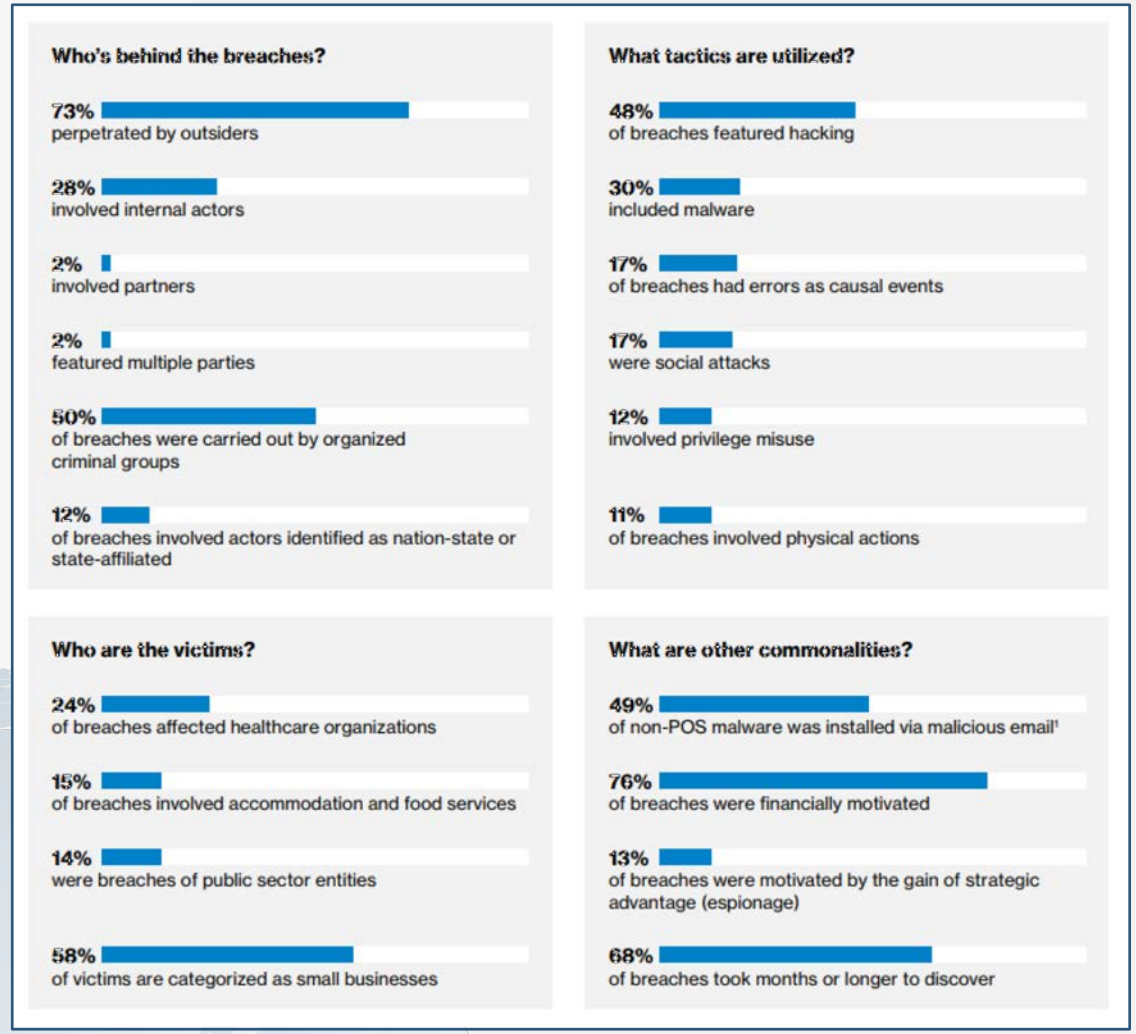
  Systematic cluster's "Innovation Success Story", EU seal of excellence, CelticPlus/ITEA awards

Software solutions and tools:

- Prevention and detection of cyberthreats (high/low bandwidth, IoT, cloud, 4G/5G): MMT-Framework, DPI, IDS/IPS, Box, APS
- Instant creation of 4G/5G networks: EPC-in-a-Box
- Cyber Threat Intelligence services

The Problem

- 58% of malware and cyber attack victims are categorized as small businesses.
- 52% of all web traffic is now automated or which 23% is bad bots and automated threats
- 2018 -53,000 incidents and 2,216 confirmed data breaches.
- 2021 – 79,000 incidents and 3,300 data breaches
- Cost of €400,000/breach for mid-SME (est)



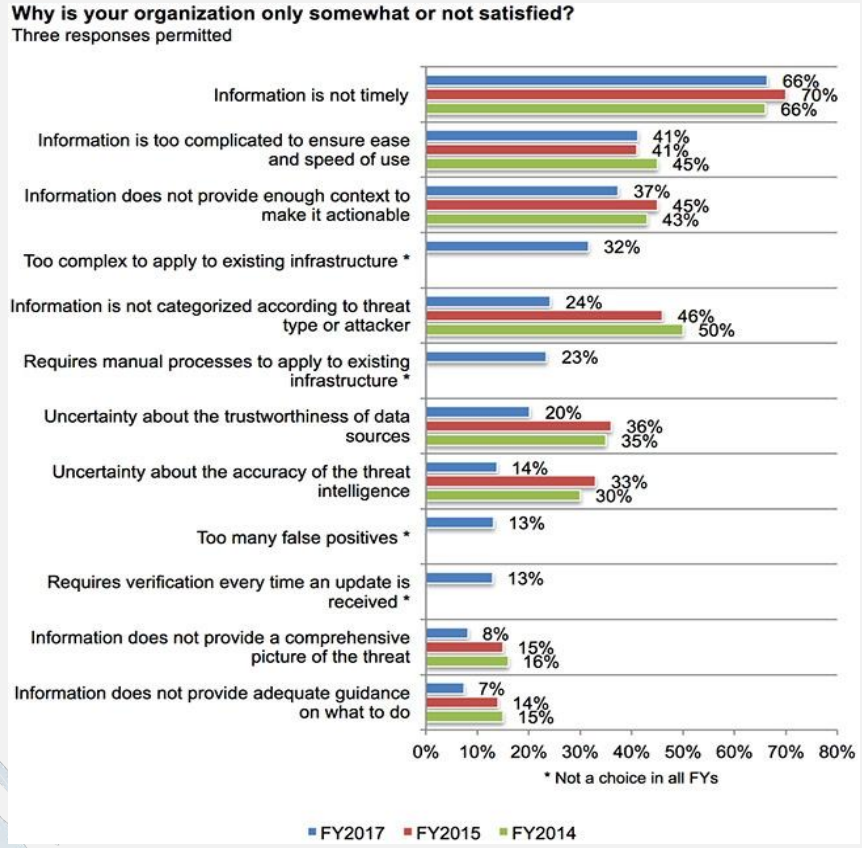
The Opportunity

Class size	Number of enterprises		Number of persons employed		Value added	
	European Union		European Union		European Union	
	Number	Share	Number	Share	Billion €	Share
Micro	22 231 551	93.0 %	41 662 352	29.8 %	1 482	20.9 %
Small	1 391 642	5.8 %	27 981 751	20.0 %	1 260	17.8 %
Medium-sized	225 422	0.9 %	23 398 194	16.8 %	1 288	18.2 %
SMEs	**23 848 615**	**99.8 %**	**93 042 297**	**66.6 %**	**4 030**	**56.8 %**
Large	45 194	0.2 %	46 602 999	33.4 %	3 065	43.2 %
Total	**23 893 809**	**100.0 %**	**139 645 296**	**100.0 %**	**7 095**	**100.0 %**

- Most cyber security providers/competitors (SOCS, SIEM, etc.) provide for large companies i.e. 0.2% of the market.
- 73% of cyber-attacks focused on the cloud were directed at Web applications. SME's are now the most dependent on cloud usage.
- 90% of enterprises feel vulnerable to insider attacks, of which 47% are insiders wilfully causing harm and 51% are from insiders by accident; compromised credentials, negligence etc.

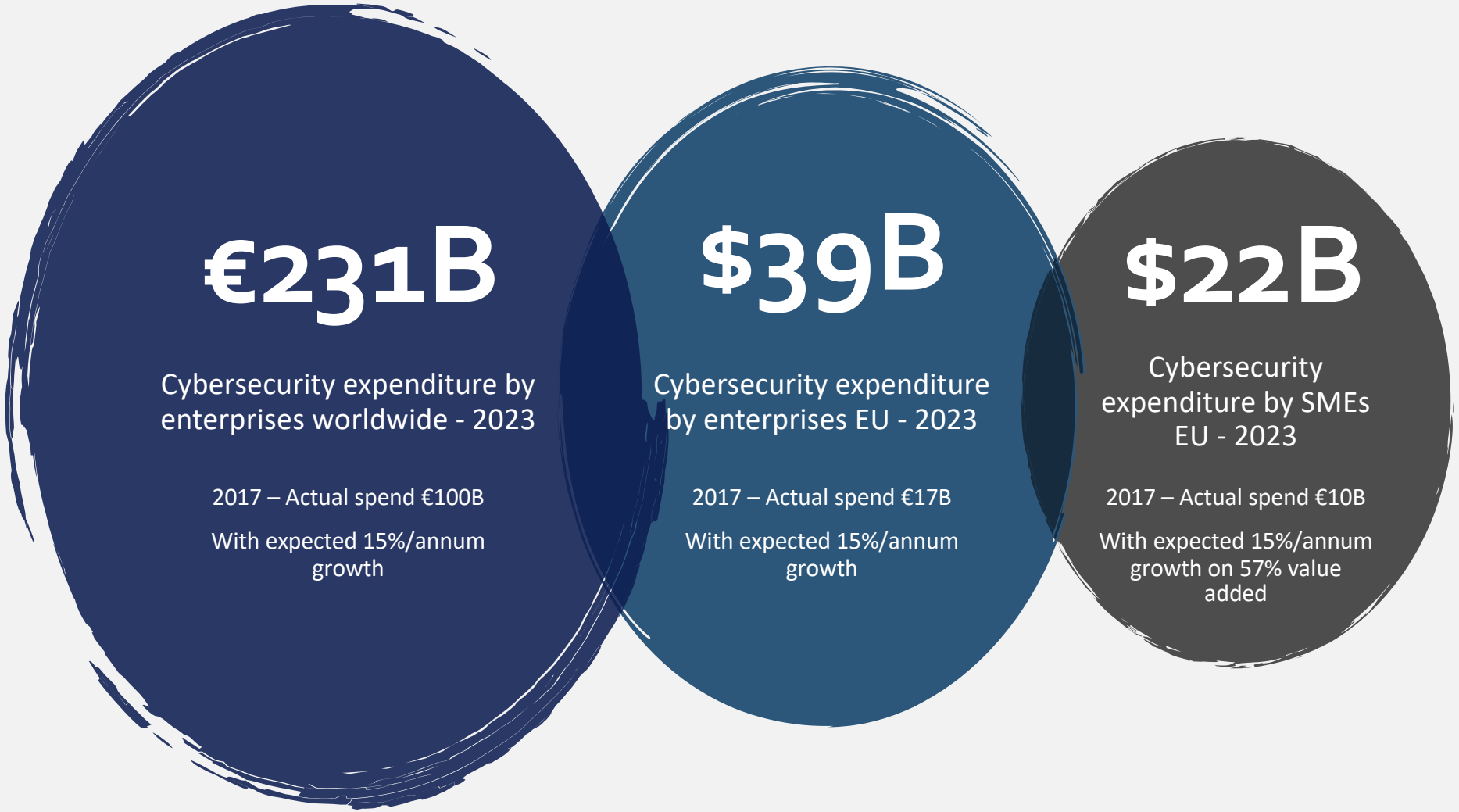
User "pain points" targeted by SISSDEN BV

- Timely: **real-time** CTI (in seconds).
- Ease of use and **comprehensive threat indicators**: open standards (e.g. STIX/TAXII) and malicious-only metadata.
- Trust in provided **intelligence and accuracy**: honeypot and darknet activity correlated with information from other sources (Open Source Intelligence and commercial blacklists).
- **Removing complexity**: automated processing and simplified use of CTI.
- **Modular and scalable**: to serve different categories of customers: SMEs and large enterprises.



Surveys (e.g. Ponemon Institute and SANS) identify "pain points"

Market Opportunity



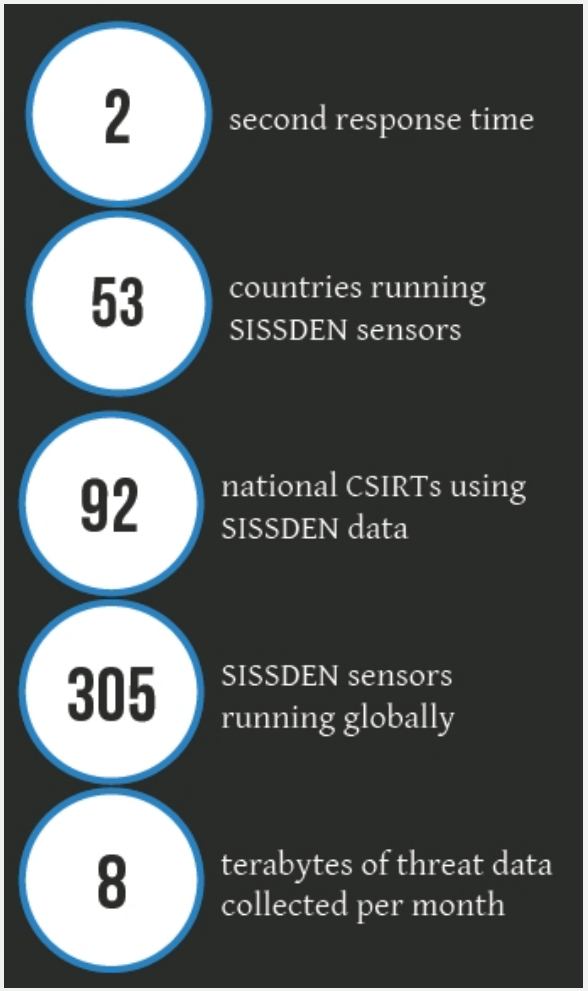
Related projects

SAINT (Cybersecurity metrics)
Analysed and identified incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cybercriminal activity, associated markets and revenues, existing solutions, and open source threat intelligence in order to improve defense from cybercriminal activities.

SISSDEN (European threat data): Deployed network of honeypots and darknet throughout the world and provided actionable Cyber Threat Intelligence to organisations (STIX/TAXII format) and curated datasets for research.

This project resulted in a spin-off created by the 3 SMEs to provide CTI in real-time that can be exploited automatically to protect SMEs from attack campaigns before they reach their networks.

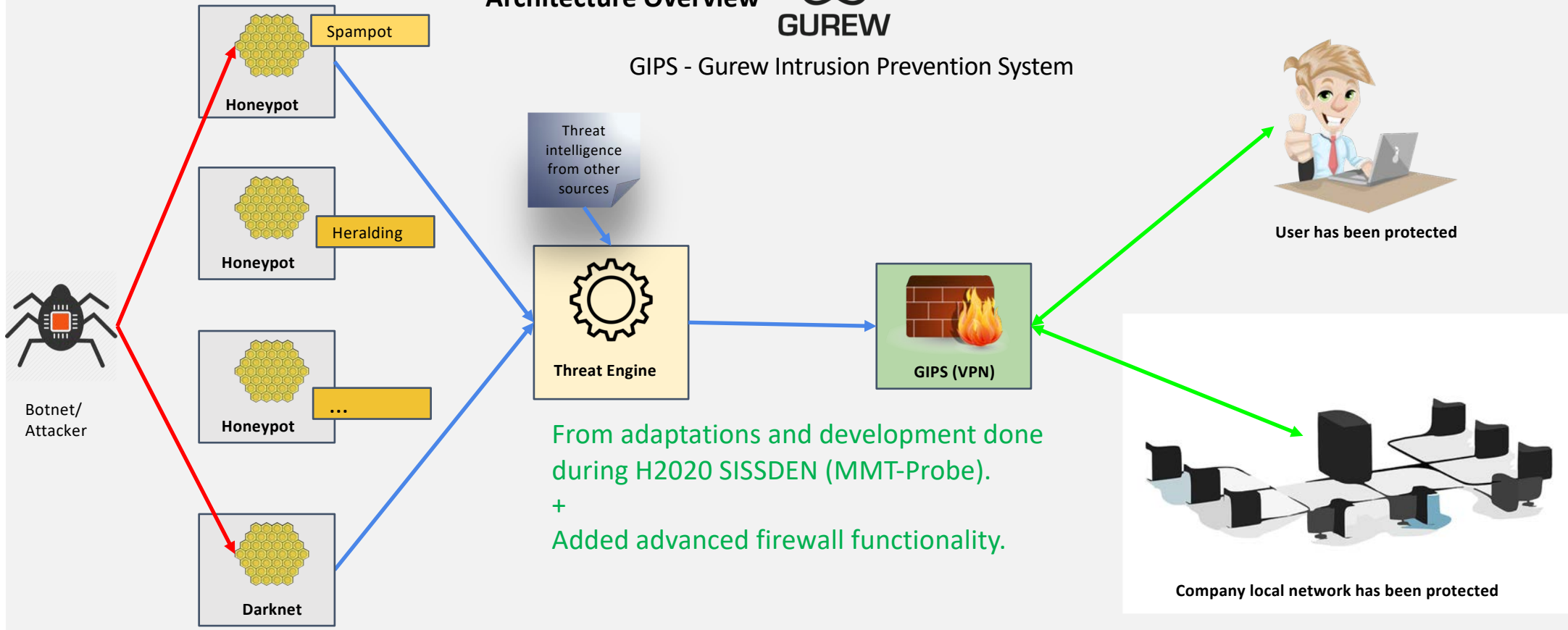
montimage



Architecture Overview

GUREW

GIPS - Gurew Intrusion Prevention System



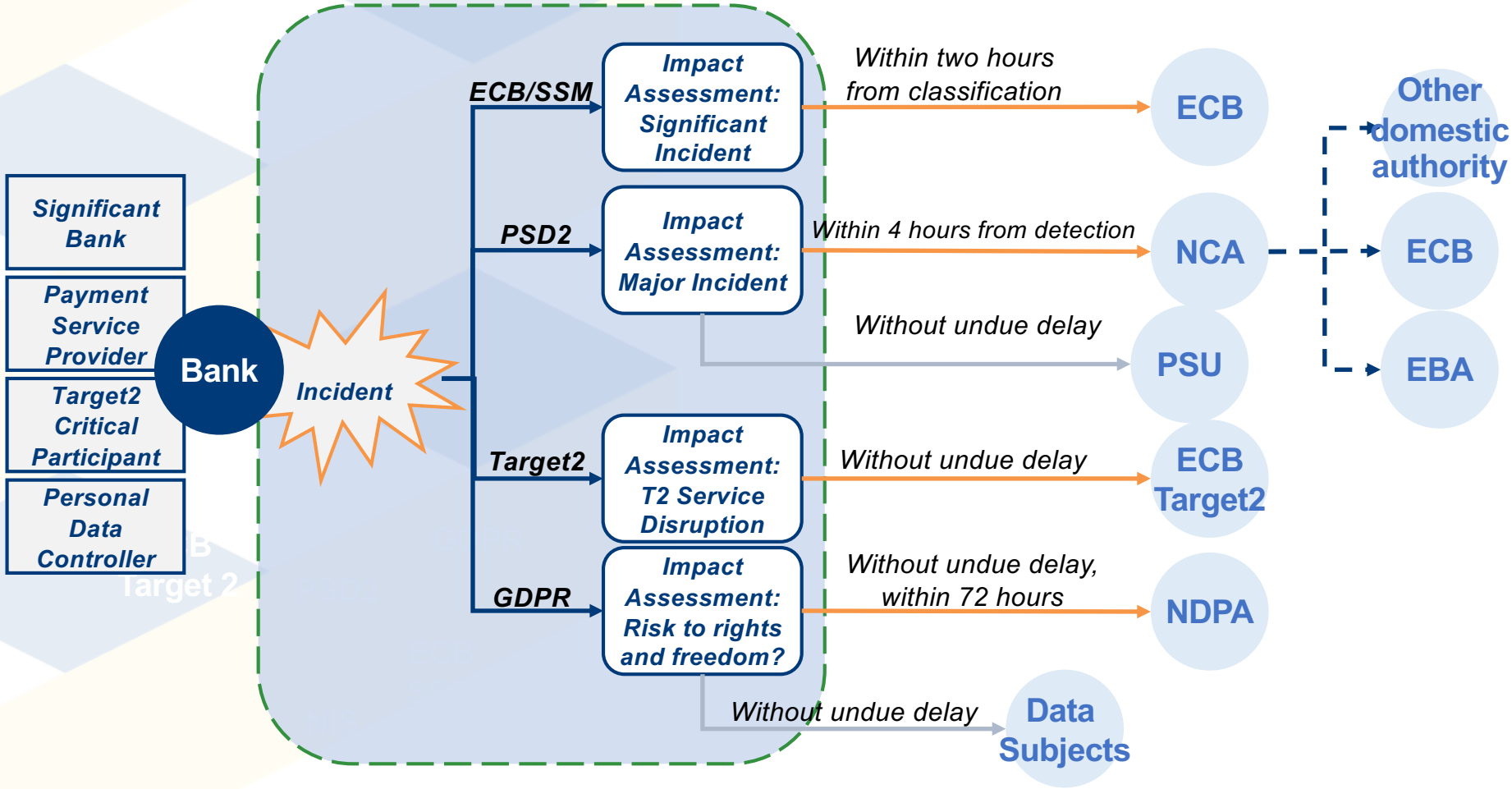
From adaptations and development done during H2020 SISSDEN (MMT-Probe).
+
Added advanced firewall functionality.

From knowledge gathered and work done during H2020 SISSDEN

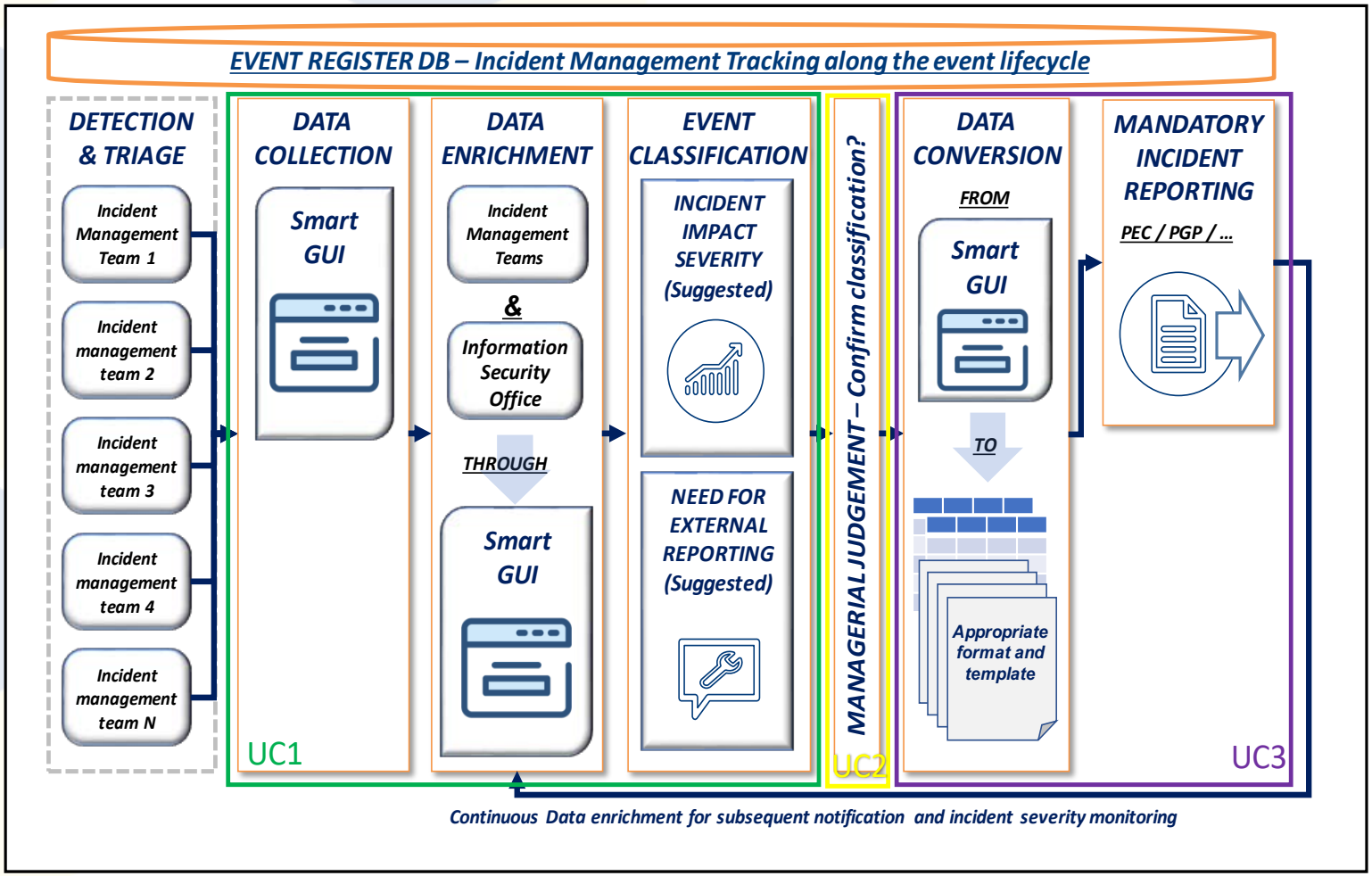
Cyber
Security
for Europe

Aljosa.Pasic@Atos.net

Introduction: simple scenario



Incident Reporting Functional Workflow



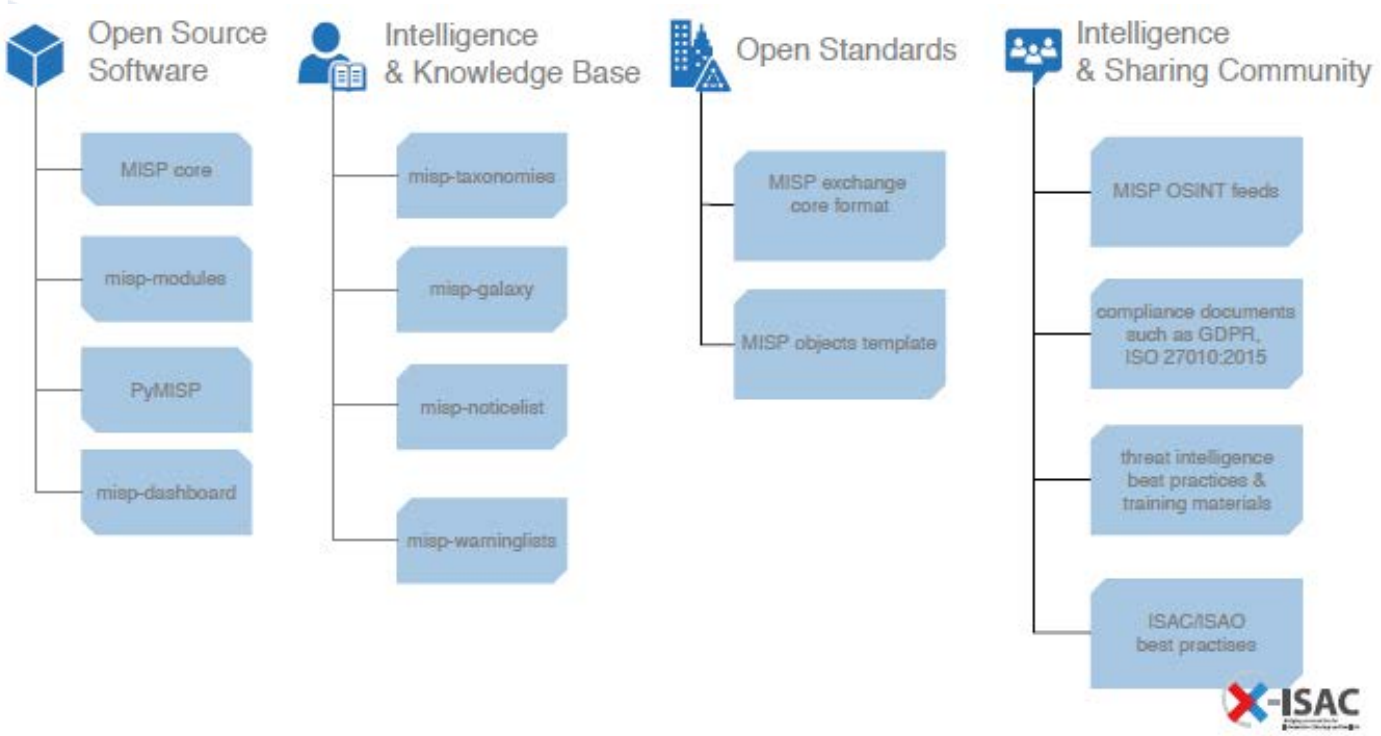
TI features and governance

Table 1: Comparison of Threat Intelligence Platforms

Evaluated Criteria	MISP	CIF	CRITs	SE
Import/Export Format	●	○	●	–
Integration Capabilities	●	●	○	○
Data Exchange Std.	●	○	○	○
Support of Collaboration	●	●	○	○
Analysis Capabilities	○	○	●	○
Graph Generation	○	○	●	○
License	●	●	●	○
Hardware Requirements	●	–	●	●

–Low/Basic ○ Medium/Average ● High/Advanced

Fomats, integration, level of automation, flexibility…



Challenges for data sharing

- Everyone can be a consumer and/or a contributor/producer.
- Many types of users such as incident responders, security analysts, intelligence analysts, LEAs, fraud analysts
- Different sharing models and policies
- Trade-offs (e.g. secrecy and efficacy or strategic vs tactical and operational levels)
- Shifting focus towards data quality and credibility
- Speed up processing and analysis (machine readable formats, enrichment, correlation with real-time data etc)

Challenges for EU

- EU context: democracy and inclusiveness vs accepting bad ideas "as is" from organisations,
- EU context: “learning by imitation” (also known as “best practice” reuse)
- EU context: GDPR roles data controller and data processor
- EU context: interoperability
- EU context: coordinated response – CACAO (collaborative automated course of action operations) standard

Cyber
Security
for Europe

Valerio Senni UTRC

Some considerations on Data Sharing for Cyber-security Incidents Handling from the perspective of Civil Aviation

November 14, 2019

Valerio Senni – UTRC Italy
valerio.senni@utrc.utc.com

UTRC and Speaker Intro

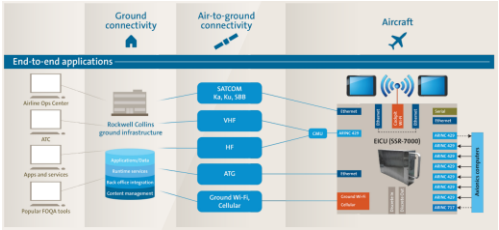
- Engineer, Computer Scientist, PhD on formal methods
- Staff Research Engineer, member of the Formal Methods group, Cyber-security Discipline Leader @ UTRC-Italy
- Key research interests:
  - Applied formal methods (theory, practice, toolchains)
  - Model-based design
  - Joint safety/security risk assessment and automation
  - Security architectures
  - Vulnerability assessment automation
  - Formally proved secure SW/HW
- Several years experience of UTC BU projects (Collins/UTAS, Otis, P&W)
- 15Y research experience, 30+ papers in formal methods area
- ERD engagement in EU H2020 programs

UTRC is UTC's **innovation engine**

United Technologies Research Center

Overview of Civil Aviation

- **Culture**
  - Safety: the highest concern
  - A notion of shared responsibility and ownership for the benefit of all the ecosystem, to reduce safety risk
  - Organizations perform extensive safety assessments to meet certification requirements (FAA, EASA, …)
  - Principle of independent audits and assessment of safety assumptions
- **Current state on cybersecurity**
  - Cybersecurity a growing concern, with increase in adoption of SW, connectivity and services
  - Regulations' focus on IUEI (Intentional Unauthorized Electronic Interaction) and induced safety risks
  - Additional obligations on operational and privacy impacts (economic & legal impacts)
  - The aviation ecosystem is looking to standardize how cybersecurity can be assured (RTCA & EUROCAE WG 72, DO-326A and related standards) > Security airworthiness
  - WG72 SG3 is currently defining new guidance material on disclosure (document currently under review)
  - The objective is to promote sharing and collaboration in cybersecurity
- **Challenges**
  - Cybersecurity threats evolve in time (not the same for safety) > ongoing regular independent assessment
  - Need to improve sharing on product side > communities (A-ISAC, EASA-ECCSA, EuroControl CERT)
  - Complex ecosystems require inclusion of all the stakeholders from the supply chain to the operators



https://www.collinsaerospace.com/

Communities

- A-ISAC (global) 

  - Build trust between stakeholders (Airframers, Subsystems providers, Service providers, …) of the aviation ecosystem
  - Different level of sharing (TLP classification):
    - Publicly known vulnerabilities (White - open to everyone, after filtering from A-ISAC WGs)
    - Weekly communications to specific communities (signed agreement on subscription)
    - Centralized info-sharing data repository (not meant to be machine-processed)
    - IOC (Indicator of Compromise) – objective to improve the ecosystem for the benefit of all
  - Support in relation with researchers' disclosures (e.g. with IoActive, see BlackHat)

- EASA - European Centre for Cybersecurity in Aviation (ECCSA) 

  - support for vulnerability disclosure to individuals, attempting to coordinate with the affected vendor and stakeholders
  - In line with the ICAO cyber strategy - to enable cooperation with 'good faith' security research activities, which are research activities carried out in an environment designed to avoid affecting the safety, security and continuity of civil aviation..

- Eurocontrol CERT 

  - Focusing on Air Traffic Management in EU
  - Computer Emergency Response Team (EATM-CERT) – monitor threats on CIA of operational IT assets and data
  - Collection, creation, distribution of ATM-relevant cyber-intel

Challenges and Directions

1. Threat modeling, assumptions and responsibilities elicitation
    i. Improve assets impacts characterization (safety, legal, economic effects)
2. Common risk models and shared knowledge base
3. Continuous airworthiness, post-EIS support and minimize re-certification efforts
4. How to provide evidence to non-tech audience
    i. How do you know an incident happened? What does it look like? (e.g. autonomous functions)
    ii. Impact evaluation in collaboration with all stakeholders
    iii. IP concerns in sharing information on incidents
    iv. Timeline for mitigation
    v. Rebuild trust after an incident

Cyber Security for Europe

Panel Discussion 5

Who's calling? Managing identities in the cyber world

Jesus Luna
Bosch

Simone Fischer-Hübner
Karlstad University

Henrich C. Pöhls
University of Passau

Stephan Krenn
Austrian Institute of Technology (AIT)

Fabio Martinelli
Consiglio Nazionale delle Ricerche (CNR)

Moderator: Javier Lopez, University of Malaga

"On the Internet, nobody knows you're a dog."

"On the Internet, nobody knows you're a dog."

"Remember when, on the Internet, nobody knew who you were?"

THE WALL STREET JOURNAL.

Cyber Security for Europe

He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers

Security researchers agree that for most people, adding text-message authentication is a big step up from only using a password, but that can leave you open to a relatively new attack called SIM swapping

By Robert McMillan

Nov. 8, 2019 9:00 am ET

THE WALL STREET JOURNAL.

He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers

Security researchers agree that for most people, adding text-message authentication is a big step up from only using a password, but that can leave you open to a relatively new attack called SIM swapping

By Robert McMillan

Nov. 8, 2019 9:00 am ET

Major vulnerability patched in the EU's eIDAS authentication system

Exclusive: Vulnerability would have allowed attackers to pose as any EU citizen or business.

By Catalin Cimpanu for Zero Day | October 29, 2019 -- 10:13 GMT (10:13 GMT) | Topic: Security

Cyber Security for Europe

THE WALL STREET JOURNAL.

He Thought His Phone Was Secure; Then He Lost $24 Million to Hackers

Security researchers agree that for most people, adding text-message authentication is a big step up from only using a password, but that can leave you open to a relatively new attack called SIM swapping

By Robert McMillan

Nov. 8, 2019 9:00 am ET

ZDNet

Major vulnerability patched in the EU's eIDAS authentication system

Exclusive: Vulnerability would have allowed attackers to pose as any EU citizen or business.

By Catalin Cimpanu for Zero Day | October 29, 2019 -- 10:13 GMT (10:13 GMT) | Topic: Security

CSO FROM IDG

Rich PII enables sophisticated impersonation attacks

By Maria Korolov

Contributing Writer, CSO | SEP 24, 2019 3:00 AM PDT

Cyber Security for Europe

The New York Times

Google to Store and Analyze Millions of Health Records

By Natasha Singer and Daisuke Wakabayashi

Nov. 11, 2019

Cyber Security for Europe

The New York Times

Google to Store and Analyze Millions of Health Records

By Natasha Singer and Daisuke Wakabayashi

Nov. 11, 2019

It has not informed patients or physicians.

ACTIVIST POST

Cyber Security for Europe

The New York Times

Google to Store and Analyze Millions of Health Records

By Natasha Singer and Daisuke Wakabayashi

Nov. 11, 2019

It has not informed patients or physicians.

ACTIVIST POST

Google given access to healthcare data of up to 1.6 million patients

Ben Quinn

The Guardian

Cyber Security for Europe

The New York Times

Google to Store and Analyze Millions of Health Records

By Natasha Singer and Daisuke Wakabayashi

Nov. 11, 2019

It has not informed patients or physicians.

ACTIVIST POST

Google given access to healthcare data of up to 1.6 million patients

Ben Quinn

The Guardian

This article is more than **3 years old**

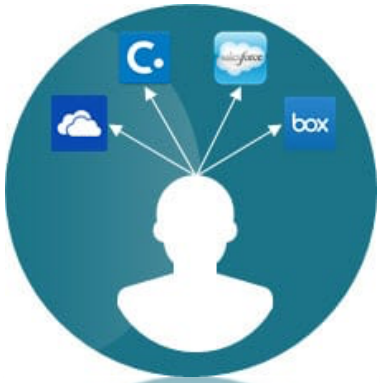
Cyber Security for Europe

Questions in the air …

Cyber Security for Europe

Questions in the air …

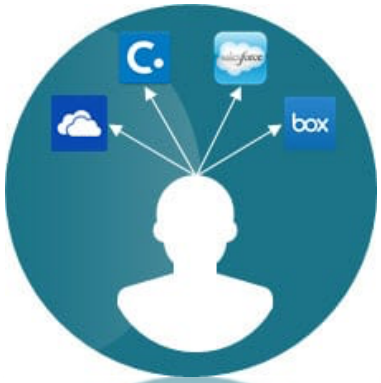
- **Has identity federation been the promised panacea?**



Cyber Security for Europe

Questions in the air …

- **Has identity federation been the promised panacea?**

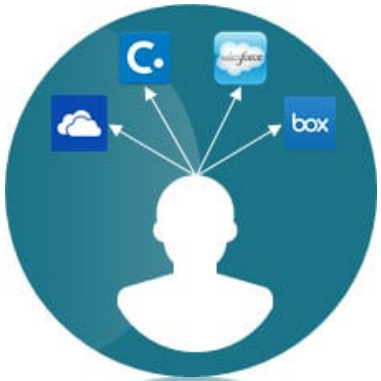


- **Will distributed ledger technology solve IDM problems?**

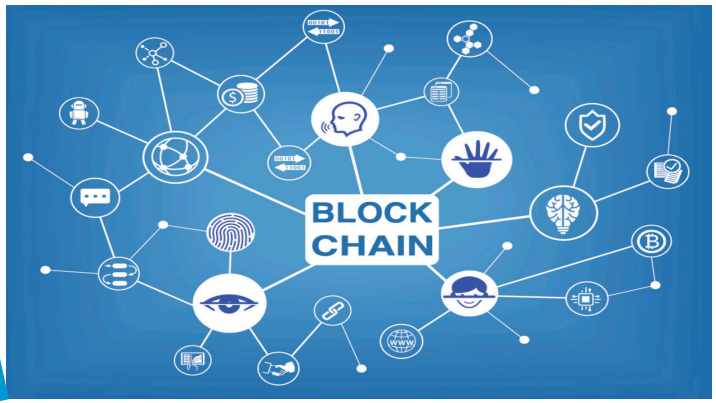
Cyber Security for Europe

Questions in the air …

- **Has identity federation been the promised panacea?**



- **Will distributed ledger technology solve IDM problems?**



Cyber Security for Europe

Questions in the air …

- **How much will IDM future be driven by biometric systems?**

Cyber Security for Europe

Questions in the air …

- **How much will IDM future be driven by biometric systems?**

Cyber Security for Europe

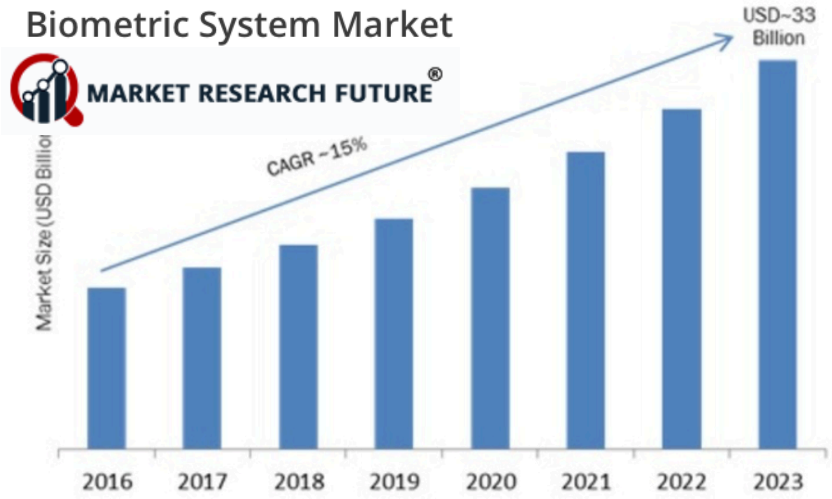
Questions in the air …

- **How much will IDM future be driven by biometric systems?**

Cyber Security for Europe

Questions in the air …

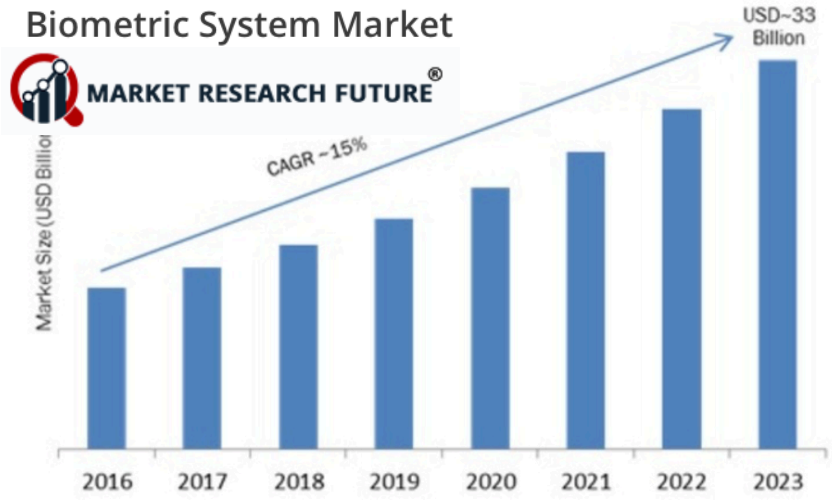
- **How much will IDM future be driven by biometric systems?**



Cyber Security for Europe

Questions in the air …

- **How much will IDM future be driven by biometric systems?**

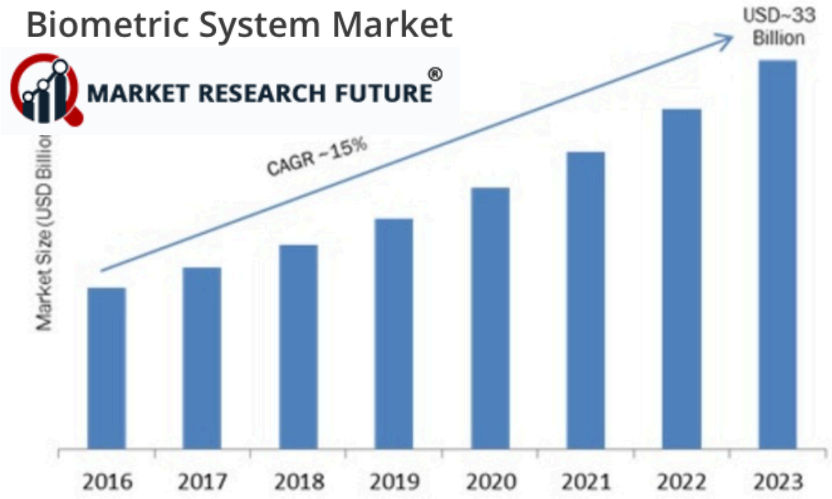


- **What level of privacy risk is introduced by IoT devices?**

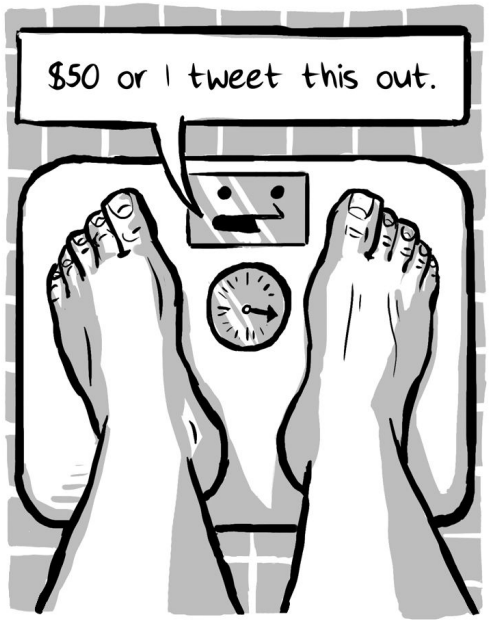
Cyber Security for Europe

Questions in the air …

- **How much will IDM future be driven by biometric systems?**



- **What privacy risks are introduced by IoT devices?**



Cyber Security for Europe

FABIO MARTINELLI CNR	Identity in data usage control
STEPHAN KRENN Austrian Institute of Technology	Offline privacy in an online world
SIMONE FISCHER-HÜBNER Karlstad University	Challenges of user-centric privacy preserving IDM
JESUS LUNA BOSCH	End-to-End Identity Management
HENRICH C. PÖHLS University of Passau	Identity is technically interdisciplinary

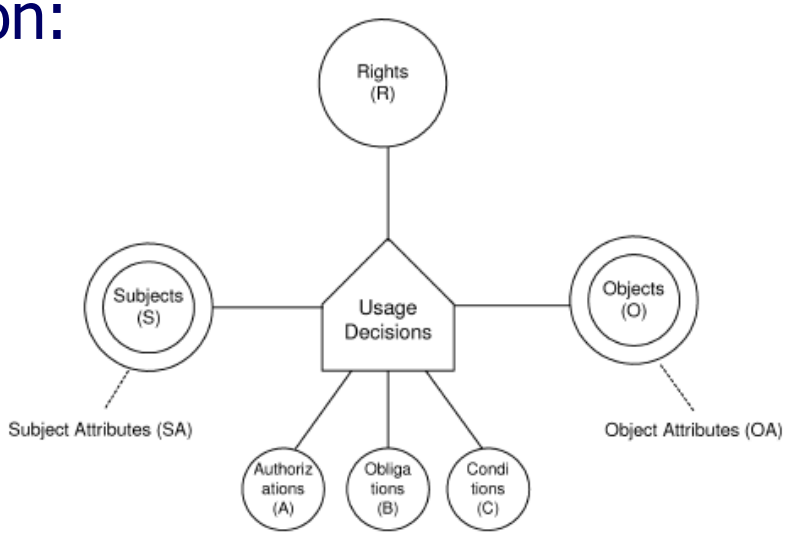
Identity and data usage control

- Fabio Martinelli - National Research Council of Italy

Usage Control Model

- Defined by J. Park and R. Sandhu (since 2004)
  - Useful on long lasting sessions on usage of resources

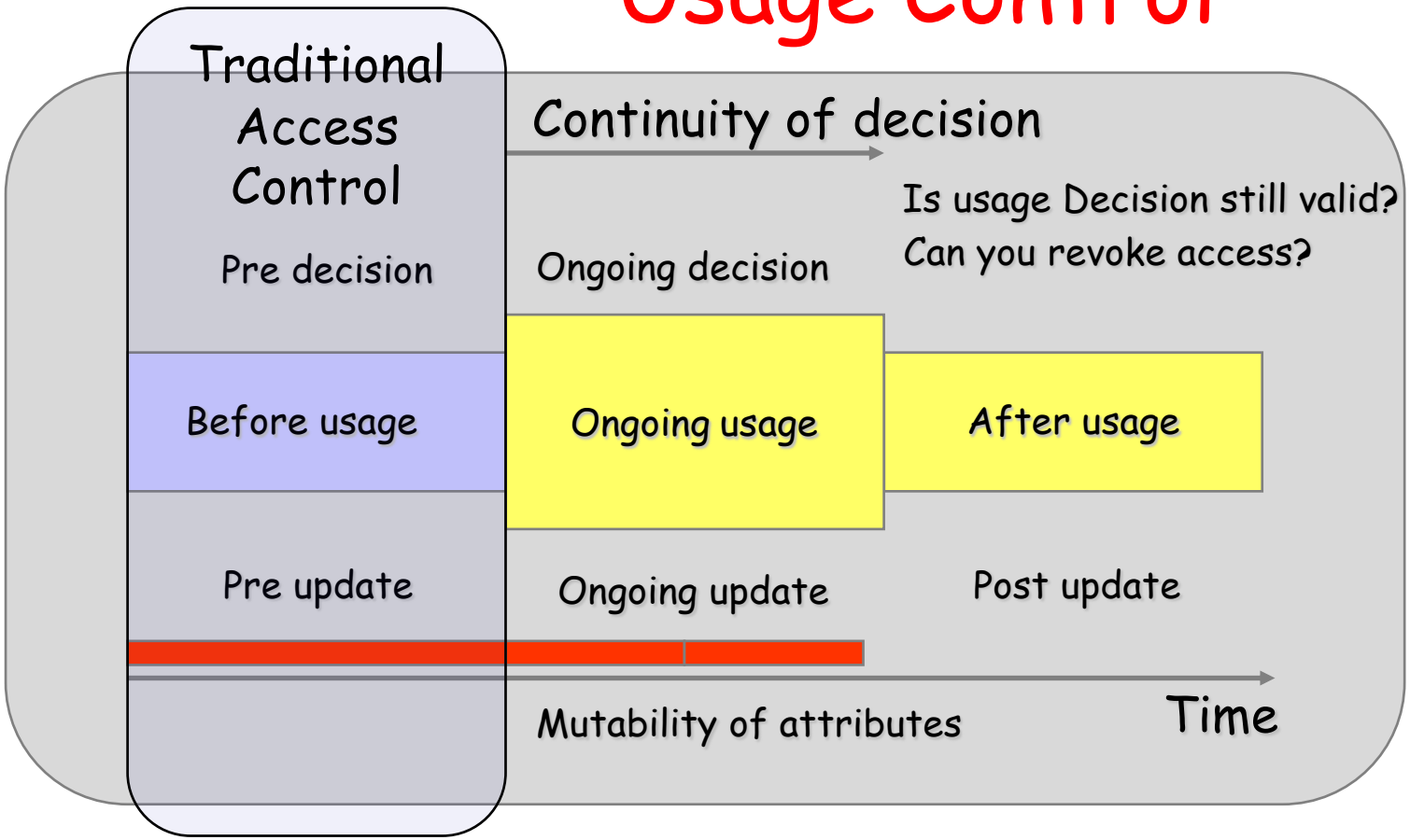
- Usage control is based on:
  - Authorizations (A)
  - Obligations (B)
  - Conditions (C)
  - Mutability of Attributes
  - Continuity of enforcement
    - Pre/Ongoing/After



Subjects and Objects

- Subjects: entities that perform actions on Objects. Are characterized by Attributes:
  - Identity
    - Role
    - Reputation (may change with time)
  - Credits
  - …
- Objects: entities that are used by Subjects. Are characterized by Attributes:
  - Value
  - Role permission
  - …

From Access Control to Usage Control



Obligations

- Mandatory actions that must have been performed by subjects (pre/on going/after) :
- Example:
  - the user of a storage service must download the license agreement before downloading any other document.
  - Before accessing an additional authentication mechanism must be used (multiple authentication factors)
    - Increasing confidence on the identity ☺
  - During access each 15 mins the user should authenticate the system
  - After usage anonymization techniques must be used on the data

Other examples

- Identity attributes may be used as a parameter of UCON policies to allow access to resources
  - Strictness of policy (e.g. ongoing usage) may depend on the reputation level of subjects
    - This may vary with time
- Attributes of certain identities may be updated based on UCON policies
  - Users not compliant with policy (e.g. sending code not respecting specific constraints) may be revoked from usage

Based on these technologies

NLP to enforceable policies

Data Usage control for CTI

Anonymization as obligations

Privacy preserving computing

Cyber Security for Europe

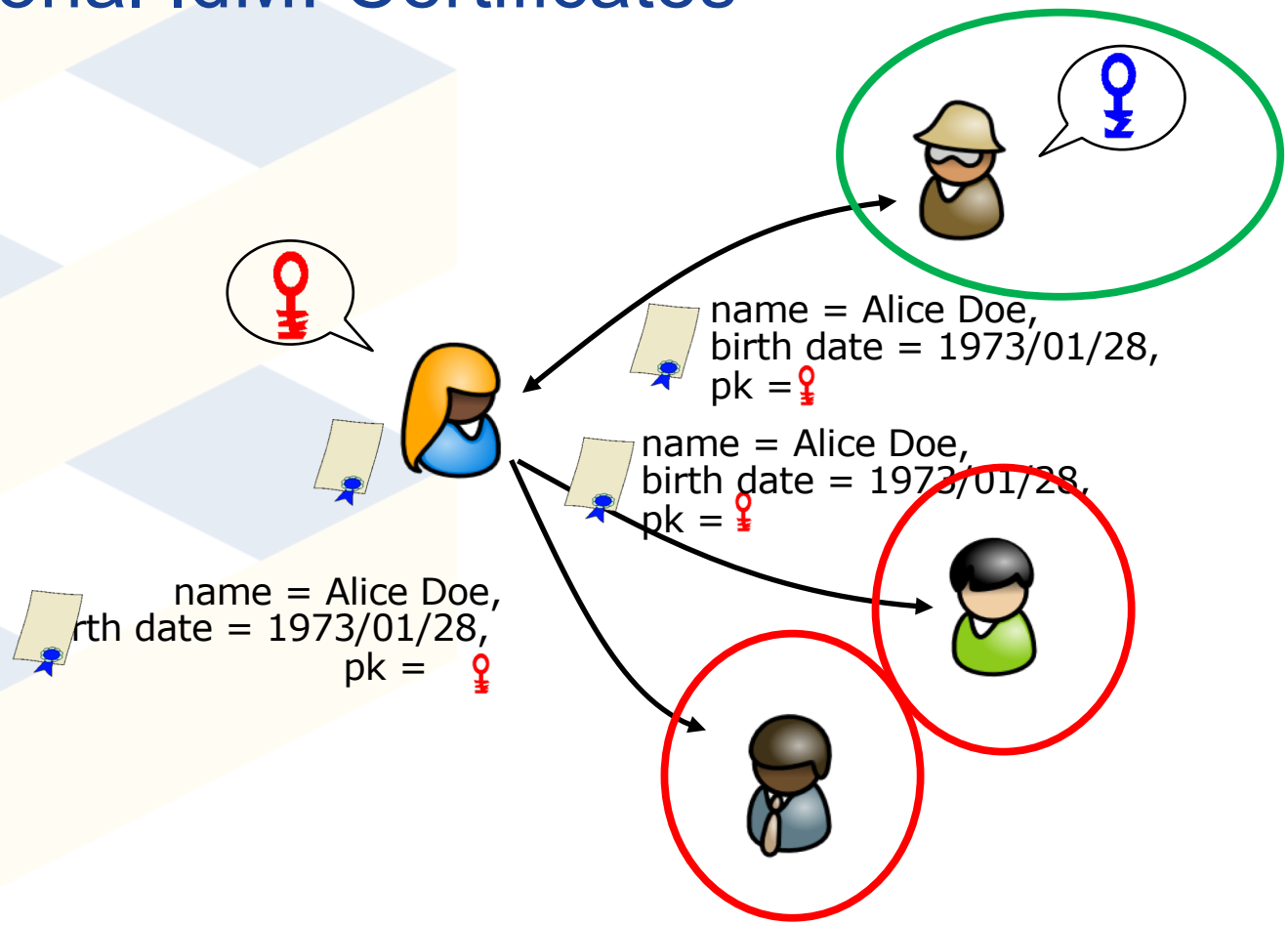
Offline-Privacy in an Online World

Stephan Krenn
Austrian Institute of Technology

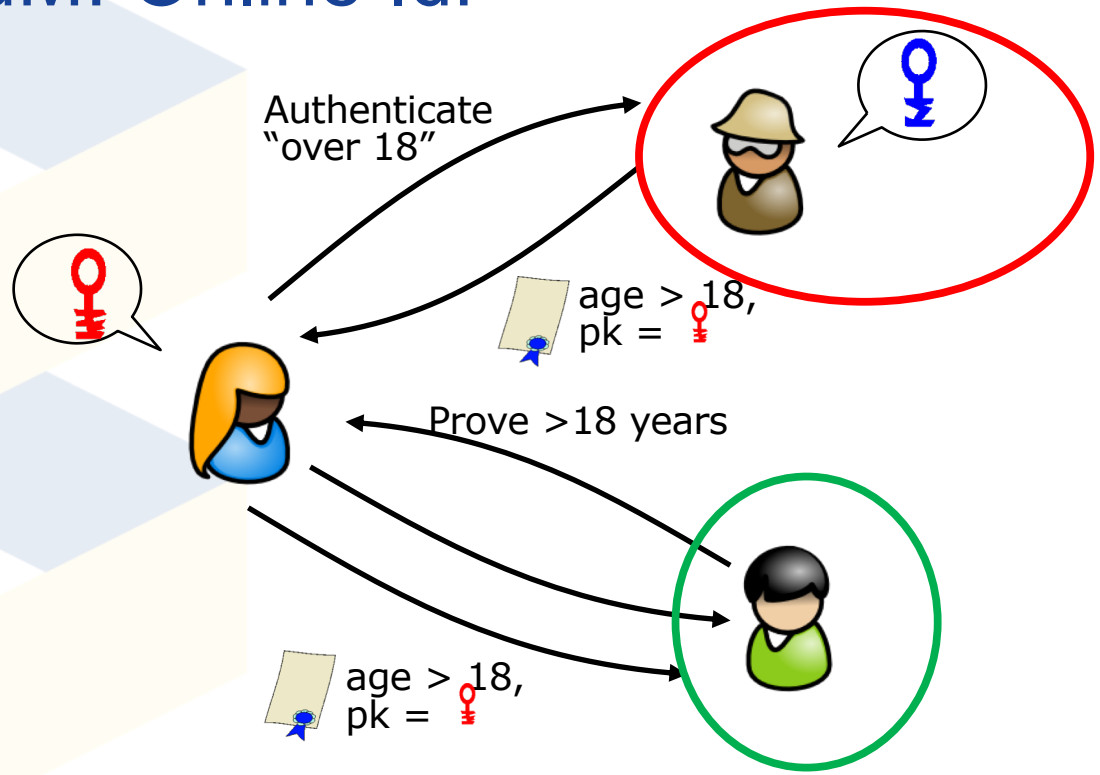
Cybersecurity for Europe 2019
Toulouse

Traditional IdM: Certificates

Cyber Security for Europe

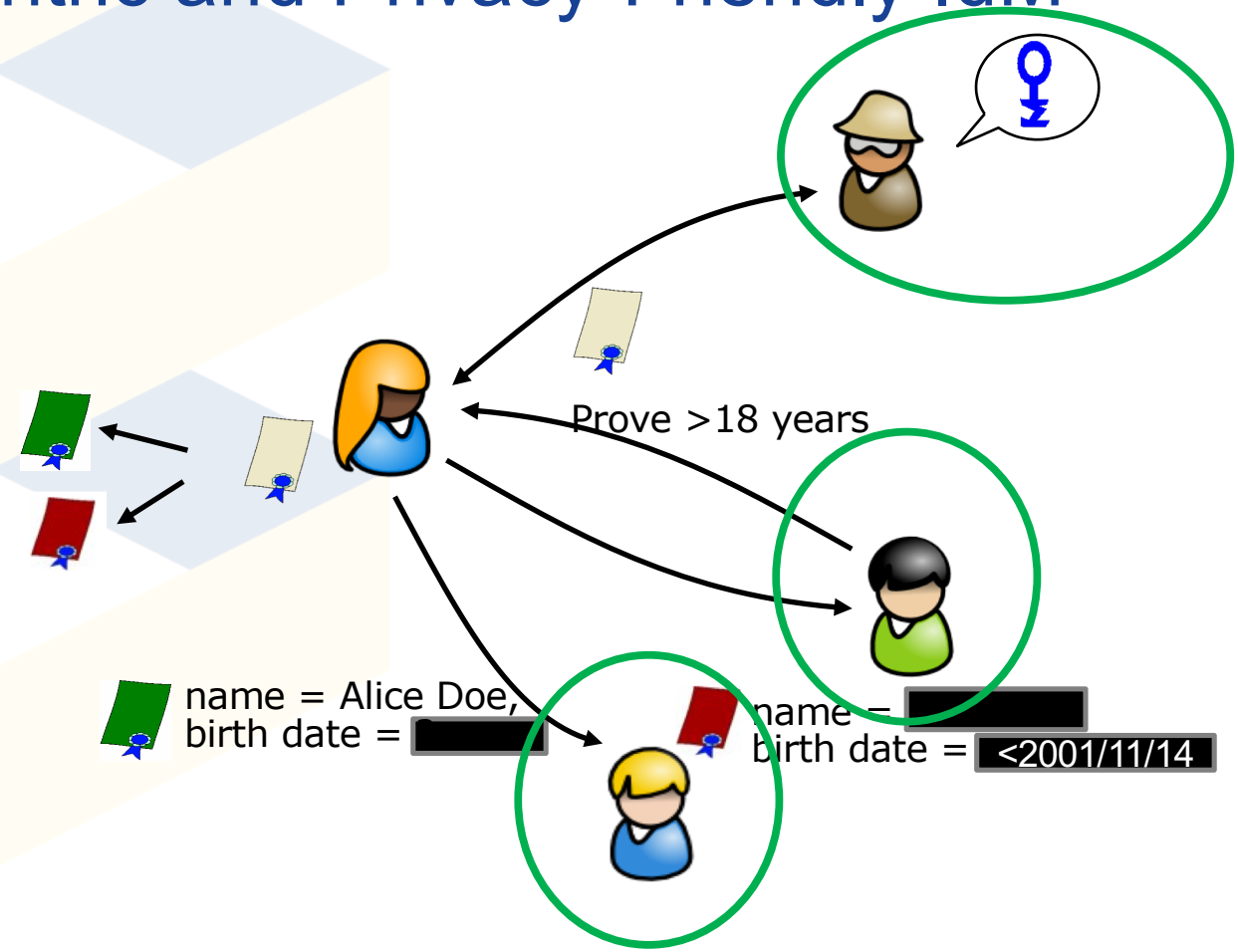


Traditional IdM: Online IdP



User-Centric and Privacy-Friendly IdM

Cyber Security for Europe



Cyber Security for Europe

Thank you!

Stephan Krenn
Austrian Institute of Technology
stephan.krenn@ait.ac.at

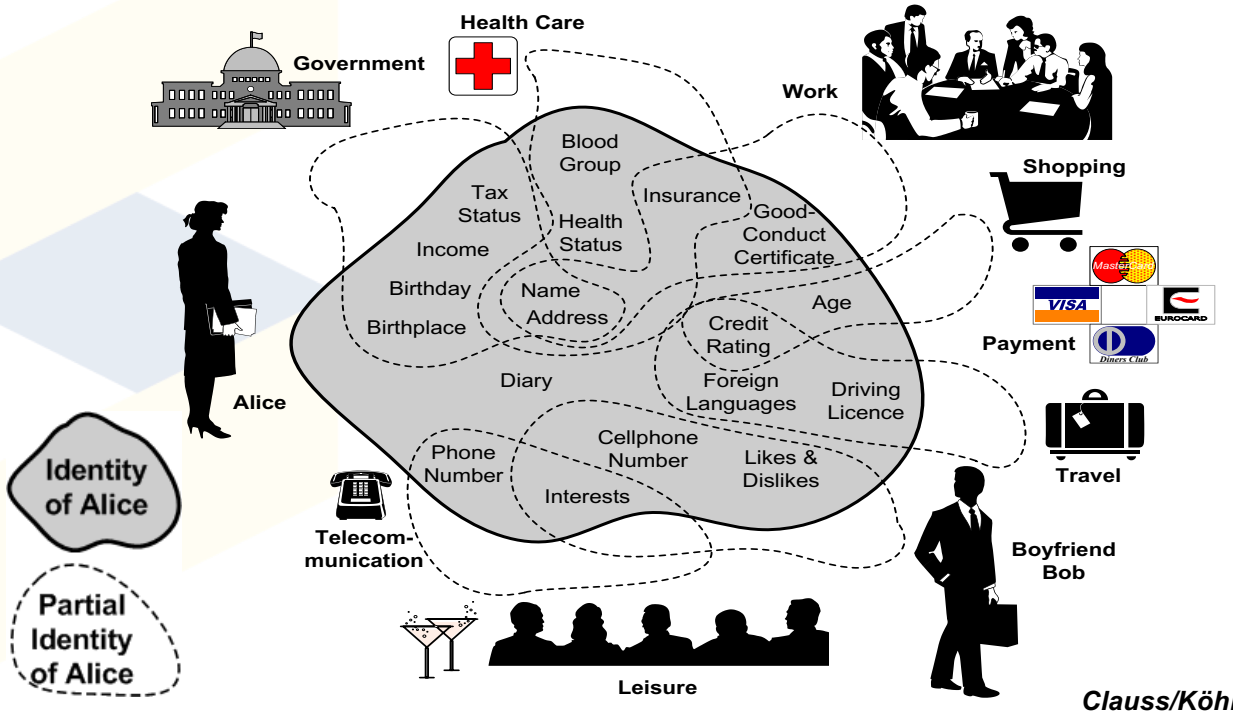
Cyber Security for Europe

Challenges of User-Centric Privacy Preserving IDM

Simone Fischer-Hübner (KAU)

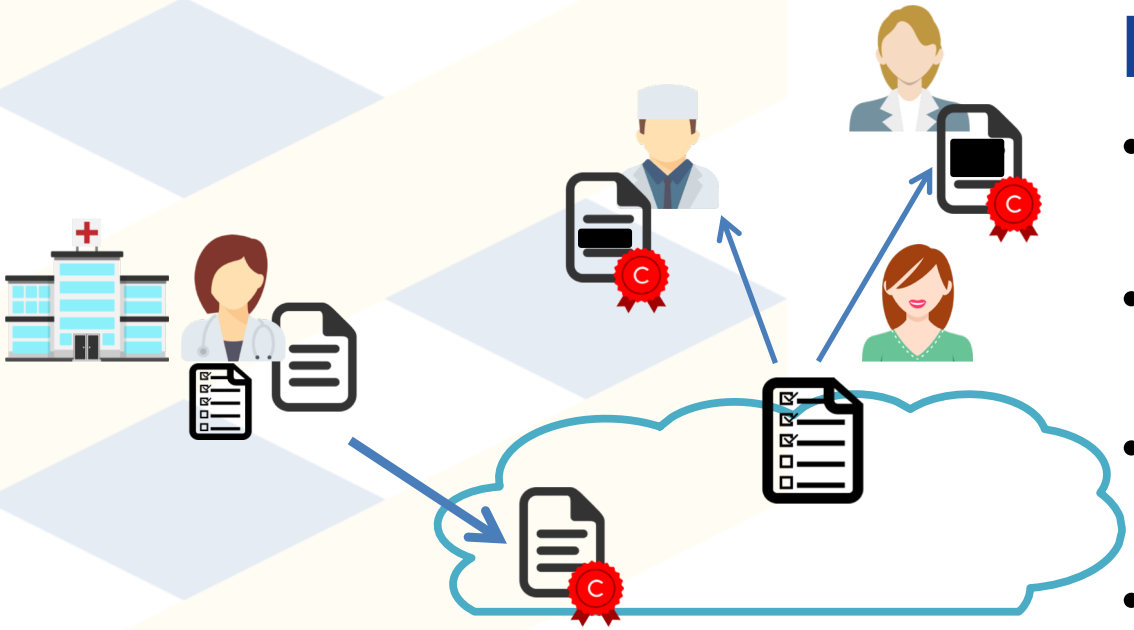
CS4E Conference 2019, Toulouse, 14th November 2019

”Classical” Model of User-centric Privacy-enhancing Identity Management (IDM)



Audience segegration: User reveal different (partial) identities based on their current roles/relationships

Example: PRISMACLOUD – eHealth Use Case (Redactable Medical Documents)

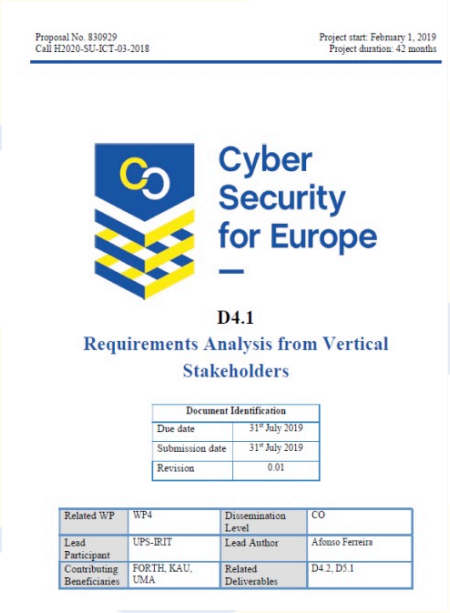


End user challenges:

- Tradeoffs between *Privacy* – *Patient Safety* – *Utility*
- Guidance via redaction templates needed
- Diverse usability and trust issues of different user groups
- Secure & usable key management

AS Alaqra, S Fischer-Hübner, E Framner. "*Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of perspectives by medical professionals and patients*." Journal of medical Internet research 20, no. 12 (2018): e10954.

Key Challenges of privacy-preserving IDM
(identified by stakeholder interviews – CS4E D4.1)


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

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe –

D4.1

Requirements Analysis from Vertical Stakeholders

Document Identification	
Due date	31st July 2019
Submission date	31st July 2019
Revision	0.01

Related WP	WP4	Dissemination Level	CO
Lead Participant	UPS-IRIT	Lead Author	Afonso Ferreira
Contributing Beneficiaries	FORTH, KAU, UMA	Related Deliverables	D4.2, D5.1

- Finding IDM solutions meeting the **all** the following requirements:
  - strong privacy protection
  - Usability
  - no single point of failure or trust

- Do we need a ”simplification” of privacy-preserving IDM needed – by findings simple, suitable tradeoff solutions with ”good enough” privacy?

  (e.g., Cloudflare & Privacy Pass, CREDENTIAL)

Problems to be solved

Cyber Security for Europe

- Finding a usable way to **manage strong authentication keys** for the end users that can be **memorised, incl. secure key backup and recovery**
- Having **good and usable implementations incl. usable configurations** – instead of research solutions of paper
- Evoking correct **mental models** of PETs (“crypto magic”)
- Transparency in regard to **consequences**
- Finding **privacy default settings**
  - Providing Privacy by Default / data minimisation
  - Matching privacy personas
  - Addressing privacy-utility tradeoffs

Cyber
Security
for Europe

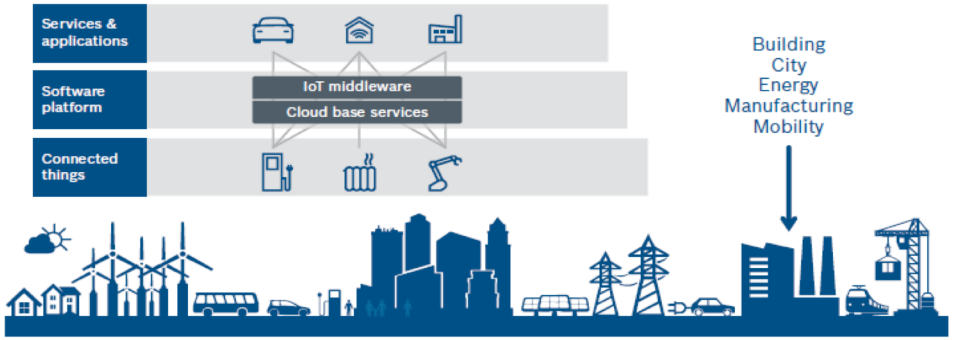
END-TO-END IDENTITY MANAGEMENT

DR. JESUS LUNA GARCIA
ROBERT BOSCH GMBH

BOSCH

Identity Management in a Hyperconnected World
Status Quo and Challenges

- **Digital Transformation is** here, so new disruptive technologies are forcing companies to become more **integrated, flexible and agile**.
  - Being digital is not easy: multiple technologies, complex IT/IoT ecosystems
- The **identity ecosystem** is also part of the digital transformation:
  - "End-to-end" identities: devices, customers, services, IT operators
- **Cybersecurity challenges** in the identity ecosystem include:
  - Integrating threat modelling / risk management into IdM processes
  - Holistic / end-to-end identity management
  - Protecting the "crown (identity) jewels"
- Regulatory aspects:
  - EU Cybersecurity Act
  - **Continuous cybersecurity certification**




Questions?
BOSCH
Parkhaus
Email: jesus.lunagarcia@de.bosch.com
LinkedIn: https://www.linkedin.com/in/jlunagar/
BOSCH

Who is calling? Managing identities in the cyber world

Henrich C. Pöhls (University of Passau)

Who is calling? Managing identities in the cyber world

Henrich C. Pöhls (University of Passau)

SEMIOTICS

Smart End-to-end Massive IoT Interoperability, Connectivity and Security

UNIVERSITÄT PASSAU

Chair of IT-Security
University of Passau,
Germany

@semiotics_eu

@henrichpoehls

What is “identity” technically?

[…] collective aspect of a set of attribute values […] by which a system user or other system entity is recognizable or known. (See: authenticate […]

from RFC 4949

what is “identity” technically?

[…] collective aspect of a set of attribute values […] by which a system user or other system entity is recognizable or known. (See: authenticate […]

from RFC 4949

Networks

e.g. MAC-address

what is “identity” technically?

[…] collective aspect of a set of attribute values […] by which a system user or other system entity is recognizable or known. (See: authenticate […]

from RFC 4949

Networks
e.g. MAC-address

Cryptography
e.g. key-material

What is “identity” technically?

[…] collective aspect of a set of attribute values […] by which a system user or other system entity is recognizable or known. (See: authenticate […]

from RFC 4949

Networks
e.g. MAC-address

Cryptography
e.g. key-material

Users
e.g. locally unique string
“`bedroom_light`”

What is “identity” technically?

[…] collective aspect of a set of attribute values […] by which a system user or other system entity is recognizable or known. (See: authenticate […]

from RFC 4949

Networks
e.g. MAC-address

Cryptography
e.g. key-material

Users
e.g. locally unique string “`bedroom_light`”

Law
e.g. natural/legal person

What does “identity” need to be?

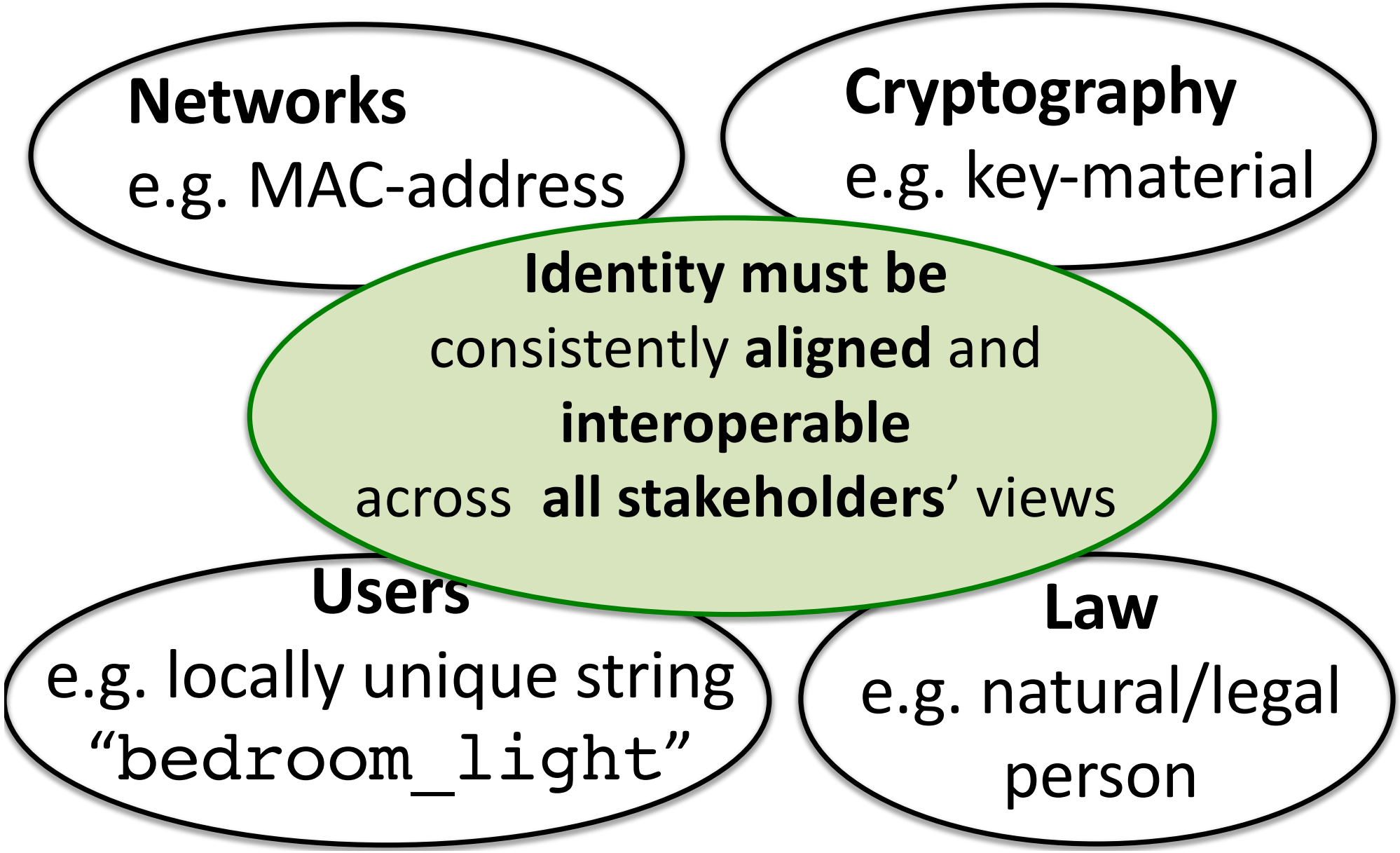
Networks
e.g. MAC-address

Cryptography
e.g. key-material

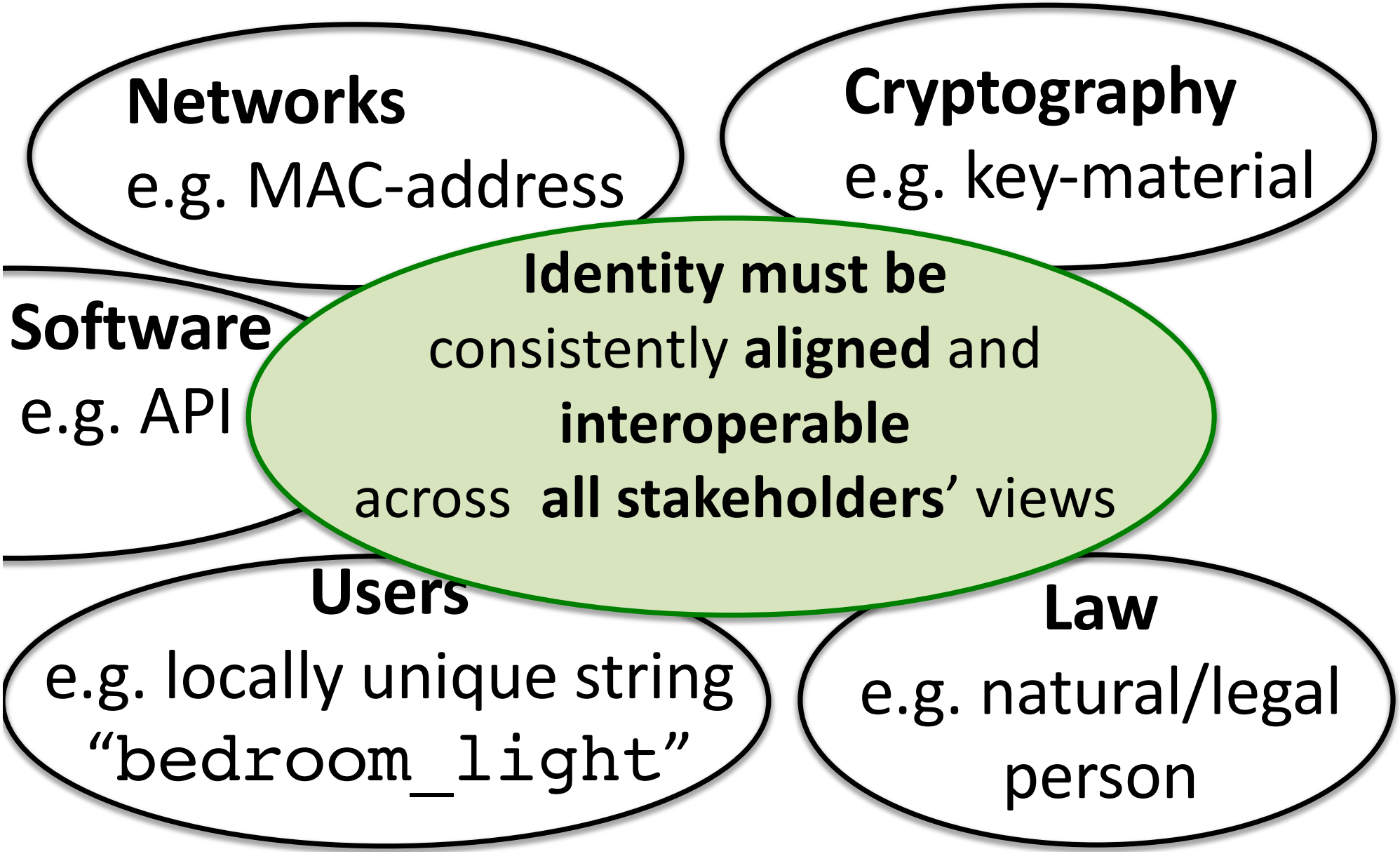
Users
e.g. locally unique string
“`bedroom_light`”

Law
e.g. natural/legal person

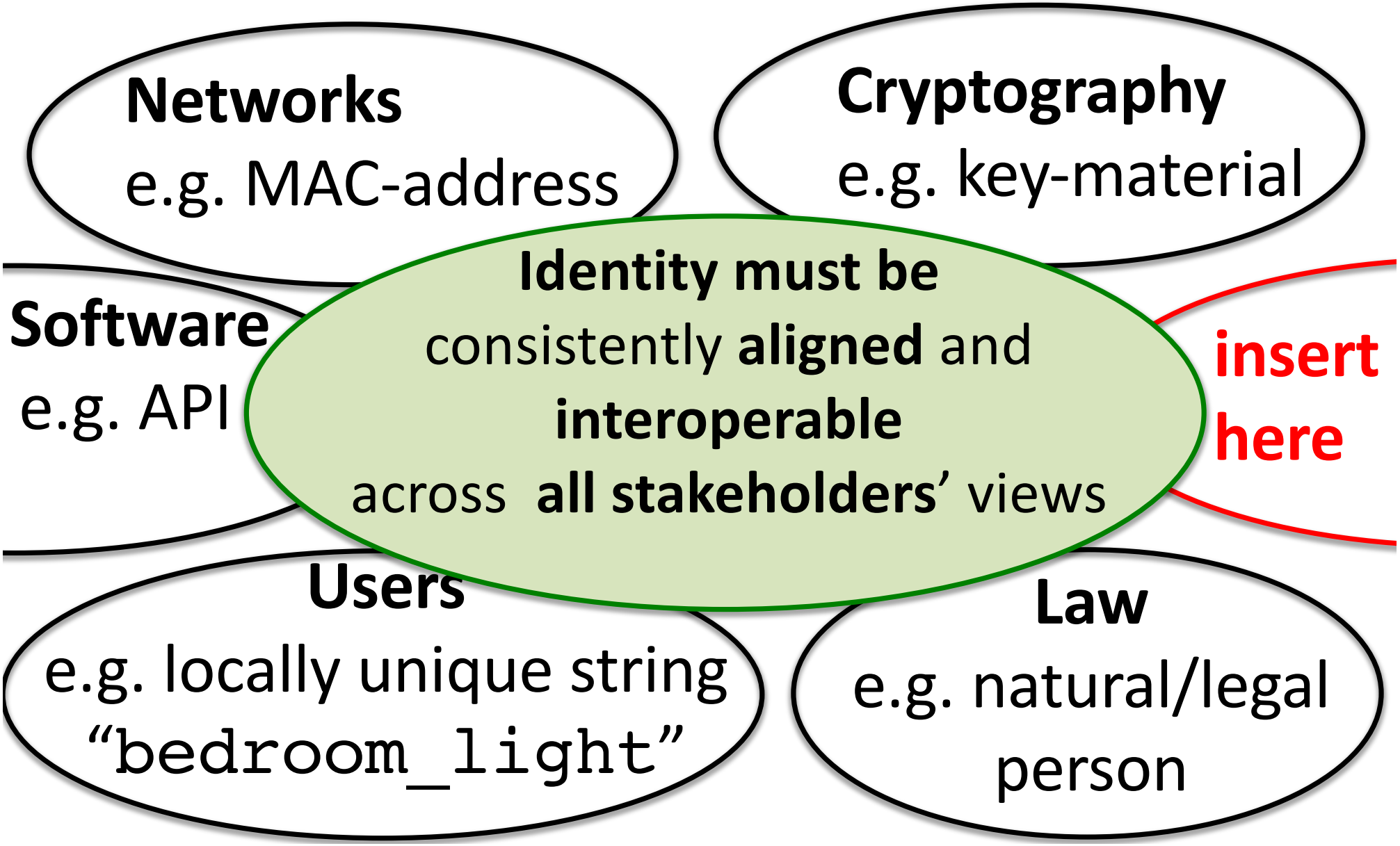
What does “identity” need to be?

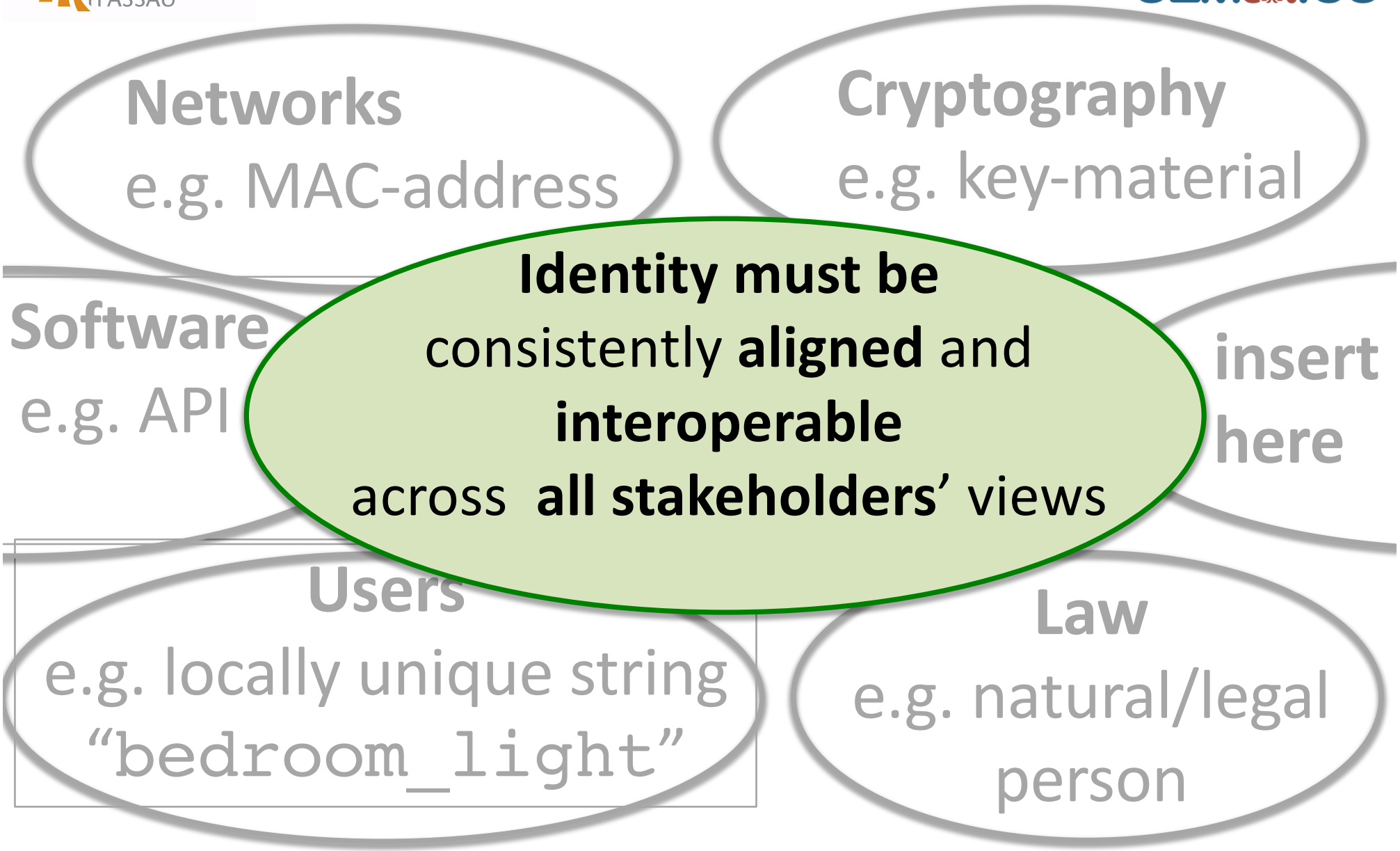


What does “identity” need to be?

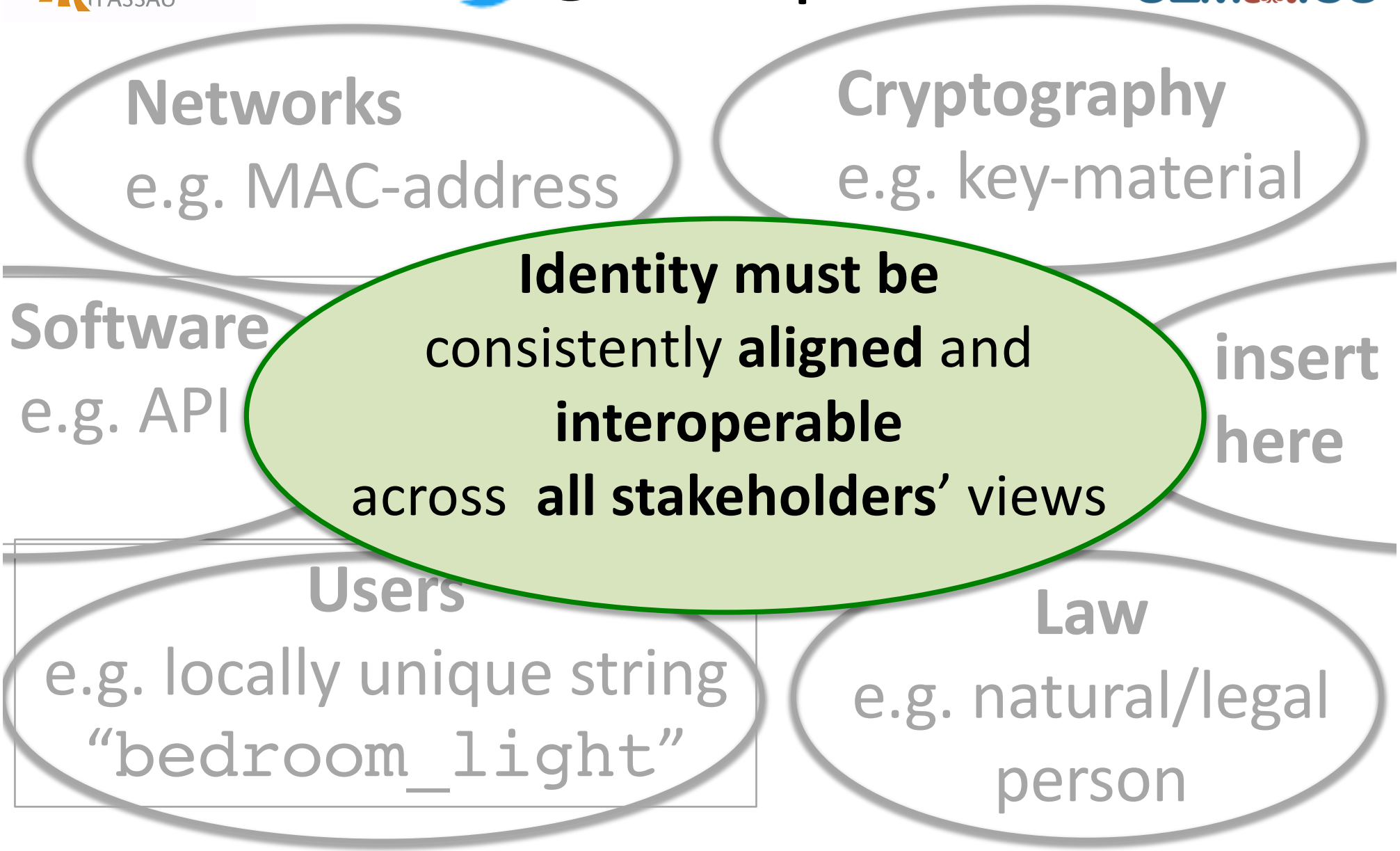


What does “identity” need to be?





Identity is technically interdisciplinary.



Identity is technically interdisciplinary.

Panel: Who is calling? Managing identities in the cyber world

Henrich C. Pöhls (University of Passau)

SEMIOTICS

Smart End-to-end Massive IoT Interoperability, Connectivity and Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 780315

Cyber Security for Europe

Panel 6:
The future of European CyberSecurity
Moderator: Evangelos Markatos

Ensuring the competitiveness of Europe

Enabling European economic growth while protecting European society

What?

Cyber Security for Europe

- Where is CyberSecurity **heading**?
- What do we (i.e. the Research Community) **need to do**?
- What does **Europe need to do**?

Who?

- Afonso Ferreira (IRIT)
- Fabio di Franco (ENISA)
- Fabio Martinelli (CNR)
- Bart Preneel (KUL)

Who: Afonso Ferreira

Cyber Security for Europe

- Afonso Ferreira
  - holds European leadership roles in institutional policy and research,
  - 15 years working in Brussels and in European-related functions,
  - six of which at the European Commission.
  - Afonso has a PhD in Computer Science and is
    - Directeur de Recherche with the French CNRS, where he is the Head of European Affairs for Digital Matters.
- Afonso has a large experience in
  - European foresight in cybersecurity and other digital sectors,
  - having in particular managed for the Commission the project that resulted in the pioneering European Strategic Research Agenda for Cybersecurity in 2015

Who: Fabio Di Franco

Cyber Security for Europe

- Fabio joined ENISA in 2017 and currently his role focuses on advising the European Union and the member states on research needs in cybersecurity with a view of enabling effective responses to the current and emerging threats.
- He is also the Project Manager for supporting the European Member states in cybersecurity skill development, both by identifying the current initiatives and by developing new technical training to support state-of-the-art information network and security capabilities.
- Fabio has a PhD in Telecommunication engineering and he is a Certified Information Systems Security Professional (CISSP).

Who: Fabio Martinelli

Cyber Security for Europe

- Fabio Martinelli is a research director of the Italian National Research Council (CNR).
- His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust.
- He usually manages R&D projects on information and communication security and in particular,
- He has been Project Coordinator of the
  - EU Network on Cyber Security (NeCS) and of the
  - Collaborative information sharing and analytics for cyber protection (C3ISP) project.
- He serves in the Board of the European Cyber Security Organization (ECSO) and as Partnership Director in the SPARTA competence network.

Who: Bart Preneel

Cyber Security for Europe

- Bart Preneel is head of the
  - COSIC research group at the KU Leuven;
- His research interests are
  - cryptography, cybersecurity and privacy.

How?

Cyber Security for Europe

- Each panelist will give a short presentation.
- Then we will have a round of questions

Question 1

Cyber Security for Europe

- How has the field of CyberSecurity changed over the past five years?

Question 2

Cyber Security for Europe

- What is the biggest challenge that Europe faces in the area of CyberSecurity?

Question 3

Cyber Security for Europe

- What will be the biggest cybersecurity problem five years from now?

Question 4

Cyber Security for Europe

- What do we need to change in the funding models we have today?

Question 5

Cyber Security for Europe

- What do we need to do so that Europe will make a difference 10 years from today?

Question 6: Which role do you see for certification in cybersecurity in Europe?

Cyber Security for Europe

Panel 6:
The future of European CyberSecurity
Moderator: Evangelos Markatos

Ensuring the competitiveness of Europe

Enabling European economic growth while protecting European society

Acks - images

- Pixabay
- Publicdomain vectors
- Pxhere

Through the Cristal Ball

Afonso Ferreira

CNRS – IRIT

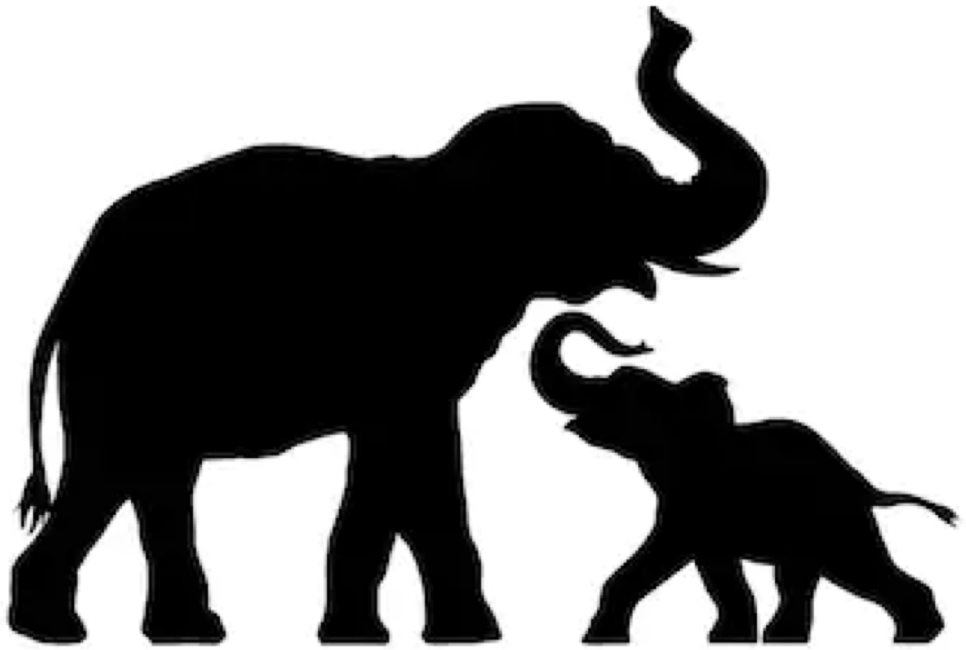
Trends, Trends, and Mega-trends

- AI, blockchain, quantum, IoT, 5G, HPC, Cloud, Fake news, Deep fake, Games, Robots, Autonomous systems, Cyber-Physical systems, Drones, Augmented Reality / Virtual Reality
- GAFAM, Social Engineering, Cyber hygiene, Digital Transformation, Verticals, ICS, Legacy systems, GDPR
- Rogue states, Organised Crime, Hybrid threats
- Geopolitics

Weak signals?

- Digital sovereignty

Black elephants and Low-probability/high-impact events



©

Changes in the landscape

- Attacks on networks: CIA is fine. Currently (ie, yesterday), mainly to exfiltrate data
- But ubiquitous ICT => Using and attacking digital systems to achieve goals – Hybrid attacks
- Infrastructure attacks: Disruption, Breakdown, or even actually Protect (because it’s a necessary medium for the attack vector)
- The digital systems (ICT assisted, ICS, Robots and other autonomous): Command & Control. This is rather like ‘spying’ and infiltrating

Some insights

- Then it seems that Finding and Patching vulnerabilities will continue.
- AI everywhere
- But now: Intelligence and Counter-Intelligence will become more and more important

Complicating factors

- The higher the stakes, the larger the means employed
- Lack of nuclear deterrence

A good thing

- In CyberSec4Europe we’re helping build the future

enisa

THE EU CYBERSECURITY AGENCY

STRATEGIC RESEARCH PRIORITIES IN CYBERSECURITY

Fabio Di Franco, Ph.D.

CyberSec4Europe:
The Future of European CyberSecurity

15 | 11 | 2019

SECURING EUROPE'S INFORMATION SOCIETY

POSITIONING ENISA ACTIVITIES

CAPACITY

- ✓ Hands on activities

POLICY

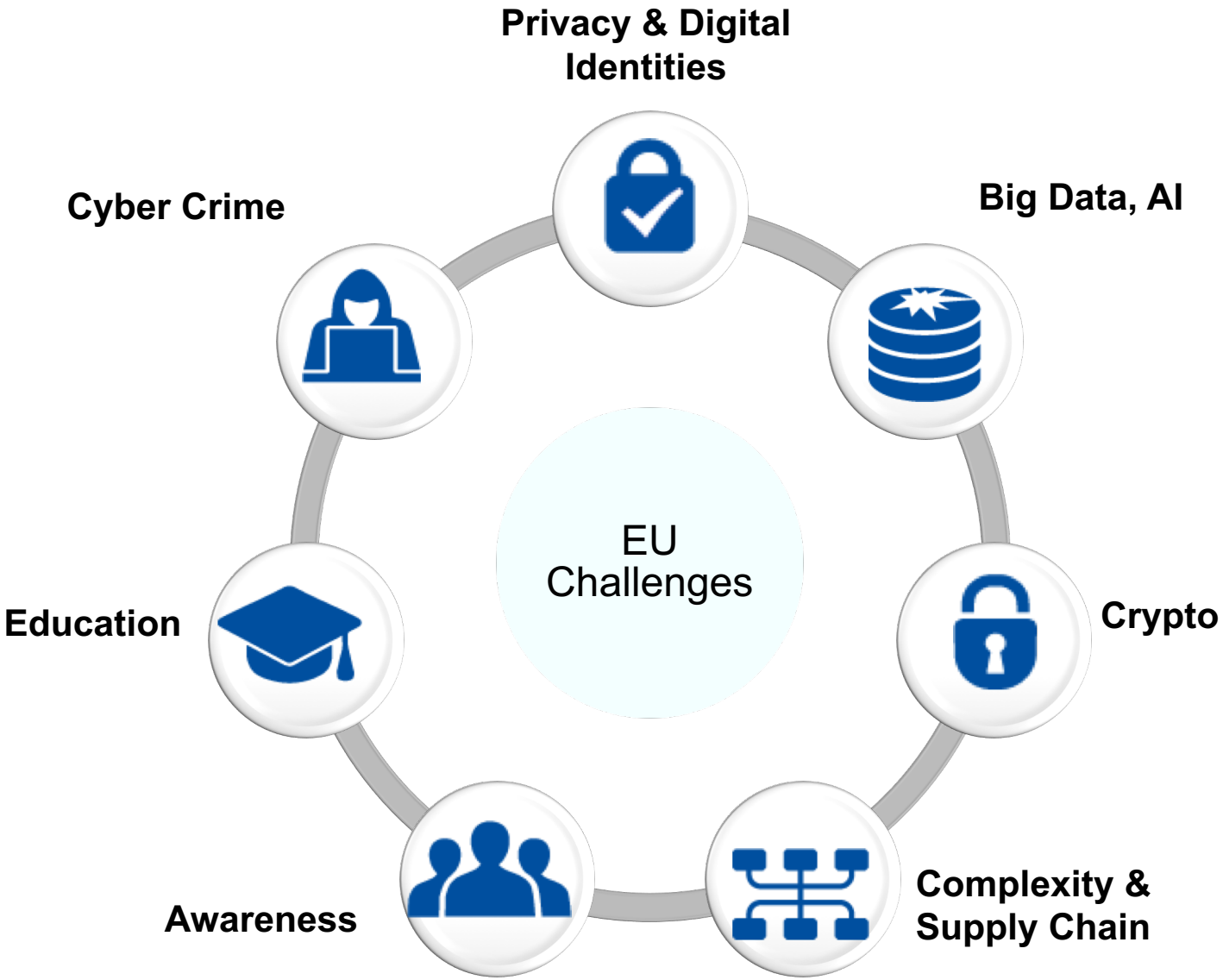
- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice


Privacy & Digital Identities
Big Data, AI
Crypto
Complexity & Supply Chain
Awareness
Education
Cyber Crime
EU Challenges

Education

Capacity Building

Cybersecurity in computing

- Software security is not included in the standard educational programs
- Security and privacy by design are often taught only in specialized courses

Multidisciplinary Approach

Technical, Human, Organizational and Regulatory have different incentives, views, knowledge bases, languages

Simulation and visualization

More exercises and cyber ranges for testing operational and technical skills

Awareness Building -Digital Transformation

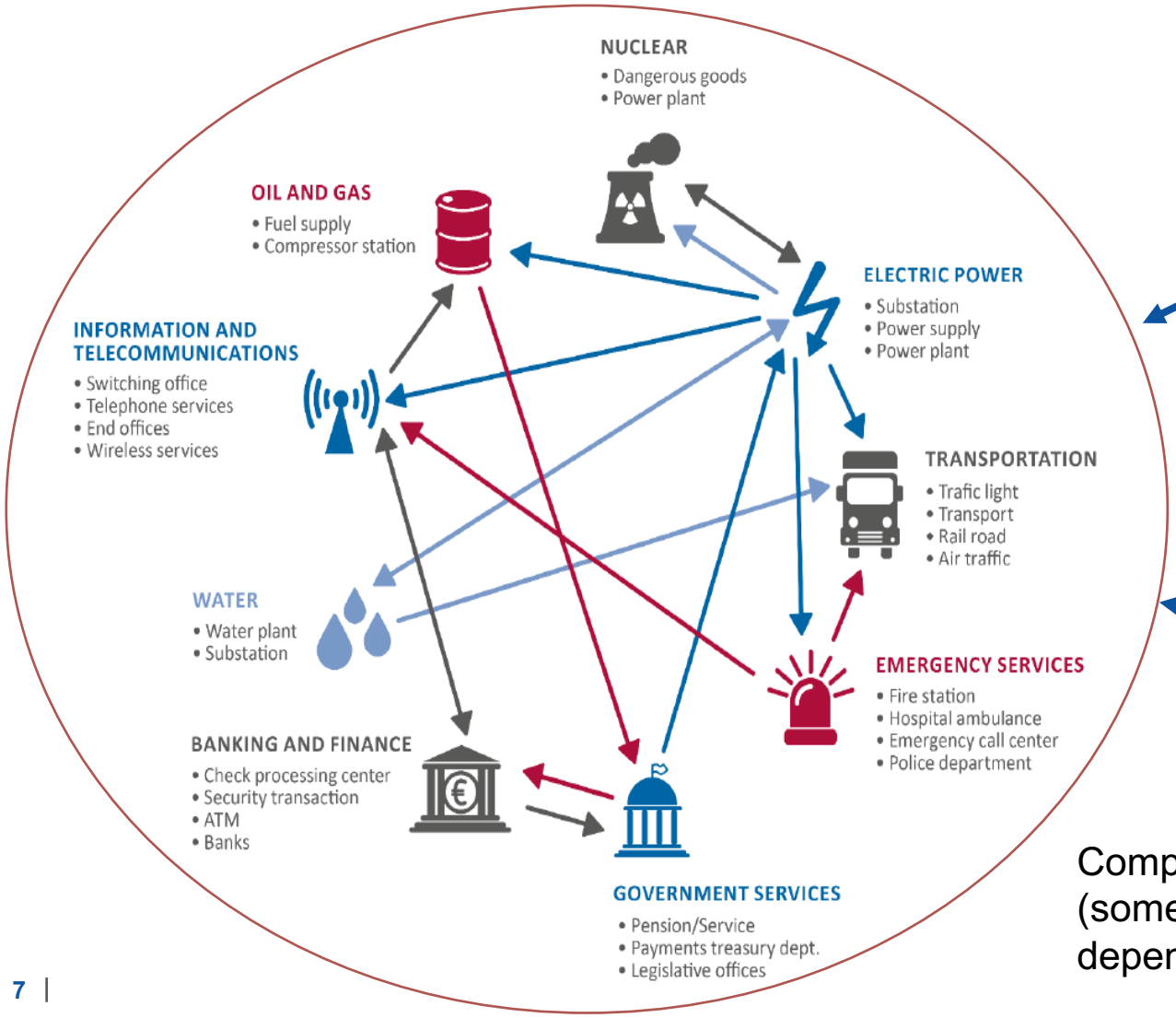
Speed
The digital world is moving too fast for social norms to develop

Everywhere
Digital connected devices are everywhere

Boring
- "I know but I don't care"
  - "It's too boring"
  - "I did not know"

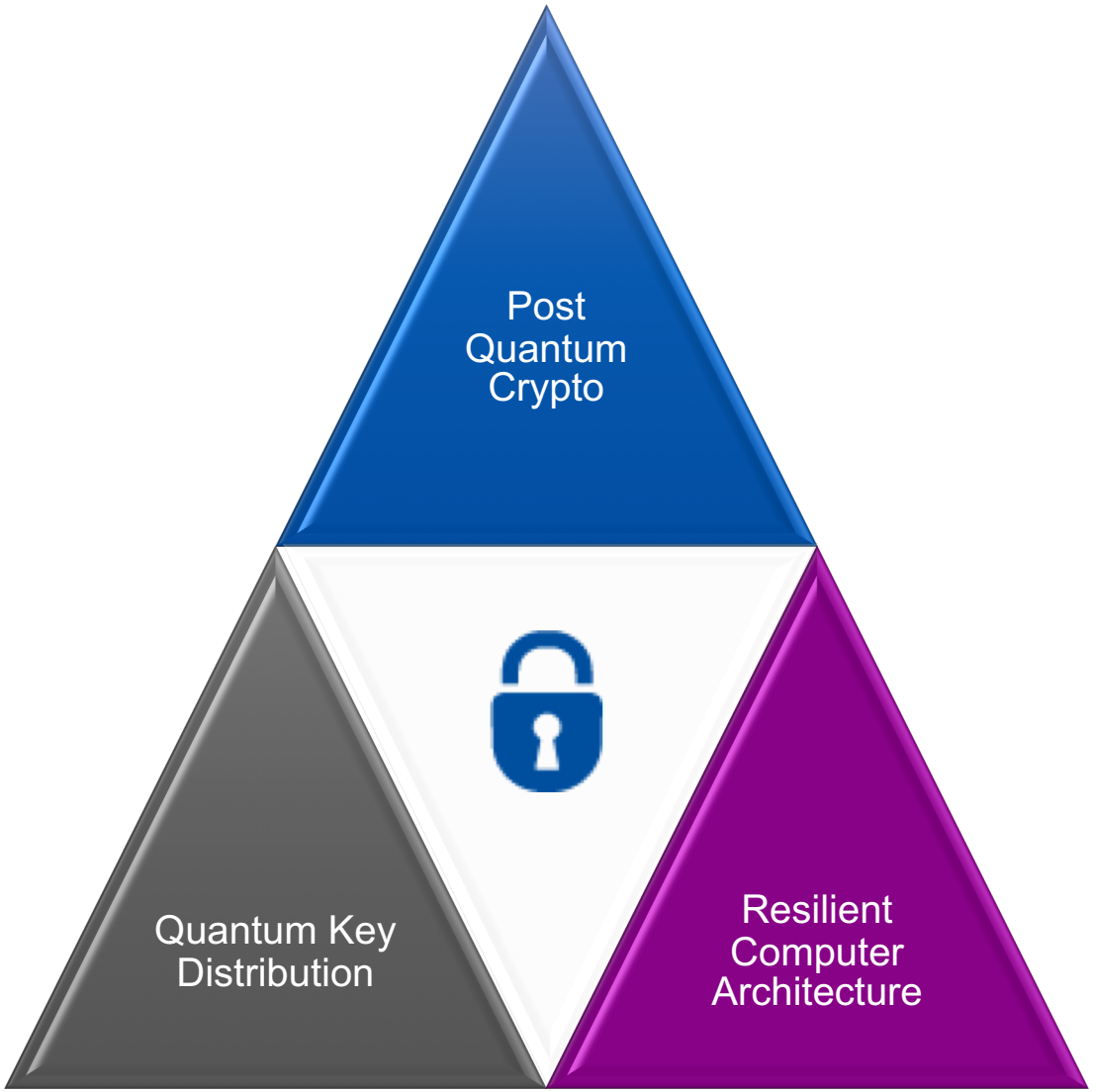
Adaptability
How to manage risks and opportunities for a secure and inclusive digital Europe?

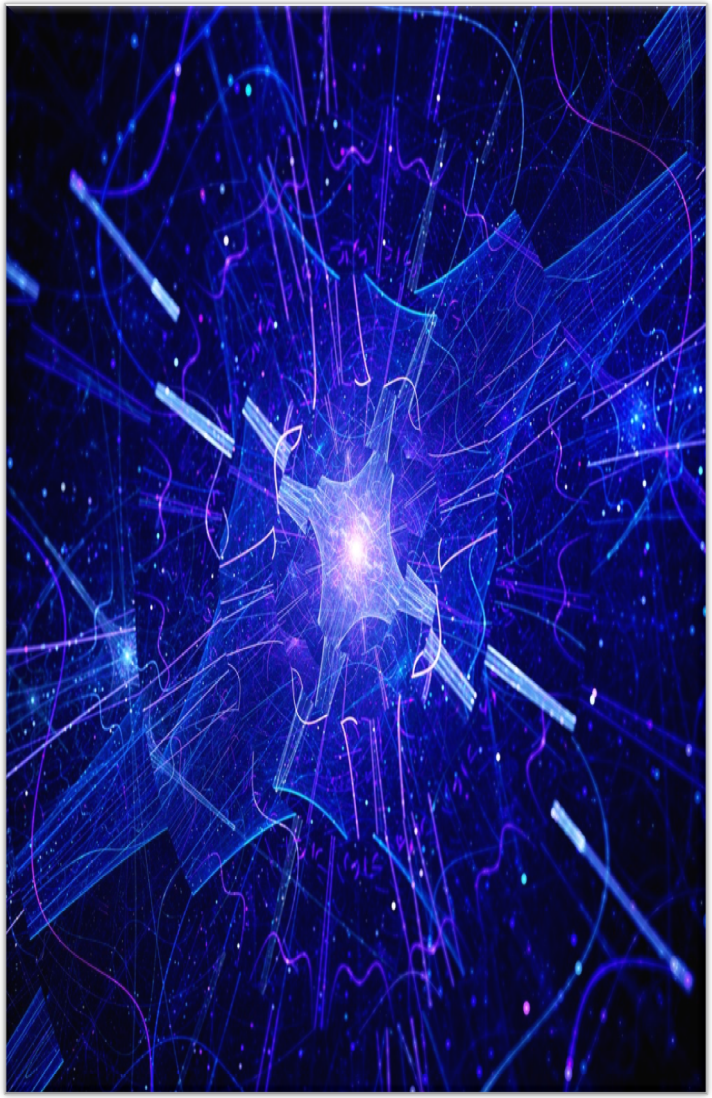
Complexity and Supply chain



Complexity of Service Supply Chains (sometimes second-order dependencies)

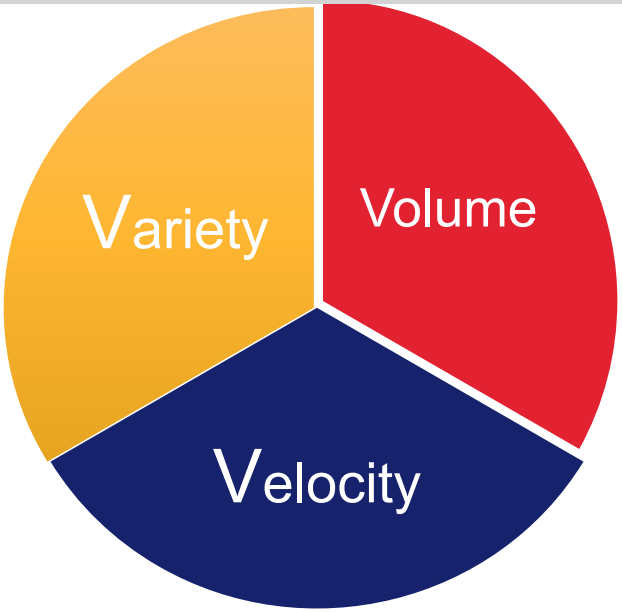
Crypto System in Era of Quantum Computing





Privacy in Big Data & Digital Identities

BIG DATA Characteristics



RISK : electronic surveillance, profiling and disclosure of private data

Privacy-By-Design challenges:

- Efficient Privacy-Preserving Analytics (better if decentralized)
- Support and automation of policy enforcement
- PET in big data

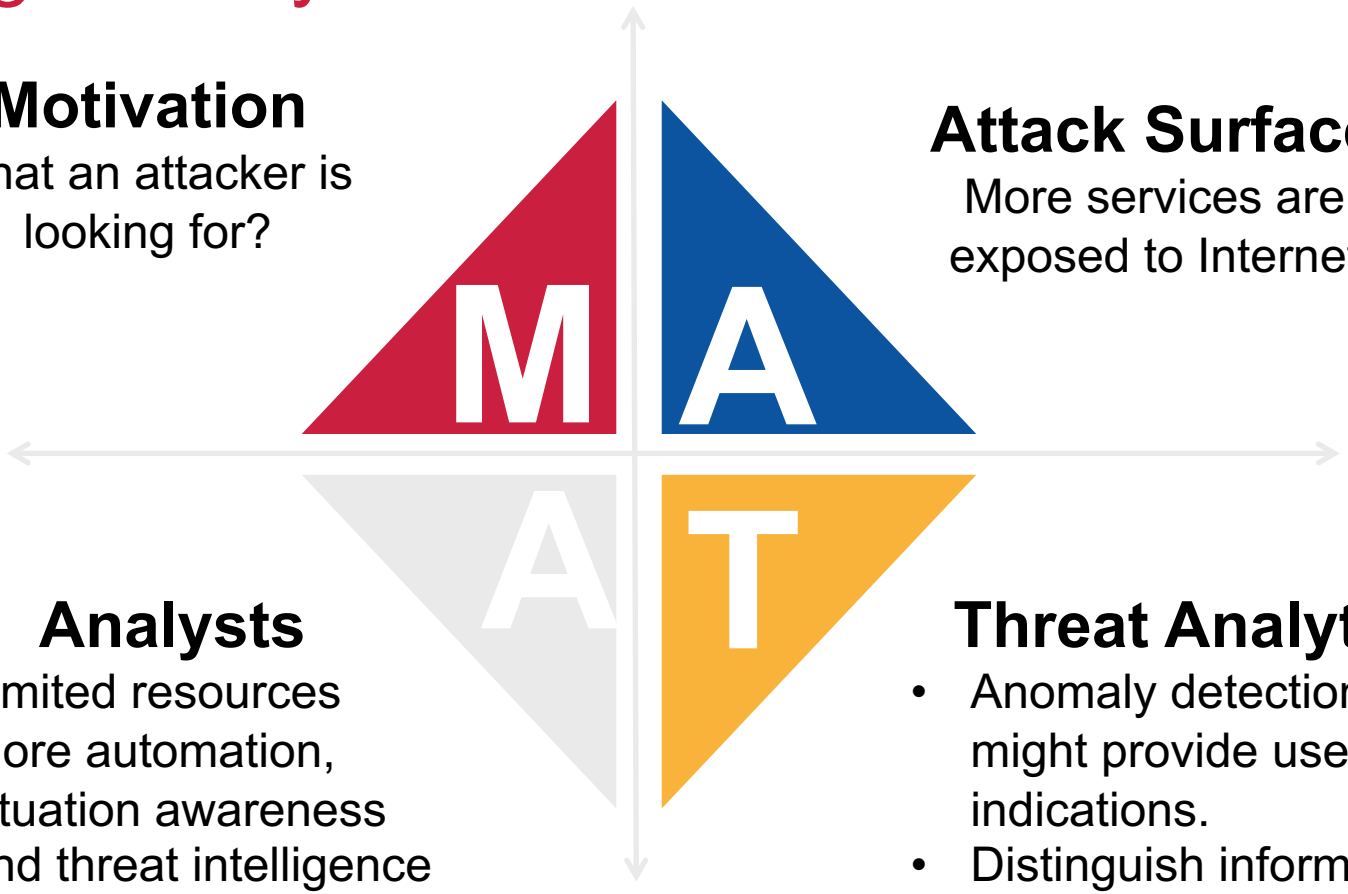
Detection, Mitigation and Response against Cyber Attacks

Motivation

What an attacker is looking for?

Attack Surface

More services are exposed to Internet



Analysts

- Limited resources
- More automation, situation awareness and threat intelligence

Threat Analytics

- Anomaly detection might provide useful indications.
- Distinguish information from noise is still a challenge

AI capabilities & maturity level

AI Capabilities

- SENSE
- COMPREHEND
- ACT
- LEARN

Automated intelligence:
Automation of manual/cognitive and routine/non-routine tasks.

Assisted intelligence:
Helping people to perform tasks faster and better.

Augmented intelligence:
Helping people to make better decisions.

Autonomous intelligence:
Automating decision making processes without human intervention

INTELLIGENCE

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 281 440 9665

fabio.difranco@enisa.europa.eu

www.enisa.Europa.eu

Fabio Martinelli – National Research Council of Italy (CNR)

Outline of presentation:

- Current research topics at CNR
- Some elements of ECSO WG6 SRIA

… and a bit of my taste

Cyber Security @ CNR

- **Cyber-Physical Systems (CPS) Security**
- **Intrusion Detection and Protection**
- **Network Security**
- **Privacy**
- **Access Control and Trust Management**
- **Cyber insurance**
- **Cyber-intelligence on Social Media**
- **Information Sharing and Analytics**
- **Cryptography**
- **Secure Software Engineering**
- **Cloud Security**

ECSO WG6 SRIA elements

Present and future opportunities / challenges

- **Autonomous systems** (cars, trains, drones, delivery, robotics, medical diagnostics)**:** will change our lives and business models
- **Mass transportation** vehicle likely initially more impacted than personal cars
- **Constant monitoring of many aspects of our life**: huge (and sensitive) data storage (local storage becoming obsolete)
- **Self-sustaining mobile devices** (thanks to microelectronics and battery technologies).
- **5G networks** will support growth of mobility and industrial development
- Massive presence of **IoT and IIoT** will impact supply chain and logistics with automatic decisions and real time adaptable**,** but will introduce large “attack surface” to cyber threats and little patching capability
- **Additive manufacturing and 3D printing** enabling to create “everything everywhere”
- Expected **major cyber attacks** to critical infrastructure elements
- Massive **fake news will fundamentally stress democratic** rights and will distort views of reality for citizens (also with the support of social media). “Trust” could become an obsolete word (deep fake).
- **Quantum computers** will break traditional crypto and dramatically increase access to encrypted data: will post-quantum crypto provide some security?
- **Cryptocurrencies** will proliferate (towards digital states).
- High use of **digital twins** (digital replica of a living or non-living physical entity) also as means to secure cyber physical systems
- Citizen science to tackle complex security issues that could be exploited to prevent attacks and make the systems more resilient
- **AI capabilities** will provide a large portion of **decisions about systems, humans and society to be done by algorithms instead of humans.**
- AI will lead to significant **improvement of parts of cyber and physical security provisioning process**. On the other hand, the same development will **empower the attackers and contribute to a great number of novel and extended security threats**

Key Technologies - future basic and disruptive technologies, for the digital society: what future?

Key technologies for the future and their link to cyber security:

- **Artificial Intelligence and cognitive science** (an enabler to anticipate and understand threats, but also a potential cyber weapon)
- **5G and new disruptive communication networks** (a technological, economic and political challenge)
- **Internet of Things and Cyber Physical systems** (tens of thousands of connected objects: how to make them safe?)
- **Blockchain and Distributed Ledger Technologies** (from bitcoin to use in a growing number of applications)
- **Quantum computing and post-quantum cryptography** (a help and a threat to cyber security)
- **Robots and cyborgs** (support to growth or threat, in particular when coupled to AI?)
- **Digital Twins**
- **Biotechnologies and augmented human** (computing, communication, etc.)

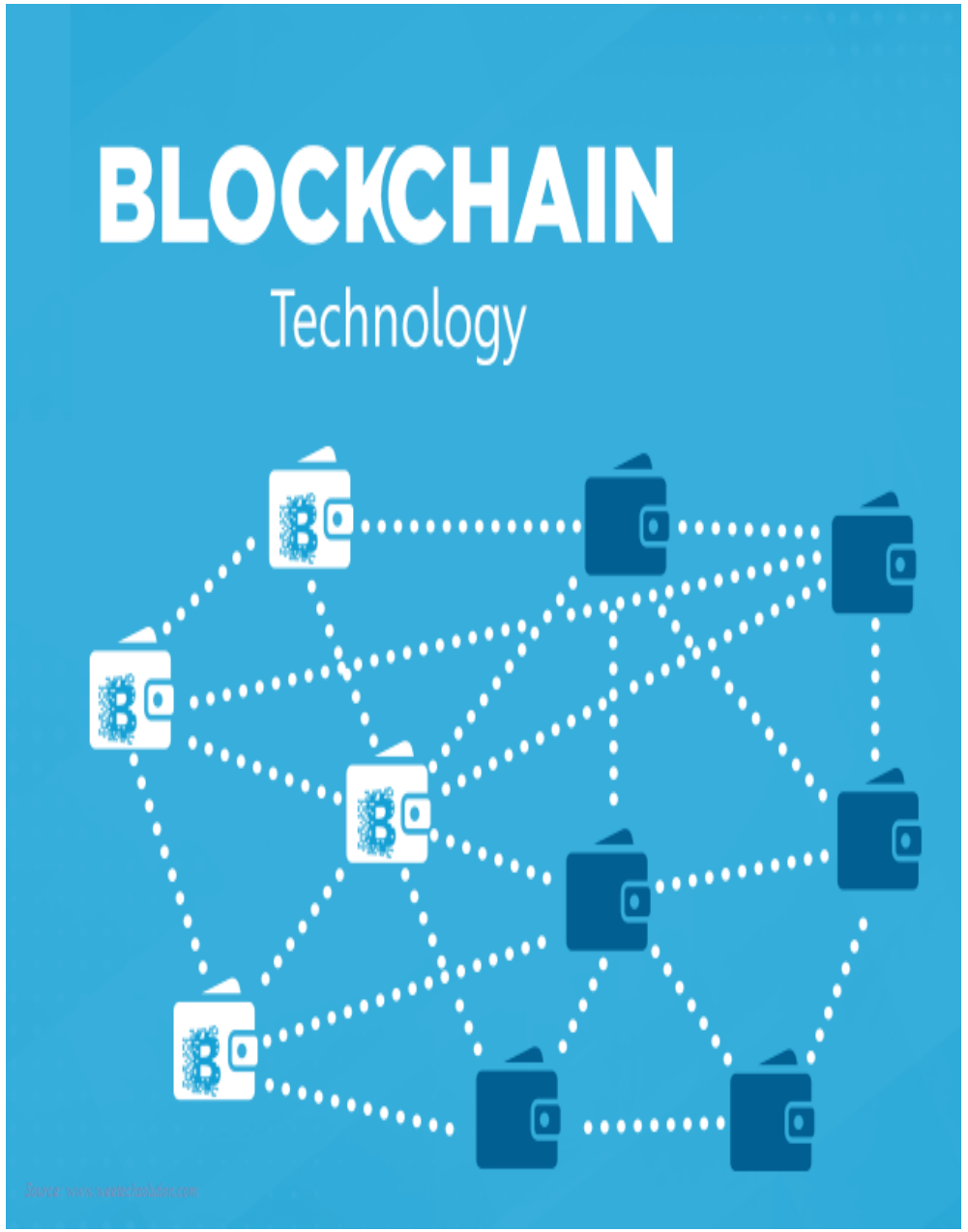
Blockchain

- A Disruptive technology that opens new possibilities for improving many services and even offers the possibility for the creation of new ones and new business models
- Even though the possibilities are enormous, its knowledge and application are still in the preliminary stage. 2 different points of view: Traditional and Disruptive

→ Blockchain as a technology that (i) can solve certain cybersecurity issues and (ii) needs to be properly secured

Some cyber security challenges

- Cryptocurrency economy and cryptojacking
- Data integrity & availability
- Global identity of users and devices
- Security and integrity of software/firmware and log files
- Data sovereignty
- IoT security and blockchain (P2P communication)
- Cyber Threat Intelligence (secure synchronization between different information systems)
- Traceability and transparency of processes



Artificial Intelligence

- A Disruptive technology that is a subfield of computer science and it refers to any technique which enables computer to mimic human brain manifesting intelligence.
- Artificial Intelligence and Cyber security: a tight link:
  - Deep understanding of AI vulnerabilities that may allow an attacker to subvert the output of the system.
  - Artificial intelligence could be used and even be more efficient to attack a system rather than protecting it.
  - AI as a defensive technique

Some cyber security challenges

- Privacy-aware big data analytics/data mining.
- Big data secure storage
- Trust and big data
- Big data analytics and AI for security
- Secure protocols for big data processing
- Provenance of big data
- Protection against internal and external data theft
- Adversarial machine learning
- Explicable AI
- Machine learning for cyber security
- Model cloning (protection of the AI model)
- Ethical and legal aspects (explicable AI for cyber security)

IoT

- IoT is a central element in the global digitalisation trend that is reaching our industry, our economy and our society.
- The key to success is the adequate implementation (secured and trustable) of technical enablers that should be addressed to enable IoT cybersecure deployment: physical devices, connectivity and networking, IoT platforms and services, and IoT applications.

Some cyber security challenges

- At device level
  - Secure execution
  - Firmware and application integrity, and updates delivery.
  - Protection against advanced physical attacks
  - Protection against micro-architectural attacks
  - Secure migration to post-quantum cryptographic algorithms
- Connectivity and network layer
  - Security and privacy of data
  - Transition to edge computing
  - Secure key management
  - Secure routing, cryptography, network level privacy
- IoT platform and IoT service layer
- Application layer and related to end-users Big data analytics and AI for security
- Cross-cutting

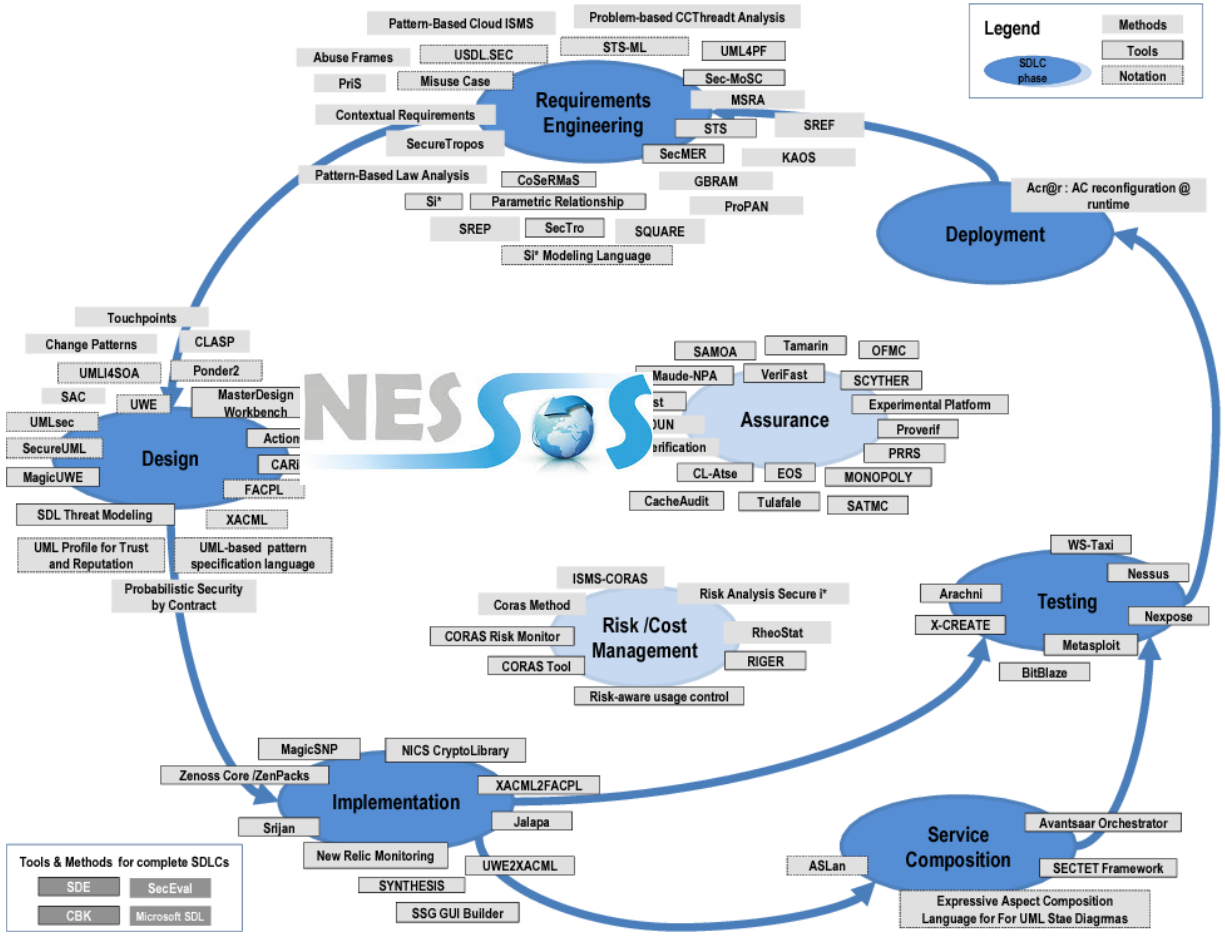
future communication networks (5G)

- High complexity
  - Convergence of IoT, Cloud and 5G at the infrastructure level
  - Convergence of different technologies: Virtualization, Artificial Intelligence, SDN, etc…
  - Serving diverse applications, also critical and strategic services
- Large attack surface (also due to the use of new technologies)
- Risk assessment
- Continuous evolving systems
  - Orchestration of the security needs to be fully integrated with the orchestration of the network
- End to end security, and not only network security!
  - Network and application security coupling
- Multi-tenant and complex access control management
- Need and opportunity for Data Sharing, Data Usage control (including obligations management)
- …

My own taste

Assurance

- Secure system engineering
- Security by design
- Designed for assurance
- Language based security
- Risk and cost analysis also in System Life Cicle
- Management of evolving systems and services
- Interplay of security and safety
- ..



For cyber experts in the next 5 years ….

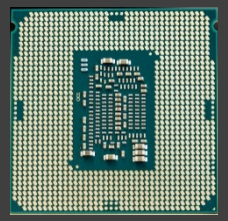
The Future of European Cybersecurity

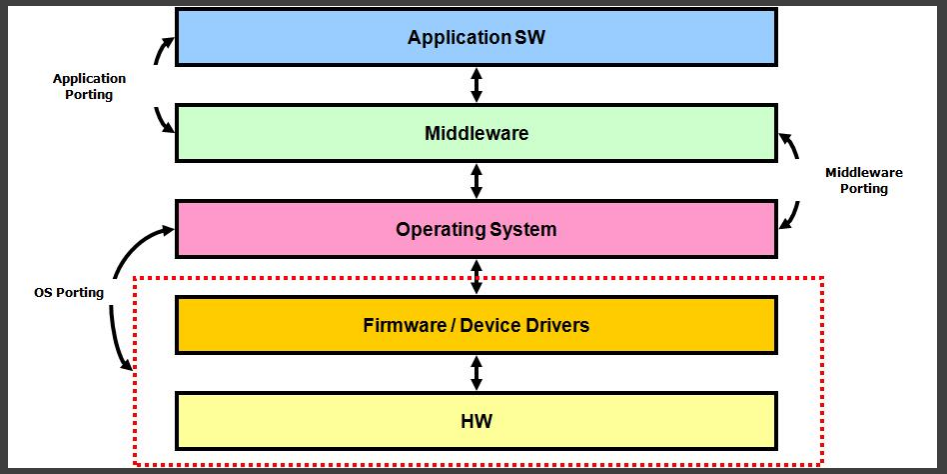
Bart Preneel
COSIC, KU Leuven
firstname.lastname@esat.kuleuven.be
@cosic.be

15 November 2019

Supply chain risk

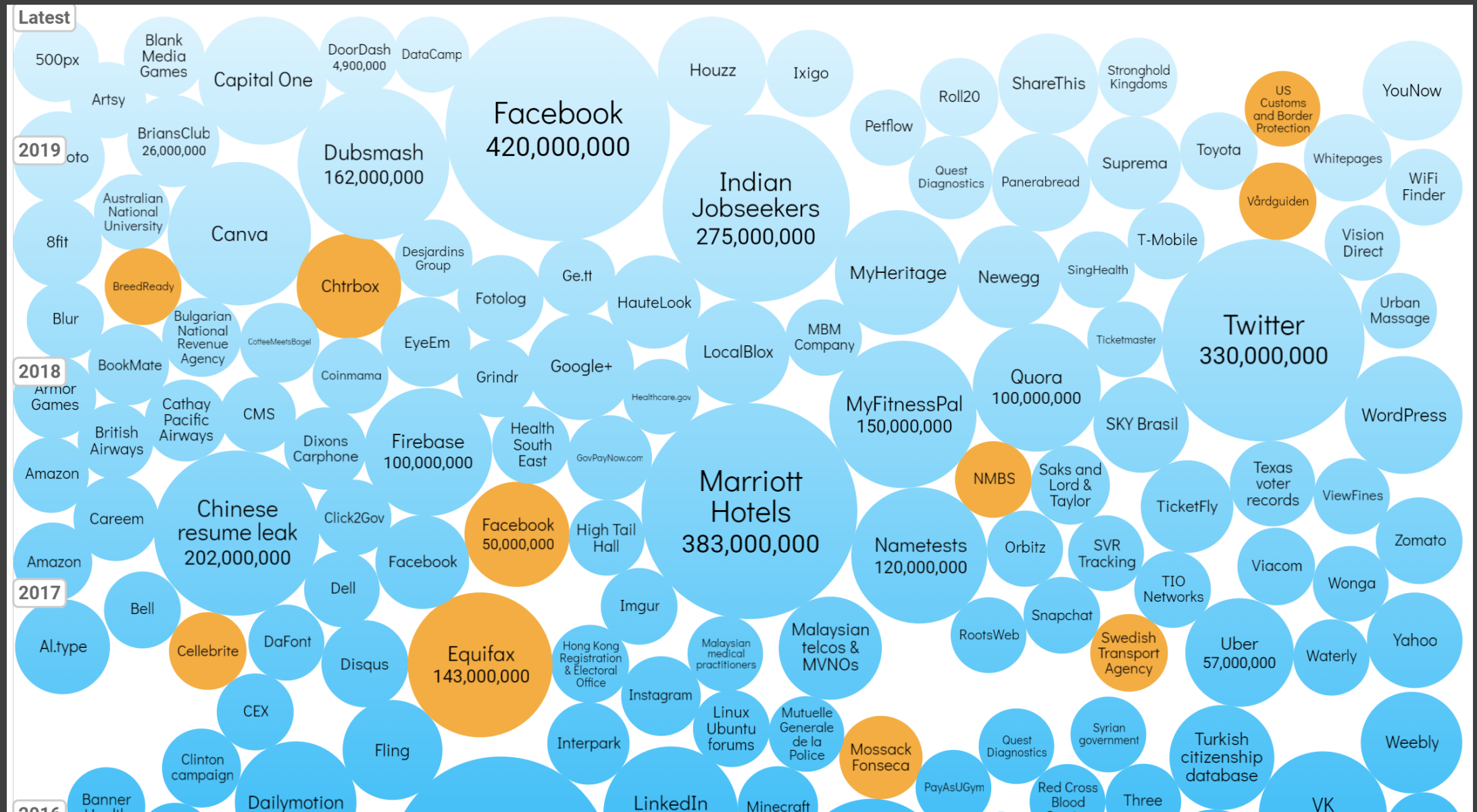
Cybersecurity without sovereignty?



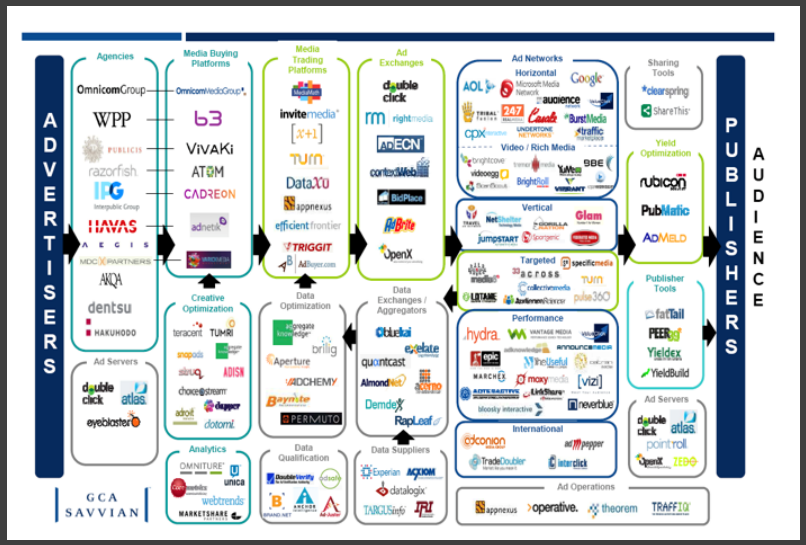


World's biggest data breaches and hacks

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks



Mass surveillance



industry

(surveillance capitalism)

users

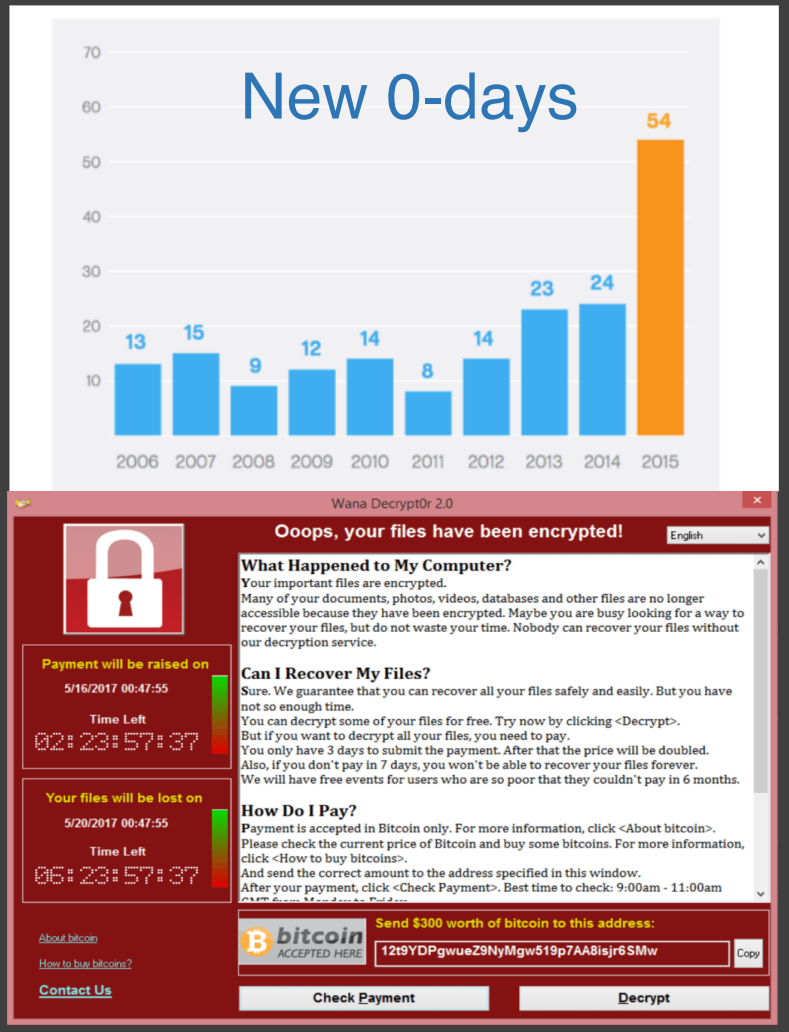
government

Cyberwar: offense trumps defense?

Hoarding of 0-days

Backdoors

0-days stolen by Shadow brokers from Equation Group resulting in Wannacry, Petya, notPetya
US$ 250+ M loss for Maersk



European fragmentation

No EU crypto policy – conflict with member states

No EU crypto competitions - NIST (and the NSA) take decisions

Even algorithms and parameters document is controversial

https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014/

https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf

SWOT

Hardware security

Embedded system security

Verification

Cryptography

Privacy Enhancing Technologies

Distributed systems

Systems research

Strategic research funding (excellence + market)

Venture capital

Fragmented market

Open software and hardware

Verification (not CC)

Distributed architectures for privacy

Diversity

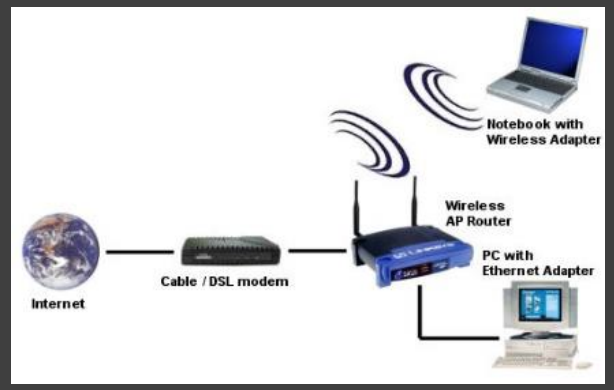
Overall ICT ecosystem

Supply chain

National security

Changing role of cryptography

communications

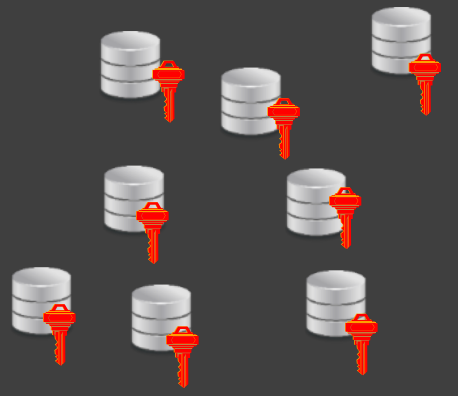


storage

during computation

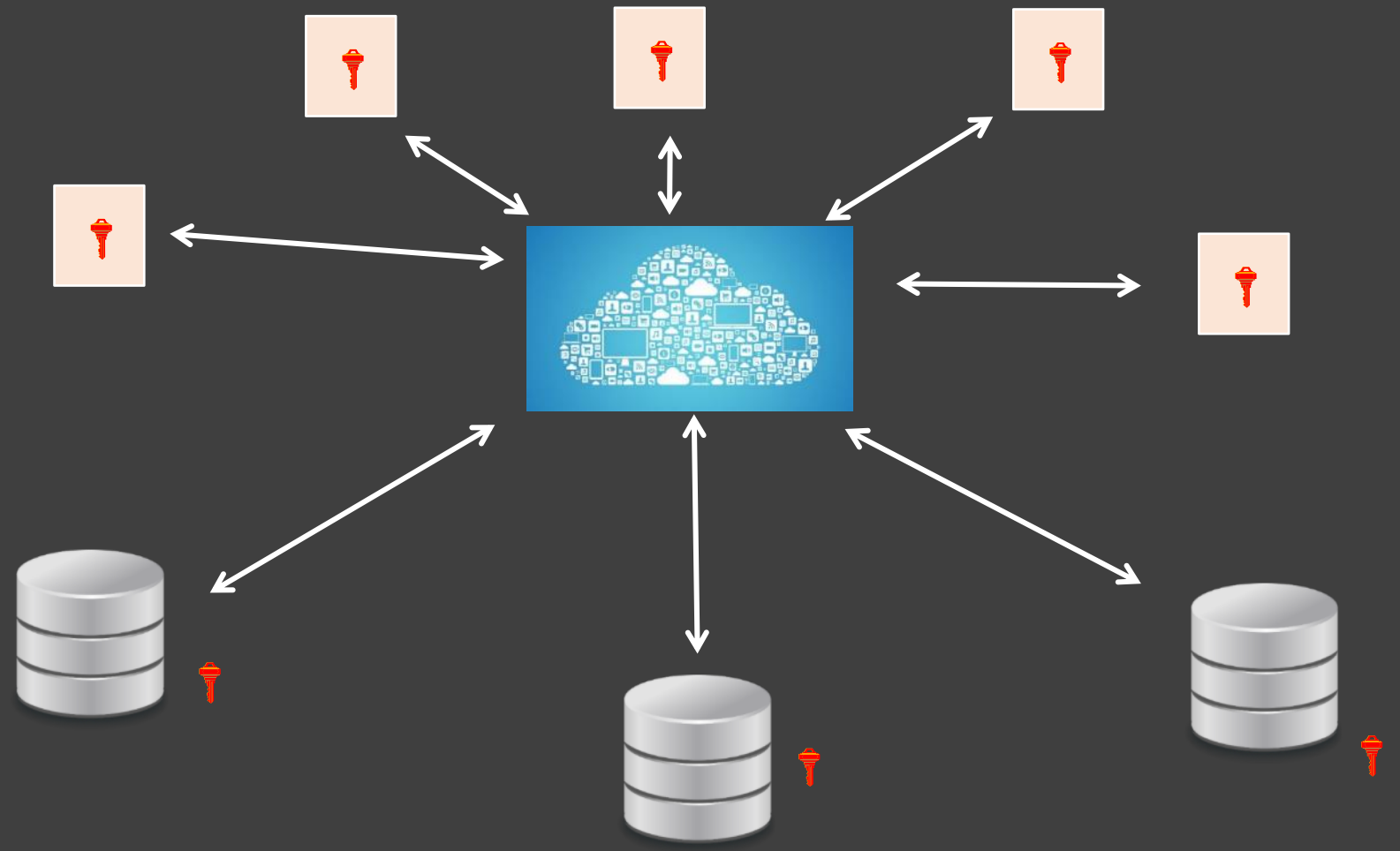
C. Bonte, E. Makri, A. Ardeshirdavani, J. Simm, Y. Moreau, F. Vercauteren, Towards Practical Privacy-Preserving Genome-Wide Association Study, 2017

From Big Data to small local data

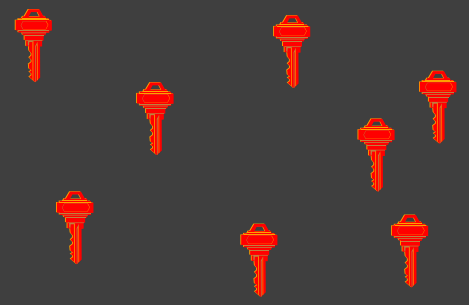


Data stays with users

From Big Data to encrypted data
MPC (Multi-Party Computation)



From Big Data to encrypted data



Local encryption with low multiplication depth

Encrypted data

Can still compute on the data with somewhat Fully Homomorphic Encryption

Architecture is politics [Mitch Kapor'93]

Avoid single point of trust that becomes single point of failure

Open (source) solutions

Effective governance

Transparency for service providers

EU-FOSSA

EU Free and Open Source Software Auditing

Bart Preneel, COSIC, an imec lab at KU Leuven

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: homes.esat.kuleuven.be/~preneel/

EMAIL: Bart.Preneel@esat.kuleuven.be

TWITTER: @CosicBe

TELEPHONE: +32 16 321148

BIOGRAPHIES OF SPEAKERS AND PANELISTS
At CyberSec4Europe Concertation Event 2019

Pascal Andrei, Airbus Senior-Vice-President Chief Security Officer. Biography is found on page 7 of this Annex.

Ana Ayerbe is the Manager of TECNALIA TRUSTECH Business Area where she works in trying to create trust in the digital and hyperconnected world developing technology to reinforce the digital immunological system of companies and society. Member of the Board of Directors of ECSO, RENIC, Permanent Committee of the Basque Cybersecurity Center, WOMEN4CYBER Council and mentor of the INSPIRA STEAM project, in the last year she has been part of the experts committee for the elaboration of the "Spanish National Strategy on Cybersecurity 2019".

Bénédicte Bejm, Head of European Affairs Department at AD'OCC the Economic Agency of the Occitanie Region. Profile in LinkedIn.

Abdelmalek Benzekri is Full Professor at Paul Sabatier University - Toulouse III, Toulouse, France, since 1999, where he is Director of the Master's degree in CyberSecurity. He is the leader of Service IntEgration and netwoRk Administration (SIERA) Research Group. His research activities, conducted at IRIT, focus on systems and networks management and specifically on information security management. He is formally in charge of security research policies at IRIT since 2016.

Médéric Collas, *Responsable de l'innovation au sein du Centre d'Expertise en Sécurité Métier pour le compte du groupe BPCE.* Profile in LinkedIn.

Pierre-Henri Cros is a graduate of Law and Management. Since 2013, he is in charge of scientific prospecting and partnerships at IRIT (Institute in Computer Science of Toulouse). In 1992, he was Deputy Director of CERFACS in charge of administration, finance and valorisation. In 1987, he was Secretary General of CERFACS (European Center in Research and advanced training in High Performance Computing). In 1979, he was Director of the STME which was a non-profit organisation mainly working on study contracts for the European Community. Some other activities of Pierre-Henri:

- 2005 - 2011: In charge of the Innovation, Economy and Society Committee of the Advisory Board (CCRDT) of the Midi-Pyrénées Government,
- Since 2008: President of CUSI which is a think tank that works on how Information Systems impact the development of our economy. This non-profit organization is gathering industrialists, local authorities and Toulouse Universities,
- 2009 – 2013: In charge of the "Access to Government Procurement" Committee of the Advisory Council of Toulouse Metropole,
- Since 2013: Member of the Board of the Advisory Council of Toulouse Metropole.

Caroline De Rubiana is Cybersecurity Project Manager at AD'OCC the Development Agency of Occitania, in the Innovation Department. Caroline's mission is to federate the Cybersecurity regional ecosystem and create a cybersecurity technical center. She studied mathematics and computer science. Before joining AD'OCC, Caroline was an IT manager in an e-commerce SME and, previously, she was an algorithms and programming teacher. Caroline is passionate about Cybersecurity since 10 years and she has organized many meetings and conferences on this subject.

Olivier Dellenbach, CEO at ChapsVision and Founder of eFront SA. Profile in LinkedIn.

Fabio Di Franco joined ENISA in 2017 and currently his role focuses on advising the European Union and the member states on research needs in cybersecurity with a view of enabling effective responses to the current and emerging threats. He is also the Project Manager for supporting the European Member states in cybersecurity skill development, both by identifying the current initiatives and by developing new technical training to support state-of-the-art information network and security capabilities. Fabio has a PhD in Telecommunication engineering and he is a Certified Information Systems Security Professional (CISSP).

Nicholas Ferguson, Digital Communications Strategist & Project Manager. Nicholas has an MSc in Educational Management and a BA Hons in Politics and Sociology. He is the coordinator of cyberwatching.eu the European watch on cybersecurity and privacy; and the EC's Common Dissemination Booster (CDB). Previously, he was the coordinator of the CloudWATCH2 project and deputy coordinator of CloudWATCH, SLA-Ready, SIENA and OGF-Europe. He excels in community engagement & promoting innovative tools and services in the ICT innovation landscape.

Afonso Ferreira holds European leadership roles in institutional policy and research, thanks to 15 years working in Brussels and in European-related functions, six of which at the European Commission. Afonso has a PhD in Computer Science and is Directeur de Recherche with the French CNRS, where he is the Head of European Affairs for Digital Matters. Afonso has a large experience in European foresight in cybersecurity and other digital sectors, having in particular managed for the Commission the project that resulted in the pioneering European Strategic Research Agenda for Cybersecurity in 2015.

Simone Fischer-Hübner holds a Doctor Degree from the Computer Science Department of Hamburg University in 1992. Since June 2000 she is Full Professor at Karlstad University. She has been the Coordinator or Principal investigator for privacy research projects, like PAPAYA (PPlatform for Privacy-Preserving Data Analytics) 2018-2021, Privacy&Us (Privacy & Usability) 2015-2019, Credential (Secure Cloud Identity Wallet) 2015-2018, and PRISMACLOUD (PRIvacy and Security MAintaining Services in the CLOUD) 2015-2018. Additionally, she participates or has participated in different very well-known scientific committees: Swedish Representative for IFIP Technical Committee 11 (Information Security & Privacy), Chair of IFIP Working Group 11.6 (Identity Management), Vice Chair of the Board of IEEE Sweden, Section Computer/Software Engineering Chapter, and Board Member of STINT (The Swedish Foundation for International Cooperation in Research and Higher Education). Furthermore, she also has received a number of awards: Best Paper Award, ACM SAC 2018 – System and Software Security Track, ISD 2017 Conference Best Paper Award, William Winsborough Award by the IFIP Working Group 11.11 on Trust Management in 2016, Google Research Award in 2010 and 2012, and IFIP Silver Core Award in 2001.

Mariya Gabriel, Commissioner for Digital Economy and Society, European Commission. Biography (from ENISA web site) is available on page 8 of this Annex.

Miguel Gonzalez-Sancho - Since July 2018 Head of the Unit "Cybersecurity Technology and Capacity Building" at the European Commission, where he has worked for over 20 years, particularly on policy files, as well research and innovation programmes, focusing on the social and economic impact of digital technologies. His previous responsibilities include Head of Unit for eHealth, Well-Being and Ageing; Head of Unit for Administration and Finance; Deputy Head of Unit for Policy Coordination; Deputy Head of the Unit for Technologies and Social Inclusion, and member of cabinet of a European Commission Vice-President. Miguel holds degrees in law, business administration, international relations and European policies.

David Goodman has over 25 years' experience in senior identity management and security positions in Europe and the United States. He led two prominent pioneering EC-funded identity/security projects while working for IBM, firstly with Lotus in the Notes/Domino product management team and later with Tivoli's security division. He has led several start-ups in the identity space and spent eight years in senior product management roles for telecom providers Apertio, Nokia Siemens Networks and Ericsson. His work has included database and directory services technologies and architecture, meta-directory services, role management and role-based access controls, digital certificates and PKI. More recently he has been engaged in privacy and trust services, cloud services, big data analytics and the Internet of Things. He worked as a technology analyst and consulted with some of the largest companies in Europe and the US and is a Principal Consultant and Analyst with TechVision Research. He has particular insights in the European privacy/regulatory environment, European clients and vendors.

For 13 years David was chairman of EEMA, the leading European identity and security membership association and is currently executive director of OIX (Open Identity Exchange) and senior consultant with TDL (Trust in Digital Life). David, who is based in Scotland, graduated from the University of Manchester and completed a doctorate at Oxford University's Oriental Institute.

Nicole Harris, Head of Trust and Identity Operations at Géant. Profile in LinkedIn.

Liina Kamm is a researcher and Research Project Manager at Cybernetica (an SME in Estonia). She started her professional career designing software for the Estonian Genome Foundation and for cross-border clinical trials. She then focused her research on enabling privacy-preserving statistical analysis for social sciences and genomics. She is Cybernetica's PI for CyberSec4Europe and leads the project's standardisation work package.

Stephan Krenn holds a PhD in computer science from University of Fribourg (Switzerland) in 2012, followed by post-docs at IST Austria and IBM Research – Zurich. He is currently Scientist at the Austrian Institute of Technology (AIT) in the cryptography group. His main research interest is in the cryptographic protocols area, in particular privacy-enhancing technologies such as anonymous authentication. 40+ publications in the field, and actively contributing/editing different ISO standards in the domain of privacy-preserving technologies. Stephan has participated in various FP7/H2020 projects in the domain, such as ABC4Trust, PRISMACLOUD, CREDENTIAL, etc. and within CyberSec4Europe, he leading the demonstrator on privacy-preserving IdM.

Javier Lopez is Full Professor at the University of Malaga and Head of the Network, Information and Computer Security Laboratory (NICS Lab). His research activities focus on network & information security and Critical Information Infrastructures. He is currently Editor-in-Chief of the International Journal of Information Security, and member of the editorial boards of the journals Computers & Security, IET Information Security, IEEE Wireless Communication, Journal of Computer Security, and IEEE Internet of Things Journal, amongst others. Prof. Lopez has been the Spanish representative at IFIP Technical Committee 11 Security and Protection in Information Processing Systems from 2003 to 2018.

Jesus Luna joined Robert Bosch GmbH in 2016, and currently is member of the central security governance team based in Stuttgart, Germany. His main responsibilities include leading topics related to cloud security governance, and cloud security automation. Furthermore, Jesus represents Bosch in working groups of the European Commission and US NIST related to cloud security certification. Jesus has worked on the ICT security field since 1995 with industry and academia, both in America and Europe. Jesus obtained his PhD degree (Cum-Laude) in Computer Architecture from the Technical University of Catalonia (2008, Spain), has participated in several ISO and NIST security standards, and has co-authored more than 50 peer-reviewed publications. Among Jesus' previous roles are EMEA Research Director of

the Cloud Security Alliance (U.K.), team lead in cloud security at Barcelona Digital (Spain), and fellow researcher at the Foundation for Research and Technology (Greece). His professional interests include security automation, and security for cloud and IoT.

Evangelos Markatos is a Professor of Computer Science at the University of Crete. He received his diploma in Computer Engineering from the University of Patras and the MSc and PhD in Computer Science from the University of Rochester. He is the founding head of the Distributed Computing Systems Lab at FORTH-ICS where he conducts research in the broader area of computer systems with a special emphasis in Network Security and Privacy. He is the Coordinator (i) of the PROTASIS Marie Sklodowska-Curie project dealing with Security and Privacy for the IoT (http://www.protasis.eu/) and (ii) of the REACT project that deals with secure software. He has been a member of the permanent stakeholders group of ENISA (European Network and Information Security Agency) and he is now a member of the Academic Advisory Network of Europol's EC3 (European Cybercrime Center). He has served (i) as the founding coordinator of SysSec: The European Network of Excellence in Threats and Vulnerabilities for the Future Internet, consisting of 8 partners and more than 70 associated partners funded in part by the European Commission, (ii) as the coordinator of the NoAH project which installed one of the largest academic Network of honeypots in Europe, and (iii) as the founding member of SENTER: The European Network of the National Centers of Excellence in Cybercrime Research Training and Education. Prof. Markatos has co-authored more than 150 publications in top conferences and journals including ACM SOSP, IEEE HPCA, ACM/IEEE ToN, IEEE JSAC, USENIX Security, INFOCOM, etc. According to Google Scholar his work has received more than 7,000 citations with an h-index of 42.

Fabio Martinelli is a Research Director of the Italian National Research Council (CNR). His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He usually manages R&D projects on information and communication security and in particular, He has been Project Coordinator of the EU Network on Cyber Security (NeCS) and of the Collaborative information sharing and analytics for cyber protection (C3ISP) project. He serves in the Board of the European Cyber Security Organization (ECSO) and as Partnership Director in the SPARTA competence network.

Mark Miller is the Founder and CEO of CONCEPTIVITY, he has over 30 years of experience in defence, security, information technology and international supply chain security issues. He is the Vice Chairman of the European Organisation for Security (EOS) as well a Member of the Board of Directors of the European Cyber Security Organisation (ECSO). He is a graduate of the Massachusetts Institute of Technology (MIT) holding a degree from the MIT Electrical Engineering and Computer Science Department as well as an MBA from the International Institute for Management Development (IMD). He has competed certificates in 10 areas as a cybersecurity expert under the US DHS (FEMA) covering broad aspects such as policy, legislation, regulation, ethics, white-collar crime, planning, prevention, mitigation, and forensics. He is also a designated expert in the-ERNCIP Smart Grids and Industrial Control Systems Expert Group (under the EC JRC) addressing cyber security issues in the industrial and smart grids context. He also was an important contributor to the development of the European Security Label concept. Mr. Miller is also a designated cybersecurity expert with EC-3 (IoT) at EUROPOL.

Edgardo Montes de Oca graduated both as a Computer and Electronics engineer in 1985 from Paris XI, Orsay and DEA in Computers from Paris VI, Jussieu in 1986. He started out as CEO of Plurar, a company offering software development and database mining services. He then worked as research engineer and project leader in Euriware, Alcatel Research centre in Marcoussis and in Ericsson's Research centre in Massy. In 2004, he founded MONTIMAGE selected as Success Story by the French Systematic cluster, and is currently its CEO. His main interests are cyber threat intelligence; designing innovative tools to test and monitor applications and telecommunication protocol exchanges; and, the development of software

solutions with strong performance and security requirements. He also has very good experience in managing companies and associations, acting as Value-Added Reseller, and particularly in setting up national/international collaborations (research and public tenders). He has created startups in France, Spain and The Netherlands. He has published more than 40 papers and book chapters, and is or has been member of several program committees. He is board member of Networld 2020 and the French cluster Systematic's Telecom Pilot Committee. He has been leader in several Europena projects and is currently leader of the dissemination and exploitation activities in the INSPIRE-5Gplus H2020 project.

Bertrand Monthubert, *Président & Conseiller Régional d'Occitanie*. Profile in LinkedIn.

Aljosa Pasic's current position is Technology Transfer Director in Atos Research & Innovation (ARI), based in Madrid, Spain. He graduated Information Technology at Electro technical Faculty of Technical University Eindhoven, The Netherlands, and has been working for Cap Gemini (Utrecht, The Netherlands) until the end of 1998. In 1999 he moved to Sema Group (now part of Atos) where he occupied different positions. During this period, he was participating in more than 70 international research, innovation or consulting projects in the areas of information security. He collaborates regularly with various international organisations and has been frequent speaker at major international conferences. Currently, he works in several EU projects, such as CONCORDIA or Cybersecurity4Europe.

Henrich C. Pöhls received his PhD. from University of Passau for his work interdisciplinary at the intersection of applied cryptography and law. His research currently focuses on practical applications of advanced cryptography to foster the exchange of authentic data while upholding data-minimisation for increased privacy and legal compliance. He has authored and co-authored many academic publications, especially on the topic of tailoring cryptographic signature primitives for legally compliant applications in various domains, like supply chain, Internet-of-Things, and the cloud. He is keen on interdisciplinary work especially in the field of cryptography, software development and law, as he thinks the more gaps between those three worlds can be bridged the more sound (=safe, secure and legally compliant) ICT-enhanced products and environments like smarthomes or smartcities become. He also holds a graduate diploma in computer science (Dipl. Inf.) from the University of Hamburg and an M.Sc. in Information Security from Royal Holloway University of London. He currently works in the EU-funded SEMIoTICS project to enhance the security and privacy of large of IoT deployments.

Bart Preneel is Head of the COSIC Research Group at the KU Leuven; his research interests are cryptography, cybersecurity and privacy.

Kai Rannenberg - Chair of Mobile Business & Multilateral Security (www.m-chair.de) at GUF. Visiting Professor National Institute for Informatics (Tokyo, Japan) since 2012. Chair CEPIS (www.cepis.org) Legal & Security Issues Special Interest Network since 2003. Since 2015 Vice President IFIP (www.ifip.org). Since 2007 Convenor ISO/IEC JTC 1/SC 27/WG 5 "Identity management & privacy technologies". 2004-2013 academic expert in the Management Board of EU Network and Information Security Agency, ENISA; since 2013 member of ENISA's Permanent Stakeholder Group. 1999-2002 with Microsoft Research Cambridge focussing on Personal Security Devices & Privacy Technologies".

Kai has been coordinating several leading EU research projects, e.g. the Network of Excellence "Future of Identity in the Information Society (FIDIS)" and the Integrated Project "Attribute based Credentials for Trust" (ABC4Trust). Currently he is coordinating CyberSec4Europe, a pilot for the European Cybersecurity Competence Network the EU is aiming for.

Kai's research interests include:

- Mobile and embedded systems and Multilateral Security in e.g. M-Business, LBS, transport systems, and industrial applications
- Privacy and identity management, especially attribute based authorisation
- Communication infrastructures and devices, e.g. personal security assistants and services;
- Security and privacy standardisation, evaluation, and certification.

Luigi Rebuffi is the Secretary General and founder of ECSO (European Cyber Security Organisation). After having graduated in Nuclear Engineering at the Politecnico di Milano (Italy), he worked in Germany on the development of high power microwave systems for the next thermonuclear fusion reactor (ITER). He continued his career at Thomson CSF / Thales in France where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, scientific, and became, in 2003, Director for European Affairs for the civilian activities of the Group. In 2007, He suggested the creation of the European Organisation for Security (EOS) and coordinated its establishment, being for 10 years its CEO. In 2016 he contribute to the creation and was the founder of ECSO, signing with the European Commission the cPPP on cybersecurity. Until 2016 and for 6 years, he has been an advisor to the European Commission for the EU Security Research Programme and President of the Steering Board of the French ANR for security research.

Valerio Senni (UTRC), holds a Ph.D. in Applied Formal Methods and has more than 10 years of industrial and academic research experience after the PhD. He has been actively involved in several EU funded projects, including FP7 ASCENS, FP7 QUANTICOL, FP7 DANSE, CleanSky2 MISSION, where he served as technical contributor, task leader and acting Scientific and Technical Manager (DANSE). He is currently a Staff Research Scientist at UTRC, Principal Investigator in Formal Methods, Model-based Design and Cyber Security projects, and Lead of Cyber Security research area. He is currently working on model-based risk assessment methods and tools, and formal methods for automated vulnerability assessment.

Antonio Skarmeta received an M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and a Ph.D. degrees in Computer Science from the University of Murcia, Spain. Since 2009, he is Full Professor at the same department and University. Antonio F. Skarmeta has worked on different research projects in the national and international area in the networking, security and IoT area. He now coordinates the H2020 project IoTCrawler focusing on IoT advanced discovery on IPv6 networks and OLYMPUS on privacy preserving IdM. His main interested is in the integration of IPv6, security services, identity, IoT and Smart Cities. He has been head of the research group ANTS since its creation in 1995. Currently, he is also Advisor to the Vice-Rector of Research of the University of Murcia for International projects and Head of the International Research Project Office. Since 2014, he is the Spanish National Representative for the MSCA within H2020. He has published over 200 international papers and is a member of several program committees. He has also participated in several standardization fora like IETF, ISO and ETSI and being nominated as IPv6 Forum Fellow. He is also CTO of the spinoff company Odin Solution S.L. (OdinS) in the area of IoT and Smart Infrastructure.

Renaud Vedel, *Préfét coordonnateur ministériel en matière d'intelligence artificiel chez Ministère de l'Intérieur*. Profile in LinkedIn.

AIRBUS

Biography

Dr. Pascal Andrei

Airbus Senior-Vice-President Chief Security Officer

Pascal ANDREI has a French state PhD degree in Competitive Intelligence & Security from Paris University after a Mathematics and Physics Masters.

He started his career at AEROSPATIALE in 1992 as head of Competitive Intelligence before leading e-business activities in Munich for EADS headquarters.

He created and led Aircraft Security within Airbus before becoming Chief Product Security Officer and Executive Expert for all Airbus divisions overseeing all Airbus products (aircraft, helicopters, satellites, launchers…).

Pascal ANDREI is currently **Airbus SVP Chief Security Officer**, leading all Security activities globally for Airbus companywide.

He plays a very active role in international cooperative efforts to guarantee the overall (Cyber and Physical) security of the commercial aviation industry infrastructure. For this contribution, he was nominated personality of the year in 2015 by the Air Transportation System Security community in Dubaï.

He is a reservist of the “GIGN” the elite police tactical unit of the French National Gendarmerie and was decorated Knight of the Legion d’Honneur in 2017.

(Source: Downloaded from ENISA web site on 24.02.2020
https://ec.europa.eu/commission/commissioners/sites/comm-cwt2019/files/maryia_gabriel-cv_1.pdf)

European Commission

Mariya Gabriel

Bulgarian nationality

First Vice-President of the European People's Party (EPP)
November 2019 – present

European Commissioner for Digital Economy and Society
2017-present

Member of the European Parliament, EPP/GERB (Citizens for European development of Bulgaria)
2009-2017

Vice-President of the EPP Group in the European Parliament
2014-2017

Vice-President of the EPP Women
2012-present

Parliamentary secretary to MEPs from GERB political party within the EPP Group
2008-2009

Research Assistant, Institute of Political Sciences, Bordeaux (France)
2004-2008

ATER (Attaché Temporaire d'enseignement et de Recherche), Institute of Political Science, Bordeaux
2004-2007

Master in Comparative Politics and International Relations Academy for Political Science, Bordeaux
2002-2003

Certificate in Political Science, IEP Institute for Political Studies, Bordeaux
2001-2002

BA in Bulgarian and French Languages, Paisii Hilendarski Plovdiv University, Bulgaria
1997-2001