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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D10.3
Concertation Conference Year 3

Document Identification	
Due date	2022.12.22
Submission date	12 January 2023
Revision	1.0

Related WP	WP10	Dissemination Level	CO
Lead Participant	CONCEPT	Lead Author	Mark Miller (CONCEPT) / Victoria Menezes Miller (CONCEPT)
Contributing Beneficiaries	GUF, FORTH, UMU, UMA, UPS-IRIT	Related Deliverables	D10.1, D10.2

Abstract:

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.

This deliverable is intended to capture the key discussions and messages resulting from the last CyberSec4Europe Concertation Event (entitled "CONVERGENCE NEXT") held in hybrid format in Brussels from 1-3 June 2022. In addition, the document also includes a summary of collaboration activities undertaken by CyberSec4Europe project partners over the second year of the project.

Significant results have been achieved during the course of this CyberSec4Europe project and the conclusions and recommendations section is clearly addressing challenges both current and in the future. The intent of this deliverable is to document the final concertation event, document the key collaboration and engagement activities undertaken by the CyberSec4Europe consortium partners during this final period and to provide conclusions and recommendations that point toward areas to be addressed in 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

The third CyberSec4Europe Concertation Event was held in Brussels from 1-3 June 2022 (with the generous support of the Representation of the State of Hessen to the European Institutions). This third CyberSec4Europe Concertation Event was the second and last event for the Joint Pilots (CONCORDIA, CyberSec4Europe, ECHO and SPARTA).

The event was given the title "**CONVERGENCE – NEXT**" to represent the Four Pilots "converging" together being multiple "lanes" on one road. The objective of this last event was to highlight and focus on the future of the community, the European Cybersecurity Competence Centre (ECCC) and look at the key issues for cybersecurity in the future

The first chapter of this deliverable D10.3 covers the community engagement activities of the CyberSec4Europe partners during the period from January 2021 – September 2022. This represents a significant effort in achieving the cooperation, engagement and integration orientation of the CyberSec4Europe project within the cybersecurity landscape in Europe. Furthermore, it demonstrates the direct connection that CyberSec4Europe has in the cybersecurity ecosystem both in Europe and globally.

The second chapter of this deliverable D10.3 summarizes the CONVERGENCE NEXT event and the key elements from each session. Further details (including presentations, short biographies) can be found in the Annexes.

Finally, the last chapter of the deliverable summarizes the conclusions and recommendations from CONVERGENCE NEXT, with a focus upon the future. Every session could be done differently, and it was up to the session organiser to decide on the format and content (speech, panel, demonstrations, conclusions/recommendations) with the fellow panellists. Thus, the structure of every session was different and is reported herein as such.

In conclusion and in essence, the underlying goal of what we are trying to achieve in Europe is Digital Sovereignty with a core of cooperation and collaboration in Europe. CONVERGENCE NEXT is a clear demonstration of the current successful efforts in the European cybersecurity ecosystem and cybersecurity community in order to achieve this goal.

Table 1 below provides a brief summary of the chapters of this deliverable.

Chapter	Title
Chapter 1	Provides a summary of collaboration activities undertaken by CyberSec4Europe project partners over the second year of the project
Chapter 2	Provides a summary of the Four Pilot CONCERTATION NEXT event
Chapter 3	Summarises the conclusions and recommendations

Table 1: Summary of Chapters

Document information

Contributors

Name	Partner
M. Miller/V. Menezes Miller	CONCEPT
A.Skarmeta	UMU
E. Evangelos	FORTH
N. Kadenko	TUD
N. Arastouei	GUF
A. Niknia	GUF
W. Tesfay	GUF
S. Pape	GUF
P. Hamm	GUF
L. Kamm	CYBER
D. Preuveneers	KUL
A. Lluch Lafuente	DTU
L. Colombini	Intesa Sanpaolo
S. Viddor	UNITN
S. Krenn	AIT
J. Carlos Perez Baun/A. Pasic	ATOS
C. Budde	UNITN
C. Fernandez Gago	UMA
R. Tordi	ABI
A. Sforzin	NEC
C. Grigoriadis	UPRC
D. Goodman	TDL
C. Jamieson	TDL
G. Rodosek	CONCORDIA
I. Buntic-Ogor	CONCORDIA
A. Iannillo	CONCORDIA
B. Feng	CONCORDIA
T. Van Do	CONCORDIA
B. Santos	CONCORDIA
B. Madalina	CONCORDIA
W. Mees	ECHO
J. Torres	ECHO
F. Kirchner	SPARTA
L. Rebuffi	ECSO
N. Olesen	ECSO

Reviewers

Name	Partner
Afonso Ferreira	IRIT
Liina Kamm	CYBER
Kai Rannenberg	GUF

History

Version	Date	Authors	Comment
0.01	03.06.2022	M. Miller/V. Menezes Miller (CONCEPT)	1st Draft
0.02	14.06.2022	A. Skarmeta (UMU)	Section 2.9
	21.06.2022	G. Rodosek (CONCORDIA) I. Buntic-Ogor (CONCORDIA) A. Iannillo (CONCORDIA)	Section 2.5.1
0.03	12.07.2022	N. Kadenko (TDK)	Section 2.6
0.04	29.08.2022	E. Marketos (FORTH)	Chapter 1
	30.08.2022	D. Preuveneers (KUL)	Chapter 1
	01.09.2022	A. Lluch Lafuente (DTU)	Chapter 1
	21.09.2022	L. Colombini (Intesa Sanpaolo)	Chapter 1
	30.09.2022	S. Vidor (UNITN)	Chapter 1
	30.09.2022	S. Krenn (AIT)	Chapter 1
	30.09.2022	J. Carlos Perez Baun/A. Pasic (ATOS)	Chapter 1
	30.09.2022	L. Kamm (CYBER)	Chapter 1
	04.10.2022	C. Fernandez Gago (UMA)	Chapter 1
	12.10.2022	A. Skarmeta (UMU)	Chapter 1
	13.10.2022	R. Tordi (ABI)	Chapter 1
	13.10.2022	M. Miller/V. Menezes Miller (CONCEPT)	Sections 2.5.2., 2.5.3., 2.5.4
V0.05	17.10.2022	W. Mees (ECHO)	Section 2.5.2
		F. Kirchner (SPARTA)	Section 2.5.3
		B. Feng (CONCORDIA) C. Budde (CyberSec4Europe) N. Olesen (ECSO)	Section 2.14
		W. Tesfay (GUF) N. Arastouei (GUF) S. Pape (GUF) A. Niknia (GUF) P. Hamm (GUF) V. Menezes Miller (CONCEPT)	Sections 2.5, 2.7, 2.16
V0.6	18.10.2022	M. Miller/V. Menezes Miller (CONCEPT)	Review Sections 2.5, 2.7, 2.14, 2.16
V0.7	19.10.2022	L. Rebuffi (ECSO)	Section 2.5.5
		V. Menezes Miller (CONCEPT)	Section 2.12, 2.1
V0.8	24.10.2022	M. Miller/V. Menezes Miller (CONCEPT)	Review Section 2.12 Section 2.1, 2.2, 2.3
V0.9	26.10.2022	A. Sforzin (NEC) C. Grigoriadis (UPRC)	Section 2.10.1
		V. Menezes Miller (CONCEPT)	Review Section 2.10.1
	28.10.2022	J. Torres	Section 2.10.3
V0.10	02.11.2022	M. Miller (CONCEPT)	Full review
V0.11	03.11.2022	C. Jamieson (TDL)	Section 2.3.1
V0.12	07.11.2022	M. Miller/V. Menezes Miller (CONCEPT)	Abstract / Conclusions / Full Document Edits
V0.13	14.11.2022	M. Miller/V. Menezes Miller (CONCEPT)	Implementing feedback from first Peer Reviewer

Version	Date	Authors	Comment
V0.14	17.11.2022	TDL, KAU, GUF	Chapter 1
V0.15	21.11.2022	M. Miller/V. Menezes Miller (CONCEPT)	Implementing feedback from second Peer Reviewer
V0.16	22.11.2022	M. Miller/V. Menezes Miller (CONCEPT)	Implementing feedback from High-Level Review
		D. Goodman/C. Jamieson (TDL)	Chapter 1
V0.17	30.11.2022	M. Miller/V. Menezes Miller (CONCEPT)	Section 4 Final edits Adding Chapter 1
V0.18	01.12.2022	GUF	Chapter 1 edits
V0.19	24.12.2022	GUF	Chapter 1 additions
V0.20	04.01.2023	K. Rannenberg (GUF)	Chapter 1 additions
V0.21	09.01.2023	M. Miller/V. Menezes Miller (CONCEPT)	Insertion Chapter 1, final edits, clean-up
V0.22	09.01.2023	M. Miller/V. Menezes Miller (CONCEPT)	Final Review
V1.0	10.01.2023	A. Niknia (GUF)	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AFME**	Association for Financial Markets in Europe
	AI	Artificial Intelligence
C	**CAPE**	CAPE Continuous assessment in polymorphous environments
	CCN	Competence Centre Network
	CCCN	Cybersecurity Competence Centre and Network
	CEG	Cyber Expert Group
	CEN	European Committee for Standardization
	CENELEC	European Committee for Electrotechnical Standardization
	CERTFin	Certification in Finance
	CESICAT	Centre de Seguretat de la Informació de Catalunya
	CHECK	Community Hub of Expertise and Cybersecurity Knowledge
	CMTMF	CONCORDIA Mobile Threat Modelling Framework
	CNO	Collaborative Network Organization
	CONCORDIA	Cyber security cOmpeteNCfOr Research and InnovAtion
	CSF	Cybersecurity Skills Framework
	CTI	Cyber Threat Incident
D	**DIN**	German Standardization Body for Information Technologies
E	**EARTO**	European Association of Research and Technology Organisations
	EBF	European Banking Federation
	ECCC	European Cybersecurity Competence Centre
	E-CCS	E-Cybersecurity Certification Scheme
	ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
	ECSO	European Cyber Security Organisation
	EDPS	European Data Protection Supervisor
	E-FCR	ECHO Federated Cyber Range
	EFG	Education Focus Group
	E-GCS	Governance Consultancy Services
	ENISA	European Union Agency for Cybersecurity
	ETSI	European Telecommunications Standards Institute
	EUROPOL	European Union Agency for Law Enforcement Cooperation
	E-EWS	Early Warning System
H	**HAII-T**	High-assurance intelligent infrastructure toolkit
	HCO	Health Care Organizations
	HE	Horizon Europe

I	**ICS**	Industrial Control Systems
	IDSA	International Data Spaces Association
	IEC	International Electrotechnical Commission
	IEEE	Institute of Electrical and Electronics Engineers
	IPEN	Internet Privacy Engineering Network
	IoT	Internet of Things
	ISO	International Organization for Standardization
J	**JTC**	Joint Technical Committee
M	**MEP**	Member of European Parliament
N	**NCC**	National Coordination Centres
	NCCC	National Cybersecurity Coordination Centres
	NCP	National Contact Point
S	**SAFAIR**	Secure and Fair AI Systems for the Citizen
	SCOS	SpaceCraft Operational Software
	SDO	Standards Development Organizations
	SISP	Secure Information Sharing Platform
U	**UNE**	Spanish Association for Standardization
W	**WG**	Working Group
	WP	Work Package

List of acronyms of CyberSec4Europe Consortium Partners

A	ABI	ABI LAB-CENTRO DI RICERCA E INNOVAZIONE PER LA BANCA
	AIT	AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH
	ARCH	ARCHIMEDE SOLUTIONS SARL
	ATOS	ATOS SPAIN SA
B	BBVA	BANCO BILBAO VIZCAYA ARGENTARIA SA*
	BRNO	MASARYKOVA UNIVERZITA
C	C3P	UNIVERSIDADE DO PORTO
	CNR	CONSIGLIO NAZIONALE DELLE RICERCHE
	CONCEPT	CONCEPTIVITY SARL
	CONCORDIA	CYBER SECURITY COMPETENCE FOR RESEARCH AND INNOVATION
	CTI	INSTITOUTO TECHNOLOGIAS YPOLOGISTONKAI EKDOSEON DIOFANTOS
	CYBER	CYBERNETICA AS
	DAWEX	DAWEX SYSTEMS
D	DTU	DANMARKS TEKNISKE UNIVERSITET
E	ECHO	EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS
	ENG	ENGINEERING - INGEGNERIA INFORMATICA SPA
F	FORTH	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS
G	GEN	COMUNE DI GENOVA
	GUF	JOHANN WOLFGANG GOETHE-UNIVERSITAT FRANKFURT AM MAIN
I	I-BP	INFORMATIQUE BANQUES POPULAIRES
	ICITA	INTERNATIONAL CYBER INVESTIGATION TRAINING ACADEMY SDRUZHENIE
	ISGS	INTESA SANPAOLO SPA
J	JAMK	JYVASKYLAN AMMATTIKORKEAKOULU
K	KAU	KARLSTADS UNIVERSITET
	KUL	KATHOLIEKE UNIVERSITEIT LEUVEN
N	NEC	NEC LABORATORIES EUROPE GMBH
	NTNU	NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET NTNU
O	OASC	OPEN & AGILE SMART CITIES
P	POLITO	POLITECNICO DI TORINO
S	SIE	SIEMENS AKTIENGESELLSCHAFT
	SINTEF	SINTEF AS
	SPARTA	
T	TDL	TRUST IN DIGITAL LIFE
	TLEX	TIME.LEX
	TUD	TECHNISCHE UNIVERSITEIT DELFT
U	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
	UNILU	UNIVERSITE DU LUXEMBOURG
	UNITN	UNIVERSITA DEGLI STUDI DI TRENTO
	UPRC	UNIVERSITY OF PIRAEUS RESEARCH CENTER
	UPS-IRIT	UNIVERSITE PAUL SABATIER TOULOUSE III
V	VAF	VaF, S. R. O.
	VTT	TEKNOLOGIAN TUKIMUSKESKUS VTT Oy

1 Partner Activity for the Third 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.

Although during the 2021, personal participation in meetings and travel to meetings was still heavily influenced by Covid, partners still engaged significantly via online means. A summary of the CyberSec4Europe partner collaboration activities for the period January 2021 to September 2022 is contained in the tables that follow.

1.1 DG CNECT

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
14.01.2021 (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, TDL, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
04.03.2021 (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
06.05.2021 (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
01.07.2021 (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
08.07.2021 (Virtual)	Call on Joint Cyber Unit	Intesa Sanpaolo	Meeting with European Commission in order to discuss about Joint Cyber Unit (JCU)
07.10.2021 (Brussels, Belgium) (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
01.12.2021 (Brussels, Belgium) (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
03.02.2022 (Belgium, Brussels) (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO
06.04.2022 (Belgium, Brussels) (Virtual)	Meeting of EC Unit CNECT H1, REA and JRC with the 4 pilot projects' coordinators and ECSO	GUF, CONCEPT	Synchronisation with EC Unit CNECT H1, REA and JRC and with the fellow pilot projects' coordinators and ECSO

Table 2: Participation/collaboration with DG CNECT

1.2 ENISA

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
02.02.2021-04.02.2021 (Virtual)	Cybersecurity Standardization Conference 2021 https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021/	CYBER, GUF, CONCEPT	ENISA/CEN-CENELEC/ ETSI Cybersecurity Standardization Conference 2021: European Standardization in support of the EU Cybersecurity Act Maintenance of ENISA and Standardisation Community
23.04.2021 (Publication date)	Title of publication: Cybersecurity Research Directions for the EU's Digital Strategic Autonomy	FORTH. Prof. Evangelos Markatos (FORTH) was a co-author of this publication.	The focus of this work is to identify the necessary research priorities to support the EU's digital strategic autonomy and thus digital sovereignty. In this introductory chapter, we (i) analyse how the terms 'digital strategic autonomy' and 'digital sovereignty' have been used and propose the definition used in this report, (ii) define the scope and target audience, and (iii) outline the structure of the report.
17.06.2021-18.06.2021 (Virtual)	ENISA Annual Privacy Forum (APF) 2021 https://2021.privacyforum.eu/	GUF	Maintenance of Policy, Scientific, and Industry Community
16.07.2021 (Virtual)	EGFI group	Intesa Sanpaolo	Meeting about NISD and update and feedback on DORA
15.10.2021-17.10.2021 (Turin, Italy)	2nd Bootcamp for EU cybersecurity team candidates	CYBER	Taking part in the training

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
03.03.2022-05.03.2022 (The Hague, The Netherlands)	Bootcamp for EU cybersecurity team candidates https://www.facebook.com/ENISAEUAGENCY/posts/325696169597200 https://securitydelta.nl/news/overview/cybersecurity-talent-from-all-over-europe-get-bootcamp-in-the-hague https://twitter.com/enisa_eu/status/1499352820134387713 https://www.nature.com/articles/s42256-021-00337-8	CYBER	Participated in the training
14.03.2022-15.03.2022 (Brussels, Belgium) (Virtual)	Cybersecurity Standardization Conference 2022	GUF	Maintenance of ENISA and Standardisation Community
11.07.2022 (Virtual)	Cybersecurity Research and Innovation Needs and Priorities – A scoping Roundtable	FORTH	Prof. Evangelos Markatos (FORTH) gave a presentation titled “AI: Threats and Opportunities”
02.06.2022 (Hybrid)	ENISA Cybersecurity Certification Conference https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2022/agenda	Atos, CONCEPT	Aljosa Pasic was presenter
23.06.2022-24.06.2022 (Warsaw, Poland)	ENISA Annual Privacy Forum (APF) 2022 https://2022.privacyforum.eu/	GUF	Maintenance of Policy, Scientific, and Industry Community
06.09.2022 (Virtual)	Meeting/SMEs	TDL, CONCEPT	Participated in meeting
11.07.2022 (Virtual)	Cybersecurity Research and Innovation Needs and Priorities – A scoping Round Table https://www.enisa.europa.eu/topics/research-and-innovation/	GUF	Maintenance of Policy Community

Table 3: Participation/collaboration with ENISA

1.3 EDPS

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
09.12.2021 (Virtual)	IPEN Webinar 2021 https://edps.europa.eu/ipen-webinar-2021-pseudonymous-data-processing-personal-data-while-mitigating-risks_en	CYBER	Participated as attendee

Table 4: Participation in EDPS event

1.4 ECSO

Date & Venue	Working Group	Title	Partners	Comments / Remarks /Outcomes
ECSO WG1				
All year	WG1	Standardisation, certification, labelling, supply chain management	CYBER, UMU, CONCEPT	
01.07.2021 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CYBER, CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
25.01.2021 (Virtual)	WG1, WG2, WG3, WG4, WG5, WG6	ECSO Brokerage Event	CONCEPT	
27.01.2021 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CONCEPT, CYBER, GUF	Taking part in the WG meeting, contributing to documents and discussion. Maintenance of ECSO and EC Community, further development of ECSO
21.04.2021 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CYBER, CONCEPT, GUF, UMU	Taking part in the WG meeting, contributing to documents and discussion
01.07.2021 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CONCEPT, GUF	Maintenance of Policy Community
26.11.2021 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CYBER, CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
11.04.2022 (Virtual)	WG1	Standardisation, certification, labelling, supply chain management	CYBER, UMU, CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
ECSO WG2				
22.06.2021 (Virtual)	WG2	WG2 Market Deployment	CONCEPT	Taking part in the WG meeting, contributing to documents and discussion

Date & Venue	Working Group	Title	Partners	Comments / Remarks /Outcomes
17.02.2022 (Virtual)	WG2 and WG4	WG2 Market Deployment WG4 SMEs & Regions	CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
ECSO WG3				
15.07.2021	WG3		Intesa Sanpaolo	Meeting organized by ECSO for presenting the Italian Chapter of Women4Cyber
28.10.2021 (Virtual)	WG3	1st meeting of the ECSO Community of Verticals (CoV)	Intesa Sanpaolo	Meeting in order to have a first exchange with user and suppliers on SOC (Security Operation Centre), contractual obligations between users/operator and suppliers
07.06.2021 27.01.2022 11.03.2022 (virtual)	WG3	ECSO's CISOs European Community	Intesa Sanpaolo	Recurrent meeting of CISO's European Community about cybersecurity topics
24/02/2022 (virtual)	WG3	Webinar "Log4J"	Intesa Sanpaolo	Webinar for the creation of an exchange platform between CISO at European level
13.04.2022 30.06.2022 29.09.2022 (Virtual)	WG3	ECSO - EU Legal and Policy Task Force	Intesa Sanpaolo	Recurrent meeting in order to discuss about cybersecurity regulations such as DORA, NIS2, CER (critical Entities Resilience), eID Regulation, AIA (Artificial Intelligence Act) etc.
29.06.2022 – (Bruxelles)	WG3	ECSO - High level event	Intesa Sanpaolo	Meeting to discuss developments of European cyberesecurity regulatory landscape
06.07.2022 (Virtual)	WG3/WG6	ECSO TF on Cloud and Data Spaces	ATOS	Aljosa Pasic was participatng in the meeting and contributing to ToR
ECSO WG4				
All year virtual	WG4	Support to SMEs, coordination with countries and regions	CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
14.01.2021 (Virtual)	WG4	Support to SMEs, coordination with countries and regions	CONCEPT	Virtual Coffee
12.05.2021 (Virtual)	WG4	Support to SMEs, coordination with countries and regions	CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
ECSO WG5				

Date & Venue	Working Group	Title	Partners	Comments / Remarks /Outcomes
13.04.2021 (Virtual)	WG5	Education, Training, Awareness, Cyber Ranges	CONCEPT	9th Online Meeting
03.05.2021 (Virtual)	WG5	Education, Training, Awareness, Cyber Ranges	CONCEPT	Strategy/KPI meeting
16.11.2021	WG5	Education, Training, Awareness, Cyber Ranges	CONCEPT	10th Online Meeting
ECSO WG6				
All year (Brussels, virtual)	WG6	SRIA and Cyber Security Technologies	FORTH, UMA, CONCEPT	FORTH Contributes to the development of ECSO's Strategic Research and Innovation Agenda, co-chairs SWG 6.3 (Data and the Economy), and co-authors the "Global vision for future EU cyber security" (last version May 2022)
08.04.2021 (Virtual)	WG6	SRIA and Cyber Security Technologies	CYBER, CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
08.04.2021 (Virtual)	WG6	ECSO WG6 Meeting on EC Roadmaps and Research Programs	GUF, CONCEPT	EC Roadmapping and Research Programs
28.02.2022	WG6	WG6 SRIA and Cyber technologies	CONCEPT	Participated in the meeting.
07.07.2022	WG6	WG6 SRIA and Cyber technologies	CONCEPT	ECSO Brokerage Event (hybrid)
28.10.2021 (Virtual)		1st ECSO Community of Verticals (CoV) meeting	CYBER	Participated in the meeting.
28.02.2022 (Virtual)	WG6		CYBER, CONCEPT	Taking part in the WG meeting, contributing to documents and discussion
General Assembly				
30.06.2021 (Virtual)	ECSO General Assembly	ECSO General Assembly	GUF, CONCEPT	Maintenance of Policy Community

Date & Venue	Working Group	Title	Partners	Comments / Remarks /Outcomes
29.06.2022 (Brussels, Belgium) (Virtual)	ECSO General Assembly	ECSO General Assembly	CONCEPT	Maintenance of Policy Community
Board of Directors :				
31.03.2021 (Virtual)	ECSO Board of Directors	ECSO Board of Directors	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO
30.06.2021 (Virtual)	ECSO Board of Directors	ECSO Board of Directors	GUF, CONCEPT	Maintenance of Policy Community
14.12.2021 (Virtual)	ECSO Board of Directors	ECSO Board of Directors	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO
18.01.2022 (Virtual)	ECSO Board of Directors Meeting	ECSO Board of Directors Meeting	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO
29.03.2022-31.03.2022	ECSO Board of Directors Meeting	ECSO Board of Directors Meeting	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO
28.06.2022	ECSO Board of Directors Meeting	ECSO Board of Directors Meeting	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO
ECSO Strategy Committee Meeting				
14.12.2021 (Virtual)	ECSO Strategy Committee Meeting	ECSO Strategy Committee Meeting	GUF, CONCEPT	Maintenance of ECSO and EC Community, further development of ECSO

Table 5: Collaboration/Participation in ECSO WGs

1.5 Standardization Organizations

1.5.1 CEN/CENELEC

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
CEN/CLC JTC 13/WG 1				
18.02.2021 (Virtual)	CEN/CENELEC JTC 13/WG 1	Cybersecurity and Data Protection WG 1 "Chairman advisory group"	GUF	Comments and votes on organisation of European standardisation in JTC 13
09.03.2021 (Virtual)	CEN/CLC JTC 13/WG 1	Cybersecurity and Data Protection WG 1 "Chairman advisory group"	GUF	Comments and votes on organisation of international standardisation in JTC 13
13.09.2021 (Virtual)	CEN/CLC JTC 13/WG 1	Consumer protection: privacy by design for	GUF	Comments and votes on standardisation project ISO 31700, Maintenance of Standardisation Community

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
		consumer goods and services		
13.12.2021 (Virtual)	CEN/CLC JTC 13/WG 1	Cybersecurity and Data Protection WG 1 "Chairman advisory group"	GUF	Comments and votes on ENISA documents on standardisation
10.03.2022 (Virtual)	CEN/CLC JTC 13/WG 1	Cybersecurity and Data Protection WG 1 "Chairman advisory group"	GUF	Comments and votes on organisation of European standardisation in JTC 13
21.03.2022 (Virtual)	CEN/CLC JTC 13/WG 1	Cybersecurity and Data Protection WG 1 "Chairman advisory group"	GUF	Comments and votes on organisation of European standardisation in JTC 13
CEN/CLC JTC 13/WG 3				
23.12.2021 (Virtual)	CEN/CLC/JTC 13/WG 3	Security evaluation and assessment	GUF	RED DA SR Risk Assessment approach
01.07.2022 (Virtual)	CEN/CLC/JTC 13/WG 3	Security evaluation and assessment	GUF	Participated in meeting
CEN/CLC JTC 13/WG 5				
	CEN/CLC/JTC 13/WG 5	New study group for Feasibility study on European implementation of ISO/IEC 27701	ATOS	NWIP Additional requirements for ISO/IEC 27701 – DRAFT
04.02.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
12.03.2021-15.03.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
11.06.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
05.07.2021-08.07.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection	GUF	Comments and votes on European standardisation projects

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
22.11.2021-26.11.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection	GUF	Comments and votes on European standardisation projects
24.11.2021-26.11.2021 (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
10.02.2022 (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
06.07.2022-07.07.2022 (Berlin, Germany) (Virtual)	CEN/CLC JTC 13/WG 5	Cybersecurity and Data Protection, Privacy and Identity Management	GUF	Comments and votes on European standardisation projects
CEN/CLC JTC 13/WG 6				
23.12.2021 (Virtual)	CEN/CLC/JTC 13/WG 6	Product security	GUF	RED DA SR Risk Assessment approach
CEN/CLC CWA				
08.07.2021 (Virtual)	CEN/CLC CWA Digital sovereignty	Meeting CEN/CLC CWA Digital sovereignty	GUF	Comments and votes on European standardisation projects
15.12.2021-16.12.2021 (Virtual)	CEN/CLC CWA Digital sovereignty	Meeting CEN/CLC CWA Digital sovereignty	GUF	Comments and votes on European standardisation projects
20.01.2022 (Virtual)	CEN/CLC CWA Digital sovereignty	CEN/CLC CWA Digital sovereignty	GUF	Comments and votes on European standardisation projects
15.02.2022 (Virtual)	CEN/CLC CWA Digital sovereignty	CEN/CLC CWA Digital sovereignty	GUF	Comments and votes on European standardisation projects

Table 6: Participation in CEN/CENELEC committees and WGs

1.5.2 ISO/IEC

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
JTC 1/SC 27 AGs				

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
02.03.2021 (Virtual)	ISO/IEC JTC 001/SC 27/AG 03	Concepts and Terminology	GUF	Comments and votes on concepts and terminology of international standardisation in SC 27
09.03.2021 (Virtual)	ISO/IEC JTC 001/SC 27/AG 05	Strategy	GUF	Comments and votes on organisation of international standardisation in SC 27
09.03.2021 (Virtual)	ISO/IEC JTC 001/SC 27/AG 06	Operations	GUF	Comments and votes on organisation of international standardisation in SC 27
18.01.2022 (Virtual)	ISO/IEC JTC 001/SC 27/AG 06	Operations	GUF	Comments and votes on organisation of international standardisation in SC 27
JTC 1/SC 27/CAG				
08.02.2021 (Virtual)	ISO/IEC JTC 001/SC 27/CAG	Chair's Advisory Group	GUF	Comments and votes on organisation of international standardisation in SC 27
09.07.2021 (Virtual)	ISO/IEC JTC 001/SC 27/CAG	Chair's Advisory Group	GUF	Comments and votes on organisation of international standardisation in SC 27
22.10.2021 (Virtual)	ISO/IEC JTC 001/SC 27/CAG	Chair's Advisory Group	GUF	Comments and votes on organisation of international standardisation in SC 27
05.01.2022 (Virtual)	ISO/IEC JTC 001/SC 27/CAG	Chair's Advisory Group	GUF	Comments and votes on organisation of international standardisation in SC 27
JTC 1/SC 27/WG 2				
08.04.2021-15.04.2021 (Virtual)	ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	AIT, CYBER	Periodic ISO/IEC JTC 1/SC27 ("Information security, cybersecurity and privacy protection") working group meetings. AIT participated as liaison officer for CyberSec4Europe to WG 2, and as editor of multiple standards in WG 2
19.10.2021-24.10.2021 (Virtual)	ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	CYBER, AIT	Taking part in the WG meetings, commenting on standards
28.03.2022-07.04.2022 (Virtual)	ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	CYBER, AIT	Taking part in the WG meetings, commenting on standards. WG 2: ISO/IEC WD 4922-1 – Secure multiparty computation – Part 1: General ISO/IEC WD 4922-2 – Secure multiparty computation Part 2: Mechanisms based on secret sharing

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
26.09.2022	ISO/IEC JTC 1/SC 27/WG 2	Cryptography and security mechanisms	CYBER, AIT	Taking part in the WG meetings, commenting on standards. Commenting on the standard, liaison representative
JTC 1/SC 27/WG 5				
09.02.2021 (Virtual)	ISO/IEC JTC 1/SC 27/WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects, especially ISO/IEC 27006-2
07.04.2021-16.04.2021 (Virtual)	ISO/IEC JTC 1/SC 27/WG 5	Identity Management and Privacy Technologies	CYBER, AIT, GUF, UMA	Comments and votes on international standardisation projects CYBER is the liaison officer to WG 5
08.04.2021-15.04.2021 (Virtual)	ISO/IEC JTC1/SC 27/WG 5	Identity Management and Privacy Technologies	AIT, GUF, CYBER	Periodic ISO/IEC JTC 1/SC 27 ("Information security, cybersecurity and privacy protection") working group meetings.
15.06.2021-16.06.2021 (Virtual)	ISO/IEC JTC1/SC 27/WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on European standardisation projects
19.10.2021-22.10.2021 (Virtual)	ISO/IEC JTC1/SC 27/WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects
26.10.2021-27.10.2021 (Virtual)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects
28.03.2022-07.04.2022 (Virtual)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	CYBER, AIT, GUF	Taking part in the WG meetings, commenting on standards. WG 5: ISO/IEC WD 27559 - Privacy enhancing data de-identification framework; WD 27565 Guidelines on privacy preservation based on zero-knowledge proofs
28.03.2022-31.03.2022 (Virtual)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
04.04.2022-07.04.2022 (Virtual)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects
23.05.2022-25.05.2022 (Virtual)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	GUF	Comments and votes on international standardisation projects
26.09.2022-30.09.2022 (Hybrid) (Luxembourg)	ISO/IEC JTC 1/SC 27 WG 5	Identity Management and Privacy Technologies	CYBER, AIT, GUF	Taking part in the WG meetings, commenting on standards. Commenting on the standard, liaison representative
ISO/PC 317				
19.04.2021 (Virtual)	ISO/PC 317 and ISO/PC 317/WG 1	Consumer protection: privacy by design for consumer goods and services	GUF	Comments and votes on standardisation project ISO 31700, Maintenance of Standardisation Community
13.09.2021-16.09.2021 (Virtual)	ISO/PC 317 and ISO/PC 317/WG 1	Consumer protection: privacy by design for consumer goods and services	GUF	Comments and votes on standardisation project ISO 31700, Maintenance of Standardisation Community
16.05.2022-19.05.2022 (Virtual)	ISO/PC 317 and ISO/PC 317/WG 1	Consumer protection: privacy by design for consumer goods and services	GUF	Comments and votes on standardisation project ISO 31700, Maintenance of Standardisation Community
ISO/IEC JTC 1/SC 27				
29.10.2021 (Virtual)	ISO/IEC JTC 1/SC 27	ISO/IEC JTC 1/SC 27	GUF	Comments and votes on international standardisation projects
08.11.2021-15.11.2021 (Virtual)	ISO/IEC JTC 1/SC 27	ISO/IEC JTC 1/SC 27	GUF	Comments and votes on international standardisation projects
12.04.2022-13.04.2022 (Virtual)	ISO/IEC JTC 1/SC 27	Information technology	GUF	Comments and votes on international standardisation projects
09.05.2022-13.05.2022 (Virtual)	ISO/IEC JTC 1/SC 27	Information technology	GUF	Comments and votes on international standardisation projects

Table 7: Participation in ISO/IEC committees and groups

1.5.3 ZkProof

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
2021/04/19 – 2021/04/29	4th Workshop of the ZKProof standardization initiative	AIT	Participation in the 4th Workshop of the ZKProof standardization initiative. AIT experts presented their standardization proposal on Sigma-protocols, which was accepted for further standardization. A respective working group will be established.

1.6 National Standardization Bodies

1.6.1 ASI

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
11.03.2022 (Virtual)	AG 001.27 meeting		AIT	Remote participation in (virtual) ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27),
23.06.2022 (Virtual)	AG 001.27 meeting		AIT	Remote participation in (virtual) ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27)
23.09.2022 (Virtual)	AG 001.27 meeting		AIT	Remote participation in (virtual) ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27)

Table 8: Participation in ASI meetings

1.6.2 DIN

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
18.01.2021-20.01.2021 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	GUF	Comments and votes on international and European standardisation projects
11.02.2021 (Virtual)	DIN NIA 27 AK 05 (German Mirror Committee to ISO/PC 317)	DIN NIA 27 AK 05 (German Mirror	GUF	Comments and votes on international standardisation projects, especially ISO 31700

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
		Committee to ISO/PC 317)		
12.04.2021 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	GUF	Comments and votes on international and European standardisation projects
04.05.2021 (Virtual)	Workshop "Analyse von Bedarfen der NRM KI zum Thema KI in der Medizin und IT-Sicherheit bei KI-Systemen"	Workshop "Analyse von Bedarfen der NRM KI zum Thema KI in der Medizin und IT-Sicherheit bei KI-Systemen"	GUF	Preparation of international and European standardisation projects on IT Security wrt KI systems
07.06.2021-09.07.2021 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	GUF	Comments and votes on international and European standardisation projects
28.06.2021 (Virtual)	DIN KITS (German Expert Advisory Group for Cybersecurity)	DIN KITS (German Expert Advisory Group for Cybersecurity)	GUF	Participation Meetings DIN KITS (German Expert Advisory Group for Cybersecurity)
25.10.2021-28.10.2021 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	GUF	Comments and votes on international and European standardisation projects
07.02.2022-09.02.2022 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	GUF	Comments and votes on international and European standardisation projects
21.02.2022 (Virtual)	DIN NIA Gemeinsamer Lenkungsausschuss	DIN NIA Gemeinsamer	GUF	Preparation of Meeting of ISO/IEC JTC 1 Information technology

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
		Lenkungsausschuss		
17.03.2022 (Virtual)	DIN NIA Gemeinsamer Lenkungsausschuss	DIN NIA Gemeinsamer Lenkungsausschuss	GUF	Topics of ISO/IEC JTC 1 Information technology
04.04.2022-07.04.2022 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27	GUF	Comments and votes on international and European standardisation projects
20.07.2022-21.07.2022 (Berlin, Germany) (Virtual)	Plattform Industrie 4.0 AG "Sicherheit vernetzter Systeme", UAG "Securitystandards und Internationalisierung"	DIN/DKE Normungsroad map Industrie 4.0 (NRMI4.0), Entries Industrial Security, Privacy, Trusworthiness	GUF	Rodmapping for International, European, and German standardisation projects
06.09.2022 (Virtual)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs)	GUF	Comments and votes on international and European standardisation projects

1.6.3 EVS

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
01.12.2021	EVS/TK 75 (Blockchain and distributed ledger technologies)		CYBER	Member
08.10.2021	EVS/TK 04 (Information technology)		CYBER	Chairman of the technical committee

1.6.4 UNE

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes

22.07.2022 (Virtual)	CTN 320	Cybersecurity and personal data protection	UMA	Plenary meeting
Weekly online meeting, 16.02.2022 – 28.06.2022	CTN 320/GT CIOT2	"Modelo de Arquitectura segura de IoT-Blockchain" (Model of a secure IoT-Blockchain Architecture)	UMA	This committee aimed to create a national (Spanish) standard for the secure interaction between IoT and Blockchains (PNE 320003). Work in this standard has been paused.

1.7 Collaboration with the Fellow Pilots

Date & Venue	Event	Pilot	Comments / Remarks /Outcomes
12.01.2021	Flagship 1 event	CONCORDIA, ECHO, SPARTA, DG CNECT	
01.03.2021	Financial sector federated learning CyberSec4Europe/CONCORDIA	TDL	Participated in meeting
01.12.2021	CYTILIS CyberSec4Europe/ CONCORDIA	TDL	Participation in activities organized jointly with other EU projects
11.03.2022 (Virtual)	Building a Roadmap for the ECCC	Four pilots	Building a Roadmap for the ECCC
01.06.2022-03.06.2022 (Hybrid)	CONVERGENCE NEXT Making the Cybersecurity Competence Network a Reality https://cybersec4europe.eu/events/concertation/convergence-next/	CONCORDIA, ECHO, SPARTA, CyberSec4Europe	Report of the Conference is in this document D10.3 Presentation "CyberSec4Europe Safeguarding European values through excellence in cybersecurity"

Table 9: Summary of collaboration with other pilots

1.7.1 Four Pilots Focus Groups

1.7.1.1 Communications Focus Group

Date & Venue	Pilot	Pilots	Comments / Remarks /Outcomes
01.01.2021 (Virtual)	CCN Communication Groupmeeting	CONCORDIA, ECHO, SPARTA, DG CNECT	
20.07.2021 (Virtual)	CCN Communication Groupmeeting	CONCORDIA, ECHO, SPARTA, DG CNECT	

1.7.1.2 Cyber Range Focus Group

Date & Venue	Pilot	Pilots	Comments / Remarks /Outcomes

Table 10: Four Pilots Communication Group

1.7.1.3 Education Focus Group

Date & Venue	Pilot	Pilots		Comments / Remarks /Outcomes
15.02.2021 (Virtual)	CCN Education monthly meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Merging of different mapping efforts into the ENISA map
10.03.2021 (Virtual)	CCN Education monthly meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Skills framework alignment, plan for 2021 collaboration activities
13.04.2021 (Virtual)	CCN Education monthly meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Evaluation of the maturity of collaboration activities
18.05.2021 (Virtual)	CCN Education monthly meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Identification of the group's 2021 priorities
23.06.2021 (Virtual)	CCN Education monthly meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Status of collaboration; update on the mapping and HR survey activities
05.10.2021 (Virtual)	CCN Education meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Skills framework and events synchronization
10.12.2021 (Virtual)	CCN Education meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	ENISA draft Proposal for the EU Cybersecurity Competence Centre

Date & Venue	Pilot	Pilots		Comments / Remarks /Outcomes
04.02.2022 (Virtual)	CCN Education meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Education governance model
13.04.2022 (Virtual)	CCN Education meeting	CS4E, SPARTA, ECHO, CONCORDIA + ECSO, ENISA	UNITN	Education governance model; CONVERGENCE event synch

1.7.1.4 Governance Focus Group

Date & Venue	Pilot	Pilots	Comments / Remarks /Outcomes
01.02.2021	Meeting of 4 pilot projects' Governance Coordination Group	CS4E, SPARTA, ECHO, CONCORDIA	Synchronisation with the fellow pilot projects on Governance

1.7.1.5 Roadmapping Focus Group

Date & Venue	Pilot	Pilots	Comments / Remarks /Outcomes
All year long (virtual and Brussels)	CS3E (FORTH)	All Pilots + ECSO	FORTH (Prof. Evangelos Markatos) co-authored the "Research Priorities" document that was delivered to JRC, DG CNECT and used by ENISA.
01.12.2021	Meeting of 4 pilot projects' Road mapping Coordination Group	All Pilots + ECSO	Discuss roadmap consolidation efforts of the 4 pilots Synchronisation with the fellow pilot projects on Road mapping

1.7.1.6 Threat Intelligence in the Financial Sector Focus Group

Date & Venue	Pilot	Pilots	Comments / Remarks /Outcomes
07.06.2022 11.07.2022	CyberSec4Europe, CONCORDIA	ATOS, UMU	Two persons from Atos and UMU participated in the meetings

1.7.2 CyberSec4Europe

Date & Venue	Event	Title	Partners	Comments / Remarks /Outcomes
29.01.2021	Webinar https://cybersec4europe.eu/events/broadcasts-and-webinars/cybersecurity-standards-how-standict-eu-supports-european-specialists-in-the-international-landscape/	CyberSec4Europe Insights series webinar on Cybersecurity & Standards – How StandICT.eu supports European specialists in the international landscape	CYBER, TDL	CyberSec4Europe Insights series webinar on Cybersecurity & Standards – How StandICT.eu supports European specialists in the international landscape
19.02.2021	Webinar https://cybersec4europe.eu/events/broadcasts-and-webinars/towards-more-transparent-security-certifications-mining-common-criteria-and-fips140-2-certificates/	CyberSec4Europe Insights series webinar on "Towards more transparent security certifications – mining Common Criteria and FIPS140-2 certificates"	CYBER TDL	CyberSec4Europe Insights series webinar on "Towards more transparent security certifications – mining Common Criteria and FIPS140-2 certificates" Organisation of Webinar
24.02.2021 (Virtual)	Public event of CyberSec4Europe with Panel https://cybersec4europe.eu/event/establishing-the-competence-centre-in-bucharest-and-building-the-network/	Establishing the Competence Centre in Bucharest and Building the Network	All CS4E partners	Clarification on Cybersecurity and its governance
24.02.2021 (Virtual)	Presentation of CyberSec4Europe	CyberSec4Europe: Creating food for thought	GUF	Update on CyberSec4Europe and its results
05.05.2021	Presentation of CyberSec4Europe	CyberSec4Europe: Creating food for thought	GUF	Update on CyberSec4Europe and its results
05.05.2021	Public event of CyberSec4Europe with Panel	Developing SME Cybersecurity Resilience in Europe	All CS4E partners	Clarification on Cybersecurity Resilience and its governance
17.05.2021 (Virtual)	Webinar https://cybersec4europe.eu/developments-in-european-regulations/	CyberSec4Europe Insights series webinar on Developments in European Regulations	CYBER TDL	CyberSec4Europe Insights series webinar on Developments in European Regulations Organisation of Webinar
06.07.2021 (Virtual)	Workshop	Cross-border panel discussion	TDL	Organisation of Workshop
22.07.2021 (Virtual)	Webinar https://cybersec4europe.eu/events/broadcasts-and-webinars/introducing-fixed-	CyberSec4Europe Insights series webinar on Introducing Fixed-	CYBER TDL	Participated as attendee Organisation of Workshop

Date & Venue	Event	Title	Partners	Comments / Remarks /Outcomes
	time-cybersecurity-evaluation-methodology-for-ict-products-fitcem-pren-17640/	Time Cybersecurity Evaluation Methodology for ICT Products (FITCEM/prEN 17640)		
17.11.2021 (Virtual)	Evening Panel discussion" https://cybersec4europe.eu/event/community-perspectives-on-the-future-of-cybersecurity-in-europe/	Community perspectives on the future of cybersecurity in Europe	All CS4E partners	
02.01.22	Interview on Spanish National TV https://www.telecinco.es/informativos/a-la-carta/fin-de-semana/informativo-fin-semana-mediodia-domingo-02-01-2022_18_3260521040.html	Telecinco Informativos mediodía (2/1/2022), Telecinco news (National TV)	UMU	Interview about IoT cybersecurity, how to evaluate cybersecurity (methodology further developed within WP7 and WP3) and the award received.
17.01.2022	Interview on Spanish regional radio https://cadenaser.com/emisora/2022/01/17/radio_murcia/1642416786_998827.html	Entrevista a Sara Matheu, « Tu aspiradora o tu televisor pueden filtrar tus datos: consejos de ciberseguridad para tu hogar » (2022), Cadena SER (National Radio)	UMU	Interview about cybersecuirty issues in the home domain and how to protect ourselves
25.01.2022	Interview on Spanish regional radio https://www.orm.es/eorm/reaccionencadena/reaccion-en-cadena-104/	REACCIÓN EN CADENA. #104 Entrevista a Sara Matheu, Onda Regional (regional radio)	UMU	Interview about the cybersecurity of IoT devices and data privacy (WP3 and WP7)
27.01.2022	Interview on Spanish national radio https://www.rtve.es/play/audios/informativo-de-murcia/rne-murcia-entrevista-sara-matheu-doctora-informatica-experta-seguridad-27-01-2022/6329415/	Murcia Informativos Radio Nacional Española, RNE (2021): Entrevista a Sara Matheu, doctora en informática y experta en seguridad, Radio Nacional Española (National Spanish Radio)	UMU	Interview about cybersecurity and security evaluation.
16.02.2022	Presentation of CyberSec4Europe	CyberSec4Europe: Creating food for thought	GUF	Update on CyberSec4Europe and its results

Date & Venue	Event	Title	Partners	Comments / Remarks /Outcomes
16.02.2022 – 17.02.2022 (Hybrid)	General meeting and panel discussion “Benefits and risks of emerging technologies and the GDPR” Public event with Panel		All CS4E partners	Update on CS4E and its results
20.02.2022	Following a DPA agency article ca. 25 newspapers in Germany		GUF	Following a DPA agency article ca. 25 newspapers in DE published on the CS4E position on cybersecurity education
11.05.2022 (Virtual)	Meeting GUF Profile Section „Orders & Transformations	Presentation "CyberSec4Europe Safeguarding European values through excellence in cybersecurity"	GUF	Presentation "CyberSec4Europe Safeguarding European values through excellence in cybersecurity"
12.06.2022 – 13.06.2022 (Hybrid)	General meeting		KUL	Update on CS4E and its results
15.06.2022 – 16.06.2022 (Hybrid)	General meeting and NCC workshop		KUL	Update on CS4E and its results
15.09.2022 (Brussels, Belgium)	Workshop with NCCs	Workshop with NCCs	GUF	Workshop with NCCs
15.09.2022 (Brussels, Belgium)	CyberSec4Europe: More food for thought	Presentation of CyberSec4Europe	GUF	Update on CyberSec4Europe and its results

Table 11: Public Events of CyberSec4Europe

1.8 International Cooperation

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
21.01.2021 (Virtual	Usable Security and Privacy Day 2021	GUF	Key note “Assessing and appraising apps for privacy in mobile devices and app markets”
22.02.2021 (Virtual)	Austria Industriellenvereinigung, Arbeitsgruppe 3 „Connectivity, Infrastructure and Cybersecurity“ Task Force „Digitalisierung und Künstliche Intelligenz	GUF	Impulse Speech "CyberSec4Europe Aiming to safeguard values through excellence in cybersecurity", Update on CyberSec4Europe and its results

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
11.03.2021 (Virtual)	SECUSO Research Seminar	GUF	Support Young Academics
16.03.2021 (Virtual)	Meeting on "Gaia X" and ECUC (European Cloud User Coalition) cooperation	Intesa Sanpaolo	Meeting on "Gaia X" about cloud services
19.03.2021 (Virtual)	Meeting CEPIS Legal and Security Issues (LSI) Network	GUF	Maintenance of Scientific, Industry, and Policy Community
25.03.2021 (Virtual)	LAILEC 2021 https://www.law.kuleuven.be/citip/en/citip-conferences/lailec/lailec-2021	GUF	Panel presentation "AI for resilience and collaborative mitigation strategies for AI-driven response to cyber threats"
08.04.2021 (Virtual)	ITASEC 2021 https://2021.itasec.it/ Italian Conference on Cybersecurity	GUF	Presentation "CyberSec4Europe Aiming to safeguard values through excellence in cybersecurity" at Panel "The EU Pilot Projects for the competence centre and ECSO"
22.04.2021	ECSEL Austria – https://www.ecsel-austria.net/news-events/events/events-detail/ecsel-austria-conference-144	GUF	Presentation "Europäische Cyber Security Strategie am Beispiel des Cyber Security Competence Center Networks CyberSec4Europe" at ECSEL-Austria Konferenz "Industrial Cyber Security". Update on CyberSec4Europe and its results
10.05.2021 – 13.05.2021 (Virtual)	PKC 2021 https://pkc.iacr.org/2021/	AIT	Participation in PKC 2021 and presentation of CyberSec4Europe paper on updatable signatures
20.05.2021	Cybershare 2021 https://www.cybershareconference.com/#/home/speakers/	GUF	Panel presentation at Cybershare Conference 2021, "Building the Cybersecurity Competence Center"
21.05.2021 (Ljubljana, Slovenia) (Virtual)	12th International Conference 'Days of Corporate Security 2021: https://www.ics-institut.si/assets/uploads/images/12th-international-conference-days-of-corporate-security/Program-Days-of-Corporate-Security-2021.pdf	TDL	Participation to a Conference
01.06.2021 (Virtual)	The Robot Revolution and Industrial IoT International Symposium 2021	GUF	Impulse Speech "Data Protection in the context of

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
	https://www.jmfrri.gr.jp/english/		IoT" at at German-Japanese iSec Expert Meeting #46
01.06.2021 (Virtual)	Privacy Symposium 2021 https://exp.infosysmeridian.com/register/Privacy_Symposium_2021	GUF	Keynote Standards in Privacy Management: Assurance to demonstrate accountability at Privacy Symposium 2021
10.06.2021 (Virtual)	Discussion with Dr. Petra Raderschall (Stiftung Warentest) as part of the Mercator Science-Policy Fellowship Program	GUF	Maintenance of Policy Community
16.06.2021 (Virtual)	IPEN Webinar 2021: "Synthetic data: what use cases as a privacy enhancing technology?" https://edps.europa.eu/data-protection/our-work/ipen/ipen-webinar-2021-synthetic-data-what-use-cases-privacy-enhancing_de	CYBER	Participated as virtual attendee
22.06.2021-24.06.2021 (Virtual)	IFIP Sec 2021 https://www.ifipsec.org/2021/	AIT GUF	Participation in IFIP SEC 2021 Presentation and Panel " EU Cybersecurity Competence Centre" at IFIP Sec 2021
25.06.2021	SENSYBLE Graduate School by GUF and Rhein-Main University of Applied Sciences Wiesbaden https://www.sensyble.org/en/	GUF	Presentation on CyberSec4Europe at SENSYBLE Workshop/Seminar
14.07.2021 (Virtual)	DIGITAL SME - Cybersecurity Competence Centre pilot projects: SME impact and opportunities	TDL	Participation in Conference
19.07.2021 (Virtual)	Panel at Brazilian Computer Society Annual Congress: Lack of privacy and behavioral control in a surveillance economy: Is another world possible? https://csbc.ufsc.br/eventos/secomu/	GUF	Presentation at Conference
20.07.2021-20.07.2021 (Virtual)	Workshop with KDDI Research including Presentation on CyberSec4Europe	GUF	Presentation at Conference
21.07.2021 (Virtual)	FSB (Financial Stability Board): Virtual Workshop on Cyber Incident Reporting	Intesa Sanpaolo	Workshop aim to discuss cyber incident reporting advantages and the benefits of Cyber Lexicon
12.08.2021 (Frankfurt, DE)	Discussion with Volker Saure and Günter Schuh (Deutsche Telekom)	GUF	Maintenance of Industry Community
16.08.2021–20.08.2021	IFIP Summer School on Privacy and Identity Management	AIT, GUF, KAU	CyberSec4Europe members contributed to the program

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
(Virtual)	https://ifip-summerschool2021.uni.lu/		committee, general chairs, and steering committee of the conference; Co-Chair from SPARTA.
17.08.2021-20.08.2021 (Virtual)	ARES 2021 https://www.ares-conference.eu/	AIT, UMU	Participation in ARES 2021 and presentation of CyberSec4Europe paper in FARES Workshop
06.09.2021-09.09.2021 (Lille, France) (Virtual)	FIC Forum https://2021.forum-fic.com/en/home/programme/programme-2021.htm	TDL	Participation in conference
06.09.2021 (Virtual)	Discussion with Daniela Schilling and Svenja Mohn (Vogel IT-Medien GmbH)	GUF	Maintenance of Industry Community
15.09.2021 (Virtual)	European Association of Biometrics (EAB) Research Projects Conference 2021 https://eab.org/events/program/219	GUF	Presentation on CyberSec4Europe
28.09.2021	Informatik 2021, Workshop Security, Datenschutz und Anonymisierung https://informatik2021.gi.de/call-for-paper/security-privacy	GUF	Awareness for Security and Privacy in the IoT
07.10.2021-09.10.2021 (Jeju Island, South Korea)	MobiSec 2021 The 5th International Symposium on Mobile Internet Security	UMU	Plenary talk
04.10.2021 (Ljublana, Slovenia) (Hybrid)	Slovenian EU Presidency and University of Maribor Conference Panel https://eu2021.dihslovenia.si/en/events/the-future-of-cybersecurity-in-slovenia-and-europe/	GUF	Participation in activities organized jointly with other EU projects Presentation on CyberSec4Europe at Presentations on Cybersecurity Competence Network Pilot Projects Participation Round Table – Establishment of Cybersecurity Competence Network in EU
27.10.2021 (Virtual)	18th IEEE Symposium on Visualization for Cyber Security https://vizsec.org/vizsec2021/	CYBER	Taking part in the conference, presenting the paper
27.10.2021 (Virtual)	SOTER Project: https://soterproject.eu/2021/10/08/cybersecurity-solutions-for-the-european-finance-sector/	TDL	Cybersecurity solutions for the European finance sector Participation in activities organized jointly with other EU projects

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
27.10.2021 (Virtual)	47th Latin American Conference on Informatics (CLEI) https://clei2021.cr/keynotes	GUF	Presentation on CyberSec4Europe as part of Presentation on Security & privacy in the IoT age
31.10.2021-04.11.2021 (Eindhoven, Netherlands) (Virtual)	ICPM 2021 Conference https://icpmconference.org/2021/ 3rd International Conference on Process Mining ICPM 2021	CYBER	Taking part in the conference, presenting the paper
10.11.2021 (Virtual)	Discussion with Dr. Annika Bolten-Drutschmann (German Foreign Ministry) as part of the Mercator Science-Policy Fellowship Program	GUF	Maintenance of Policy Community
19.11.2021-20.11.2021 (Virtual)	10. IT-Rechtstag Frankfurt	GUF	Event participation
02.12.2021-03.12.2021 (Virtual)	Workshop with KDDI Research including Presentation on CyberSec4Europe	GUF	Workshop with KDDI Research including Presentation on CyberSec4Europe
09.12.2021 (Virtual)	SOTER Project: https://soterproject.eu/2021/11/19/cybersecurity-insights-emerging-threats-in-europe/	TDL	Participation in activities organized jointly with other EU projects (CyberSec4Europe/ CONCORDIA)
19.01.2022 (Trento Vason, Italy) (Virtual)	NECS 2022 Winter School https://necs-winterschool.disi.unitn.it/	GUF	Presentation CyberSec4Europe at NECS 2022 Winter School
03.02.2022 (Brussels, Belgium) (Virtual)	EP ITRE public hearing on “European Digital Identity Wallet and Trust Services”	GUF	Testimony on the legislative proposal to establish a framework for a European Digital Identity - 2021/0136 (COD)
03.03.2022 (Tel Aviv, Israel)	Conference Cybetech Global https://www.cybertechisrael.com/global	ABI	ABI Lab presented the CERTFin and the initiatives in which it is involved.
10.03.2022 (Virtual)	SPARTA Day https://sparta.eu/events/2022-03-03-sparta-day-2022.html	GUF	Presentation "CyberSec4Europe Safeguarding European values through excellence in cybersecurity"
25.03.2022	Meeting CEPIS Legal and Security Issues (LSI) Network	GUF	Maintenance of Scientific, Industry, and Policy Community
05.04.2022 – 07.04.2022 (Venice, Italy)	Privacy Symposium https://privacysymposium.org/	KUL, TDL, UMU ATOS	Participation in the Symposium. Talk on privacy redesign. Maintenance of Scientific,

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
		AIT TDL	Industry, and Policy Community Presentation of T5.3
04.05.2022-05.05.2022 (Virtual)	Workshop with KDDI Research including Presentation on CyberSec4Europe	GUF	Presentation on CyberSec4Europe as part of presentation on IoT Privacy
31.05.2022	KRAKEN project webinar Women in technology behind data-sharing, privacy preservation and SSI https://www.krakenh2020.eu/news/webinar-women-technology-behind-data-sharing-privacy-preservation-and-ssi	CYBER, ATOS	Delivered a presentation on "Privacy-preserving-precision-medicine"
03.06.2022 (Yokohama Japan) (Virtual)	iPOP 2022 18th International Conference on IP/IoT_&_Processing + Optical Network	UMU	Plenary talk
07.06.2022-09.06.2022	FIC 2022	TDL	Participated in meeting
08.06.2022-09.06.2022 (Warsaw, Poland) (Virtual)	Participation Debate: European mobile identity wallet – a potential worth exploiting	GUF	Participation Debate: European mobile identity wallet – a potential worth exploiting
11.06.2022 (Virtual	Presentation on CyberSec4Europe at SENSYBLE Workshop/Seminar https://www.sensyble.org/en/	GUF	SENSYBLE Graduate School by GUF and Rhein-Main University of Applied Sciences Wiesbaden
13.06.2022-15.06.2022 (Copenhagen, Denmark)	IFIP SEC 2022 https://ifipsec2022.compute.dtu.dk/program.html	DTU, KAU GUF	Panel on IT Security Presentation on CyberSec4Europe as part of presentation on IoT Privacy
20.06.2022-21.06.2022 (Dublin, Ireland)	4th Workshop on Internet of Things Security and Privacy (WISP)	UMU	CyberSec4Europe was one of the supporters of the workshop and delivered several presentations
22.06.2022 (Warsaw, Poland) (Virtual)	Internet Privacy Engineering Forum (IPEN) https://edps.europa.eu/data-protection/our-work/ipen/ipen-workshop-digital-identity_en	GUF	Maintenance of Policy, Scientific, and Industry Community
25.06.2022 (Warsaw, Poland)	XIV Konferencja Naukowa Bezpieczeństwo w Internecie – Hacking https://wpia.uksw.edu.pl/sites/default/files/KONFERENCJE/Klauzula%20informacyjna_hacking2022.pdf	GUF	Presentation on CyberSec4Europe as part of presentation on IT Security Certification
12.07.2022-13.07.2022 (Munich, Germany)	CODE Conference with NCC event https://www.unibw.de/code-events	GUF	Maintenance of Policy Community

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
15.07.2022 (Frankfurt, Germany)	Discussion with Markus Tschersich and Sarah Syed-Winkler (Continental Automotive Technologies)	GUF	Maintenance of Industry Community
25.07.2022-26.07.2022 (Frankfurt, Germany)	Discussion with Reinhard Botha and Luzuko Tekeni (Nelson Mandela University, Port Elisabeth, ZA)	GUF	Maintenance of Scientific Community
03.08.2022 (Vienna, Austria)	European Cybersecurity Challenge New study group for Feasibility study on European implementation of ISO/IEC 27701	BRNO	
16.08.2022-17.08.2022 (Saarbrücken, Germany)	Saarland University Summer School 2022 IT Law and Legal Informatics https://www.summerschool-itlaw.org/schedule.html	GUF	Presentation on CyberSec4Europe as part of presentation on IT Security Strategy
23.08.2022 (Vienna, Austria)	International Workshop on Continuous Software Evaluation and Certification (IWCSEC 2022) https://2022.ares-conference.eu/workshops-eu-symposium/iwcsec-2022/index.html	GUF	AssureMOSS https://assuremoss.eu/en/news/The-AssureMOSS-consortium-successfully-organized-IWCSEC-2022-in-Vienna
29.08.2022-31.08.2022 (Tokyo, Japan) (Virtual)	National Institute of Informatics (NII) Tokyo	GUF	Presentation on CyberSec4Europe as part of presentation on Long-term trends and strategies in ICT Security and cybersecurity considering multinational cooperation
30.08.2022–02.09.2022 (Virtual)	17th IFIP Summer School on Privacy and Identity Management; https://ifip-summerschool.github.io/	AIT, GUF, KAU, UMU, TDL	Steering Committee: GUF, KAU, AIT; several members in the PC; Presentation of T5.3
09.2022 (Hamburg, Germany)	Workshop Jahrestagung Gesellschaft für Informatik: Recht und Technik im Diskurs	GUF	
26.09.2022 - 27.09.2022 (Stockholm, Sweden)	Nordic Privacy Arena https://dpforum.se/seminarier/nordic-privacy-arena-2022/	KAU	Invited talk and panel on usable privacy
27.09.2022 (Hamburg, Germany)	Workshop Jahrestagung Gesellschaft für Informatik: Recht und Technik im Diskurs	GUF	Participated in Workshop

Table 12: Participation in International events

1.9 Other

1.9.1 AIOTI

Date & Venue	Committee	Title	Partners	Comments / Remarks /Outcomes
23.06.2022 (Dublin, Ireland)	Plenary	Plenary	UMU	Plenary meeting

Table 13: Participation in AIOTI

1.9.2 IoT Forum

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
20.06.2022- 23.06.2022 (Dublin, Ireland)	IoT Week	UMU	UMU coordinated several sessions and the workshop WISP within GIoTS
21.06.2022 (Virtual)	IoT Week https://iotweek.org/wp-content/uploads/2022/08/IoT-Week-2022-Program-Past-event.pdf	TDL	Participation in meeting

Table 14: Participation in IoT Forum event

1.9.3 AFME[1]

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
All year (Virtual)	AFME Cyber Security WG	Intesa Sanpaolo	Working Group organized by AFME about DORA, NISD Review and other cybersecurity topics
All year (Virtual)	AFME DORA Working Group	Intesa Sanpaolo	Meeting in order to discuss update and development about DORA regulation
15/09/2021 (Virtual)	Workshop with EBA on Incident Reporting Harmonization	Intesa Sanpaolo	Workshop with EBA on the project regarding the reporting of ICT related incident

Table 14: Participation in AFME event

1.9.4 CESICAT

Date & Venue	Event	Partner	Comments / Remarks /Outcomes
10.06.2022 (Virtual)	Collaboration T5.6 Medical Data Exchange demonstrator and CESICAT	ATOS	Juan Carlos Pérez Baún presents outcomes of Medical Data Exchange demonstrator to Centre de Seguretat de la Informació de Catalunya (CESICAT).

[1] Collaboration during all the year as Intesa Sanpaolo is an active member of this association

Date & Venue	Event	Partner	Comments / Remarks /Outcomes
			Agree on future collaboration.

Table 15: Participation in CESICAT event

1.9.5 CERTFin

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
18.03.2022 (Rome – Milan)	CERTFin's Steering Commitee meeting	ABI	Operational Directorare reported to the Steering Commitee the state of art about the European Projetcs partecipated by CERTFin.
16.02.2022 (Rome, Italy) (Virtual)	Cyber Knowledge and Security Awareness WG	ABI	Meeting of the Cyber Knowledge and Security Awareness WG of CERTFn, during which the Constituency was updated on the progress of all European projects.
25.05.2022 (Rome, Italy) (Virtual)	Cyber Knowledge and Security Awareness WG	ABI	Meeting of the Cyber Knowledge and Security Awerness WG of CERTFn, during which the Constituency was updated on the progress of all European projects.
15.07.2022 (Rome, Italy) (Virtual)	Cyber Knowledge and Security Awareness WG	ABI	Meeting of the Cyber Knowledge and Security Awerness WG of CERTFn, during which the Constituency was updated on the progress of all European projects.
28.09.2022 (Rome, Italy) (Virtual)	Cyber Knowledge and Security Awareness WG	ABI	Meeting of the Cyber Knowledge and Security Awerness WG of CERTFn, during which the Constituency was updated on the progress of all European projects.

Table 16: Participation in CERTFn events

1.9.6 EBF[2]

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
All year (Virtual)	Cloud Expert Group Meeting	Intesa Sanpaolo	Recurrent meeting of Cloud Working Group – EBF about cloud security topics
All year (Virtual)	Cybersecurity Working Group	Intesa Sanpaolo	Recurrent meeting of Cybersecurity Working Group – EBF about Cybersecurity topics
27.01.2021 (Virtual)	EBF - Incident Reporting	Intesa Sanpaolo	Meeting organized by EBF on DORA with focus on Incident reporting
17.05.2021 (Virtual)	Exchange with SSM on biggest risks for Euro area banks	Intesa Sanpaolo	Meeting organized by EBF with focus on Cyber Crime and ICT Risk during the Pandemic

[2] Collaboration during all the year as Intesa Sanpaolo is an active member of this association

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
20.10.2021 (Virtual)	SSM (Single Supervisory Mechanism) CIO (Chief Information Officer) – CTO (Chief Technology Officer) Roundtable	Intesa Sanpaolo	Roundtable organized by EBF for CIO about Single Supervisory Mechanism

Table 15: Participation in EBF event

1.9.7 Europol

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
All year (Virtual) 25/05/2022 (The Hague)	EC3 Joint Advisory Group	Intesa Sanpaolo	Recurrent meeting organized by EBF and Europol on Cybersecurity topics

Table 16: Participation in Europol event

1.9.8 G7 CEG (Cyber Expert Group)

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
All year (Virtual)	G7 CEG Industry Group	Intesa Sanpaolo	Recurrent meeting in which Intesa Sanpaolo has been involved for representing Italy on cybersecurity topics
All year (Virtual) 20-22.07.2022 (Frankfurt, Germany)	G7 CEG workstream on 3rd Party Risk	Intesa Sanpaolo	Recurrent meeting in which are review paper on fundamental elements regarding 3rd Party in cooperation with the other G7 Institutions

Table 15: Participation in G7 CEG (Cyber Expert Group) event

1.9.9 IDSA

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
22.09.2022 (Virtual)	OPENDEI: Dealing with Data Spaces	ATOS	Juan Carlos Pérez Baún presents outcomes of Medical Data Exchange demonstrator during the webinar organized by the OPEN DEI project.

Table 17: Participation in IDSA event

1.9.10 IEEE

Date & Venue	Title of Event	Partner	Comments / Remarks /Outcomes
07.08-10.08.2022 (Haifa, Israel)	IEEE 35th Computer Security Foundations Symposium (CSF) https://www.ieee-security.org/TC/CSF2022/	CYBER	Taking part in the conference, presenting the paper

Table 18: Participation in IEEE Event

1.9.11 Research collaborations

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
April 2022	Attack Trees	DTU	Exploration of research collaborations between DTU and ISTI/CNR (associated researcher) on the understandability of Attack Trees (techniques at the core of research developed within WP3).

Table 19: Research collaborations between DTU and ISTI/CNR

1.9.12 Collaboration with local entities - Denmark

Date & Venue	Title of Event	Partners	Comments / Remarks /Outcomes
27.04.2022 (Copenhagen, Denmark)	NCC Engagement	DTU	Engagement with Danish NCC. Presentation of Cybersec4Europe to NCC, presentation of Danish NCC to DTU, Exploration of cooperation possibilities.

Table 20: Collaboration with Local Entities - Denmark

2 Third Concertation Event –"CONVERGENCE NEXT"

2.1 Background

During the project which started in 2019, **CyberSec4Europe** has hosted three concertation events involving the other three pilots (SPARTA, CONCORDIA and ECHO) as well as ECSO, the European Commission and others:

i. The first CONCERTATION event took place from 13-15 November 2019 at the Hotel de Région, in Toulouse, France. With three days of collaboration, conversation and networking, the event was very successful with high-level industrial, academic and governmental perspectives from DG CONNECT, the Occitanie Region, the French Government as well as the wider European cybersecurity community. There were also opportunities to hear each of the Four Pilots explain their results thus far and to explore synergies with the other pilots and other significant stakeholders.

ii. The second event, "CONVERGENCE" brought together the Four Pilots in a completely virtual manner from 9-11 December 2020. Each pilot presented its ongoing results and demonstrations and introduced the collaborative Focus Groups that showcased the cooperation between the pilots on certain related cybersecurity topics. Albeit only virtual, the event attracted a very large audience from 34 countries.

iii. CONVERGENCE NEXT, took place in Brussels from 1-3 June 2022 in a hybrid format (virtual and physical). In brief, the event focused upon the future of the community, the European Cybersecurity Competence Centre (ECCC) and looked at key issues for cybersecurity in the future. High-level representatives from European Union institutions discussed the role of the European Cybersecurity Competence Centre (ECCC) and that of the wider stakeholder community in the next stages. The proceedings of this event are given hereafter.

2.2 Conference Program

Web site: https://cybersec4europe.eu/events/concertation/convergence-next/

The programme agenda for CONVERGENCE NEXT was jointly developed around the following five principles:

1. The first panel session would be a presentation of the highlights of the Four Pilots and ECSO.
2. The sessions thereafter would focus on the community, with the Focus Groups on Governance and Roadmapping presenting their results.
3. Each pilot would have the opportunity to present their key results and demonstrations.
4. A final panel would bring high-level representatives from the European cybersecurity community together for a discussion on the vision for the future.
5. Every session could be done differently, and it was up to the session organiser to decide on the format and content (speech, panel, demonstrations, conclusions/recommendations) with the fellow panellists.

Thus, the structure of every session was different and is reported herein as such.

In brief, the CONVERGENCE NEXT Conference Program Agenda (Annex 1) consisted of the following outline:

- 1 June 2022 (half day and evening panel) – "Setting the Scene":
  - Highlights of the Four Pilot coordinators and ECSO

- Results of the Governance Focus Group and about the Competence Centre
- Panel discussion on the Situation in Europe (network and community)
- High-level evening panel discussion on the European Cybersecurity Competence Centre

- 2 June 2022 (full day) – "Research and Innovation":
  - Pilots presented their research results and demonstrations
  - Pilots presented their verticals
  - Perspectives of JRC and ENISA
  - Roadmapping for the Future

- 3 June 2022 (half-day) – "Sustainability and Expanding the Focus"
  - Cybersecurity education including the Education Focus Group and ECSO presented its results,
  - Panel discussion on the "Evolution of the European cybersecurity ecosystem"
  - The last panel brought together representatives from the cybersecurity community for a panel discussion "What Next".

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

The YouTube links to the three days of CONVERGENCE NEXT are available at:

Day 1: "Setting the Scene" https://youtu.be/jQ0PptjZfd4
Day 2: "Research and Innovation" https://youtu.be/lrjdHJsPYaQ
Day 3: "Sustainability and Expanding the Focus" https://youtu.be/CuKZ4a1POF8

2.3 Event Statistics

2.3.1 Web Site and Social Media

Web Analytics of CONVERGENCE NEXT on cybersec4europe web site (https://cybersec4europe.eu/events/concertation/convergence-next/)	**Statistics**
Number of users	646
Number of new users	396
Number of sessions	907
Top 10 country visitors to the web site	Belgium, Germany, China, UK, Italy, Spain, US, France, Greece, Poland
Twitter Impressions	7894

Table 21: Web site and Social Media Statistics

2.3.2 Registrations

In total, 230 participants registered for the event from 25 countries. About 100 participants selected an online participation. The top 10 countries are provided in **Error! Reference source not found.**, Figure 2

shows the distribution by Sector. Figure 3 provides an indication of the participation according to the Four Pilots.

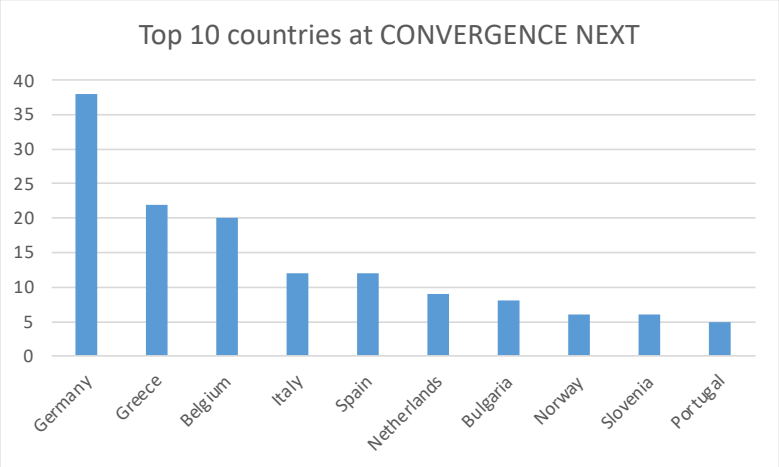


Figure 1: CONVERGENCE NEXT - Top 10 countries registered participation

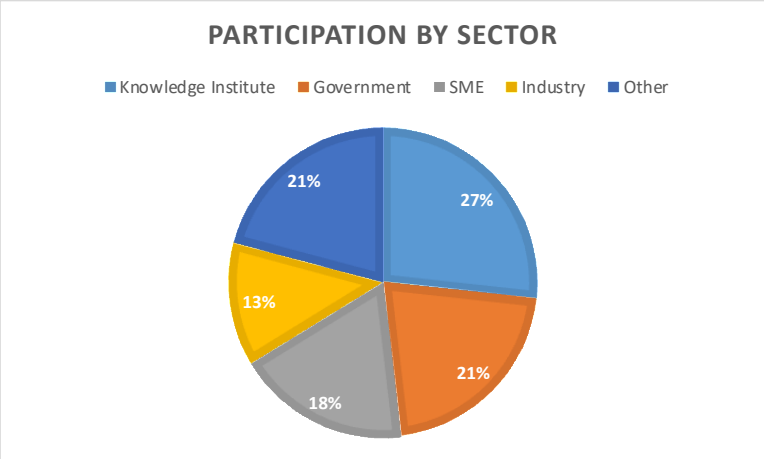


Figure 2: CONVERGENCE NEXT - Representation according to Sector

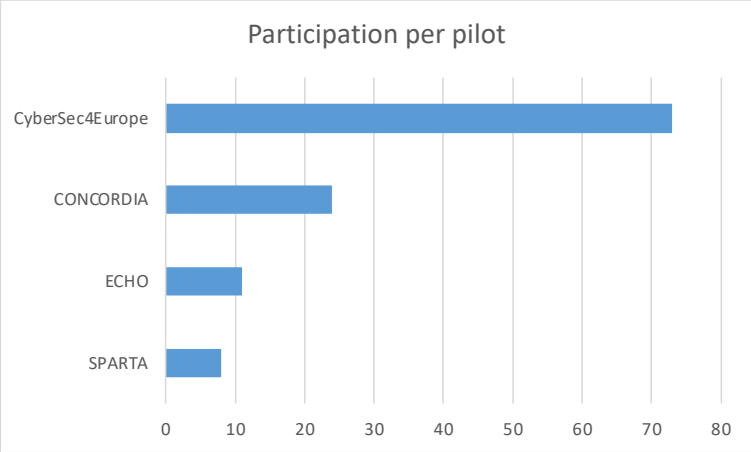


Figure 3: CONVERGENCE NEXT - Participation of Four Pilots

2.4 Opening Addresses

The event was opened by **Frank Wamser**, Head of Justice, Representation of the State of Hessen to the European Union who welcomed the guests and the panellists to the conference mentioning that it was indeed a good feeling to meet once more in person.

Kai Rannenberg (Project Coordinator, CyberSec4Europe) expressed his thanks to Frank Wamser and the Hessen representation for their hosting of CONVERGENCE NEXT in this difficult situation after Covid and further welcomed the participants to this hybrid event, which he described as partly a "working" conference given that, although much was accomplished through the pilots, there were still quite a few challenges ahead. He encouraged participants in the next days to actively engage in discussions, propose solutions to challenges as this was an opportune moment when the Four Pilots were present.

2.5 Panel Discussion: Highlights of the Four Pilots and ECSO

The Four Pilots introduced their projects' results starting with Gabi Dreo Rodosek (Project Coordinator, CONCORDIA), Florent Kirchner (Strategic Director, SPARTA), Wim Mees (Project Coordinator, ECHO), Kai Rannenberg (Project Coordinator, CyberSec4Europe).

Panellists:

- Kai Rannenberg, CyberSec4Europe
- Gabi Dreo Rodosek, CONCORDIA
- Wim Mees, ECHO
- Florent Kirchner, SPARTA
- Luigi Rebuffi, ECSO

Moderator: Kai Rannenberg, CyberSec4Europe

Annexes:

- Annex 1 – Agenda
- Annex 2 – Short Biographies
- Annex 3 – Presentation by Gabi Dreo Rodosek (CONCORDIA)
- Annex 4 – Presentation by Wim Mees (ECHO)
- Annex 5 – Presentation by Kai Rannenberg (CyberSec4Europe)
- Presentation by Florent Kirchner (SPARTA) is available only on YouTube at https://www.youtube.com/watch?v=jQ0PptjZfd4 at 06:41

View on YouTube: https://www.youtube.com/watch?v=jQ0PptjZfd4 starting at 02:04/8:38:40

2.5.1 CONCORDIA Pilot

Web site: https://www.concordia-h2020.eu/

Gabi Dreo Rodosek started with how, currently, the world faces several crises which also have a significant impact on Europe's security. Therefore, the European Union and its member states need resilience in all aspects of their functionalities. Cybersecurity is one of the main pillars of Europe's resilience strategy. The Four Pilots and ECSO are already in this area shaping the future of Europe's cybersecurity community.

In this scope, CONCORDIA provided significant contributions, primarily in building a European cybersecurity ecosystem, connecting research, the industry sector and SMEs. Figure 4 presents the highlights of CONCORDIA.

Figure 4: CONCORDIA's Highlights[3]

The project developed a CONCORDIA Service Board, with its eight aspects (Connects, Explores, Educates, Develops, Explains, Talks, Promotes and Assists), which is the main result of joint efforts to address cybersecurity-related challenges and offer the cybersecurity community in the long-term knowledge, tools and services necessary to strengthen Europe's digital resilience.

These also account for numerous research publications, the holistic CONCORDIA cybersecurity roadmap for Europe, CONCORDIA's platforms for Cyber Threat Intelligence for telcos and the finance sector, the DDoS Clearing House, the Cyber Range Ecosystem and the Kypo open source cyber range, the European Education Ecosystem for Cybersecurity, the CONCORDIA certification scheme, a network of different stakeholder groups, the manifesto on "Women in cybersecurity", as well as the ecosystem of start-ups.

2.5.2 ECHO Pilot

Web site: https://echonetwork.eu/

Wim Mees reflected on the last three years, looking back on how it all started, he recalled the importance of strategic autonomy and how the awareness or importance attached to this goal has tremendously increased over the last years. During Covid and with the conflict in Russia-Ukraine, the reliance on resources from outside Europe had a tremendous impact. In Europe, it became clear that it was important to be aware of which choices we make. In cyberspace, we need to be equally considerate and conscious of our choices, especially with regard to critical solutions and technology coming from outside Europe.

Wim further emphasized the good collaborative work between the pilots and ECSO. Each pilot and ECSO has built a community. Thus, there already is a cyber community. The real challenge is to bring those on board who are not active yet but who are dependent on cybersecurity. There was a need to reach out to this community, and therefore some questions that arise are: How can this actually be accomplished? What is

[3] Slide from Annex 3 (Presentation by Gabi Dreo Rodosek, CONCORDIA)

the value proposition that can be brought to them? What are the real needs of a particular sector, what are the interdependencies, where can a difference be made?

The partners in ECHO wanted to do more than just provide solutions, they wanted to develop solutions/platforms which would then stimulate the creation of many other solutions, i.e., creating a fertile soil where the ecosystem could grow. Some examples of this "fertile soil" are the ECHO Early Warning Systems and the Federated Cyber Range.

During the project, ECHO tried to see where value could be added to the different stakeholder groups. There was a constant process of assessing and validating, making sure that what was developed met the stakeholders needs. Thus, platforms were developed, and demonstration cases based on these assessments, then launched to test and validate those needs.

Error! Reference source not found. provides a snapshot of the Central Competence Hub and ECHO Governance model.

Figure 5: Central Competence Hub and ECHO Governance model[4]

2.5.3 SPARTA Pilot

Web site: https://sparta.eu

Florent Kirchner started with fully agreeing on the opinion of the other pilots of the need to focus on European strategic autonomy. The direction that SPARTA took was to look at European strategic autonomy through the prism of some of the developments that were necessary as an EU community to ensure European strategic autonomy. Some of the work could be incremental and could build on existing strengths or the existing momentum that was built, but some of the work needed to be in complete disruption of what has been happening, i.e. a strategic surprise.

[4] Slide from Annex 4 (Presentation by Wim Mees, ECHO)

This idea of strategic surprise defines high-risk and high-reward actions as a way to engage in both risky and complex developments, while driving those actions towards concrete and informative results.

SPARTA takes this perspective holistically, i.e., a through complete system for building mission-oriented actions towards strategic surprise, towards high risk and high reward, and looks at how this can contribute to some effect towards European strategic autonomy (Figure 6).

Figure 6: SPARTA's mission statement[5]

By using this mission-oriented research, SPARTA aimed to bring together a fragmented ecosystem and to build a coherence across a network of competence centres – a European Competence Centre. This required including a number of partners and a wider diversity of partners.

The strategic approach of SPARTA (Figure 7) was to aim at:

- Modular and responsible governance: able to adapt to changing technical landscape and geopolitical context.
- Respecting European values in Europe: SPARTA was mindful of ethical, legal and societal aspects. SPARTA used those aspects and embedded some of the questions into the work that needed to be done.
- Putting together a practical checklist for AI developers which required a lot of effort across communities, across a diversity of people.
- Building joint infrastructures – beyond the networking component – the community, Associates and Friends around shared tools and capabilities.
- Training – proactive to build better capabilities in terms of skills, mapping some education capabilities, helping design new Curricula through tools through new ways of thinking, geographies and localization.
- Outreach – contributed to the work, thought outside the box in terms of dissemination, how about the outermost regions, how are they included.

SPARTA's four high-risk high-reward research and innovation programs are:

[5] Screen shot from YouTube recording (Presentation by Florent Kirchner, SPARTA, https://www.youtube.com/watch?v=jQ0PptjZfd4 at 06:41)

- T-SHARK – Full-spectrum cybersecurity awareness,
- CAPE – Continuous Assessment in Polymorphous Environments,
- HAII-T – High-Assurance Intelligent Infrastructure Tool,
- SAFAIR – Secure and fair AI Systems.

A lot of positive results were achieved, including the ongoing work with the other pilots, in particular, on governance and the roadmap.

Figure 7: SPARTA's Strategic Support[5]

Florent expressed the hope that SPARTA has enabled and contributed to enact this vision of Europe as leaders in cybersecurity.

2.5.4 CyberSec4Europe Pilot

Web site: https://cybersec4europe.eu/

Kai Rannenberg began his presentation describing the core aspects of the common goal of the four pilots to safeguard European values through excellence in cybersecurity. All the four pilots were trying to overcome fragmentation and reach the goals of:

- Diversity and ethics;
- Risk acceptance;
- Horizontal leverage;
- Open leadership.

Kai continued to explain the four pillars of CyberSec4Europe, as given in Figure 8:

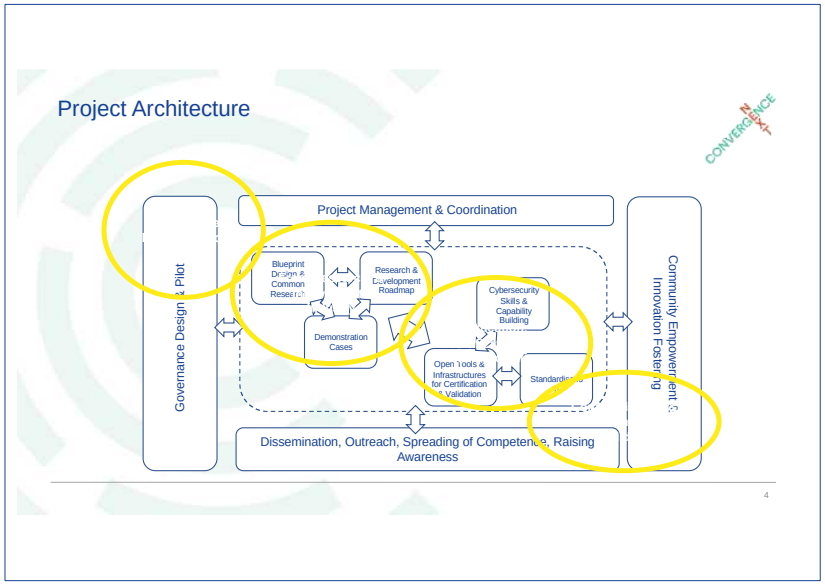


Figure 8: The four pillars of CyberSec4Europe[6]

With regard to governance some of the relevant aspects are:

- For the ECCC and any National Coordination Centre (NCC) organizing a community there are two key elements of trust:
  - Secured participation of community members even when they deliver "bad" news and
  - organizational transparency explaining what happens to delicate and sensitive information provided by community members.
- An **agile, trustful,** and **lively exchange** in and between **Cybersecurity Communities** is essential**.**
- Different stakeholders need to be integrated in the discussions.

The Focus Group on Research produced a joint perspective of the four pilots and ECSO, see Figure 9, in which their priorities in research and innovation are reflected:

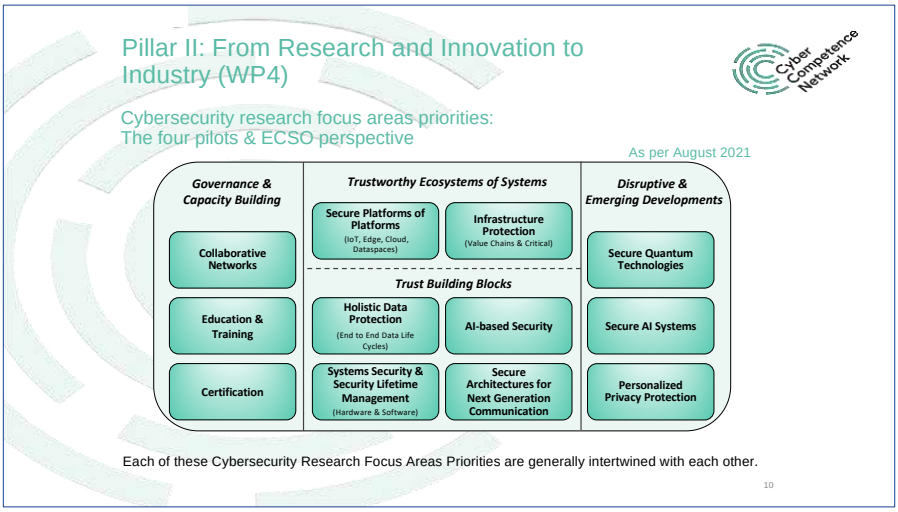


Figure 9: Cybersecurity Research Focus Area Priorities

[6] Slide from Annex 5 (Presentation by Kai Rannenberg, CyberSec4Europe)

Two of the main lessons learned were that there were two key elements of trust – secure participation and organizational transparency, and that there was an **agile, trustful,** and **lively exchange** in and between **cybersecurity communities.** Stakeholders were integrated in the discussions.

The Focus Group on Research produced a joint perspective of the Four Pilots and ECSO in which their priorities in research and innovation needed to be directed.

In conclusion, Kai highlighted the following key points.

CyberSec4Europe :

- Is a **vibrant** pilot **community**
- with an **agile approach** with regard to newly arising requirements and spontaneous requests by the EU, e.g. contributions to EC concept of strategic axis and JRC Atlas cybersecurity roadmap,
- spearheaded the design of a **distributed governance model**,
- progressed research and research planning based on **real** application requirements,
- progressed education, certification and standardization initiatives,
- integrated **all** pilots, ECSO and focus groups in a single **comprehensive event**:
    - **CONVERGENCE**, 2020-12-09/11, virtual
    - **CONVERGENCE NEXT**, 2022-06-01/03, Brussels, hybrid
- maintained an intensive made *interaction* with **ECSO** and delivered major *contributions*, implemented **principles** in **practice** (e.g. by establishing GDPR compliant open-source web conferencing through testing, using, and evaluating several Big Blue Button services and servers)

2.5.5 ECSO

Luigi Rebuffi recalled that it was in April 2017 that the idea of a European network of competence came about. What would this network or competence centre look like after having just created ECSO? Then, the pilots were formed to pave the path. Beginning January 2018, the question remained as to why the pilots were being built up. ECSO was not in the pilots, yet 40% of the pilots were also members of ECSO. Indeed, there were a number of questions at the very beginning of the pilots "The pilots - what for", "How will they cooperate with ECSO?", "What is the competition between the pilots and ECSO?", "Are they cooperating?" Are all these in competition or cooperating with ENISA and how with the new centre?

Now, at the end of the pilots, it is clear that there has been a lot of cooperation between the pilots and ECSO (and with ENISA) on many topics. It has been very interesting to listen to the achievements of the pilots. There were challenges faced and still there are challenges in the future. 65 Million EURO was invested in the pilots. At ECSO, there were very little resources but ECSO managed in a very different way. In the pilots, very interesting tools have been developed. In ECSO, there were limited resources to build tools but other ways have been found to build the community to a certain level, the point being is that the pilots and ECSO had different approaches.

Now, the challenge is to see how the very interesting tools which the pilots have produced, and the really good communities and concrete actions which have been created by ECSO and also the pilots, can survive. There is no time to reinvent the wheel. It is important to use what has been developed in the future. The question remains as to how this can be done.

A key word used this morning was TRUST. If there is knowledge or experience on how to build trust in a large community, then, there is a solid base. Trust and people working together is important in order to build whatever you want.

Europe needs to build TRUST and needs to build the communities, and then, Europe needs to build upon the community. This is the big message to the Commission – we need. It is necessary to use what has been done and **to** build on that.

In brief about ECSO, in the last six years, ECSO has worked on different activities, such as:

- **Public Private Partnership** to develop priorities for research and innovation. This work has been taken over by the different pilots as well.
- **Standards and certification**. ECSO is in the ENISA Advisory Group.
- **Investment in SMEs**. Dedicated to SMEs and start-ups, ECSO is trying to build a European Fund of Funds.
- **Different verticals**. Creating a European community of CISOs from different countries and sectors.
- **Outreach beyond Europe**. ECSO is working in different regions within Europe, already mentioned the SMEs and their capability to be visible and growing within the European market but also beyond. The first ever event in USA at RSA 2022, San Francisco, at which ECSO is trying to bring EU solutions to the USA.
- **Education and training**, Working Group 5 is working on a European Cybersecurity Skills Framework
- **Women for Cyber Foundation**. There are 15 Chapters around Europe and more to come.
- European Academy
- Job Platform
- **Technology**. Proposing priorities for technology, priorities for supporting sovereignty and strategic autonomy, link with EDA and ESA.

What ECSO has done is not so different from what the pilots have done and continue to do. It is really necessary to work together in a smart way and propose something to support what the EU institutional states want to build up but something closer to the map in real life.

2.6 Day 1 - Governance Session

"About the Competence Centre"

Panellists:

- Martin Übelhör, Head of Cybersecurity Industry and Innovation, DG CONNECT
- Natalia Kadenko, Coordinator of the Governance Focus Group
- Irena Mladenova, ECHO
- Arthur van der Wees, CONCORDIA
- Dirk Kuhlmann, SPARTA

Open floor discussion – Q&A

Session chair: Natalia Kadenko, CyberSec4Europe

Annexes:

- Annex 2 – Short Biographies
- Annex 6 – Presentation by Martin Übelhör (DG CONNECT)
- Annex 7 – Presentation by Focus Group on Governance:
  Annex 7, pages 4-13 – Natalia Kadenko's slides (CyberSec4Europe)
  Annex 7, pages 14-18 – Irena Mladenova's slides (ECHO)
  Annex 7, pages 19-28 – Arthur van der Wees' slides (CONCORDIA)
  Annex 7, pages 29-34 Dirk Kuhlmann's slides (SPARTA)

View on YouTube: https://www.youtube.com/watch?v=jQ0PptjZfd4 starting at 2:58:54/8:38:40

On June 1, 2022, to commence the "Convergence Next" afternoon session, the Governance panel was convened in order to discuss the past achievements and the future directions in this area. "Convergence Next" served as a focal point for highlighting the governance approaches at the time of ECCC and NCCC becoming active and functioning.

Martin Übelhör, Head of Cybersecurity Industry and Innovation, DG CONNECT shared the current status, ongoing processes and plans for the ECCC and NCCCs, as well as about the future calls for proposals. Martin explained the genesis and role of the Centre. He highlighted the envisioned cooperation with the national competence centres. During the Q&A, a member of the public requested to elaborate on the role of the Cybersecurity Community and their representation in the Centre. Martin has confirmed that the specially appointed Community managers for NCCCs would retain certain flexibility to design the approach best fitting for the community of their country and region.

2.6.1 CyberSec4Europe's Governance Approach

Natalia Kadenko (CyberSec4Europe) shared insights into the inspiration behind the creation of the Governance Focus Group. The underlying idea was to work together and see how different governance approaches can be complementing and help achieve the joint goal of setting up and maintaining the living and vibrant European cybersecurity community.

Natalia proceeded to share the CyberSec4Europe governance approach (**Error! Reference source not found.**), its evolution, and the case studies:

- Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs);
- The CyberSec4Europe concept: a flexible organization, accounting for the needs of the local community and creating real added value, combined with requirements for the CHECK establishment;
- Promoting the already existing and functioning structures, especially at national level, while actively pursuing the aim of a pan-European community;
- Community-level cybersecurity hubs which should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area;
- Shortening the chain between decision-making and existing needs on the ground;
- The governance model would benefit from accompanying European cybersecurity funding mechanisms in the next decade to increase funding and investment to build a pan-European community.

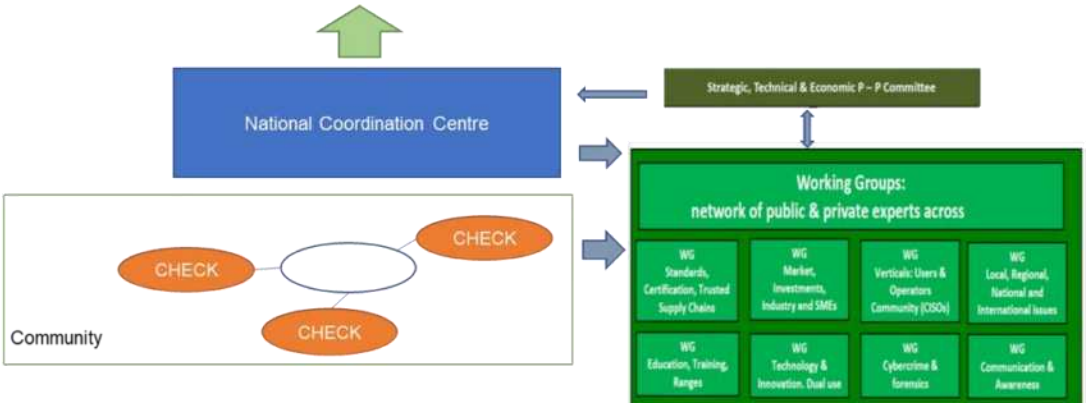


Figure 10: CyberSec4Europe governance approach[7]

2.6.2 ECHO's Governance Approach

Irena Mladenova (ECHO) shared ECHO's governance approach evolution (Figure 11). ECHO conducted extensive research and design work to identify and agree upon the best fitting governance model which would ensure sustainability and effective exploitation of the project achievements and assets. Discussions held throughout the ECHO network resulted in selecting a CNO model, with a Central Hub, National Hubs and Service Groups. Key processes were designed and tested through simulation games.

Upon decision to proceed with a "bottom-up" approach, ECHO now is piloting the establishment of one National Hub (Bulgaria) and one Service Group – Governance Consultancy Services (E-GCS).

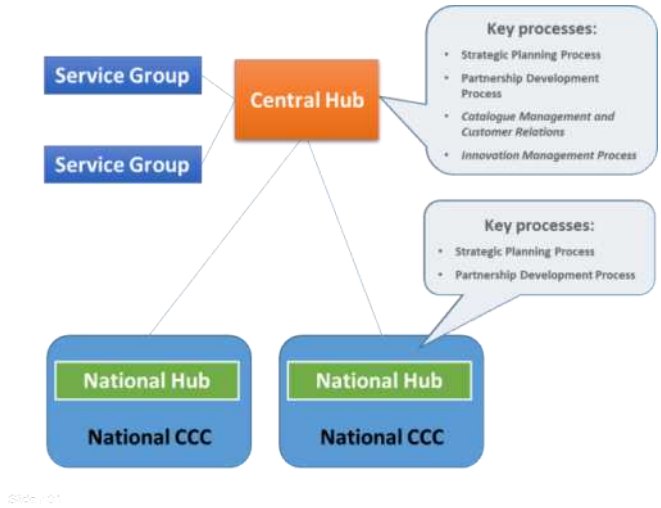


Figure 11: ECHO governance approach[8]

The Governance Consultancy Services (E-GCS) builds upon the experience of the team involved in research and design of the post-project ECHO CNO. The first consulting project is internal – E-GCS will support the implementation of the pilot National Hub in Bulgaria thus showcasing and improving the methodology developed. E-GCS has developed its Catalogue of Services and is now working on finalizing its Exploitation

[7] Slide from Annex 7 (Presentation by Natalia Kadenko, CyberSec4Europe)
[8] Slide from Annex 7 (Presenation by Irena Mladenova, ECHO)

Strategy. The business model envisaged is customer funded. E-GCS will work with the other ECHO assets to provide integrated services and will cooperate with National Hubs to extend its offering.

ECHO sees high potential of applying their expertise in supporting the structuring of the European Cybersecurity Community (our partnership development process being only one example). The transition to a sustainable cybersecurity community involves transition and change management challenges which they are preparing to support.

2.6.3 CONCORDIA's Governance Approach

Arthur van der Wees (CONCORDIA) outlined the main challenges in the form of practical implementation of the pilots' ideas for the bottom-up low-level governance (Figure 12).

He stressed the importance of trust and related trustworthiness as the main enablers, also in any of the cyber/cyber-physical domains, any community and any information sharing. He asked two important questions:

- Do we really know and understand the ecosystem and communities?
- And for these to thrive, how to team up, share and act?

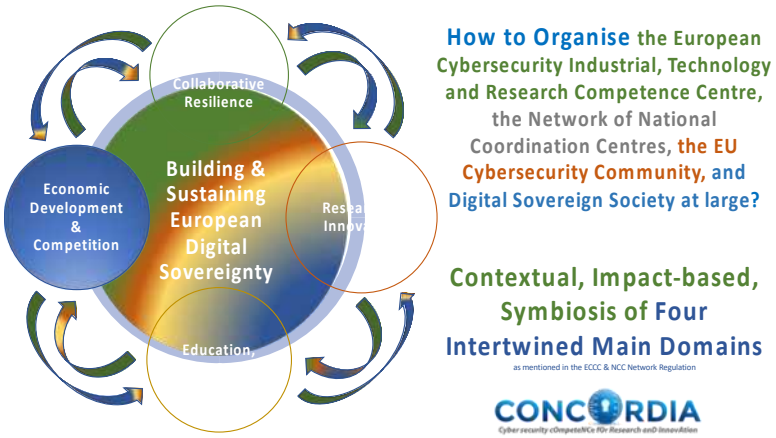


Figure 12: CONCORDIA governance approach[9]

2.6.4 SPARTA's Governance Approach

Dirk Kuhlmann (SPARTA) shared the evolution of SPARTA's governance approach (Figure 13) and outlined the main governance objectives:

- Set up the processes and governing instances for Cybersecurity Competence Networks,
- Animate the strategic direction at board and working group level,
- Ensure all stakeholder groups represented interact,
- Continuously assess performance and strategic direction.

[9] Slide from Annex 7 (Presentation by Arthur van der Wees, CONCORDIA)

Table 1: Typology of innovation agencies

	Radical innovation Shielded from interference	**Incremental improvements** Embedded in industries	
Targeted objectives	**State-led disruptors** *Radically innovative technological breakthroughs along a narrow, focused approach* Examples: DARPA, ITRI Governance goals: design new domain-specific technologies up to the level of early stage products with key industries	**Directed Upgraders** *Incremental innovation mobilizing resources around a relatively narrow range of industries and activities, facilitating large-scale change* Examples: A*Star, CORFO Governance goals: steer technological development, attract investments in key sectors	Mission-oriented and prize- driven innovation Significant resources Targeted technology fields
Wide-ranging objectives	**Transformation enablers** *Radically innovative, large number of small-scale experiments* Examples: OCS, Sitra Governance goals: develop clusters of innovative, high-productivity, research-intensive enterprises	**Productivity facilitators** *Small-scale, incremental product and process innovations across a wide range of established industries* Examples: GTS Institutes, IRAP Governance goals: creating local networks and organizing R&D communities	Delegated innovation objectives and R&D Modest resources Maximized application fields

Figure 13: SPARTA's governance approach[10]

2.6.5 Conclusions/Results

To conclude:

- The pilots have conducted extensive work on identifying stakeholders needs and have identified common objectives.
- Mapping and understanding the community has been done by all Four Pilots + ECSO, with a lot of thought going into ways of (formal) community involvement.
- The pilots have arrived at the different forms of cyber regions, regional/sectorial hubs, or similar as a form of cybersecurity community organization.
- The need to involve underrepresented actors and incorporating grassroot initiatives has been identified as an important priority

2.6.6 Next Steps (Recommendations)

The next steps/recommendations are to:

- Proceed with the ongoing concepts/tests of the hubs,
- Proceed with stakeholder mapping,
- Maintain contact in order to work out our respective priorities,
- Make sure that the cooperation experience and the established connections do not get lost after the pilots conclude,
- Ensure Long-term strategic cooperation and coordination,
- Continue to build trust.

[10] Slide from Annex 7 (Presentation by Dirk Kuhlmann, SPARTA)

2.7 Day 1 - Panel Discussion: Situation in Europe (Network and Community)

Panellists:

- Kai Rannenberg, CyberSec4Europe
- Gabi Dreo Rodosek, CONCORDIA
- Wim Mees, ECHO
- Florent Kirchner, SPARTA
- Luigi Rebuffi, ECSO
- Artur Kozłowski, EARTO SDWG

Moderator: Mark Miller, CyberSec4Europe

Annexes:

- Annex 2 – Short Biographies
- Annex 8 – Presentation by Artur Kozlowski, EARTO SDWG

View on YouTube: https://www.youtube.com/watch?v=jQ0PptjZfd4 at 5:08:08//8:38:40

2.7.1 Current Situation in Europe

Mark Miller introduced the participants and explained that the idea of this panel discussion was to reflect on the situation in Europe, the first question to the panellists being "Where are we as a network and as a community?"

The following points were made regarding the current situation in Europe from the perspective of the network and the community:

- **Relevance of pilots in a resilient Europe**: Since the pilots started in 2019, there were many challenges such as the pandemic and supply chain risks and the relevance of the Four Pilots increased significantly. The pilots provided and continue to provide solutions for the future, best practices and they continue to build the community and cooperation. Therefore, their role in the situation in Europe, in providing results and bringing together different sectors of the community for a resilient Europe is still very relevant.
- **Growing trust through the pilots**: With different countries, different procedures, and different cultures in Europe, it is clear that trust is a pillar in cybersecurity. Information sharing, especially across borders and sectors, is based on trust and connected communities. The pilots have contributed to building trust but the work is not over. The question remains how can trust be built with the new structure in place, not only within the research and technology communities, but also within the operational communities.
- **Four Pilots and ECSO**: From a community standpoint, a very positive collaboration was that of the Four Pilots and ECSO working as a "proto-community" together. This was a major step forward recognizing that these entities made partnerships, despite the constraints of two years of Covid, and used the benefits from their complementary approaches to interact with each other more. The questions covered by the pilots about how building the network complement each other have attracted a number of actors and partners and it is a solid basis to continue.
- **Collaboration of the ECCC and National Centres**: This development was deemed positive and encouraging. The national dynamics around cybersecurity are on their way and even if the level of maturity differs, this is a major step forward.

- **Promoting European products yet being cost-effective**: The challenge remains to bring European products to a marketable level.
- **Approach to community building across borders**: With diverse approaches in hand, the question of the best way forward to promote constructive community building still remained a challenge. Whilst there was no clear way forward, it was deemed important to encourage European actors to step forward and to take part in constructive contributions across borders.
- **Diversity and priorities in Europe**: There are challenges in the diversity in Europe across the community and there is still work to be done on lowering the gap between members and communities. A particularity of Europe is that priorities also change according to a geographical situation, for example, some parts of Europe may be more interested in the road map and the plans of the EC if they are situated closer to Brussels, whereas other parts of the community have to deal with other urgencies. The topics of conversations are widely different in how we perceive and state an urgency. This will be a challenge in the current setting.
- **Communities**: Across Europe, there is a homogeneity of interests within a community which is not the case for communities at a national level. With the new centre in Bucharest the idea was that there would be national communities. However, the national communities are very different from country to country, because of differences in budget, local challenges and priorities. The main challenge ECSO and some of the pilots have started to work on is the heterogeneity.

2.7.2 Pilots' Results and Achievements

Mark Miller continued the discussion with the next two questions: "What happened over the last periods and what is each one's view as the best achieved result from the Four Pilots?" The following highlights were noted:

- **Trust between the pilots developed:** At the start of the pilots, the outcome was not clear. After three years of working together and alongside, building the platforms for different sectors, building cyber ranges, educational frameworks, educational skills, and standardization, the pilots have shown how they have brought the communities together in building a network. The knowledge, confidence and the commitment make us stronger together with the most important outcome of creating proto-communities was the creation of trust.
- **Community-enabling** by the pilots – Bringing together so many people from different backgrounds:
    - **Results driven by considerable funding**: The ground for the community enabling was built by ECSO but the pilots received considerable funding (64 million) for more collaboration. Due to these resources, there were increased results. A contribution of the pilots is to have built a community working together and producing interesting results which was the borne from the fact that there were resources to work together. This was a significant achievement.
    - **Working together and learning together**: A community is not just a group sharing the same interest, but also working together with a common goal and support each other. In particular, the different groups across the pilots were working together and learning together, e.g., the governance group, the roadmapping group etc., which was supported and accelerated through the pilots.
    - **Communities and sub-communities**, e.g., educators and researchers, connected, which then contributed to the achievement of the demonstrators of all the pilots in different areas and this would not have happened without the pilots. There is a European footprint in the standardization community. Thus, community enabling was also a major achievement.
    - **Collaboration beyond the comfort zone:** Collaboration between people from other areas or groups with which one usually would not be interacting with took place on a daily basis. The resources allowed people to reach out to new parts of the community and discuss, develop and work together. They felt more comfortable and secure and trust was growing.

- **ECSO and positive actions**: One of the most interesting and rewarding results was bringing people together, finding a common interest and trying to build something where ECSO was only providing an umbrella and did not control anything, for example, Women4Cyber, the fund for European start-ups. This has been very rewarding in that there was a dynamic rising without further pushing for it.

2.7.3 Recommendations to Benefit the Community and Networks

Mark Miller continued with the next question "You have mentioned challenges, sustainability, and how to bring results to the network and the communities. Where, when and how should the European Cybersecurity competence centre invest for the benefit of the community and the networks?"

A summary of the replies received is given below:

- **EU Programs for funding:** The programs are late in being issued. The longer the wait the less competitive we will be.
- **Emphasis on the importance of education and training**. There are few resources, the outcome is very little compared to the actual needs. Education is a national priority. There should be a coalition between the countries, the European Commission and the private sector to be more active in education. It can be a long-term goal but there is need for a strategic decision as to how we can develop and keep competence in Europe.
- **Strategic thinking**: First develop IT, second build start-ups and third develop competences. It is a strategic approach. In the competence centres, there are priorities, and the pilots are developing road maps and proposing the next priorities. Europe needs to be faster and more agile. The pilots have provided the groundwork, Europe needs a push fast forward.
- **ECCC needs to think bigger** – diversity in funding models is necessary:
    - Start-ups should not be the only way forward, there should be a diversity in the funding models, including education.
    - Experts for cybersecurity are just not available in the same quantity. Thus, concentrated efforts and approaches towards the application areas are necessary.
    - The joined pilots' research road map was a great idea especially the part referring to dealing with disruptive elements.
    - There is the need to also bring citizens on board. Think about reaching all citizens in user-friendly ways, the example of the "European Digital Citizen Surf machine" was given. This is a device which elderly people can reliably and securely use without assistance.
    - A global and comprehensive strategy is necessary as technology is not sufficient for start-ups. Hiring or developing marketing skills to sell the European products and technologies is necessary. Europe lacks the competence to sell a product if compared to Great Britain or the United States.
- **Europe needs to be more ambitious, fast and proud of its accomplishments:** At the European level, we need to be more ambitious in many sectors, including building solutions in Europe and keeping them European in order to build an eco-system. A lot of work still needs to be done and Europe needs to be faster.
- **Sustainable communities**: It is important to provide communities with ways to organize themselves in a sustainable way, to come up with a structure and mechanisms which can sustain time and be the vector of the community to ensure that it can rise up in an agile manner in the face of new challenges. Mechanisms should challenge the community and enable the community to listen to each other and to create the European culture and European values around cybersecurity to build faster strategies or reactions. This is a mandatory building block.
- **Think forward**: Consider what the market will look like in years to come. From a perspective of children and human resources, what will it look like when they enter the job market? In the future,

cybersecurity will increasingly be driven by artificial intelligence and Europe needs to put more focus on this aspect of the market and what it will look like in 15 years.

To close this session, Mark asked each panellist for a 30 second statement to convey the message they want to give about the network and the community in Europe. The following statements were made:

"*The most important is trust."*

"When you have trust, you can build a community and when you have a dynamic community you can do whatever you want."

"Ambition hell yeah"

"Grow the networks."

"Think big"

"For the size we want to achieve, we need to take the citizens with us. Otherwise, we will not get the support and trust we need to mobilize the resources that we need. So, we need to have the citizens in mind, we need to be able to explain the citizens what we are aiming for and why we put this on."

2.8 Day 1 – Evening Panel discussion: The European Cybersecurity Competence Centre (ECCC)

Panelists:

- Katarzyna Prusak-Górniak, Vice-chair, ECCC Board
- Lorena Boix Alonso, Director for Digital Society, Trust & Cybersecurity, DG CONNECT
- Dörte Rappe, Chair NCCC Germany, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Luigi Rebuffi, ECSO
- Fukami, cybersecurity savant

Moderator: Kai Rannenberg, CyberSec4Europe

Annexes:

- Annex 2 - Short biographies

View on YouTube: https://www.youtube.com/watch?v=jQ0PptjZfd4 at 7:00:29/8:38:40

Frank Wamser welcomed the guests and the panellists to the evening panel discussion and event, which brought together the experts in the field European cybersecurity stakeholder community. The issue of cybersecurity was more pressing than ever, and all participants hoped that the establishment of the European cybersecurity competence centre (ECCC), in Bucharest, would contribute to stronger cybersecurity for the European Union. An important step along this path and the subject of the evening's panel discussion was the relationship between the ECCC and the wider cybersecurity community, as well as the institutions of the European Union. He wished all participants a successful evening with insights into the ECCC, noting that it was once more very agreeable to have an in-person event.

Kai Rannenberg expressed his thanks to Frank Wamser and the Hessen representation for their hosting of CONVERGENCE NEXT.

As Moderator, Kai introduced the distinguished panel of experts and put forward his first question: "In your view, where do we stand with this initiative compared to your expectations when we started?"

For the first round, each panellist was requested to state their view, before the panel was opened up for interactions. The following key points emerged and are summarized below:

- **The ECCC is an urgent body to set up:** ECCC is no longer a necessity but an urgency. Since the proposal establishing the ECCC went into force in September 2018, the issue of cybersecurity has exploded, first with Covid, and now with a rise in cyberattacks since the Russian invasion of Ukraine. These events show that the centre is not just a necessity, but it has become an urgency in order to improve the research and innovation capabilities in cybersecurity in the European Union.
- **Organizational Structure**: The Centre is a particular kind of body due to its dual role. It is not a simple implementing agency, but it has a broader, strategic task to ensure that all existing expertise is aligned, that all stakeholders are involved and that the whole framework that is foreseen in the regulation works. The centre also does not exist in a void, it has to fit in with what is already there with all its tasks and strategic objectives, with a working organisational framework incorporating the National Competence Centres (NCC), the community, and the strategic advisory group.
- **Regulations in place**: The main challenge during the negotiation phase was to ensure that all the regulations were correctly written and worked in practice. Looking forward, the main expectation is to finalise the setup of the centre and ensure all necessary documents are in place to ensure that the community involvement and that the national coordination centres work, as the regulation foresees a bottom-up approach, where the national coordination centres gather community members, assess them, and register them.
- **Priorities for investment**: There is a need to set priorities for investment.
- **Fragmentation**: the existing fragmentation of efforts has to be overcome. A lot has already happened since the ECCC came into force, the national coordination centres are coming together and defining strategic priorities. It now becomes urgent to set the strategic agenda, to have all the contributions from all the working groups and have the cyber community very active in this process.
- **The community**: The community is the third pillar next to the ECCC and the national competence centres, and the Four Pilots and ECSO are a part of that community. These bodies need to be united, also with national groups without any important player left out. The results thus far produced should be built upon and not forgotten.
- **ECCC Application process**: It is hoped that the complexity of the application process may be reduced, so that the success of an application depends on the expertise and technical knowledge of the applicants. A key issue will be finding skilled academic staff with competitive salaries within the industry so that job security can be offered and a more stable future.
- **Competence in Europe:** There is a need to develop and keep competence in Europe. There is a need to fill the 500,000 shortfalls of experts in Europe.
- **Citizens**: Whilst there is a need to educate citizens about growing threats, there is also a requirement to protect them when building technology which is continuously evolving so that there is protection on the one hand and trust that security-related concerns have been duly been addressed. It was noted that in some countries, measures are being taken, for example, schools in Germany are already teaching children what they need to be aware of. This is something that could possibly work across all of Europe, if something like this is put on the agenda so that wide groups of European citizens can be reached. On the other hand, with the advance of technology, it is necessary to ensure that senior citizens are not left behind in the development of technology, i.e., means are put in place to protect them. At the same time, on a personal family basis, generations can communicate the do-s and don't-s because the human factor is a serious threat and the means to educate people on basic rules is necessary.
- **Competitiveness in Europe**. There is a need to build competitiveness in Europe. The traditional approach of the Commission was to focus on research and innovation (R&I), for which the centre

is also dedicated, but there is more than R&I, there is a need to bring competitiveness to the European economy, not just to supply cyber security but also to protect Europe in the digital transition. For now, the private sector still considers the centre and the national coordination centres as a public-public endeavour. The key question which remains is how to involve and cooperate more with the private sector since it has the knowledge and the competence, and it has to face cyber threats every day.

- **ECSO**: While the ECCC will take a certain time to get organised and start producing results, ECSO is already discussing with the European Commission on how it will evolve and how ECSO can help during this period to bring together all stakeholders at the European level. The NCC is one of the key points and there is a quick win in this process. There is need for this national coordination, some countries are more mature and others are less mature.
- **Trust:** Trust was mentioned several times. The question remained how does the proposed structure of the ECCC and the NCCs intend building trust.
- **Good news:** The Cyber Resilience Act would be adopted in September and it would impose requirements on the producers of devices to ensure that seniors would not need to worry about cyber security because this will be a mandatory requirement.
- **Funding**: One of the reasons why the Cyber Competence Centre Network (CCCN) is important is that they trust that the NCCs will be able to advise potential applicants, and that they will be able to distribute EU funding via cascading. There is hope that this will be a way to help SMEs apply for funding. The cyber community is very important, and one of the ways to build trust is to work together from the beginning.

Kai Rannenberg closed the first round of contributions and opened the floor for questions.

Question 1: Whilst we are discussing, building these competence centres, what are the problems we are trying to solve? What are the maybe three major threats or adversaries that the panellists see? And what are the major benefits that the competence centres give the citizens?

The reply to the above question included the following comments:

- **Align the scattered expertise**: The main objective behind the centre is to pull together the scattered expertise and align it, so that there is a common vision and strategic objectives.
- **Offer citizens high quality European solutions**: The final goal is to offer citizens European solutions which are built upon the highest standards. The ultimate benefit of the Centre has to be for the citizen and citizens will only benefit if Europe is organised.
- **Diversify and widen the approach for awareness and dissemination surrounding cybersecurity**: Some ideas were discussed, for example, some of the national competence centres have departments for their citizens and would there be plans to make such departments work together. Another interesting idea was a German solution to provide young children with a story book on data protection advice – could this be something that could work across all of Europe, in an effective approach to reach a wider group of European citizens.
- **Avoid fragmentation:** It was emphasized that resources will be wasted if everything we build is fragmented.
- **Provide sound solutions by bringing communities together**: In order to ensure that the solutions selected are the right ones, it would be important to bring together the industry, the NCCs, with the public authorities.

Question: How is Working Group 4 and their work on the strategic research and innovation agenda being organised? The whole day there was talk about the need to organise the community, but not about how it is going to be achieved.

The reply to the above question included the following comments:

- **Procedures are in place**. There are four work streams, for example, work stream one for the guidelines for the assessment administration and the work there is done by the governing board members. There are procedures in place to facilitate discussion and decision making. The community will be set up top-down and bottom-up, at the national and regional level, but also by sector, and some of the structure will be created by the governing board.
- **Trust:** The community still needs to be built upon, and trust between the communities is a key factor.
- **European products:** Having a strategic agenda is positive – it helps if everyone contributes and states what is needed as the goal is to have European products.
- **Vulnerability disclosures**: The directive proposes a Coordinated Vulnerability Disclosure (CVD) system which would be held by ENISA.

Question: How would the data protection community be included in all activities of the centres? Is this something that will be done informally or is there an institutional setting?

Answers:

- **Data protection by design**: DG CONNECT employs data protection by design rule so all solutions have to be fully in line with the GDPR.
- **Certification and balance is necessary**: It is a challenge that if one wants to come up with a new and innovative product, there is a need for a lot of certifications, and NIS2 (Network and Information Security (NIS)) will also have legal requirements. The balance of making something secure and also in line with privacy and data protection requirements necessitates acting fast.

Question: Will the ECCC make cybersecurity a new European human right?

Answers:

- There is a German Federal Constitutional Court decision that makes a certain level of IT security a fundamental right.
- The European Commission adopted the communication on the digital decade that proposed an institutional charter of digital rights which includes cybersecurity as a digital right for citizens.

In closing, Kai Rannenberg asked the panellists to give one final piece of wisdom, which are summarised below:

> *Wishes of good luck to ECCC and the NCC and hopes that everything "goes down the way they hope"!*
>
> *Hopes that data protection is not just about ID protection, but for the economy it is also very important to take care about national security*
>
> *There are many expectations for the ECCC and the NCCs… hopes that they succeed in fulfilling some of those, as they are doing their best to do so.*
>
> *A number of keywords were important, like trust, as is the essence of this big project. Do not forget about the main mission, which is to protect citizens, and this as an endeavour of all of them together. They need the community, industry, the authorities, and citizens involved.*

All stakeholders are encouraged to actively engage with their NCCs, as there is a bottom-up approach so the NCCs need the import to pass it on to the ECCC, so they can build a good strategic agenda. They are waiting for the call for the director for the centre to be published, everyone is encouraged to take a take a look at the call, and if they are eligible, to make an application.

Kai Rannenberg closed the panel discussion repeating that everyone who was interacting with the ECCC and the NCCs should not just deliver problems to them and let them alone with it. The interaction is important. His message to the NCCs and the ECCC, if they ever thought this was an easy job, that was a misunderstanding, as then it would not have been given to them. He thanked the speakers and invited all to the evening social gathering.

2.9 Day 2 - Research results sessions and demonstrations

Panellists:

- Antonio Skarmeta, CyberSec4Europe
- Antonio Ken Iannillo, CONCORDIA
- Peter Hagstrom, ECHO
- Augustin Lemesle, SPARTA

Session chair: Wim Mees, ECHO

Annexes:

- Annex 2 – Short Biographies
- Annex 9 – Presentation by Antonio Skarmeta (CyberSec4Europe)
- Annex 10 – Presentation by Antonio Ken Iannillo (CONCORDIA)
- Annex 11 – Presentation by Peter Hagstrom (ECHO)
- Annex 12 – Presentation by Augustin Lemesle (SPARTA)

View on YouTube: https://www.youtube.com/watch?v=lrjdHJsPYaQ starting at 08.30/8:00:30

2.9.1 Challenges

The different pilots presented the collection of challenges covered during the last 3 years.

CyberSec4Europe presented their program for research and innovation covering:

- Privacy-preserving IdM, strong AAA and secure & private communications,
- Usability aspects of security assets,
- Certification frameworks and continuous monitoring,
- Automated tools for verification and enforcement of security policies in software,
- GDPR compliance for use in SMEs,
- Methodology for the individualized evaluation of requirements,
- Advanced threat intelligence services for deploying adaptive security solutions.

ECHO focused on different challenges, as follows:

- 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.

SPARTA presented, as a main driver, the results of their work on how to trust AI. They considered that AI has started to be used in various contexts and overall:

- A lot of progress has been made in recent years,
- AI is much more widespread,
- It has started to be used in an industrial context,
- It is sometimes used in safety critical systems,
- Apart from achieving good accuracy, there are many challenges that still need to be discussed to effectively apply AI in critical applications.

CONCORDIA covered five different areas of research considered in its pilot, in detail, as follows:

- Device-centric security,
- Network-centric security,
- System/software-centric security,
- Application/data-centric security,
- User-centric security.

All the challenges are quite complementary and they created some common vision that also contributes to the common roadmap definition in collaboration with ECSO.

2.9.2 Overall Results of the Four Pilots in Research

Regarding the results, all pilots have been quite successful in reaching most of the objectives and, more importantly, generating demonstrations in the verticals and, in some cases, an integrated combination of assets. A summary is given below:

CyberSec4Europe – all assets where integrated in a functional cybersecurity architecture based on the research work, considering:

- 75 assets that were evolved within the project lifetime,
- 18 of them in the process of integration with vertical demonstrators,
- All the assets have been described and documented with videos and papers in a GitHub repository where the reader can find a summary of each task's goals, resources (videos and papers), and asset descriptions. Each task page also contains a table where the different assets have been grouped per building block as defined in the common roadmap.

In addition, CyberSec4Europe as part of its main results summarized that:

- Multiple collaborations on research papers and asset interaction at intra- and inter-task level has been established,
- Assets have been instantiated for demonstration scenarios,
- Collaboration has been established with verticals, CONCORDIA and ECHO based on WP3 assets,
- Contributions to the joint pilot research roadmap have been done based on the work on scouting for new cybersecurity trends.

SPARTA provided examples of the different results with a video covering the main area of Secure and Fair AI Systems for the Citizen (SAFAIR) which included robustness against attacks, and explainability and fairness.

Additionally, the results described were:

- AI Threat Knowledge Base (also evaluated by experts),
- SAFAIR AI Contest,
- Study of the implication of GDPR to AI systems,
- Fairness in "The Artificial Intelligence Act".

ECHO targeted the practical use of outcomes to offer technologies and services having increased cyber-resilience by sector and among inter-dependent partners and presented the following tools:

- Use of E-FCR for experimental simulation of cyber-attack scenarios, pre-production testing, product evaluations, training,
- 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..), potentially at EU level,
- 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.

CONCORDIA concluded that research activities were developing well covering many different aspects and that there were strong links to activities in other CONCORDIA work packages.

The experience with Covid in 2021 influenced in greater or lesser ways, for example, there was limited impact on actual research itself (i.e., work often did not require access to labs), however there was a bigger but highly varying impact on the individuals doing research, and it was difficult to create spaces for creative moments within a project.

2.9.3 Recommendations

There was strong agreement about the success of the results achieved by the pilots in the area of research and innovation. Concretely, it was important to highlight that all pilots agreed that it was a critical issue to continue the collaboration as they had produced very relevant results. The idea of identifying possible innovation and work towards products and solutions was also mentioned as very important to support European digital sovereignty in cybersecurity area.

2.10 Verticals

Panellists:

- Alessandro Sforzin, Christos Grigoriadis, CyberSec4Europe
- Thanh van Do, Boning Feng, Bernado Santos, Madalina Baltatu, CONCORDIA
- José María Torres, ECHO
- Thomas Jensen, SPARTA

Session chair: Wim Mees, ECHO

Annexes:

- Annex 2 – Short biographies
- Annex 13 – Presentation by Alessandro Sforzin and Christos Grigoriadis, (CyberSec4Europe)
- Annex 14 – Presentation by Thanh van Do, Boning Feng, Bernado Santos, Madalina Baltatu (CONCORDIA)
- Annex 15 – Presentation of Verticals by José María Torres (ECHO)
- Annex 16 – Presentation of Verticals by Thomas Jensen on behalf of Gabriele Costa (SPARTA)

View on YouTube: https://www.youtube.com/watch?v=lrjdHJsPYaQ starting at 2:21:49/8:00:30

2.10.1 CyberSec4Europe

Presented by Alessandro Sforzin and Christos Grigoriadis, CyberSec4Europe.

CyberSec4Europe analysed the cybersecurity landscape of seven industrial verticals, namely Open Banking, Supply Chain Security, Privacy-Preserving Identity Management, Incident Reporting in the Financial Sector, Maritime Transport, Medical Data Exchange, and Smart Cities. The project's WP5 developed multiple solutions for each vertical, using novel tools contributed by the project's partners—some of which are the direct product of CyberSec4Europe research.

An overview of all CyberSec4Europe's verticals was presented but it was decided to focus on the Maritime Transport pilot not only because of its extensive use of the project's research assets, but also because it is an area seldom spoken of. However, a significant portion of everything we own, eat, and use as fuel for our appliances is transported by ship. Ships have, of course, a communication system which is used to talk to, for example, other ships and ports, and it must be secured because it is a target for malicious actors.

More specifically, throughout the Maritime Transport section of the presentation, the critical services in this sector were covered along with the corresponding threats that might impact their security states. Threats such as GPS spoofing, signal jamming and DOS supply chain attacks can render existing cyber physical systems of the maritime world useless or manipulate them in a way that will impact them or their environment. The specific goals of the services developed were, then, illustrated to show how to secure the maritime transport field against the enumerated threats and analyze them individually as solutions. The four services included:

- Threat modeling and risk analysis for maritime transport,
- Maritime system software hardening,
- Secure maritime communications,
- Trust infrastructure for secure maritime communication.

Furthermore, two of the demonstrators developed were presented on top of these services to illustrate their actual functionality and contribution to the security of the maritime transport field. The CyberSec4Europe Risk Assessment tool presented allows users to enumerate their maritime organization's assets and correlate them to existing vulnerabilities and threats; provided that a complete map of the infrastructure is entered to the system, the user can move forward and execute multiple risk assessments for different scenarios and business processes entailing their assets. The Risk Assessment results offer a detailed analysis along with visual analytics and visual representation of underlying attack paths. The PKI tool demo presented afterwards as the implementation of the Trust infrastructure for the secure maritime communication service, entailed a description of the procedure required to request and issue validated certificates for maritime communications.

In addition, the architecture and some results for the Secure Maritime Communications and the Maritime system software hardening were presented to illustrate its performance throughout the recompilation of widely known open-source communication software such as OpenSSL. Finally, to conclude, the research output created throughout this work was presented and options for future implementations and extensions were discussed.

2.10.2 CONCORDIA

Presented by Thanh van Do, Boning Feng, Bernado Santos, Madalina Baltatu, CONCORDIA

CONCORDIA developed vertical industrial pilots and cross-sectoral pilots using innovative cybersecurity tools. CONCORDIA focused on five industrial fields, namely, Telecom, Finance and insurance, E-Mobility / E-Charging, E-Health and Vehicular Communication Systems. Due to time limitations, only the Telecom industrial field was presented at the CONVERGENCE event. The main objective from the Telecom Pilot was to enhance the CONCORDIA Threat Intelligence platform, but from a telecom operator's perspective with three different use cases as follows:

- Use case by Telecom Italia: Automated Processing of Threat Intelligence Information
- Use case by Telenor: Preventing Flood Attacks on mobile network from IoT devices with Machine Learning,
- Use case by Telefonica: Handling Privacy & Anonymity with Machine Learning.

Only the use cases by Telenor and Telecom Italia were presented at the CONVERGENCE event.

For the use case by Telenor a CONCORDIA Mobile Threat Modelling Framework (CMTMF) was designed and elaborated. While there is an urgent need for understanding the behaviours, tactics and techniques of attackers on mobile networks, MITRE ATT&CK, the current most popular and efficient modelling framework addresses only enterprise networks, Industrial Control Systems (ICS) and mobile devices and not mobile networks. Telenor, Ericsson and Oslo Metropolitan University with the collaboration of CIRCL Luxembourg, Siemens and Telecom Italia has proposed and implemented the CMTMF, an extension to MITRE ATT&CK which enables the modelling of threats on mobile networks, in particular, 5G. The CMTMF is fully integrated as a galaxy in MISP and publicly available to everyone.

The use case of Telecom Italia consists of the definition and prototype implementation of an automated mechanism to prioritize the consumption of large numbers of Indicators of Compromise provided by heterogeneous Cyber Threat Intelligence (CTI) sources, based on a suite of supervised Machine-Learning algorithms.

The use case has two main phases: the implementation, integration and testing of the ML-based approach in the anti-SPAM system of Telecom Italia, followed by the extension and re-definition of the approach to cover all the indicators collected by the internal Threat Intelligence platform of our organization. While the first phase finished in 2021 with the publication of a paper[11] , the second one is currently in the consistency check phase and the approach and lesson learned will be shared in the last deliverables of the CONCORDIA project. The target level of the TIM prototype is TRL-6.

2.10.3 ECHO

Presented by José María Torres, ECHO

[11] "2 Years in the anti-phishing group of a large company" published in 2021 by Elsevier Computers and Security Journal

ECHO performed an analysis of transversal and inter-sectoral challenges and opportunities to support development of cybersecurity technology roadmaps. After the examination of more than 140 reports and the identification of 83 technical cybersecurity challenges, the following inter-sector technology roadmaps were defined:

- ECHO Early Warning System (E-EWS) provides the infrastructure needed to support trusted and secure information sharing among across a network of competence centres and their respective constituents.
- ECHO Federated Cyber Range (E-FCR) interconnects cyber range capabilities through a portal that operates a broker and enables access to emulations of complex realities and inter-sector dependencies.
- Two innovation roadmaps to be addressed in the future Cybersecurity Competence Network: AI CISO to support Chief Information Security Officers with Artificial Intelligence; and AI/ML Cybersecurity for Aviation/Space & Maritime Autonomous Transport
- ECHO's inter-sector prototypes. These are 14 different prototypes addressing the most pressing cybersecurity challenges. They cover four different critical sectors, Energy, Health, Maritime and Space.

The presentation focused on these early prototype tools but due to time constraints, only two of them were demonstrated covering two different verticals: monitoring of Spacecraft Operational Software to detect cyber security events in the Space sector and the delivery of secure sharing of health care information between different Health Care Organisations (HCO).

SISO, the first one of the demonstrated prototypes is a two-part prototype that aims to monitor Spacecraft Operational Software (SCOS) to detect security events that have the potential to cause harm. The first part, SISO, employs a SIEM system configured to monitor logs generated by SCOS (through login user behavior and unexpected telemetry), as well as monitoring the SCOS filesystem for changes that may affect how SCOS itself behaves. The second part, SISO-AD, applies a state-of-the-art cluster-based anomaly detection system to EDDS – an intermediary between users and SCOS itself. Working on the logs of EDDS, which contain information of requests sent to SCOS, anomalous and thus potentially harmful patterns in user requests can be identified and marked for further investigation.

The second prototype demonstrated was SISP (Secure Information Sharing Platform). This is a sector-specific tool solving a set of identified security challenges in healthcare. The goal of SISP is to deliver secure sharing of health care information between different HCO, cross-border and between disparate organizations within a single country. The current approach adopted for exchanging information is using obsolete procedures such as fax, email and exchanging physical medium. SISP should enable healthcare professionals to exchange healthcare information more efficiently, in compliance with regulations and more securely than the current baseline by promoting interoperable file formats, cryptographic methods and a mutual trust model. The SISP tool will allow HCOs to guarantee the confidentiality, accountability, integrity, and availability of the data.

An important activity in the project was to find synergies among the different prototypes in order to combine them into extended scenarios. In principle, each prototype has been developed by one ECHO partner and can work independently from one another to provide a particular functionality. However, this does not prevent that the functionality of one prototype complements the functionality of the others to provide a better value for a particular vertical.

In the scope of ECHO, these combinations are called Demo Cases and they contain different prototypes used in synergy. Some of the prototypes in these scenarios were also integrated into other ECHO projects

assets, namely the ECHO Federated Cyber Range (E-FCR) and ECHO Early Warning System (E-EWS) in order to provide an even better added value. At the time of the presentation, a total of six Demo Cases had been identified and implemented. Out of them, only three were described in the presentation due to time limitations:

- Demo Case #4. Included protypes: CyMS (Cyber Management System) and SISP (mentioned above). The purpose of this Demo Case was the demonstration of the E-FCR to support certification activities following the E-CCS for the ECHO products.
- Demo Case #5.
- Demo Case #6. Under the name of Demco Case #6 we have included three different clusters containing at least three prototypes. Each of those clusters was presented in a thematic workshop addressing one sector.

At the end of the presentation, ECHO highlighted the dissemination activities performed not only to give visibility to the Demo Cases but also to get feedback from users and stakeholders. The output of these activities can be accessed online using the different publication channels of the project, including the ECHO:

- Website (www.echonetwork.eu) and
- the YouTube channel: https://www.youtube.com/channel/UCDQBXrQhoLJ2lnf38x1X6Uw.

2.10.4 SPARTA

Presented by Thomas Jensen on behalf of Gabriele Costa

Thomas Jensen presented the topic of the High-Assurance Intelligent Infrastructure Toolkit (HAII-T) program, the overall objective being to develop a foundation for secure-by-design Intelligent Infrastructures, built on truly reliable approaches, addressing multiple cybersecurity facets.

The main challenge faced in intelligent infrastructures is the heterogeneity in the network. The scope and objectives were covered by the following tasks:

T6.1 – Securing Operating System Software
T6.2 – Hardening Legacy Components
T6.3 – Secure Orchestration of the II
T6.4 – Resilience-by-design of II
T6.5 – Privacy by design

There was good collaboration despite having to go virtual and the following events and milestones were highlighted. Four deliverables were published (D6.1-4) including two demonstrators and 3 annual strategic meetings took place (2019 physical (Lucca), 2020 virtual, 2021 hybrid (Graz)). The overview of the SPARTA project and its relationship within the Work Packages is given in Figure 14.

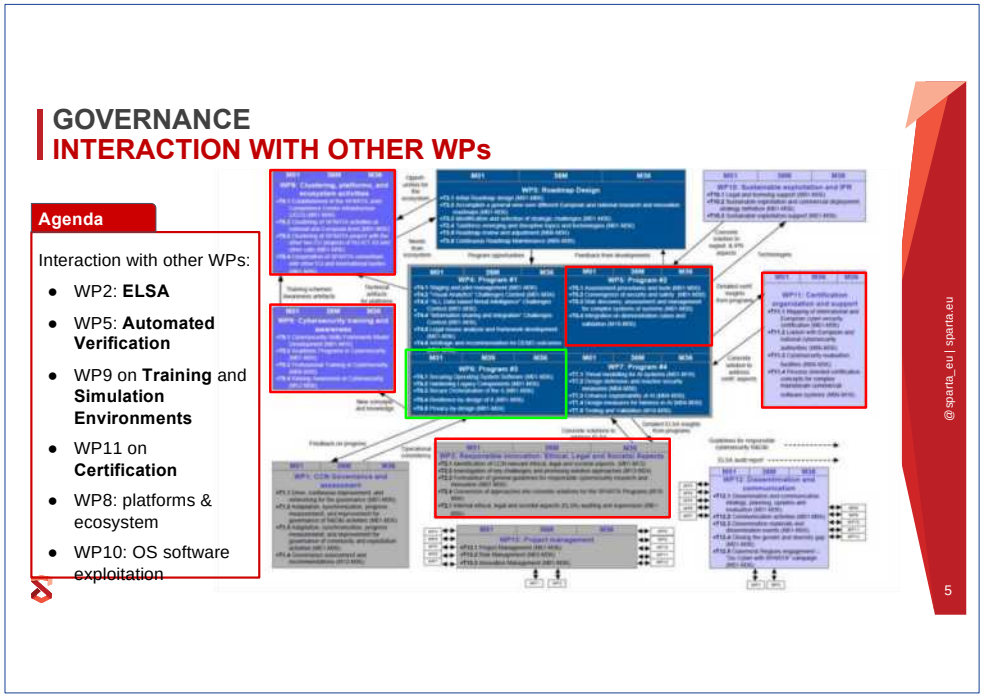


Figure 14: Overview of the SPARTA project and its relationship within the Work Packages[12]

In order to secure orchestration/securing the II lifecycle necessitated:

- Supporting all the phases of the lifecycle of an Intelligent Infrastructure
- Relying on extensible, state-of-the-art orchestration technologies
- Embedding methodologies developed in WP6

The technological contributions developed and certified for each task are listed in Figure 15.

[12] Slide from Annex 16 (Presentation by Thomas Jensen, SPARTA)

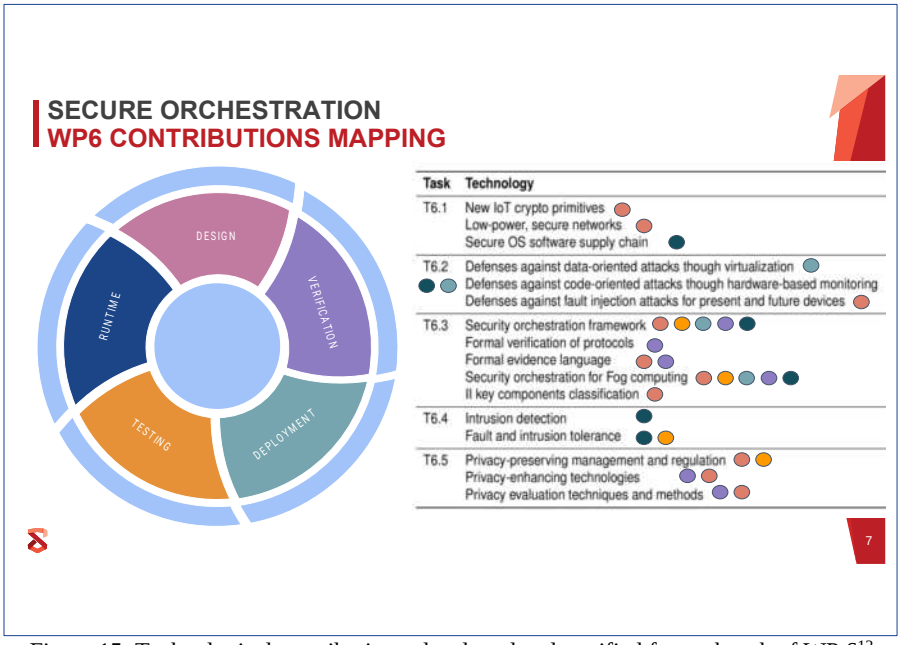


Figure 15: Technological contributions, developed and certified for each task of WP 6[12]

The outcome was a case study in the area of smart buildings in Genova, specifically:

- It was part of the Savona Polygeneration Microgrid (University of Genova)
- It was not yet a "digital twin", but decorated with 8 security scenarios
- A publicly available asset!

To conclude, the following SPARTA "lessons learned" were mentioned:

- There is no silver bullet in security
- Rarely can a security concern be solved with a single technology
- Effective security mechanisms are often domain-specific
- Whilst the SPARTA's implementation followed security by design inspiring principles, customized security processes can be reviewed and maintained over time

2.11 Perspectives from JRC Atlas and ENISA

Panellists:

- Wide Hogenhout, DG CONNECT
- Marco Barros Lourenco, Research and Innovation Lead, ENISA

Session chair: Evangelos Markatos

Annexes:

- Annex 17 – Presentation by Wide Hogenhout, DG CONNECT
- Annex 18 – Presentation by Marco Barros Lourenco, ENISA

View on YouTube: https://www.youtube.com/watch?v=lrjdHJsPYaQ starting at 4:53:16/8:00:30

Evangelos Markatos opened the session on "Perspectives from JRC, Atlas and ENISA", presented **Wide Hogenhout**, DG CONNECT, who joined remotely, and **Marco Barros Lourenco**, Research and Innovation Lead, ENISA.

2.11.1 Atlas Perspective

https://cybersecurity-atlas.ec.europa.eu/

Wide Hogenhout presented an overview of the EU Cybersecurity Atlas on behalf of Francesco Barbato, who was unable to attend. The EU Cybersecurity Atlas started with the following foundations: the European Cybersecurity Taxonomy, the Cybersecurity Patent and Research Analysis, and the Pan-European Survey 2018.

There was a need to have an online portal at the European level where knowledge could be shared in the domain of the cybersecurity field (cybersecurity taxonomy, technologies, expertise, key researchers, networks, specialties, funding, trends and so forth).

It was established that the goals of the JRC Atlas were to:

- Facilitate the establishment of a community of practice,
- Help identify collaboration opportunities,
- Map the different cybersecurity competencies in Europe,
- Provide a knowledge management tool for the ECCC,
- Raise the visibility of participants within the community,
- Support European cybersecurity R&I coordination,
- Contribute to the development of EU funding programmes,
- Provide input to cybersecurity policymakers.

The questions arose as to how the JRC should evolve with the CCC. The CCC would be linked to a network of NCCs. In this domain, the cybersecurity competence community played a vital role as it is composed of a diverse group of stakeholders, private and public actors, academy and research organizations, public authorities, union bodies with relevant experience, industry (demand and supply side). The cybersecurity competence community at large would:

- Support the Centre and the Network in achieving the mission and objectives,
- Enhance and disseminate cybersecurity expertise across the European Union,
- Participate in activities promoted by the Network and the Centre,
- Participate in the working groups on specific activities,
- Promote the outcomes of specific projects.

The benefits of the JRC Atlas would provide:

- Networking within research: the Atlas provides tools which were opportunities to enlarge the research network;
- Visibility within the EU: the Atlas wants to become the preferred source of information on cybersecurity activities in the EU;
- Contributions to EU policies, showcasing programmes and events (e.g. when the Commission plans something on AI for cybersecurity, it will consult entities flagged as “A” in the Atlas);
- Links with ENISA in sectorial activities;
- Access to relevant information from and on EU projects;
- Engagement for students to apply for a particular course;
- Visibility of job listings;
- Better marketing studies / insights;
- Visibility of key researchers.

Thus far, there are 845 organizations listed in the JRC Atlas. The governance discussion of JRC Atlas is ongoing with the ECCC, along with the technical components for this European platform. It means

transforming JRC to a federation of portals of NCCs, linked to a communication strategy at the EU level with visibility beyond national borders.

The Atlas evolution in short would cover the federation of NCCs national digital portals, a European level communication strategy, cross-country visibility, cross-country collaborations. The adoption of semantic technologies and transition of the taxonomy to an ontology is currently being explored.

A short Q&A followed:

Question: Why should companies in my region register, who is actually using Atlas and for what purpose?

Answer:

Registering in Atlas provides visibility, somewhat like the yellow pages of cybersecurity in Europe. It is also possible to search for staff in a particular field. At the same time, in building this EU platform, each NCC has a role to create maximum benefit and make it as attractive as possible.

Question: It seems that the Commission is leaving the community up to the NCCs completely, why is that so? Why is the Commission not using the large amount of funds that it put into the pilots to kick-start the community with the Four Pilots. In six months' time, the Four Pilots will be over and it seems that the Commission is not doing anything to keep them alive as a community which has already formed a community through 160 organizations and that community has worked together for 3 years. We have this huge event going on these 3 days here in Brussels, and we don't have representatives from the Commission here so why is that?

Answers:

- The pilots have had an extremely important role and they have made a huge impact, bringing together many people across Europe to work together. It is important to realize that the competence centre is setting a research agenda and executing it. There is a very direct interest in working with the community. Within the NCCs, there are many local events happening, cross-border events and it would be very difficult for the competence centre to work on its own without help from the local community. This is an opportunity for NCCs to develop expertise and so forth.

- For the pilots, we are looking at what is possible it is known how the funding system works. Possibly, in the context of the competence centre, there will be new projects and new ways of working. It is always very hard when you have such a large and successful effort built up and when the grant runs out, that ends. Let us try to make the most of what we have with the pilots and the great results they have produced. But let us also think of new initiatives so that these communities can work together and be effective.

- Concerning physical participation in the event, unfortunately the timing is really difficult right now, and there are very limited resources. At the same time, there are a number of legislative actions ongoing following on from the Ukraine crisis. We are under extreme pressure which is why I could not be physically be present. We are doing our best and we are following very closely these meetings.

Question: I know you have been involved in other communities, like the Graphene community, which was very successful, are there are any other best practices which we could adopt for our cybersecurity community?

Answer:

The Graphene community was very interesting. They prepared a very detailed program of where they wanted to go and that actually became a big reference tool. This kind of roadmapping is very

important and very helpful. From that experience, I know, it was extremely important to have such a reference in detail so as to see what should take place in the next steps. Having a narrative is really important.

Question: I would like to ask how dynamic is Atlas, how easy is it to update (from personal experience, it took a long time). How do you accept a company which declares a high level of cybersecurity.

Answer:

When we started with the pilots was it was not so difficult to assess the level of cybersecurity if a partner was in one of the pilots. However, later, we started receiving many ad hoc requests. There is now a WG from the ECCC on how to assess community membership. The updating is currently taking a little time but we are working on improving that.

2.11.2 ENISA Perspective

https://www.enisa.europa.eu/

Evangelos Markatos introduced the next speaker, **Marco Lourenco**, Head of the Research and Innovation Team at ENISA.

Marco Lourenco introduced ENISA mentioning that a great transformation took place during the last 3 years:

- ENISA welcomed the new Executive Director,
- new strategies were identified,
- discussions on how member states could further be supported,
- discussions on how to support interaction and growth of communities,
- support to the Commission in developing policies.

The community is at the centre of everything ENISA does. ENISA wants to make sure that the community, also in terms of the Four Pilots and CONVERGENCE, is built, develops, grows, is inclusive and covers all spectrums of cybersecurity.

With the new mandate, the cybersecurity certification instrument is very important in order to ensure that European products are certified. The role of ENISA is to make sure that there are certification schemes that can be used by the member states, certifying processes products and services. Other aspects which are equally important are capacity building, education, awareness raising, traditional areas of cybersecurity. ENISA is also introducing a new capability for operations not only for Europe but also internationally and in terms of the continued work in support to the EC and to the cybersecurity policy development. There are also other activities related to knowledge management and information, also in foresight, such as identifying evolving trends.

An important aspect is that ENISA has a strategy that is fit for the challenge, in terms of how we position ourselves according to a vision defined and agreed upon with ENISA's stakeholders and within ENISA, with the Executive Director.

ENISA identified 7 strategic objectives (Figure 16) with the first one being to empower communities.

Figure 16: ENISA Strategic Objectives[13]

ENISA has a new article 11 of the Cybersecurity Act, which states that ENISA is expected to contribute to the EU Strategic Research Agenda in the field of the cybersecurity.

It is important to note that ENISA is not a research body or organisation, it is a technical body. ENISA's role is to advise EU Institutions, Bodies, Agencies and Member States on Research and Innovation priorities in the field of cybersecurity. In other words, ENISA works with the research community, to create the links, to empower the community in order to flourish in terms of the products and innovation in the cybersecurity space. ENISA does not provide funding to projects but ENISA does advise and identify the areas in the funding programmes which should be considered as a priority.

> *"ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union." CSA (4)*

Concerning the Competence Centre, ENISA will advise the ECCC on defining a strategic agenda and a work program. ENISA needs to make sure that there is consistency, i.e., the Centre should invest in areas which are new but also acknowledge the work already be done, and scale up so that more products, services and innovation comes into play. ENISA is an advisor on the Governing Board of the Centre so that ENISA serve as an instrument, as a vehicle for the needs of the research community.

Basically, one message to convey:

> **ENISA is trying to get to know you, to understand what you are doing, so that bridges are established in such a way that information can be brought to the member states and to the ECCC.**

Another important aspect is that Atlas contains a lot of information, but it is a database. How can we build a stronger community? It is important to create a strong community for researchers that are working on cybersecurity. Further, the community should be inclusive, it should not only focus on cybersecurity professionals, but also people from law enforcement working on cyber, defense, societal and other areas.

[13] Slide from Annex 18 (Presentation by Marco Barros Lourenco)

Who should be brought in so that the community is inclusive in order to cover different angles. As indicated in Marco Lourenco's presentation (Annex 18),

> *"Cybersecurity relies on a multi- and inter-disciplinarity of topics and specialties to achieve success. Research is at the forefront of learning more about threats and how to protect from them."*
>
> *"A stronger research community will generate the drive and perspective to create long lasting change and face the challenges through collaboration and cooperation."*[13]

The next steps identified by ENISA are:

- Establish the ECCC Competence Community.
- Atlas as the main reference to identify members from the Community
- Interlink other sources of information with Atlas (Cordis, etc.)
- Call for action to build a stronger Community
- Mobilize the community to continue discussing the needs and priorities

One of the next steps is trying to understand how to build a stronger community. The starting point for establishing the community is the Four Pilots, since this community has been working together for the last three years and it is important to leverage from that. But it is also necessary to understand who is not included in the Four Pilots so that they can be brought in as part of the community

Atlas has its own challenges, in terms of a database and there is a need to understand how to maintain it. It is a central database but it should be linked to member states, and directly to research organizations. There should be more information added which can be shared and which should be actionable.

Once it is defined how the community is structured, it will be necessary to envisage how the community can continue to grow. Whilst ENISA is a partner for support, and it is not ENISA that will build the community, ENISA can help mobilizing, facilitating, or take such initiatives.

The ECCC is an opportunity for all. It will pave the way for us to continue making a stronger community and to work together as one union in cybersecurity research.

A short Q&A followed:

Question:
Is my understanding correct that the community will be created on the national level and then something will be done at the European level. There is WG1 at the ECCC which is creating the protocol to create these communities at the national level. Could you clarify how you see the interaction between these two communities.

Second question: You mentioned that one of your roles is to foster the research agenda. My understanding that this this is for WG 4. I mention this because in the next presentation you will see all the work that the pilots have done with JRC to create a common roadmap. Could you clarify what has been done in the roadmaps and how will things proceed starting from now?

Answer:

It terms of clarity, ENISA is advisor to the Governing Board so we are in WG1 and WG4. But those Working Groups are from the member states. ENISA is the cybersecurity agency of the European Union. Our perspective is European. There will be communities at the local level and at the

European level. We also favor communities should be sectorial and it may make sense to be sub-regional as well. There are still a lot of discussions that need to take place and we need to be involved in research with the community. There is a role for ENISA to play.

There is this great opportunity with the Competence Centre. We need to create the cybersecurity and research community in Europe. People want to work together and build something together. There is a momentum now because the Four Pilots are ending and there are a lot of people motivated to continue working on what has been built.

Concerning the roadmaps, unfortunately we were not invited to those discussions. However, the work developed in the roadmaps is extraordinary. If we are given the opportunity to participate at least in a forum, we can build on something. Our intention is to mobilize the community and engage.

Question: You mentioned the cybersecurity area community. I missed the deployment community in the equation. Do you think this is something that already exists or is it envisioned in some way?

Answer:

I believe that community already exists. If you look at the pilots, it is such a representation of that community. ENISA produced a study of the Four Pilots and ECSO. We had the opportunity to see the great work done by the Four Pilots but somehow an opportunity was not explored, i.e., more convergence between the Four Pilots. There is room to explore together with the Four Pilots to build on this. There is a community but maybe not organized as one community at the EU level. In discussion with one of the pilots, there was a comment that the community should grow from those that can inspire.

Question: What can we do in order to help your work at ENISA?

Answer:

We are now starting to get in touch with different members of the communities, visiting research institutes. We want to understand what you are doing, what you have delivered as we are gathering all that information and when we develop our own studies, we can call you. ENISA being the EU Agency for cybersecurity, we have a lot of visibility, and we want to give you that visibility. Please reach out to us to tell us what you are doing. Tell us about your projects you are working on.

2.12 Roadmapping for the Future

Panellists:

- Thomas Jensen, Coordinator, Roadmapping Focus Group
- Evangelos Markatos, CyberSec4Europe
- Theodora Tsikrika, ECHO

Session chair: Thomas Jensen, SPARTA

Annexes:

- Annex 2 – Short biographies
- Annex 19 – Presentation of the Roadmapping Focus Group

View on YouTube: https://www.youtube.com/watch?v=lrjdHJsPYaQ starting at 6:54:26/8:00:30

Thomas Jensen (SPARTA) opened the Roadmapping session and presented the work of the Roadmapping Focus Group which involved the Four Pilots and ECSO. A lot of work had been done and it would be

important to present the outcomes, especially as several initiatives were due to come up in the ECCC and the pilots were supposed to provide some input there.

First, the background of the Roadmapping Focus Group was briefly presented, i.e., in early 2019, the Four Pilot cybersecurity competence networks were launched. At the end of 2020, a cross-pilot Focus Group on Roadmaps was established. Between spring and summer of 2021, roadmap content and processes were exchanged between the Four Pilots, and cybersecurity challenges were prioritised. From Autumn 2021 to Winter 2022, the document "Cybersecurity Research Focus Areas Priorities" was delivered and is to be integrated into the EU Cybersecurity Atlas.

Each pilot took a different route as to how they prepared their roadmaps. Monthly meetings of the Roadmapping Focus Group took place with some brainstorming resulting in a number of priorities being selected and defined. A 10-page condensed document entitled "Cybersecurity Research Focus Areas Priorities" was the result of these discussions, a summary of the challenges is summarized in Figure 17 under four blocks:

- Governance and Capacity Building,
- Trust-building blocks,
- Trustworthy Ecosystems of Systems,
- Disruptive and Emerging Developments.

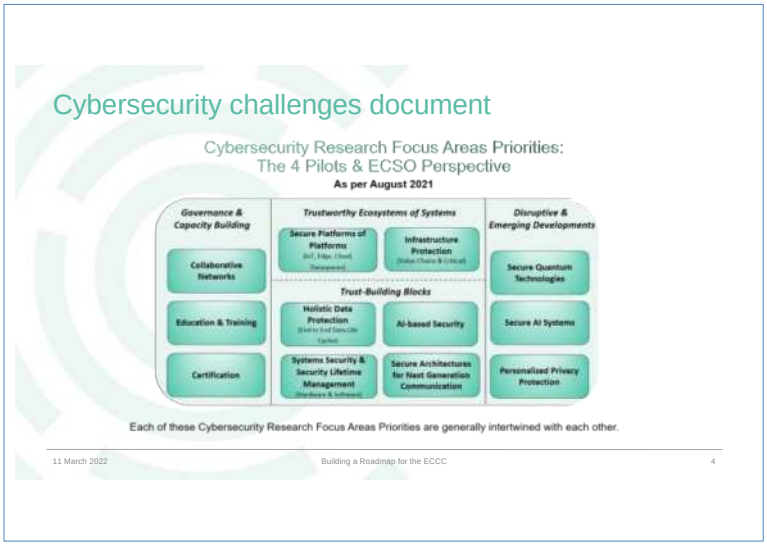


Figure 17: Roadmapping Focus Group Perspectives on Cybersecurity Challenges[14]

The building block "Trustworthy Ecosystem of Systems" was presented by Evangelos Markatos who described how security of IT systems, networks and services had developed over the last 40 years resulting in a dependence on an ecosystem of systems, see Figure 18.

[14] Slide from Annex 19 (Presentation by Thomas Jensen, Roadmapping Focus Group)

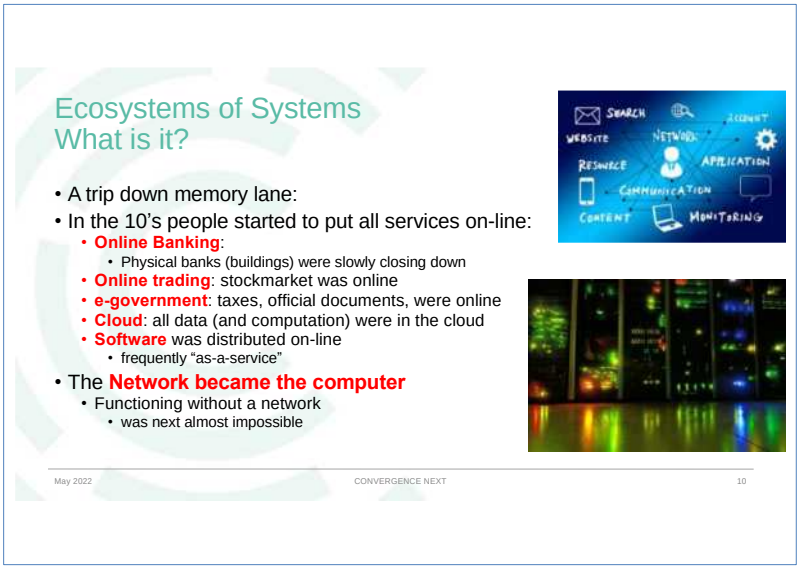


Figure 18: Roadmapping Focus Group - Ecosystem of Systems[15]

Taking a trip down memory lane, it became clear that the dependency on the network became a necessity in daily life and there was a growing need for protection, security and trust surrounding this ecosystem of systems in two main areas: Secure Platforms of Platforms (IoT, Edge, Cloud, Dataspaces) and Infrastructure Protection (Value Chains, Critical Infrastructures).

Table 22 illustrates the broad break-down of the two main focus areas and the challenges.

Secure Platforms of Platforms	Infrastructure Protection
Cloud Infrastructures Vulnerabilities Mitigation ➢ Mitigate the vulnerabilities that exist in the cloud Secure Integration of **Untrusted IoT** in Trusted Environments ➢ Not all components will be trusted **EU** Multi-Cloud, Edge & IoT Trust & Security **for Massive connected IoT Ecosystems** & Lifecycle Management ➢ How do you make sure that they are secure for life?	Security **across Value Chains**: From Industry 5.0 to Supply Chains ➢ Supply chains involve several actors… Critical Infrastructures Protection & Resilience Trusted **Information Sharing** & Collaborative Threat Intelligence Management ➢ Sharing brings knowledge

Table 22: Challenges in Secure Platforms and Infrastructure Protection[15]

Due to this dependency on this ecosystem of systems, and especially during COVID when there was a global turn towards almost totally usage of online services, trust in online services became of paramount importance, especially with many software modules being developed in countries outside Europe. Thus, securing the Ecosystems of Systems became necessary for **European Digital Sovereignty.**

[15] Slide from Annex 19 (Presentation by Evangelos Markatos, CyberSec4Europe)

The next building block "Governance and Capacity Building" was presented by Theodora Tsikrika (ECHO) who gave a consolidated view across all pilots of the three main priority areas for research to be performed, namely:

- Collaborative Networks
- Education & Training
- Certification

The first priority area agreed upon by the Four Pilots was Collaborative Networks, which addressed the landscape and Research Focus area. In brief:

- In the Collaborative Networks Landscape, there was growing diversity and sophistication of the cyber threat landscape which entailed a need to integrate a broad spectrum of competencies and resources from human, technological and financial aspects. The landscape had become so complex that it was no longer possible for a single organization or country to manage this landscape but a collaborative network.

iv. In the Collaborative Networks Research Focus area, there was a need to establish efficient and sustainable collaborations among a variety of organisations, with varying legal, organisational and cultural contexts. In addition, there was a need to understand the requirements, design and implement effective norms and models, and the supporting infrastructure. In the pilots, this was successfully achieved but it was now important to see how to move forward and leverage this knowledge in the future.

Another challenge was the diverse contexts from legal, organizational and cultural perspectives. There was also a need to understand the requirements in order to design and implement effective norms and models to support such infrastructure and government models for such collaborative networks.

The next priority area was "Education and Training", the landscape and focus on research summaries are found below noting that "The Human Factor" is key for both cybersecurity and competitiveness of Europe's digital economy:

Education and Training Landscape

- Growing demand for cybersecurity professionals,
- New levels of awareness for policy-makers, non-technical personnel, and citizens.

Education and Training Research Focus

- Shared understanding of the evolving requirements to the competences of professionals,
- Developing more comprehensive frameworks and infrastructures,
- Supporting the enhancement of cybersecurity skills and competencies,
- Cyber ranges, federations, re-use of training scenarios, monitoring and evaluating trainees' knowledge and performance.

Whilst there was a growing demand for cybersecurity professionals, education and training was also necessary for other personnel in their professional context, as well as citizens and the various levels of government and policy makers.

The third priority area was "Certification" which responded to the need to deliver high levels of confidence. The "Certification" landscape and focus on research areas are summarised below:

Certification Landscape

- Need for high levels of confidence that a particular device, product, system, process, or service are designed, delivered, and operate according to defined security policies,

- Increased interconnectedness among systems and organisations,
- Cybersecurity certification is expected to facilitate these guarantees and formally attest or confirm certain security characteristics.

Certification Research Focus

- Further investigation and development of the (currently complex) evaluation process (risk assessment, requirements analysis, verification and testing procedures),
- Existing standardised approaches cover only partially the needs of cybersecurity certification,
- Ensure security throughout the lifetime of the design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation.

The last part of the session was about the various types of roadmap processes and this was presented by Thomas Jensen. In particular, the CONCORDIA and SPARTA processes were explained.

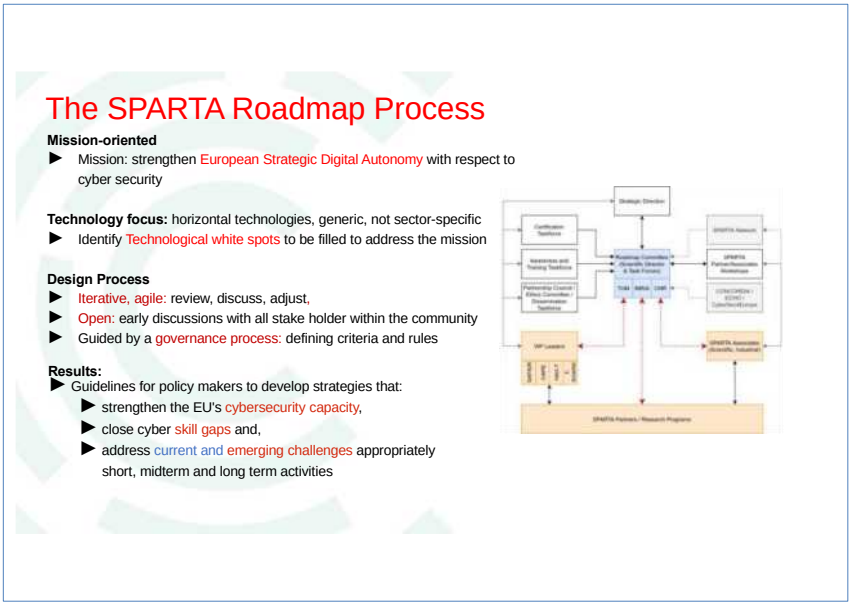


Figure 19: SPARTA Roadmap Process[16]

The roadmap for SPARTA (Figure 19) was technology focused. The design process iterative and agile. The results were presented in the form of guidelines for policy makers to develop strategies strengths, gaps and emerging challenges.

[16] Slide from Annex 19 (Presentation by Thomas Jensen, SPARTA)

Figure 20: SPARTA Roadmapping – Some Lessons Learned[16]

Thomas Jensen presented the CONCORDIA roadmap (Figure 20) on behalf of Artur van der Mees. Similarly, the goal for CONCORDIA was to produce a roadmap which would build and sustain European Digital Sovereignty. There were four parts to this roadmap:

- Sovereignty and Collaborative Resilience,
- Economic Development and Competition,
- Research and Innovation,
- Education, Skills and Jobs.

The roadmap was built from the stakeholder perspective, i.e., a human, persona, societal-centric, use case-driven, data-centric and technology-agnostic approach.

The CONCORDIA roadmap looked at the following areas:

Research and Innovation
Education and Skills
Economic Perspectives
Legal & Policy Perspectives
Certification and Standardisation
Investment Strategies
Community Building
Other Objectives, Challenges and Scenarios

The different angles from where analysis could be made was also provided, for example, a perspective on the human-centric digital ecosystems and multi-angled omni-stakeholders and influencers, as given in Figure 21:

Figure 21: CONCORDIA's Perspective on Human-Centric Digital Ecosystems and Stakeholders[17]

A short Q&A session followed.

3 Sustainability and Expanding the Impact

3.1 Day 3 - Capacity Building (Education, Skill Sets)

Panellists:

- Boning Feng, CONCORDIA
- Carlos E. Budde, CyberSec4Europe
- Nina Olesen, ECSO WG 5

Session chair: Boning Feng, CONCORDIA

Annexes:

- Annex 2 – Short biographies
- Annex 20 – Presentation by Feng Boning on the Education Focus Group Results
- Annex 21 – Presentation by Feng Boning of the CONCORDIA European Education Ecosystem for Cybersecurity
- Annex 22 – Presentation by Nina Olesen (ECSO)

View on YouTube: https://youtu.be/CuKZ4a1POF8 starting at 28:27/5:48:26

3.1.1 Education Focus Group

Feng Boning (CONCORDIA) presented the activities of the Education Focus Group (EFG) which was established in 2020 by ENISA, ECSO, and the Four Pilot projects (SPARTA, CONCORDIA, ECHO,

[17] Slide from Annex 19 (Presentation of CONCORDIA by Thomas Jensen on behalf of Arturvan der Mees)

CyberSec4Europe). The CCN Education Focus group aimed at the creation of a European education ecosystem for cybersecurity.

Figure 22: European Education Ecosystem for Cybersecurity[18]

The main activities of the EFG were:

- Sharing information and outcomes;
- Supporting the initiatives of the Four Pilot projects;
- Collaborating in building specific methodologies and solutions.

The activities and domains (called further "strands") covered by the pilot projects were:

- Mapping existing programs and courses;
- Common skills framework;
- Creation of innovative certification schemes;
- Development of methodologies, content and educational/ training courses;

The pilot projects had common goals but the approaches towards the achievement of these goals were different. Building a common governance model is the next logical step in the work of the EFG. So far, the EFG created the structure of the governance model. The key elements of this structure are:

- Identification of the stakeholders;
- Definition of mission, vision and goals of the Education Competence Centre Network;
- Organizational structure and strategy identification;
- Definition of roles and responsibilities of the participating partners.

A short introduction on the activities of CONCORDIA was provided, as follows:

1. Mapping courses and trainings for professionals. The main function of the platform was to promote the training products of the organizations that provides such products. The Concordia's map complements the ENISA's database of university programs.

[18] Slide from Annex 21 (Presentation by Feng Boning, CONCORDIA)

2. Development of a methodology for creation and deployment of training courses.
3. Based on the methodology Concordia developed a course targeting cybersecurity consultants role profile.
4. Development of a skills certification scheme.

3.1.2 Results of the Four Pilot Projects in Capacity Building

Carlos Budde (CyberSec4Europe) presented the results of the 4 pilot projects:

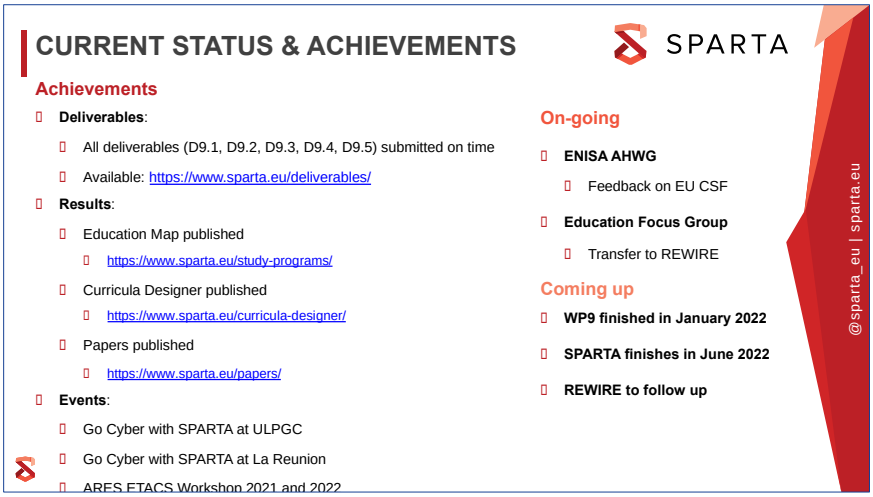


Figure 23: SPARTA's Focus on Capacity Building in Cybersecurity [19]

SPARTA focused on the cyber skills framework, mapping of bachelor and master courses, curricular designer, educational events (workshops) (Figure 23).

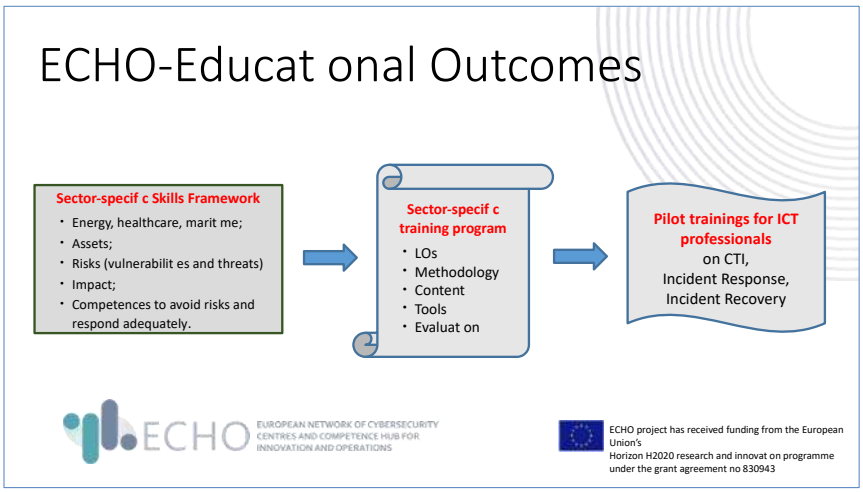


Figure 24: ECHO's Focus on Capacity Building in Cybersecurity[19]

[19] Slide from Annex 20 (Presentation by Carlos Budde, Education Focus Group)

ECHO focused on the cyberskills framework covering vertical industries energy, healthcare and maritime transportation, sector-specific training programs, content and tools development and pilot delivery including assessment of the efficiency of the course from industrial point of view. See Figure 24.

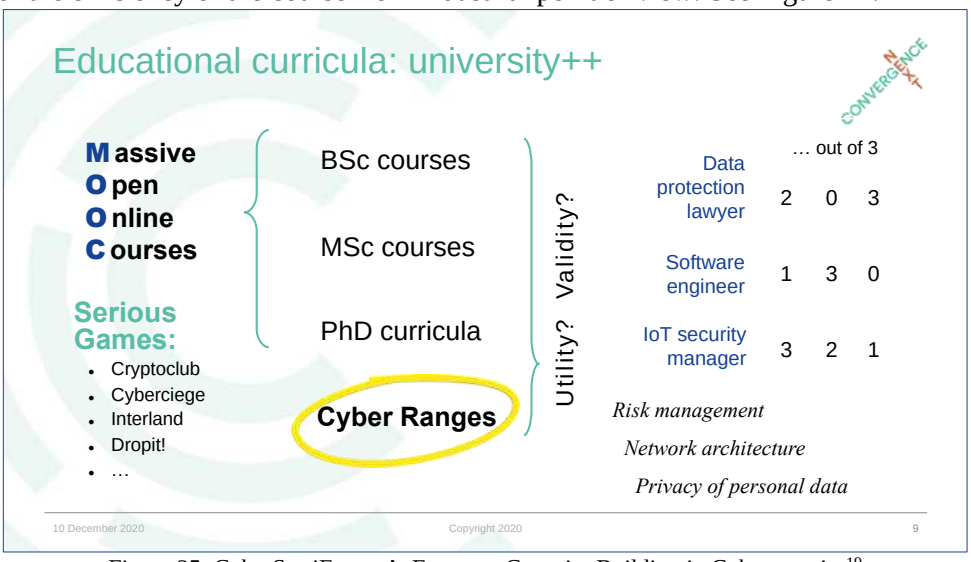


Figure 25: CyberSec4Europe's Focus on Capacity Building in Cybersecurity[19]

Cybersec4Europe focused on the academic sector, evaluation of the quality of Massive Open Online Courses (MOOCs), serious games, cyber ranges as a learning method, collecting data to answering the question how the education match the needs of the industry, defining job profiles (data protection lawyer, IoT security engineer), skills assessment framework, assessment study. See Figure 25.

A short Q&A followed.

Question: How can I use the presented frameworks and results to assess the level of expertise of people in the organization who perform the functions of SOC members? Also, how can we use the presented methods and frameworks for building training scenarios?

Answer:

The assessment and competence frameworks are created under the Four Pilot projects with the aim to provide a basis for contextualization and common understanding about the skills and abilities expected by the professionals in the mentioned domains. Then we collect an input from the academia and industry to assess better the needs and create specific use cases and scenarios for filling the existing gaps in the competences of the employees.

Question: How can we address the social aspect of the cyber-vulnerabilities, the human factor in the cyber-attack cycle?

Answer:

We consider the serious games as a powerful learning tool appropriate for approaching young people. We could propose using of serious games in the training and educational programs.

3.1.3 ECSO – Working Group 5

Nina Olesen (ECSO) presented the results of the European Cybersecurity HR and hiring processes report. A survey implemented in 2021 with the support of the Four Pilot projects was carried out on how the HR

departments attract, recruit and retain cybersecurity professionals and how the community could support these processes.

One of the main outputs was highlighting the need for a common cybersecurity skills framework (as given in Figure 26). ENISA's effort in building a cybersecurity skills framework is the right action in this direction. All of the respondents (medium and large sized organizations) said that they have dedicated cybersecurity team. The most frequently hired professional roles are IT administrators, IT developers and cybersecurity risk analysts. Filling the open cybersecurity positions is the biggest challenge. It takes six months on average. Building an open minimum reference curriculum is key.

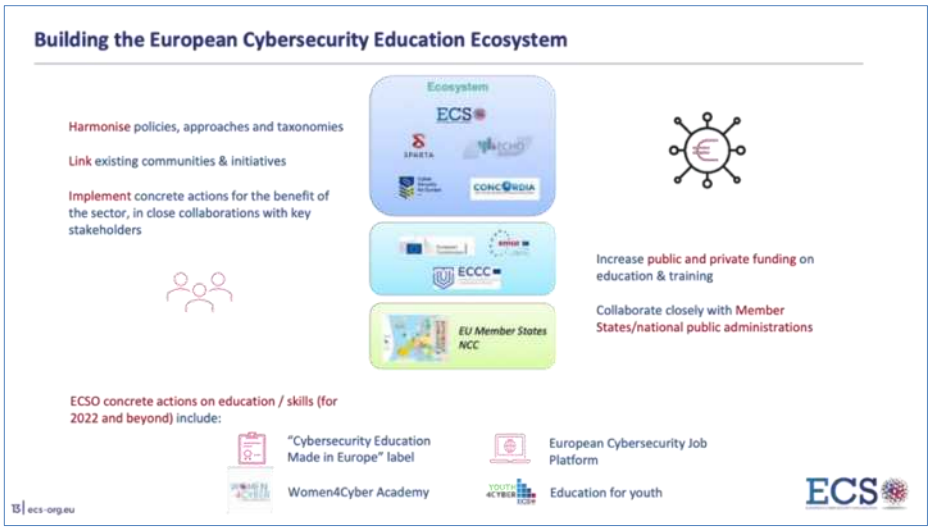


Figure 26: ECSO – Building the European Cybersecurity Education Ecosystem[20]

3.2 Evolution of the European Cybersecurity Ecosystem

Panellists:

- Roberto Cascella, ECSO 2.0 / 3.0
- Afonso Ferreira, CyberSec4Europe
- Thanh van Do, CONCORDIA
- Wim Mees, ECHO
- Fabio Martinelli, SPARTA

Moderator: Mark Miller, CyberSec4Europe

Annexes:

- Annex 23 – Presentation by Robert Casella
- Annex 24 – Presentation by Afonso Ferreira

View on YouTube: https://youtu.be/CuKZ4a1POF8 starting at 2:28:07/5:48:26

Mark Miller opened the panel, introduced the participants and explained that each participant would be given five minutes to introduce themselves and to have the opportunity to share their message, after which

[20] Slide from Annex 22 (Presentation by Nina Olesen, ECSO)

a panel discussion would take place, followed by a Q&A session. A summary of the shared messages follows.

- **Ecosystem of communities**: There has been a lot of discussion on the roles of ecosystems and their relationship to communities. Communities can have different actors with specific goals in mind, such as SMEs, initiatives such as the Women4Cyber Foundation, and non-cybersecurity experts such as end consumers or organisations that may not be involved in or aware of cybersecurity. Moving from communities to ecosystems, it is possible to have multiple partially overlapping ecosystems that involve different communities. These ecosystems have different stakeholders, different physical environments and specific needs and objectives. An example was the role of ECSO which so far has been to establish different communities thanks to the work of different members in the Working Groups. This needs to continue and expand especially with regard to the exchange of information, between manufacturers and end users in a dialogue for the same goal, which could be cyber-resilience or critical infrastructure.

- **Funding of pilots coming to term:** The end of the pilots is in sight, the partners are disappearing and it seems that the whole process will need to start again. This is something that is disappointing in Europe, as one sees that the maximum funding is three to five years and that is it. To build an ecosystem in Europe, a time frame which is a bit longer is necessary. As things stand right now with the funding programmes, projects restart from scratch, which results in wasted time and resources.

- **Collaboration of the Four Pilots and ECSO:** There has been a lot of value in the joint events and other events, in which the Four Pilots and ECSO have met and exchanged ideas. A group has been formed that is enthusiastic, creating solutions and trying to move forward. Looking at the COVID situation and the digital transformation which took place on an unprecedented scale, everyone was suddenly deploying all kinds of solutions and going digital without considering cybersecurity, as they felt that they did not have the time and it was not the most pressing concern at that time. Cyber risk is about operational risk as a whole and there is a trade-off between the risk to business and risk from cyber attacks. If there are opportunities that are so important that you accept a certain higher level of cyber risk, then you do so and that is what we did during the COVID crisis. Now, looking at the numbers, investments in cybersecurity are three times higher than in IT as a whole, people are becoming more aware of the risk. But we see that the investment is mainly in services and that they are outsourced outside of Europe. Is this really what we want, and does this contribute to our strategic autonomy or to our sovereignty?

- **Investment in the ecosystem:** There is a need to invest a lot more resources into creating this ecosystem, to really make it into a very successful group of SMEs that grow and provide services from within European borders. Europe already has regulations in place that require a lot of compliance and those are working really well. What is missing is the motivation. What are we offering at the European level to facilitate not just the industry but also the users of cyber and those that rely on digital solutions. Do we provide services, threat intelligence that is really organised and structured at the right level for different sectors, and that is controlled in terms of quality? The pilots are the seeds that were put into the ground. The question is whether the necessary water and fertilizer will continue to arrive on that fertile soil, so as to create successful plants, that will then become a forest that is our ecosystem. More is needed, and we should be ambitious and invest in really making sure that these seeds grow and which were planted by the pilots, by ECSO, by all the collaboration and thought processes that were developed.

- **What is the "community"?** When speaking about a community, the term found in the legislation has a specific meaning: the community at a national level is managed by the member states

according to charter rules that they are discussing. There is a notion of accreditation, which is very different from what was done in the Four Pilots. With the pilots, the best expertise at the European level was brought together, based on how they could cooperate to achieve European digital sovereignty in the field of cybersecurity. Consider that at the European level, we speak about pertaining to the Four Pilots and not specific nationalities, which is a major feature that to be kept. The pilots became familiar with each other, they hosted many events, they started to merge their activities together, to optimise and converge in what they were doing. It is important to keep this alive even after the Four Pilots, and in order to do this some motivation is necessary.

- **Communication mechanisms need to continue**: The Four Pilots were very successful and have developed a lot of tools. It is important to keep the ball rolling at the European level, as we need the four communities plus ECSO to communicate with each other under a truly European umbrella. There are already common dissemination tools in place but, for example, a mailing list for the community that has been built could be useful. Nevertheless, the latter is not sufficient on its own, it is necessary to have a broader outlook and not only to just bring people together, but also to have the instruments that will enable people to work together and have discussions in a smart and proper way.

Question: What is the most important result that came out from your pilot – or from ECSO - during this period that leads to supporting the future and how the community and the network is going to expand, grow, change, adapt etc. for all of the things that are happening with the European Cybersecurity Competence Centre?

Answers:

CyberSec4Europe: In Work Package 2, a lot of work was covered in governance. The notion of bottom-up community hubs of expertise in cybersecurity knowledge was identified. 50 local players were interviewed from academia to SMEs and large organisations, as well as end-users and solution providers. It emerged that all of them were willing to do something together because they felt the need to do so. It is necessary to put these people together in order to provide solutions for the users. The seeds have been sown. There is, however, some concern as to what happens at the national level as the pilots have performed at the European level. Overall, and from a cybersecurity perspective, the notion of getting closer to the citizens, to the users and the solution providers, to those in need is necessary in order to build this community from the bottom up and in order to grow in the future.

CONCORDIA: The most important achievement for CONCORDIA was collaboration. This was achieved through collaboration between academia and industry, with both big companies and SMEs in different sectors, and across all of Europe, and through which common needs and topics were identified. This was a good start which took a few years to reach a European level, but there is concern that at the national level, this may be lost. The NCCs will still promote collaboration but will most likely focus on the national level.

ECHO: The most beautiful result was more than 200 people have worked together on different aspects, starting with a thorough analysis of what was needed, creating the building blocks for certification, education and training as well as technology building blocks, and bringing it all together. There were “demo cases” which were practical examples of how they solved problems in sectors such as energy and transport. They could go to the end user with a value proposition. As a group, seeing how people interacted, one could note that they were all proud of what they had achieved and what they could show. This is an accomplishment as a project in that they were able to build solutions as a group of people that are proud of their work and want to show it to the end users.

SPARTA: At the beginning, the best expertise was sought at the national level in order to then work at the European level. Once the project was structured, there was no longer a relationship with the national aspects, it was just about science and technology. SPARTA wanted to be inclusive and came to the understanding that the 50 partners could not be enough to represent the community, so the notion of "associates" was conceived. Then, it was found that this notion was not inclusive enough, so another tier of involvement was added called "friends", and they reached 120 to 130 organisations, enlarging the community as there were different needs of commitment, and not just the accredited people in the community. Although, in retrospect, the meetings with the highest attendance were those in which there was some motivation to attend, e.g., where there were brokerage events, encouraging the community to work together and create new project proposals together which naturally created the highest participation rates. This motivation is a way to stimulate a bilateral community, i.e., developing the ideas together and implementing them. This is how one reaches the European level. The national and the European levels should be considered together.

ECSO: The importance of creating the community has already been amply emphasized. ECSO was there at the beginning of the story. Stakeholders contributed within different working groups. They succeeded in moving beyond research and innovation by trying to tackle industrial policy and, in this way, different communities were talking to each other, expressing their problems and coming up with solutions. The enriching part is to go beyond the silos of the researchers, the large companies, SMEs, and end users, and put them together try to address the concrete problems that they need to face in Europe. There are different kinds of services that are needed at the European level. ECSO does not have funding money to build up solutions, but the key is to put all the different parties together, including with investors, create a dialogue, get to know each other and to avoid overlapping and reinventing the wheel.

Question: Are there any ideas to give some sustainability to the work of the Four Pilots?

Answers:

Concerning adding some **sustainability,** the following suggestions were made:

- **Continue with events which are in place**. As a community, summer schools for example, or other events were created where all the Four Pilots were represented, and ECSO, thus bringing together some 300 organisations. It is necessary to sustain what exists, understand what is missing, work together to identify what is missing. This is what is being discussed, for example, even the winter school which was organised together. These are opportunities to try to work as a community. There is the benefit of speaking to each other rather than competing for the same thing, so complementarity at the national-European level should be enhanced, to show that as a community there is a dialogue going on.

- **Avoid duplication of efforts** is equally important, coordination is key. Start coordinating the needs and coordinating the solutions, and this holds for infrastructure as well. It is not necessary to build four communication systems, when work can be done together to build one, or if there are multiple systems, then merge them.

- **A community is there and should continue**. The Commission provided an opportunity to create a community and this should continue once the needs are identified so that they can deliver in a coordinated fashion, rather than repeating some of the objectives when they were producing results as separate pilots. The Four Pilots are more focused on academia, whereas ECSO is more inclined towards industry, but together, they can work in a coordinated fashion. In the past, the scientific community did not work that well, but now their impact is bigger as they know each other better, and this conference here should last.

Question: What measures could be taken to make this community sustainable? Where should the focus be?

Answers:

A strategy is necessary to identify and invest in valuable outcomes from the pilots. Usually, in a European-funded program, the project life cycle is to form a consortium, write a proposal, win a proposal, start working, which amounts to a certain delay until the project can produce value, and the delay and effort involved may not always be necessary each time. It may be sensible to develop a strategy, to look at what came out of the pilots and what is really valuable for Europe to support the initiative(s) further without going through the whole circle of consortium building and so on. The pilots have shown that they can work together and, therefore, they can create even more value by working together. The network is there, the people know each other, they have been working together in inter-pilot focus groups, the whole set of dynamics is there, and it should not die. It should not be a case that everyone is forced to start over in a new investment cycle. It is up to a group of experts (outside of the pilots) to decide what is valuable. There is a sincere wish all round that all the effort invested in the Four Pilots is not thrown away, and that at least some outcomes are picked up and invested in further, so the fruit of the Four Pilots can grow into really big plans. Concerning a selection process, perhaps the right instrument would be the ECCC. Otherwise, the community can define topics, and the ECCC can identify subparts in the community worth funding in order to act quickly. If not now, it may be required in a revision in the next part of the regulation for a direct instrument to avoid this time loss.

- **Focused funding**. It is key to come up with a focused strategy for the different communities in order to really understand where investment is needed, based on the operational capabilities that need to be strengthened in Europe. There are a lot of priorities in the Four Pilots and in ECSO. The European Cybersecurity Competence Centre and the different national actors need to talk together and come up with the three or four most relevant projects that can all together work immediately and produce results.

  There will be a procurement for the community, as is stated in the work programme. The group should go forward with small steps as they try to renew this conference which requires some funding not in the size of these projects, measured in millions of euros, but some funds so as to continue the work. Another idea that was discussed is the merging of the mailing lists of each group, to avoid losing that momentum and losing the degree of coordination that was achieved. After the end of this year, the pilots will be gone. There will be no money to do this and the pilots will be competitors again. There is less money in cybersecurity research as it is being moved to deployment in chips. Competition will increase, but some coordination should be kept up as that the seeds which have been sown do not die.

  Public money is being spent, and it is a social responsibility as citizens to advise that this money be spent in the most appropriate and most efficient way, and this is what the group is doing. However, the group does not have powers of decision, but they can try to show that they have ideas, and it is the responsibility of the public institutions to decide what to do with it.

- **Recognition of the work of the Four Pilots**. If the pilots performed well, there needs to be some sort of recognition. It does not make sense to start all over again. At the European level, it should be recognized that that cybersecurity is an important topic and that that the work the Four Pilots have been doing has produced positive results which needs to be built upon. If the thought process moves back to the national level, the focus will be fragmented again.

Question from ENISA:

What are the plans after this conference? ENISA is willing to support, they agree that the momentum should not be lost and wanted to know about the plans for the next move.

Answers:

- ECSO is not linked to funding, it is easier for them, but it still is complicated as they do not have money to do what they plan to do. The next step for them is to work on this vision and put it all together and still have the dialogue enriched. But this is not just done within ECSO by itself, but linked to the pilots and via the common members, the relationship with ENISA and with the EC as well as all the other different stakeholders. It is crucial to work on this vision, both with regards to R&I and the operational part, so they can choose what to invest on. They aim to conclude this in one month, and then continue the work in putting the stakeholders together, but also establish the content to create the ecosystems together. This has to be done together with the pilots and the results that they have achieved so far, but also considering what the Commission plans in terms of policy, industry needs, as well as the individual strategies of the member states. All of this has to be coordinated to see what ECSO can bring up to the European level for a coordinated effort. More important than resources is having all the minds sitting together.

- The European system is very complex. The Four Pilots plus ECSO represent research and innovation, markets, and even member states although not in the same way as an NCC, but there is a good spectrum and their voice needs to be heard.

Mark Miller closed the session by announcing the next panel titled "What Next?". This was the last CONVERGENCE event, there were three such events with the first concertation meeting in 2019, the first CONVERGENCE meeting in December 2020, a virtual-only event during COVID. He also announced that on the 15th of September there would be an evening event related to CyberSec4Europe, and the final event for that project will be on the 1st and 2nd December towards the end of the year.

3.3 Panel discussion: "What Next?"

Panellists:

- Pascal Steichen, Chair of ECCC Board, SECURITYMADEIN.LU
- Miguel González-Sancho, Head of Cybersecurity Technology and Capacity Building, DG CONNECT
- Juan Díez González, NCCC Spain, INCIBE
- Corinna Schmitt, NCCC Germany, Universität der Bundeswehr
- Joanna Świątkowska, ECSO
- Marcel van Berlo, EARTO SDWG

Moderator: Fabio Martinelli, SPARTA

View on YouTube: https://youtu.be/CuKZ4a1POF8 starting at 4:29:05/5:48:26

Fabio Martinelli welcomed the panel and asked for their initial view on how they see the future of the European Cybersecurity Ecosystem from their organizational perspective. The following comments were made below on the future of the European Cybersecurity Ecosystem.

- From a general perspective of cybersecurity skills, there are big challenges of the future in cybersecurity, due to the **lack of skills and the lack of human resources**. This particular challenge needs to be tackled in order to achieve technological autonomy in Europe, which will allow managing different situations such as serious crisis or incidence, independently.

- From the perspective of the European Commission, **cybersecurity threats have accelerated enormously** recently, fuelled by the pandemic and then geopolitical situation.

- From the policy perspective, cybersecurity moved into a more **relevant position on the European agenda** as an issue that needs coordination in terms of situational awareness and exchange between member states and different structures.

- From the side of the Commission, there is an important strand of **proposals on the rules for cooperation and capacities; the cyber resilience act; security of products** is being boosted already. The cyber community and the Competence Centre and the national coordination centres interact in the economic industrial dimension. There are still horizon Europe calls for that matter, but the first cybersecurity digital Europe program call is already closed.

- From the point of view of an NCC, there is a need for setting up the European centre and the national coordination centre in the public sector so as to **enlarge the community** with more end users, practitioners and entities from different sectors with an interest in cybersecurity. From the German NCC perspective, for example, it was felt that services can be better defined once all national centres are brought put together.

- From the ECSO perspective, always remember that **private partnership** should be at the centre of the of all the activities. The **dual nature of this organization** is the secret ingredient for **ECSO's success** in building and developing communities over the years.

- From the perspective of the Four Pilots and ECSO, there is **need to sustain the networks** and the results that have been built upon thus far by the Four Pilot projects and ECSO. The ECCC can support and help in making the selections of topics in the follow-up research programs and initiatives to facilitate the technology.

Fabio Martinelli opened the floor for questions from audience.

Question: How are we going to save the momentum and the community spirit? Do we have ideas for this kind of dimension of investments that also the citizens can understand?

Answer:

- As cybersecurity is getting to be a part of very different areas, we need to make sure that cybersecurity is being addressed in other initiatives. We also need to make sure that the cybersecurity is a part of a European cloud infrastructure. Cyber incident **detection and sharing are big topic** areas in the world program of the digital Europe program of the cybersecurity

Question: What should stakeholders do to achieve European strategic autonomy in cyber security?

Answers:

v. From a very high-level perspective, strategic digital autonomy in Europe should start with identifying where are we are, what we want to achieve, understand what we have in terms of technology skills, and also examine the outcomes coming from the work of the pilots and working groups. Then we can move to the implementation phase.

vi. In a paper on digital autonomy in Europe, five main objectives are listed accompanied with ten very concrete recommendations: focusing on cyber risk management and making Europe a leader in

cyber threat prevention detection response; resiliency and trusted supply chains; focusing on research and development; the importance of the investment factor - human element; how to use private public cooperation.

vii. The European cybersecurity solutions should compete in the global arena. We need to support those people with innovative ideas.

viii. The key message is not only to look at the national market but at the European market and team up as member states. The problem is that the economic and the societal and security interests are not always aligned, that is why it is necessary to find a good and correct balance between the economic perspective, the societal and security perspectives.

ix. Digital technologies have become one of the critical resources. From the European union side, data on artificial intelligence needs to be pushed higher to the top of the political priorities next to the green agenda and health aspects.

Question: Which kind of mechanisms of direct funding the ECCC or others have?

Answers:

x. The European Competence Centre is not only about European funding, it is also about what happens at member state level and lower and trying to align all these.

- The NCCs will have the possibility to decide if they want to use these cascading funding mechanisms. An important mission is to create this visibility across European companies that provide cybersecurity services. Interoperability and openness are key to ensuring that we achieve a resilience mechanism in that system. There should also be more meetings where the different NCCs meet to discuss.

Question: How are you going to counteract the drift towards fragmentation of the community?

Answer:

- There is positive feedback about this approach of the competence network from member states, but we also need to ensure that the NCCs cooperate. We could complement this national kind of structural coordination from a topic perspective.

Question: Fabio Martinelli noted that this Panel of "What's next" is a panel on convergence of the Four Pilots and he asked the panel would be the next big thing that the Four Pilots could do for the ECCC.

Answers:

- The mission of the ECCC and the national coordination centres is to provide some restructure to help to support European community. It is necessary to **take the experience of the pilots** into consideration when creating the national coordination centres.

- The community which has been built up should continue and could be rearranged, but it is important to **be in touch with the national competence centres** so that they are aware of all the partners involved.

- Every meaningful conversation about the future, every single action or decision that will shape what is coming next must be respectful to the past. The **pilots should not be forgotten and are willing to cooperate.**

- In order to have interaction, there is a need to develop and install field labs, innovation hubs so that everybody can make use of actual services and in this way **cooperation amongst the centres** in a more international context could be better arranged.

- The **network of ECCCs is a tool to have this cooperation and exchange** between different member states. There are many companies that are already involved in entities, but there are still more to bring into this community. To achieve this, although there are already educational programs in cybersecurity, but we need to fill them better. **We need to create the visibility that cybersecurity is an important topic in Europe.**

Question: A proposal of the creation of the European defence community with the only joint a structure organization – the consortium. What about UK? Why shouldn't the UK join our cybersecurity community?

Answer:

- This is the time for cooperation with many other forces, including Norway and the UK. The art of the cooperation is having an **open and interoperable market.**

Fabio Martinelli invited to the panel to make their **final statements**, which are noted below:

*"Stay connected**,** joint work, keep performance and discuss very good!"*

"To the commission and to the national entities: make some decisions and choices very soon."

"To the ECCC and the NCCs: we need a strong community, so help us to put the initiative in the field and make it successful."

"To the European competence: the ECCC needs good resources, so watch the positions and apply."

In closing the CONVERGENCE NEXT event, Kai Rannenberg thanked the panel for showing both sides of the equation with great results and things that we have ahead of us. There are ideas in terms of which areas work is required. There is feedback that there is still fragmentation in the market. There are positive evolutions for example in terms of the collaboration infrastructures that are following our cyber security principle such as big blue button. The format of this hybrid meeting was equally enjoyable.

4 Conclusions and Recommendations

CONVERGENCE NEXT showcased and recognized the positive and successful collaboration between the Four Pilots (CyberSec4Europe, CONCORDIA, ECHO and SPARTA) and ECSO.

CONVERGENCE NEXT therefore provided an opportunity for the Four Pilots to share their project results in one setting, while giving the European institutions and the wider European cybersecurity community a snapshot of where they started, what they had worked on and where they were heading as a community, including a look into the future with the last panel session.

This chapter looks at the achievements of the Four Pilots and presents a summary of the challenges encountered in such a way to highlight key points for the future.

4.1 Achievements of the Four Pilots:

Some of the community-building achievements of the Four Pilots during their three years of working together are summarized in this subsection.

4.1.1 Building Trust

With Europe being built up of different countries, different procedures, and different cultures, it is clear that **trust is a pillar in cybersecurity**. Information sharing, especially across borders and sectors, is based on trust and connected communities.

The Four Pilots started with consortiums from different countries but successfully moved on to working together on cybersecurity at a European level. After more than three years of working together and alongside, building the platforms for different sectors, building cyber ranges, educational frameworks, educational skills, and standardization, the pilots have shown how they have brought the communities together in building a network. The knowledge, confidence and the commitment made them stronger together with the most important outcome of creating proto-communities was the **creation of trust**.

4.1.2 Community-Enabling

The Four Pilots successfully brought together many Europeans from different backgrounds, different countries and this was enabled by considerable funding to produce a specific set of results. The "community-enabling" process grew in the following ways:

- **Working together and learning together with a common goal** and supporting each other, also through the different groups across the pilots, e.g., the governance group, the roadmapping group.
- **Connecting communities and sub-communities**, for example, educators and researchers connected, which then contributed to the achievement of the demonstrators of all the pilots in different areas. There is a European footprint in the standardization community.
- **Collaboration beyond the comfort zone.** Collaboration between people from other areas or groups with which one usually would not be interacting took place on a daily basis. The resources allowed people to reach out to new parts of the community and discuss, develop and work together. They felt more comfortable and secure and trust was growing.
- **Collaboration of the Four Pilots and ECSO**. From a community standpoint, a very positive collaboration was that of the Four Pilots and ECSO working as a "proto-community" together. There has been a lot of value in the joint events and other events, in which the Four Pilots and ECSO have met and exchanged ideas. A group was been formed that is enthusiastic, creating

solutions and trying to move forward. These entities made partnerships, despite the constraints of two years of Covid, and used the benefits from their complementary approaches to interact with each other more.

- **Relevance of pilots in a resilient Europe**: Since the pilots started in 2019, there were many challenges such as the pandemic and supply chain risks and the relevance of the Four Pilots increased significantly. The pilots provided solutions for the future, best practices and they continued to build the community and cooperation. Therefore, their role in the situation in Europe, in providing results and bringing together different sectors of the community for a resilient Europe is still very relevant.

4.1.3 Results of the Four Pilots

The investment in the Four Pilots have produced significant results in all areas of their expertise. All Four Pilots presented key highlights of their projects (see Section **Error! Reference source not found.** and 2.10) and it would be important to use these results, in addition to maintaining and growing the community it has built to strengthen cybersecurity in Europe.

The pilots have shown that they can work together: the network is there, the people know each other, they have been working together in inter-pilot focus groups, the whole set of dynamics is there, and it should not die. The momentum created should be built upon. It may be necessary to develop a strategy and to look at what came out of the pilots and what is really valuable for Europe to support the initiative(s) further without going through the whole circle of consortium building.

4.2 Looking into the Future

The ultimate challenge is to ensure that the capabilities, network and cooperation developed within the context of the four pilot projects and ECSO is not lost during the period of transition to the full operation of the European Cybersecurity Competence Centre and the associated community. To that end a number of conclusions and recommendations have resulted from the work of the pilots and ECSO and during the CONVERGENCE NEXT event these aspects have been brought to the forefront for discussion and consideration, as summarized in Figure 27. It is in that context that the next sections cover these issues in detail from the event.

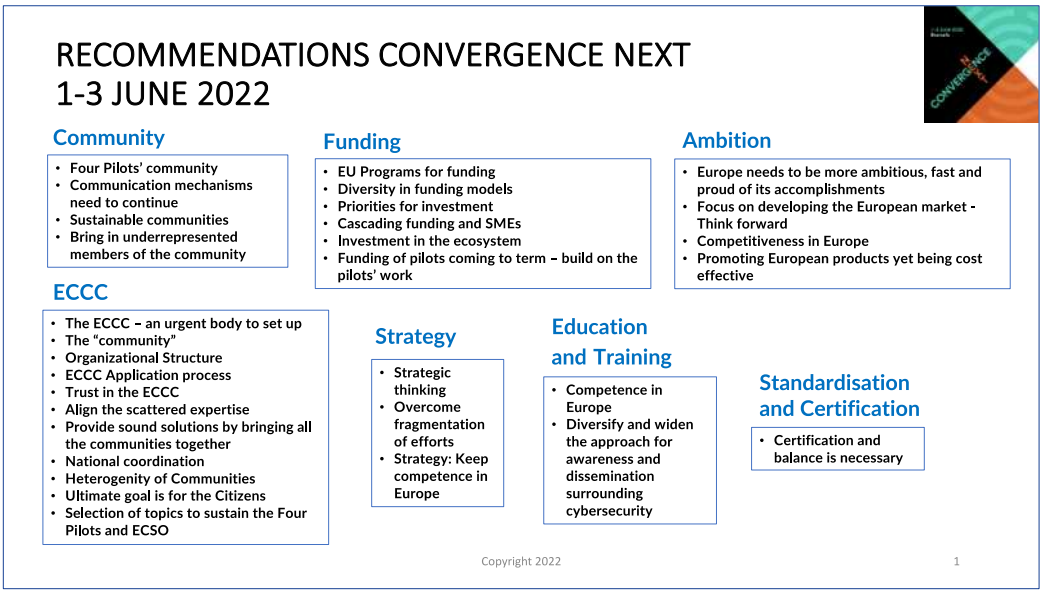


Figure 27: Recommendations of CONVERGENCE NEXT

4.2.1 Benefits for the Community / Networks / Stakeholders

The following points relate specifically to the community

- **Four Pilots' community.** With the pilots, the best expertise at the European level was brought together, based on how they could cooperate to achieve European digital sovereignty in the field of cybersecurity. At the European level, the subject pertained to the Four Pilots and not specific nationalities, which is a major feature that needs to be kept. It is important to keep this alive even after the Four Pilots, and in order to do this some motivation is necessary.
- **Communication mechanisms need to continue.** It is necessary to keep the four communities plus ECSO communicating with each other under a truly European umbrella. There are common dissemination tools in place but it is necessary to have a broader outlook, not only to just bring people together, but also to have the instruments that will enable people to work together and have discussions in a smart and proper way. Find a way to keep the ball rolling at the European level.
- **Sustainable communities.** It is important to provide communities with ways to organize themselves in a sustainable way. To come up with a structure and mechanisms which can sustain time and be the vector of the community to ensure that the community can rise up in an agile manner in the face of new challenges. Mechanisms should challenge the community and enable the community to listen to each other and to create the European culture and European values around cybersecurity to build faster strategies or reactions. This is a mandatory building block.
- **Bring in underrepresented members of the community**. It is an important priority to involve underrepresented actors and incorporate grassroot initiatives.

4.2.2 ECCC

- **The ECCC – an urgent body to set up:** ECCC is no longer a necessity but an urgency. Since the proposal establishing the ECCC went into force in September 2018, the issue of cybersecurity has exploded, first with COVID, and now with a rise in cyberattacks since the Russian invasion of Ukraine. These events show that the centre is not just a necessity, but it has become an urgency in order to improve the research and innovation capabilities in cybersecurity in the European Union.
- **The "community"**: The community is the third pillar next to the ECCC and the national competence centres, and the Four Pilots and ECSO are a part of that community. These bodies need to be united, also with national groups without any important player left out. The results thus far produced should be built upon and not forgotten.
- **Organizational Structure**: The Centre is a particular kind of body due to its dual role. It is not a simple implementing agency, but it has a broader, strategic task to ensure that all existing expertise is aligned, that all stakeholders are involved and that the whole framework that is foreseen in the regulation works. The centre also does not exist in a void, it has to fit in with what is already there with all its tasks and strategic objectives, with a working organisational framework incorporating the National Competence Centres (NCC), the community, and the strategic advisory group.
- **ECCC Application process**: It is hoped that the complexity of the application process may be reduced, so that the success of an application depends on the expertise and technical knowledge of the applicants.
- **Trust in the ECCC:** The question remained how does the proposed structure of the ECCC and the NCCs intend building trust. The challenge remains as to how can trust continue to be built with the new European structure in place, not only within the research and technology communities, but also within the operational communities.
- **Align the scattered expertise**: The main objective behind the centre is to pull together the scattered expertise and align it, so that there is a common vision and strategic objectives.

- **Provide sound solutions by bringing all the communities together**: In order to ensure that the solutions selected are the right ones, it would be important to bring together the industry, the NCCs, with the public authorities.
- **National coordination**: The NCC network is one of the key points and there is a quick win in this respect. There is need for national coordination, in particular as some countries are more mature and others are less mature.
- **Heterogeneity of Communities**: Across Europe, there is a homogeneity of interests within a community which is not the case for communities at a national level. National communities are very different from country to country, because of differences in budget, local challenges and national priorities. The main challenge will be the heterogeneity of communities.
- **Ultimate goal is for the Citizens**: There is the need to also bring citizens on board. The ultimate benefit of the centre has to be for the citizen and the citizens will only benefit if Europe is organised.
- **Selection of topics to sustain the Four Pilots and ECSO**: There is need to sustain the networks and the results that have been built upon thus far by the four pilot projects and ECSO. The ECCC can support and help in making the selections of topics in the follow-up research programs and initiatives to facilitate the technology. The work of the Four Pilots was widely recognized. There is concern that if the thought process moves back to the national level, the focus will be fragmented again.

4.2.3 Funding

- **EU Programs for funding:** It was noted that the programs for funding are late in being issued. The longer the wait the less competitive Europe is.
- **Diversity in funding models:** Diversity in funding models is necessary, including education. A global and comprehensive strategy is necessary as technology is not sufficient for start-ups. Hiring or developing marketing skills to sell the European products and technologies is necessary.
- **Priorities for investment**: There is a need to set priorities for investment. It is key to come up with a focused strategy for the different communities in order to really understand where investment is needed, based on the operational capabilities that need to be strengthened in Europe. There are a lot of priorities that emerged from the Four Pilots and in ECSO. The European Cybersecurity Competence Centre and the different national actors need to communicate and identify three or four of the most relevant projects to work on immediately and to produce results.
- **Cascading funding and SMEs**: There is hope that NCCs will be advise potential applicants for EC funding via cascading mechanisms and this could be a way to help SMEs applying for funding.
- **Investment in the ecosystem:** There is a need to invest a lot more resources into creating this ecosystem, to really make it into a very successful group of SMEs that grow and provide services from within European borders. Incentive/motivation is missing.
- **Funding of pilots coming to term – build on the pilots' work:** It was recognized that the Four Pilots were successful and building on their work is an important step in the future.
    - With the end of the pilots is in sight, the partners are disappearing and it seems that the whole process might need to start again. In Europe, the maximum funding is three to five years. To **build an ecosystem in Europe, a longer time-frame is necessary**.
    - A **group of experts** (outside of the pilots) should examine the efforts invested in the Four Pilots and pick up on at least some of the **outcomes for further investment**, so that the fruit of the Four Pilots can grow into really big plans. Concerning a selection process, perhaps the right instrument is the ECCC. Otherwise, the community could define topics, and the ECCC could identify subparts in the community worth funding in order to act quickly. If not now, it may be required in a revision in the next part of the regulation for a direct instrument to avoid this time loss.

4.2.4 A More Ambitious Europe

- **Europe needs to be more ambitious, fast and proud of its accomplishments**. At the European level, we need to be more ambitious in many sectors, including building solutions in Europe and keeping them European in order to build an eco-system. Europe needs to be faster.
- **Focus on developing the European market - Think forward**: In the future, cybersecurity will increasingly be driven by artificial intelligence and Europe needs to place more focus on this aspect of the market and how it will develop in 15 years.
- **Competitiveness in Europe**. There is a need to build competitiveness in Europe. The traditional approach of the Commission was to focus on research and innovation (R&I), for which the centre is also dedicated, but there is more than R&I, there is a need to bring competitiveness to the European economy, not just to supply cyber security but also to protect Europe in the digital transition. The private sector which holds knowledge and competence faces daily cyber threats and needs to be involved more.
- **Promoting European products yet being cost effective**: The challenge remains to bring European products to a marketable level.

4.2.5 Strategy

- **Strategic thinking**. The pilots developed road maps and proposed next priorities for Europe. Europe needs to be faster and more agile and use the groundwork of the pilots in order to move forward.
- **Overcome fragmentation of efforts**. It now becomes urgent to set the strategic agenda, to gather the contributions from all the working groups and have the cyber community very active in this process.
- **Strategy: Keep competence in Europe.** There should be a coalition between countries, the European Commission and the private sector to be more active in education. It can be a long-term goal but there is need for a strategic decision as to how we can develop and keep competence in Europe.

4.2.6 Education and Training

- **Competence in Europe.** There is a need to develop and keep competence in Europe. There is a need to fill the 500,000 shortfalls of experts. Concentrated efforts and approaches towards the application areas are necessary.
- **Diversify and widen the approach for awareness and dissemination surrounding cybersecurity**. Explore individual national approaches which work within Europe and strategically adopt success stories in an EU-approach to reach a wider group of European citizens.

4.2.7 Standardization and Certification

- **Certification and balance is necessary**. It is a challenge that if one wants to come up with a new and innovative product, there is need for a lot of certifications, and NIS2 will also have legal requirements. The balance of making something secure and also in line with privacy and data protection requirements necessitates acting fast.

4.3 Overall Conclusion

Significant results have been achieved during the course of this CyberSec4Europe project and the conclusions and recommendations section was clearly addressing challenges both current and in the future. The intent of this deliverable was to document the final concertation event, document the key collaboration and engagement activities undertaken by the CyberSec4Europe consortium partners during this final period and to provide conclusions and recommendations that point toward areas to be addressed in the future.

5 List of Annexes

Annex 1	Conference Program
Annex 2	Short Biographies
Annex 3	Day 1 – Highlights of CONCORDIA – Presentation by Gabi Dreo Rodosek (CONCORDIA)
Annex 4	Day 1 – Highlights ECHO – Presentation by Wim Mees (ECHO)
Annex 5	Day 1 – Highlights CyberSec4Europe – Presentation by Kai Rannenberg (CyberSec4Europe)
Annex 6	Day 1 – Governance Session – Presentation by Martin Übelhör (DG CONNECT)
Annex 7	Day 1 – Governance Session – Presentation by Focus Group on Governance
Annex 8	Day 1 – Panel Situation in Europe – Presentation by Artur Kozlowski (EARTO SDWG)
Annex 9	Day 2 Research Results – Presentation by Antonio Skarmeta (CyberSec4Europe)
Annex 10	Day 2 Research Results – Presentation by Antonio Ken Iannillo (CONCORDIA)
Annex 11	Day 2 Research Results – Presentation by Peter Hagstrom (ECHO)
Annex 12	Day 2 Research Results – Presentation by Augustin Lemesle (SPARTA)
Annex 13	Day 2 Verticals Results – by Alessandro Sforzin and Christos Grigoriadis, (CyberSec4Europe)
Annex 14	Day 2 Verticals Results – Presentation by Thanh van Do, Boning Feng, Bernado Santos, Madalina Baltatu (CONCORDIA)
Annex 15	Day 2 Verticals Results – Presentation by Presented by José María Torres (ECHO)
Annex 16	Day 2 Verticals Results – Presentation of Verticals by (SPARTA)
Annex 17	Day 2 – Presentation by Wide Hogenhout of JRC Atlas
Annex 18	Day 2 – Presentation by Marco Barros Lourenco (ENISA)
Annex 19	Day 2 – Presentation of the Roadmapping Focus Group
Annex 20	Day 3 – Presentation of the Education Focus Group
Annex 21	Day 3 – Presentation by Boning Feng of the CONCORDIA European Education Ecosystem for Cybersecurity
Annex 22	Day 3 – ECSO's work in education - Presentation by Nina Olesen (ECSO)
Annex 23	Day 3 – Presentation by Robert Cascella (ECSO)
Annex 24	Day 3 – Presentation by Afonso Ferreira (IRIT)

AGENDA

CONVERGENCE NEXT
1-3 June 2022

At the beginning of June 2022, CyberSec4Europe, CONCORDIA, ECHO and SPARTA hosted **CONVERGENCE NEXT** online and at the Representation of the State of Hessen to the EU, rue Montoyer 21, Brussels B-1000. It followed in the tradition set in the first CONVERGENCE event on 9-11 December 2020 which successfully presented results and demonstrations from the four pilot projects and the collaborative focus groups.

CONVERGENCE NEXT focussed on the future of the community, the European Cybersecurity Competence Centre (ECCC) and looked at the key issues for cybersecurity in the future. This event was not to be missed for those interested in European cybersecurity issues. High-level representatives from EU institutions discussed the role of the ECCC and that of the wider stakeholder community in the next stages.

If you were there and would like to remember **CONVERGENCE NEXT** or catch up with the event if you missed it, you can follow all three days of the event, at the following links :

YouTube Links:

Day 1 - Wednesday, 1 June 2022 : https://youtu.be/jQ0PptjZfd4
Day 2 - Thursday, 2 June 2022 : https://youtu.be/lrjdHJsPYaQ
Day 3 – Friday, 3 June 2022 : https://youtu.be/CuKZ4a1POF8

Wednesday, 1 June 2022

Setting the Scene

11:00 Welcome

- **Frank Wamser**, Head of Justice, Representation of the State of Hessen to the EU
- **Kai Rannenberg**, CyberSec4Europe

11:15 Highlights of the four pilots and ECSO

- **Gabi Dreo Rodosek**, CONCORDIA
- **Wim Mees**, ECHO
- **Florent Kirchner**, SPARTA
- **Kai Rannenberg**, CyberSec4Europe
- **Luigi Rebuffi**, ECSO
  - Moderator: **Kai Rannenberg**, CyberSec4Europe

13:00 Lunch

14:00 Governance
About the Competence Centre

- **Martin Übelhör**, Head of Cybersecurity Industry and Innovation, DG CONNECT

Work / results of the Governance Focus Group

- **Natalia Kadenko**, Coordinator, Governance Focus Group
- **Irena Mladenova**, ECHO
- **Arthur van der Wees**, CONCORDIA
- **Dirk Kuhlmann**, SPARTA

Open floor discussion – Q&A
Session chair: **Natalia Kadenko**, CyberSec4Europe

15:15 Coffee break

15:45 Panel discussion: **Situation in Europe (network and community)**

- **Kai Rannenberg**, CyberSec4Europe
- **Gabi Dreo Rodosek**, CONCORDIA
- **Wim Mees**, ECHO
- **Florent Kirchner**, SPARTA
- **Luigi Rebuffi**, ECSO
- **Artur Kozłowski**, EARTO SDWG

Moderator: **Mark Miller**, CyberSec4Europe

16:45 Summary of the day: **Gabi Dreo Rodosek**, CONCORDIA

Wednesday, 1 June 2022

Evening Session

17:00 Social networking
18:00 Welcome

- **Frank Wamser**, Head of Justice, Representation of the State of Hessen to the EU

Panel discussion: **The European Cybersecurity Competence Centre (ECCC)**

- **Katarzyna Prusak-Górniak**, Vice-chair, ECCC Board
- **Lorena Boix Alonso**, Director for Digital Society, Trust & Cybersecurity, DG CONNECT
- **Dörte Rappe**, Chair NCCC Germany, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- **Luigi Rebuffi**, Secretary General, ECSO
- **fukami**, cybersecurity savant

Moderator: **Kai Rannenberg**, Coordinator, CyberSec4Europe

19:30 Evening social event

Thursday, 2 June 2022

Research and Innovation

09:00 Welcome – **Wim Mees**, ECHO

09:15 Research results sessions and demonstrations

- **Antonio Skarmeta**, CyberSec4Europe
- **Antonio Ken Iannillo**, CONCORDIA
- **Peter Hagstrom**, ECHO
- **Augustin Lemesle**, SPARTA

Session chair: **Wim Mees**, ECHO

10:45 Coffee break

11:15 Verticals

- **Alessandro Sforzin**, **Christos Grigoriadis**, CyberSec4Europe
- **Thanh van Do**, **Boning Feng**, **Bernado Santos**, **Madalina Baltatu**, CONCORDIA
- **José María Torres**, ECHO
- **Thomas Jensen**, SPARTA

Session chair: **Wim Mees**, ECHO

12:45 Lunch

13:45 Perspectives from JRC ATLAS and ENISA

- **Wide Hogenhout**, DG CONNECT
- **Marco Barros Lourenco**, Research and Innovation Lead, ENISA

Session chair: **Evangelos Markatos**

15:15 Coffee break

15:45 Roadmapping for the future

- **Thomas Jensen**, Coordinator, Roadmapping Focus Group
- **Evangelos Markatos**, CyberSec4Europe
- **Theodora Tsikrika**, ECHO

Session chair: **Thomas Jensen**, SPARTA

16:45 Daily summary – **Augustin Lemesle**, SPARTA

17:00-18:30 Social networking

Friday, 3 June 2022

Sustainability and Expanding the Impact

09:00 Welcome – **Boning Feng**, CONCORDIA
09:15 Capability building (education, skill sets, etc)

- Cybersecurity education including the Education Focus Group
  - **Boning Feng**, CONCORDIA
  - **Carlos E. Budde**, CyberSec4Europe
  - **Nina Olesen**, ECSO WG 5

  Session chair: **Boning Feng**, CONCORDIA

10:30 Coffee break

11:00 Evolution of the European cybersecurity ecosystem

- **Roberto Cascella**, ECSO 2.0 / 3.0
- **Afonso Ferreira**, CyberSec4Europe
- **Thanh van Do**, CONCORDIA
- **Wim Mees**, ECHO
- **Fabio Martinelli**, SPARTA

  Moderator: **Mark Miller**, CyberSec4Europe

12:15 Lunch

13:00 Panel discussion: **What Next?**

- **Pascal Steichen**, Chair of ECCC Board, SECURITYMADEIN.LU
- **Miguel González-Sancho**, Head of Cybersecurity Technology and Capacity Building, DG CONNECT
- **Juan Díez González**, NCCC Spain, INCIBE
- **Corinna Schmitt**, NCCC Germany, Universität der Bundeswehr
- **Joanna Świątkowska**, ECSO
- **Marcel van Berlo**, EARTO SDWG

  Moderator: **Fabio Martinelli**, SPARTA

14:00 Summary of **CONVERGENCE NEXT: Kai Rannenberg**, CyberSec4Europe

14:15 Coffee & pastries

Annex 2

SHORT BIOGRAPHIES OF SPEAKERS AND PANELLISTS
(CONVERGENCE NEXT, 1-3 JUNE 2022)

Lorena Boix Alonso (DG CONNECT)

Lorena Boix Alonso is Director for Digital Society, Trust and Cybersecurity in the Directorate General for Communications Networks Content and Technology (DG CONNECT), at the European Commission. She is a member of the Executive and Management Board of the European Network and Information Security Agency (ENISA) and as well as the Commission representative in the Governing Board of the European Cybersecurity Competence Centre (ECCC) and a member of the Management Board of the Computer Emergency Response Team for the EU Institutions (CERT EU). In the context of the Horizon Europe Programme, she co-chairs the Cluster 1 "Health" and Cluster 3 ''Civil security for society'' and is as well a member of the board Innovative Health Initiative (IHI) Joint Undertaking. Formerly, she was Acting Director for Policy Strategy and Outreach and Head of Unit for Policy Implementation and Planning, in DG CONNECT at the European Commission Previously, she was Deputy Head of Cabinet of Vice President Neelie Kroes, Commissioner for the Digital Agenda. During Ms Kroes' mandate as Commissioner for Competition, she commenced in October 2004 as a member of her cabinet and became Deputy Head of Cabinet in May 2008. She joined the European Commission Directorate-General for Competition in 2003. Prior to that, she has worked for Judge Rafael García Valdecasas, at the European Court of Justice, as well as Deputy Director and Legal Coordinator of the IPR-Helpdesk Project and in private practice in Brussels. She holds a Master of Laws from the Harvard Law School. She graduated in Law from the University of Valencia and then obtained a Licence Spéciale en Droit Européen from the Université Libre de Bruxelles.

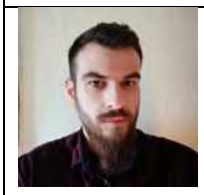
Madalina Baltatu (CONCORDIA)

Madalina Baltatu has been a security researcher for the cybersecurity department of Telecom Italia Mobile since 2002. She has a Ph.D. in Network Security from the Politecnico di Torino (2001). Her main areas of interest are cyber security, cyber threat intelligence, network security, anomaly detection techniques for IDS/IPS systems, biometrics-based authentication and encryption, mobile security (mobile malware analysis). She is a member of GSMA, was involved in many security related European funded projects, recent ones being NEMESYS (as TIM coordinator and work package lead), 5G-ENSURE (as privacy task lead) and CONCORDIA (threat intelligence and DDoS pilots). She is also the author of various of several international patents.

Marcel van Berlo (EARTO SDWG)

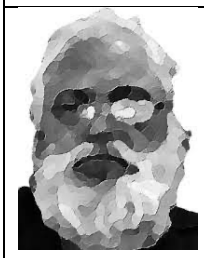
Dr. Marcel van Berlo is a senior program and project manager in the field of human factors and security at TNO (the Netherlands) and holds a Ph.D. in Instructional Psychology and Technology from the University of Leuven. An important part of his activities is building coalitions between different stakeholders and networks both at a national and European level, with the purpose of conducting applied and meaningful research benefiting society. Within the TNO Unit Defence, Safety & Security, Marcel

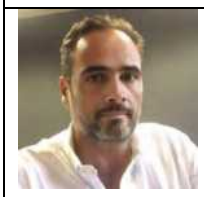
	is the EU manager security research. Since 2019, he has been the chair of the EARTO Working Group security & defence research. From 2017-2020 Marcel was the technical coordinator of the European research project DRIVER+ which was labelled by REA as a "success story" and selected as one of ten most impactful, innovative breakthrough projects of 2020 funded by the EC.
	**Carlos E. Budde (CyberSec4Europe)** Carlos E. Budde received his PhD degree in Computer Science in 2017 from the Universidad Nacional de Córdoba (AR), specialising in rare event simulation for formal methods. From 2017 to 2021 he worked as a post-doc researcher at the Universiteit Twente, also in collaboration with Dutch Railways, applying simulation and machine learning to big data for risk management. Since 2021 Carlos has held a position as assistant professor at the Università di Trento, using simulation-based analyses to assess the cybersecurity resilience of system models.
	**Roberto Cascella (ECSO)** Roberto Cascella is Head of Sector "Technology, Supply Chain & Strategic Autonomy" at the European Cyber Security Organisation (ECSO). He coordinates the two technical ECSO WGs with a high impact on the European cybersecurity strategy: WG6 defines the cybersecurity R&I roadmap for trusted and resilient technologies, and WG1 focuses on standardisation and certification in cybersecurity with the mission to establish trusted supply chains at EU level. He also represents ECSO in different committees, including the SCCG established under the Cybersecurity Act. Before joining ECSO, he worked as Innovation and Research Project Manager and Research Scientist contributing to several EU projects. Roberto holds a Ph.D. (2007) in ICT from University of Trento, an M.Sc. in Telecommunication Engineering from Politecnico di Torino and KTH
	**Gabi Dreo Rodosek (CONCORDIA)/** Gabi Dreo is Professor for Communication Systems and Network Security at the Bundeswehr University Munich and the Founding Director of the Research Institute CODE. She is the Coordinator of the EU H2020 project CONCORDIA and holds several supervisory and advisory mandates in industry. Besides, she is member of the Digital Council of the German Ministry of Defence, member of the World Economic Forum's Global Future Council on Cybersecurity, member of the Board of the Security Network Munich etc. Professor Dreo studied computer science at the University of Maribor, Slovenia and got her PhD and habilitation from the Ludwig-Maximilians-University in Munich. Her research interests include AI-based network security, software-defined networks, 5G/6G, moving target defence.
	**Boning Feng (CONCORDIA)** Associate Professor Boning Feng received M.Sc. and Ph.D. degrees from the Norwegian University of Science and Technology in 1985 and 1990 respectively. Since 2005 he has been an Associate Professor with the Department of Computer Science, Oslo Metropolitan University. Prior to that, he was Senior Research Scientist at Telenor R&D (1998–2004) and Associate Professor at the Norwegian University of Science and Technology (1990–1998). From 1996 to 1997 Boning Feng was Visiting Scholar at the University of California at Davis (UCD). He has also been adjunct associate

	professor at the University Graduate Center at Kjeller, Norway (now a part of the University of Oslo). He has participated in several EU research projects coordinating the activities of the Oslo Metropolitan University. His field of interests include 5G networks, network security, IoT, identity management, threat modelling, performance- and dependability analysis.
	**Afonso Ferreira (CyberSec4Europe)** Afonso Ferreira, PhD, is Head of European Digital Matters and senior researcher at the French CNRS, a research institution with more than 11.000 scientists. He is working in two European projects at the intersection of digital technologies, policy and regulation, and foresight, in the areas of cybersecurity and artificial intelligence. Afonso worked for 12 years in European Institutions, including the European Commission, and in 2021 he advised the CNRS in the elaboration of its European strategy, guiding its 30,000 staff to consolidate its position as the largest recipient of H2020 funds. He has published more than 150 papers at the forefront of scientific research, and is an advisor to private companies, research & innovation agencies, and the European Commission.
	**Fukami (Cybersecurity savant)** A consultant in IT security for more than 15 years, **fukami** works on identifying vulnerabilities in digital systems and developing tools for securing systems and applications. Deeply involved in the security and privacy communities in Europe and North America, he helps by analysing developments at the intersection of public policy and technological aspects, while primarily focusing on human rights concerns.
	**Christos Grigoriadis (CyberSec4Europe)** Christos Grigoriadis is a PhD candidate and an experienced security researcher with a background in secure engineering technologies (MSc) and production and management engineering (MEng). From his experience in research and development positions in multiple EU-funded cybersecurity projects, he has taken a specific focus in vulnerability databases and risk assessment methodologies. He has produced a set of papers related to automated risk assessment for cyber-physical systems and cybersecurity ontologies to support risk information gathering.
	**Juan Díez González (INCIBE)** Juan has a Master Degree in Computer Science from the University of León and has more than 18 years experience on IT projects, the last 11 years of which have been field of information security / cybersecurity. Juan is currently working as a project leader of cybersecurity programmes specifically on research and innovation activities at a national level. He leads the European project management office at INCIBE to coordinate the participation on research and innovation projects. He also participates in ECSO, representing the Spanish delegation. He is part of the NCC-ES team of the ECCC initiative. He has led initiatives to support and stimulate research and innovation in cybersecurity from INCIBE, such as the creation of the Spanish Network of Excellence in Cybersecurity Research (RENIC), the launch of the Cybersecurity Research National Conference (JNIC), and

	programmes for advanced cybersecurity research team excellence. He has also participated in security consulting projects at INCIBE (for Spanish Administration Agencies), such as the development of strategic security master plans, IPV6 transition scenarios or digital and federated identity with electronic identity cards. He has a good knowledge of security governance and compliance, with great communication and leadership skills. He previously worked as R&D team leader at INCIBE-CERT (the governmental CSIRT managed by INCIBE), creating security tools and participating actively in security projects related to the incident handling service, from which he has a deep knowledge in development life cycle, and technical security issues. He is certified on PMP (PMI), CISA and CISM (ISACA), CISSP (ISC2), CEH (EC-Council), S0A-ISO27001 lead auditor and S0B-ISO27001 lead implementer (AENOR), CSM (Scrum Alliance) and others.
	**Miguel Gonzalez-Sancho (DG CONNECT)** Since July 2018, Miguel Gonzalez-Sancho has been Head of Unit for "Cybersecurity Technology and Capacity Building" at Directorate-General CONNECT of the European Commission, being responsible in particular for EU funding, policy on supply chain security including 5G, cybersecurity certification, and cyber threat detection, sharing and response. In addition, since September 2021 he has been interim Executive Director of the European Cybersecurity Competence Centre, an EU body of around 40 staff based in Bucharest, tasked with identifying investment priorities, managing EU and national funds, and liaising with National Coordination Centres for cybersecurity innovation and market uptake. Prior to that, he held different positions at the European Commission, dealing mainly with EU policies, legislation and funding for digital services, including Head of Unit for eHealth and Head of Unit for Administration and Finance. Miguel holds degrees in law, business administration, international relations and European policies.
	**Peter Hagstrom (ECHO)** Peter Hagstrom is currently one of the R&D Managers for RHEA security services business unit. He has since 2019 also been leading a multi-national team of professionals and the development of the collaborative cyber security information sharing platform – CIRP. At RHEA he has been an integral part of several ESA and European Commission projects, for instance the ECHO project for which he lead the development and design activities for the early warning system. With over 13 years of experience, Peter specializes in software development, team leading, software architecture and is well versed in several technologies and programming languages.
	**Thomas Jensen (SPARTA)** Thomas Jensen is INRIA director of research, adjunct professor at the University of Copenhagen, and scientific leader of the INRIA Celtique team on software analysis and security. He received a PhD from Imperial College London in 1993 and a Habilitation from University of Rennes in 1999. Before joining INRIA, he worked at CNRS where he was research director until 2010. Thomas Jensen's research is concerned with programming languages, semantics-based program analysis and software security. His research results include abstract interpretation in logical form,

	the first formally verified data flow analyzer, analysers for Java and Java Card, and hybrid information flow analysis techniques for estimating attacker knowledge in Web applications. Thomas Jensen leads the security track in the French CominLabs Laboratory of Excellence and is co-editor of the SPARTA road map.
	**Natalia Kadenko (CyberSec4Europe)** Natalia Kadenko is a postdoctoral researcher at the Organisation and/ Governance section of the Faculty of Technology, Policy and Management at/Delft University of Technology in the Netherlands. Her past and current research/ interests include disinformation, European and national cybersecurity policy, the role of/ discourse in policy-making and conflict resolution, and populism. She completed her PhD in Political Problems of/International Systems and Global Development and contributed her expertise to diverse projects. Natalia has/researched policy implications for conflict resolution, edited a magazine to introduce international politics to a wide audience, as well as participated in developing diverse tools to strengthen user resilience to disinformation./ Currently Natalia is leading research on cybersecurity governance in the EU for the CyberSec4Europe H2020 project and is coordinating governance collaboration between cybersecurity competence pilot projects. Additionally, she is teaching and supervising students, conducting workshops,/and organizing events for her team./
	Antonio Ken Iannillo (CONCORDIA) Antonio Ken Iannillo is a research scientist at the Interdisciplinary Centre for Security, Reliability, and Trust (SnT), University of Luxembourg. He received his PhD in Information Technologies and Electrical Engineering from the University of Naples, Federico II. His current research activities focus on software dependability and security, especially software verification and assessment. His targets include new and innovative technologies such as ARM Trustzone for Cortex-M, Ethereum Smart Contract, and ROS. Dr. Iannillo is leading the stakeholders community for CONCORDIA, organising its annual public event (CONCORDIA Open Door) and hosting periodic trusted forum for national cybersecurity entities (NSG).
	**Florent Kirchner (SPARTA)** Florent Kirchner leads the Systems and Software Engineering Division as well as the Cybersecurity Program at CEA LIST. As a senior expert scientist, he has developed and applied several approaches to high-confidence software verification, as part of both academic explorations and industrial projects. He was active in launching and heading collaborative efforts with a wide variety of international partners, including collaborations with Airbus, Bureau Veritas, Thales, NASA, and NIST. As a Head of Division he is responsible for a group of 150 scientists working on the research and development of next-generation engineering methods and tools, and the associated dissemination and communication activities. He is an active member of several working groups on High-Confidence Software and Systems at Allistene, Campus

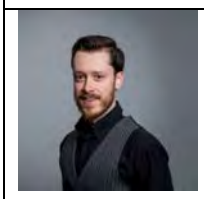
	Cyber, and OECD. Since 2019 he is a member of the ECSO Board of Directors, and the Strategic Director of the SPARTA cybersecurity competence network pilot.
	**Artur Kozłowski (EARTO SDWG)** Artur Kozłowski is a manager and scientist with 15-years experience in management with a PhD in technical sciences. His professional experience in team management as well as the management of financial and intellectual capital was gained during 18 years as a manager and chief executive of R&D projects and implementation projects, both in Poland and abroad. Mr Kozłowski uses a fresh approach to challenges and long-term experience of an R&D manager in the implementation of new projects/technologies and in fulfilling the R&D strategy of the EMAG Institute. Mr Kozłowski is a member of the steering committees of many projects in the realm of ICT, telecommunications, power engineering, new technologies, and security, such as National Scheme for Assessment and Certification of IT Products according to Common Criteria, Regional Cyber Security Centre, Public Administration Catalogues. He is also an active member of numerous associations, technical, scientific and organisational committees, scientific councils, expert councils, and technical committees. He is a graduate of the Faculty of Electrical Engineering of the Silesian University of Technology, specialising in processing and the use of electricity. Mr. Kozłowski completed his postgraduate studies at the Faculty of Automatic Control, Electronics and Computer Science of the Silesian University of Technology in the field of "Computer networks, microcomputer systems and databases" as well as postgraduate studies at the Faculty of Organisation and Management of the Silesian University of Technology in the field of "Modern methods of organisation management". He participated in a number of national and overseas training activities which supplemented his education in the scope of science financing, commercialisation, technology transfer and project management.
	**Dirk Kuhlmann (SPARTA)** Dirk Kuhlmann received his diploma in Computer Science from Technical University Berlin, where he also worked from 1999-1995 as a Research Assistant. In 1995, he took up a position with Hewlett Packard Labs in Bristol, (UK) for more than 20 years as a senior research engineer. There he worked open security platforms and distributed architectures, standardisation and policy aspects of secure ICT in local, national, and transnational contexts. He gained extensive experience as participant, lead, evaluator and reviewer of EU funded research projects on IT security. In 2019, Dirk joined Fraunhofer ISI as a senior research scientist and project manager. For the SPARTA ECCC pilot, he covers the areas of governance analysis and policy evaluation for IT security, big data and AI, data protection, and open source.
	**Augustin Lemesle (SPARTA)** Augustin Lemesle is a research engineer at the Software Safety and Security Laboratory at CEA. He works at the application of formal methods to artificial intelligence safety verification both as part of academic or industrial projects. Since 2019 he has been part of the SPARTA coordination team and since 2020 he has acted as the Technical Manager of the ENSURESEC project.

	**Marco Barros Lourenco (ENISA)** Marco Barros Lourenco is a technologist and researcher in the field of digital policy. He has had a career spanning nearly 30 years, 20 of which were spent in international organisations and multinational corporations such as the World Bank, the EU Council, the United Nations, Microsoft, and the EU Cybersecurity Agency. For nearly two decades, Marco served as an advisor to several governments in Africa, Europe and the Middle East, particularly in the area of digital policy. He helped define national digital and cybersecurity strategies for more than 17 countries. Since 2018, Marco has been responsible for the research and innovation programme for the European Union Cybersecurity Agency (ENISA).
	**Irena Mladenova (ECHO)** Irena Mladenova is a member of the Business Administration Department at Faculty of Economics and Business Administration, Sofia University St. Kliment Ohridski. Her research interests include organisational change and development, organisational culture, strategic management and sustainable development. Irena has over 20 years of experience in the private and public sectors. She worked at international management consultancy companies (Kearney, PwC) delivering projects for regional and local leaders in Eastern European countries. She managed projects for structuring and restructuring processes, procurement costs, optimisation strategies, analysis and optimisation of product portfolio, assessment and planning the launch of new products and new market entries. Her experience includes the development and implementation of new organisational structure and strategy, development of tactical and business plans. She participated in several business potential and market sizing assessments as part of merger and acquisition deals, both on the buyer and the seller sides. She served as Head of Corporate Development and a member of the managing board at a group level for a regional energy services company. Irena worked for five years in the public sector in Bulgaria as an advisor at the Ministry of Economy and the Administration of the President and served as Deputy Minister of Economy at three caretaker governments (2013, 2014, 2021). She is a practising management consultant. As part of the IICT-BAS team, Irena participates in the ECHO project where she is involved in work package 3 with focus on developing the governance model and governance consultancy services.
	**Evangelos Markatos (CyberSec4Europe)** 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 an MSc and PhD in Computer Science from the University of Rochester. He is the founding head of the Distributed Computing Systems and Cybersecurity 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 has been a member (i) of the permanent stakeholders group of ENISA (European Network and Information Security Agency) and (ii) of the Academic Advisory Network of Europol's EC3 (European Cybercrime Center). He is currently a member of the partnership board of ECSO: the European Cyber Security Organisation. 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 eight 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. Professor Markatos has co-authored more than 150 publications at top conferences and in journals including ACM SOSP, ACM SIGMETRICS, IEEE HPCA, ACM/IEEE ToN, IEEE JSAC, USENIX Security, INFOCOM, etc. According to Google Scholar his work has received more than 8,000 citations with an h-index of 47.
	**Fabio Martinelli (SPARTA)** Fabio Martinelli is a research director of the Italian National Research Council (CNR) where he is referent for cybersecurity activities. His main research interests involve security, trust and privacy in distributed and mobile systems. He founded and chaired the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM) and the WG 11.14 in secure engineering of the International Federation of Information Processing (IFIP). He coordinated the EU NESSoS Network of Excellence in Future Internet Security and the EU Training Network on Cyber Security (NeCS). He chaired the WG3 on Research and Innovation of the Network and Information Security (NIS) Platform promoted by the European Commission. He is currently partnership Director of SPARTA. He acts as first director on the Board of ECSO and co-chairs ECSO WG6 SRIA. Fabio Martinelli also served as expert in the H2020 Protection and Security Advisory
	**Wim Mees (ECHO)** Wim Mees is Professor in computer science and cyber security at the Royal Military Academy and is leading the Cyber Defence Lab. He is also teaching in the Belgian inter-university Master in Cybersecurity, and in the Master in Enterprise Architecture at the IC Institute. Wim has participated in and coordinated numerous national and European research projects as well EDA and NATO projects and task groups. He is currently project coordinator for ECHO.
	**Mark Miller (CyberSec4Europe)** Mark Miller is the Chief Executive of CONCEPTIVITY, a Swiss security think tank, specialising in supply chain security and cybersecurity issues. He is also the Vice Chairman of the European Organisation for Security (EOS) Board of Directors and the Vice Chairman of the European Cyber Security Organisation (ECSO) Board of Directors and is a Member of the Trust in Digital Life Board of Directors as well. Mr. Miller is also the Chairman of the Security Industry Task Force on Artificial Intelligence as well as the Chairman of ECSO Working Group 1 (cybersecurity standards, certification and supply chain). He holds a degree in Electrical Engineering from the Massachusetts Institute of Technology (MIT) as well as an MBA from the International Institute for Management Development (IMD).

	**Nina Olesen (ECSO)** Nina Olesen is Head of Sector at the European Cyber Security Organisation (ECSO) which she helped establish in 2016 and which is today the unique European public-private organisation focusing on cybersecurity and offering a 360° view on the rapid evolution of the digital environment. In her current role, Nina is responsible for coordinating and supervising all activities related to WG3 on 'Cyber Resilience of Economy, Infrastructure, and Services' and WG5 on 'Education, Training, Cyber Ranges, and Human Aspects', including overseeing ECSO's Women4Cyber and Youth4Cyber initiatives.
	**Katarzyna Prusak – Górniak (ECCC)** Katarzyna Prusak – Górniak, legal adviser, graduate of the Jagiellonian University and the National School of Public Administration, cyberattaché at the Permanent Representation of the Republic of Poland to the EU in Brussels, responsible for negotiations of the draft NIS2 Directive, eIDASv2 Regulation and all matters related to cybersecurity, personal data protection, eID, e-government and cloud computing. Former Director of the Legal Department in the Ministry of Digital Affairs. Vice Chair of the Governing Board of the European Cybersecurity Competence Centre (ECCC)
	**Kai Rannenberg (CyberSec4Europe)** Professor Dr Kai Rannenberg has held the Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt since 2002 and has been a Visiting Professor at the National Institute for Informatics (Tokyo) since 2012. Until 2002, he was working with the System Security Group at Microsoft Research Cambridge on "Personal Security Devices & Privacy Technologies". From 1993-1999 Kai coordinated the interdisciplinary "Kolleg Security in Communication Technology", sponsored by Gottlieb Daimler & Karl Benz Foundation researching Multilateral Security. In parallel he did his PhD at Freiburg University on IT Security Evaluation Criteria and the protection of users and subscribers. Before Kai had completed an Informatics-Diploma (Master) at TU Berlin with a focus on privacy, security, and distributed and real-time systems. • Since 1991 Kai has been active in ISO/IEC standardisation in JTC 1/SC 27/WG 3 "Security evaluation criteria". • In 2007 he became Convenor of SC 27/WG 5 "Identity management and privacy technologies". • In 2015/16 Kai served as the Chair of the Strategic Advisory Group on Industry 4.0/Smart manufacturing of the ISO Technical Management Board. • Kai has been IFIP Honorary Treasurer since September 2021, before which he was an IFIP Vice President (from 2015) and an IFIP Councillor (from 2009). • Since 2014 he has been chair of the IFIP Publications Committee and editor-in-chief of the IFIP Advances in Information and Communication Technology.

	• From 2007 till 2013 Kai chaired IFIP TC-11 "Security and Privacy Protection in Information Processing Systems", after having been its vice-chair since 2001. • Kai is also active in the Council of European Professional Informatics Societies (CEPIS) chairing its Legal & Security Issues Special Interest Network (LSI) since 2003 and serving in its Board of Directors since 2019. • From 2004 till 2013 Kai served as the academic expert in the Management Board of the European Network and Information Security Agency, and from 2013 till 2022 in ENISA's Advisory Group. • Kai has coordinated several leading EU research projects, e.g. the Network of Excellence "Future of Identity in the Information Society" and the Integrated Project "Attribute based Credentials for Trust" (ABC4Trust) and is currently coordinating CyberSec4Europe. 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. Website with list of publications: www.m-chair.de/rannenberg
	**Dörte Rappe (BSI)** Dr. Dörte Rappe is a cybersecurity expert with a strong background in cryptography (PhD) and mathematics. She is head of the "Technology and Research Strategy" section at The Federal Office for Information Security (BSI), where the SPoC of the German NCC is located. For the last 18 years she has been working at the BSI, with 11 years of experience in the "Development of Cryptographic Systems" section and serving as a national expert for cryptography in NATO working groups. She was also involved in setting up and managing different new sections and positions within BSI. Furthermore her tasks included strategic consulting of the BSI management, coordination of national and European cybersecurity research and project leadership of cybersecurity projects. Currently, Dr. Rappe is the alternate German representative at the ECCC GB and supporting different working groups of the ECCC.

	**Luigi Rebuffi (ECSO)** 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 contributed to the creation and was the founder of ECSO, signing the cPPP on cybersecurity with the European Commission. For six years until 2016, he was 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.
	**Bernardo Santos (CONCORDIA)** Bernardo Santos is originally from Lisbon, Portugal. He holds a MSc degree in Telecommunications and Informatics, obtained from the Technical University of Lisbon, with a major in peer-to-peer and cloud applications. At the moment, he is engaged as a researcher in the Secure 5G4IoT Lab and he is a PhD candidate at the Oslo Metropolitan University (OsloMet), where he can apply his programming and software development knowledge in practice. His research areas are web/mobile development and security, location awareness and physical tracking, 5G networks, IoT, identity management, machine learning and anomaly detection, threat modelling, among others.
	**Alessandro Sforzin (CyberSec4Europe)** Alessandro Sforzin received his Master of Science in Computer Science from the University of Padua in December 2015. He is currently a scientist in the security group of NEC Laboratories Europe. His research areas include blockchain security and trusted execution environments.
	**Corinna Schmitt (NCC Germany)** Dr. Corinna Schmitt received her diploma in informatics from the Eberhard-Karls Universität Tübingen and continued her research at the Technische Universität München. In 2013 she received her PhD for the research on secure data transmission in wireless sensor networks. In 2013 she joined the Communication Systems Group (CSG) at the University of Zurich (UZH) as Head of Mobile and Trusted Communications. Since 2018 Dr. Schmitt has been Head of Secure IoT at the Universität der Bundeswehr München / Research Institute CODE conducting research on a wide range of topics such as the Internet of Things (IoT), mobile communications, and embedded/distributed systems. In 2021 she concluded her habilitation leading to ***venia legendi*** in informatics. Since October 2021 she has been the local contact point at the RI CODE for the National Cybersecurity Competence Centre Germany.

	**Antonio Skarmeta (CyberSec4Europe)** Antonio Skarmeta received a M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia. Since 2009 he has been Full Professor in the same University department. Antonio has worked on different national and international research projects in the networking, security and IoT areas, like ENABLE, DAIDALOS, SWIFT, SEMIRAMIS, SMARTIE, SOCIOTAL and IoT6 and is now involved in CyberSec4Europe and BIECO. He coordinates the H2020 project IoTCrawler focusing on IoT advanced discovery on IPv6 networks and coordinated OLYMPUS on privacy preserving identity management His main interest 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 on 1995. 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. From 2010 until 2014 he was Spanish National Representative for the MSCA within H2020. He has published over 200 international papers and is a member of several programme committees. He has also participated in several standardisation activities such as IETF, ISO and ETSI and has been nominated as an IPv6 Forum Fellow. Dr. Skarmeta is the owner of several patents on telemonitoring-based IoT solutions. He is also CTO of the spin-off company Odin Solution S.L. (OdinS) in the area of IoT and smart infrastructure.
	**Pascal Steichen (ECCC)** Pascal is founder and CEO of SECURITYMADEIN.LU, the Cybersecurity Agency for the Luxembourg Economy and Municipalities. For 20 years, Pascal has been involved in the main cybersecurity initiatives of the Luxembourg Government, *CYBERSECURITY Luxembourg*, the national platform to foster and empower the Luxembourg ecosystem in the field of cybersecurity, being his latest achievement. Laureate of the *Information Security Personality of the Year award* in 2017, Pascal Steichen has dedicated his professional career to cybersecurity. Pascal holds a master degree in *astrophysics* and, in parallel with starting his career as a software engineer, he graduated in *applied information technology*. In 2002 he joined the Luxembourg Government, as advisor and project manager in the area of network and information security for the Ministry of the Economy, where he participated in the creation of *LuxTrust (www.luxtrust.com)*, *CASES (www.cases.lu)* and *CIRCL (www.circl.lu)* as part of his activities. From 2003 to 2014, he represented Luxembourg as an alternate member of the management board of ENISA. In 2017, Pascal led and contributed to the creation of the *Cybersecurity Competence Centre (C3 – www.c3.lu)* a unique facility to strengthen the resilience of the Luxembourg economy by helping organisations to test and improve their cybersecurity competence.

	Building on his huge experience in cybersecurity, today Pascal is involved in key communities in Luxembourg and Europe, as a member of the *Luxembourg Cybersecurity Board*, a lecturer in information security at the *University of Luxembourg*, a board member of *CLUSIL* (the main association representing the cybersecurity landscape of Luxembourg), a member of *WomenCyberForce*; he has also been involved in the *curricular board* of the *BTS cybersecurity*. At an international level, Pascal was involved in the founding of *ECSO,* is an active member of the *FIC advisory board*, is part of the 2021 judging panel of the *IFSEC Global Influencers in Security and Fire Award*, and until very recently represented Luxembourg on the Governing Board of the *ECCC.*
	**Joanna Świątkowska (ECSO)** Dr. Joanna Świątkowska is the COO at the European Cyber Security Organisation (ECSO). From 2020 to 2022 she held the role of Director in the Supply Chain Cyber and Information Security team at UBS. She was the initiator and Programme Director of the European Cybersecurity Forum – CYBERSEC from 2014 to 2019. In addition, she worked as Assistant Professor at AGH University of Science and Technology from 2018 to 2020 and cooperated with the Kosciuszko Institute as the Senior Cybersecurity Expert from 2009 to 2019. The author of numerous articles, reports, and analyses concerning cybersecurity, Ms. Świątkowska is a recognised speaker in many national and international conferences and seminars and brings her contributions to a wide range of cybersecurity topics. She was listed among the 100 Eastern Europe's emerging technology stars by the Financial Times & New Europe 100 for 2017, as well as inserted among the Top 20 Women in Cybersecurity by the Women in Tech summit for 2019.
	**José María Torres (ECHO)** José María Torres is a software engineer and project manager with more than 15 years' experience in the aerospace domain, mostly in the industry but also at ESA/ESTEC. Since 2013, José María has been a project manager at Telespazio Belgium, formerly Vitrociset Belgium, and since 2018, he has been the project manager of different security-focused projects in the space domain. These projects include sMMGS, a study for the definition of a secure multi-mission ground station or CyTEF, a cybersecurity test facility for drones. Since mid-2021, José María has been the project manager for the Telespazio Belgium activities in the ECHO project.
	**Theodora Tsikrika (ECHO)** Theodora Tsikrika, PhD is a research fellow at the Information Technologies Institute of the Centre for Research and Technology Hellas (CERTH-ITI). She received the Degree in Computer Science from the University of Crete, and the MSc and PhD degrees in Computer Science from Queen Mary, University of London. Prior to joining CERTH-ITI in 2013, she worked as a postdoctoral researcher at Centrum Wiskunde & Informatica (CWI) (The Netherlands), the University of Applied Sciences Western Switzerland, and the Royal School of Library and Information Science (Denmark). Her research interests are in the areas of data mining with particular focus on AI technologies for security/cybersecurity applications. She has participated in several

	H2020 projects in the areas of security/ cybersecurity (e.g., ECHO, FORESIGHT, CONNEXIONs, CREST) and has co-authored more than 60 publications in refereed journals and international conferences.
	**Martin Übelhör (DG CONNECT)** Martin Übelhör works in the European Commission, Directorate-General for Communications, Networks, Content and Technology (DG CONNECT). He currently is a Head of Sector for Cybersecurity Industry and Innovation, where he works on setting up a European Cybersecurity Competence Centre and Network and manages funding programmes for cybersecurity research, innovation, and deployment. Prior to that, he worked as policy assistant to the Director for Digital Society, Trust and Security, dealing with topics such as cybersecurity and digital privacy, smart mobility and smart energy, as well as eGovernment and eHealth. Martin studied political science and sociology in Mannheim, Baltimore and Bruges. After first experiences in international affairs (United Nations HQ) and research (Fraunhofer Institute for Systems and Innovations Research), he joined the European Commission in 2008.
	**Frank Wamser (Representation of the State of Hessen to the EU)** Frank Wamser studied law in Germany, where he received a doctorate, and in the US, where he graduated as Masters of Law (LL.M.). He worked as an attorney-at-law in an international US law firm and was appointed a judge in several district courts, in a regional court and in the Higher Court of Appeals. After having served as a clerk for the Supreme Court of Germany he worked in the Ministry of Justice, was Vice-President of the Law-Exam Authorities and Vice-President of a regional court. He is currently head of the Justice unit at the Representation of the State of Hessen to the European Union.
	**Arthur van der Wees (CONCORDIA)** Arthur van der Wees is founder and managing director of Arthur's Legal & Strategies, an international strategic law firm with a global reach. Arthur is attorney at law, standardisation and policy expert, entrepreneur, strategist and frequent speaker worldwide. He has in-depth experience and is well-connected in the world of digital ecosystems, data, digital identity, cyber-physical and autonomous systems, accountability, resilience and global sustainable prosperity. He is (co-)author of various publications about innovation, digital transformation, data, IoT, computing, security and privacy and trust, and he has contributed to several EU regulations and other policy instruments for the Digital Age. Furthermore he is an advisory board member and partner respectively in more than 15 European projects. Arthur's Legal, Strategies & Systems is a member of the EU Alliance for Industrial Data, Cloud & Edge, and is leading both the taskforce on sovereignty, as well as the taskforce on cybersecurity. And, of course, it is a consortium partner of CONCORDIA (strategies, roadmap, data, policy, legal, chair ethics committee and data protection officer).

	**Thanh van Do** Prof. Dr. Thanh van Do obtained his MSc in Electronic and Computer Sciences from the Norwegian University of Science and Technology and his PhD in Informatics from the University of Oslo. In 1991 he joined Ericsson R&D Department in Oslo after 7 years of R&D at Norsk Data, a minicomputer manufacturer in Oslo. In 2000 he joined Telenor R&D and has been working in a variety of fields such as distributed computing, mobile service personalisation, mobile commerce, privacy and security. He is now at Telenor Research in charge of cybersecurity, identity management and SIM research activities. He has been project leader of multiple EU research projects and a member of multiple conference technical committees. He is also professor in the Department of Computer Science at the Oslo Metropolitan University. He is the author of over 250 publications at international conferences and journals. He is also theinventor of 22 patents.


1–3 June 2022
Brussels
CONVERGENCE NEXT
Cyber Competence Network

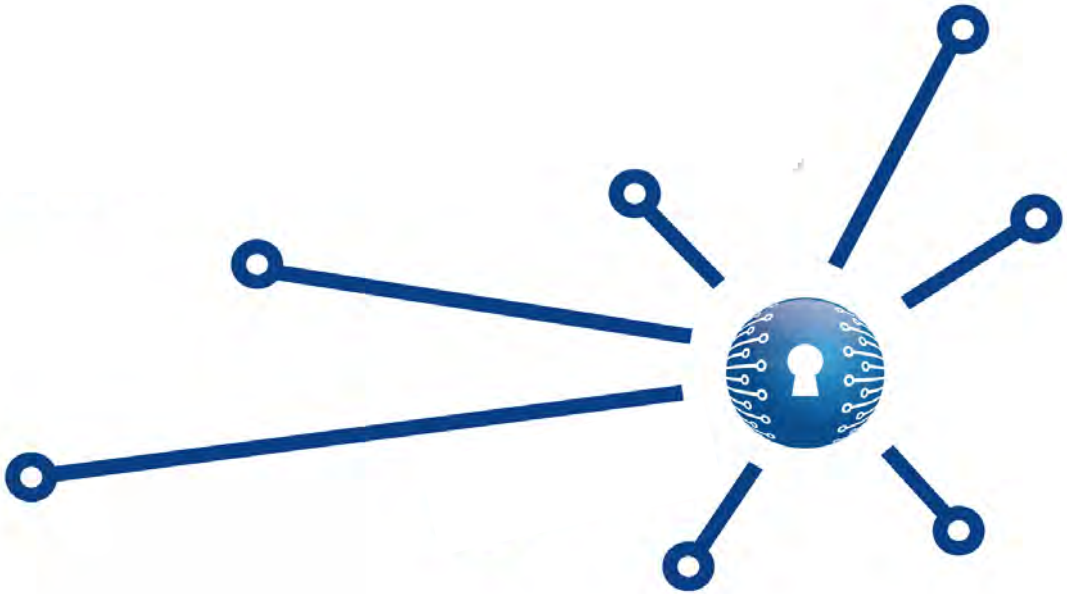
CONCORDIA
The leaders for boosting Europe's cybersecurity future

Gabi Dreo

Coordinator of CONCORDIA

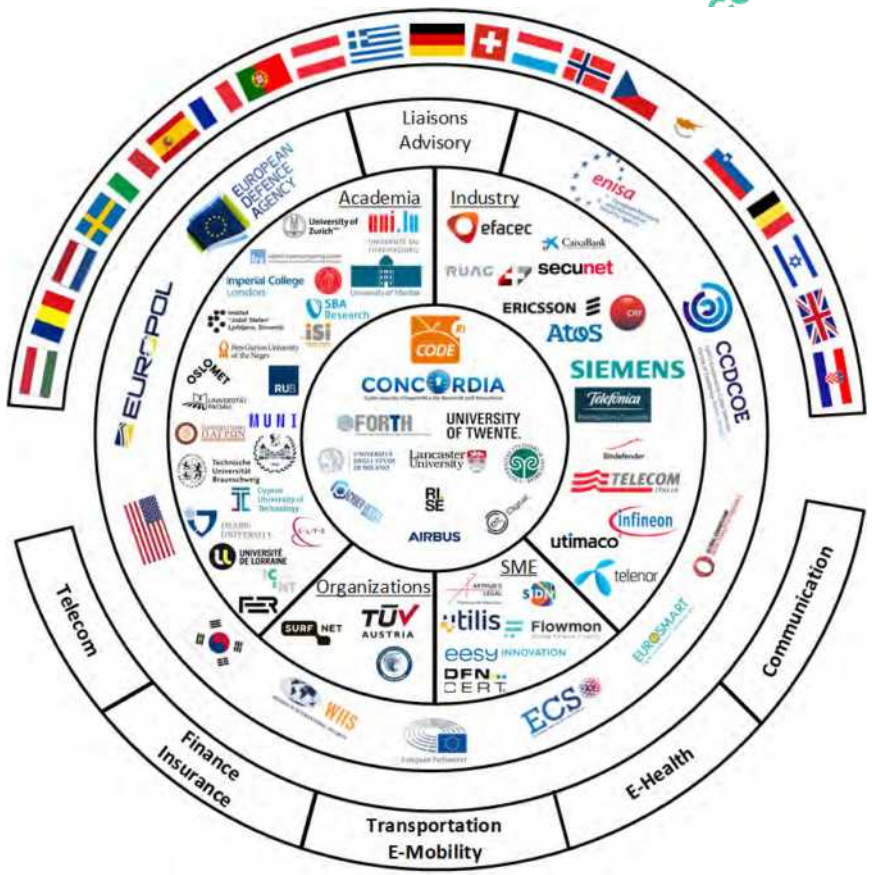
CONCORDIA's VISION

Building the European Secure, Resilient and Trusted Cybersecurity Ecosystem



CONCORDIA Consortium

- Current consortium with 56 official partners:
  - 30 research organisations or academia
  - 24 industry partners (including 7 SMEs)
  - 2 public bodies and other types of organisations
- Representing **17 EU member states** and **3 Horizon 2020 associated** countries and **UK**



CONCORDIA Service Board: Shaping the Community

CONCORDIA's Highlights

CONCORDIA Platforms for Cyber Threat Intelligence for the Telco and Finance Sector
(New Services, Legal Framework „Code of Engagement", CONCORDIA Mobile Threat Modelling Framework, Security Metrics)

DDoS Clearing House
(nominated for the EC Innovation Radar, DDoS fingerprints testbed in Netherlands and Italy operationalized, ..)

Cyber Range Ecosystem
(**Kypo Cyber Range**
(won the EC Innovation Radar, Disruptive Technology, Cyber Range Open Format Exchange ...)

Stakeholder Groups
(CONCORDIA Open Door**)**

240+ research papers

Holistic CONCORDIA's Cybersecurity Roadmap for Europe

Dissemination
Over 90 blog post, 56 000+ engagements on social media, Over 1600+ followers on Twitter and 2400+ on LinkedIn ...

European Education Ecosystem for Cybersecurity
(Methodology for building Courses for Professionals, Course for Cybersecurity Consultants, C3 by CONCORDIA Certification scheme, Skills Certification Framework, Map with courses & trainings for professionals, Teach-the-Teachers methodology)

Framework for Risk Analysis, optimal investments, and critical steps
CONCORDIA Insurance Model

Women for Cybersecurity
(Manifesto, Role models database, Workshops, Awards, Equity Policy)

Ecosystem of Startups
30+ Exploitable Results

Highlights (2): CONCORDIA and CCN cross-collaboration, also external

- Focus Group on **Education** – CONCORDIA lead
- Focus group on **Threat Intelligence in the Finance Sector** – CONCORDIA lead
- Focus group on **Communication**
- Focus group on **Cyber Ranges**
- Focus group on **Roadmapping**
- Additional **Cross-pilot activities** (e-Health, Innovation and Exploitation, Certification) and other EU projects

ECHO

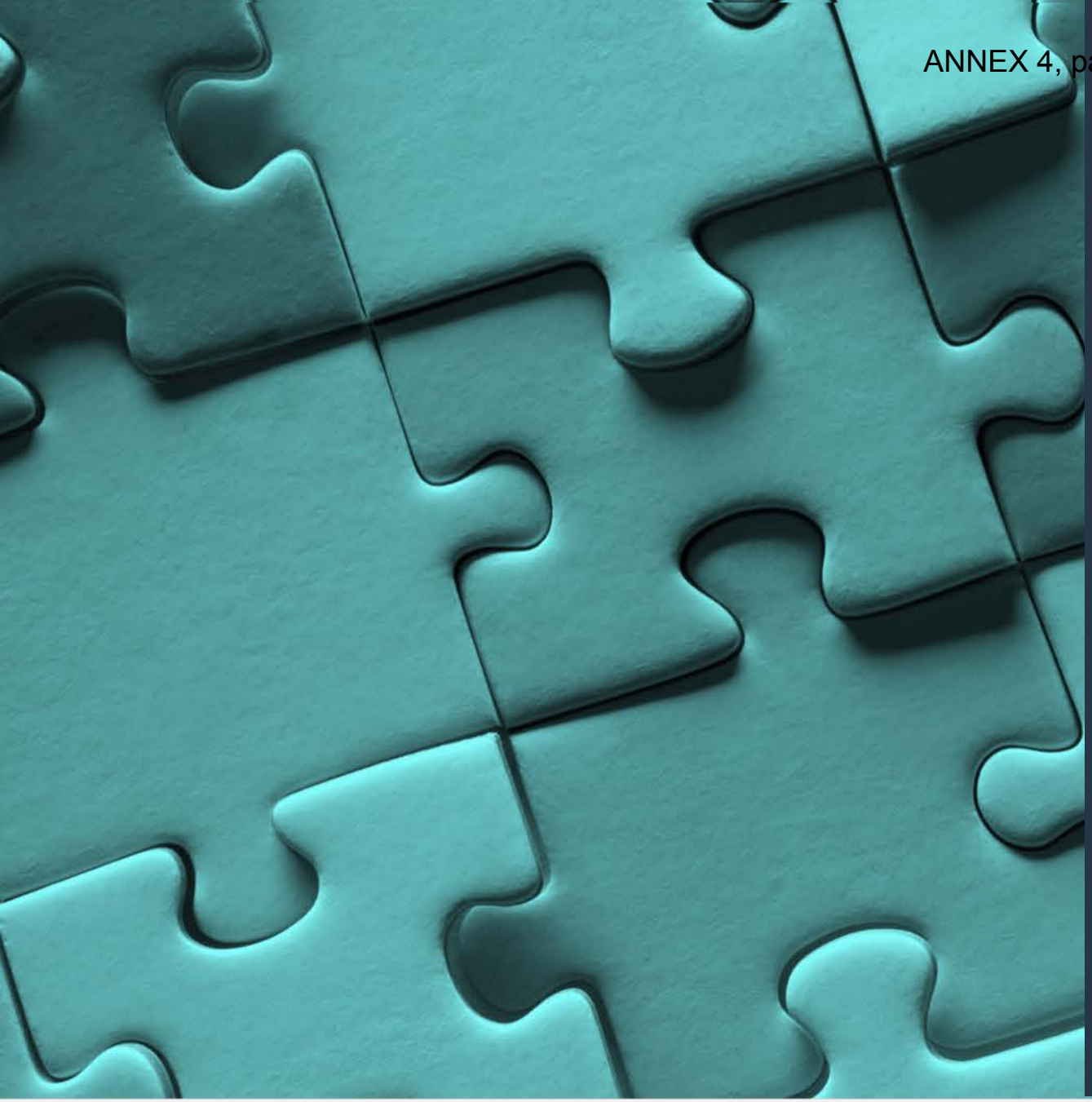
EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

ECHO Overview

Wim Mees

Royal Military Academy (BE)
ECHO Project Coordinator

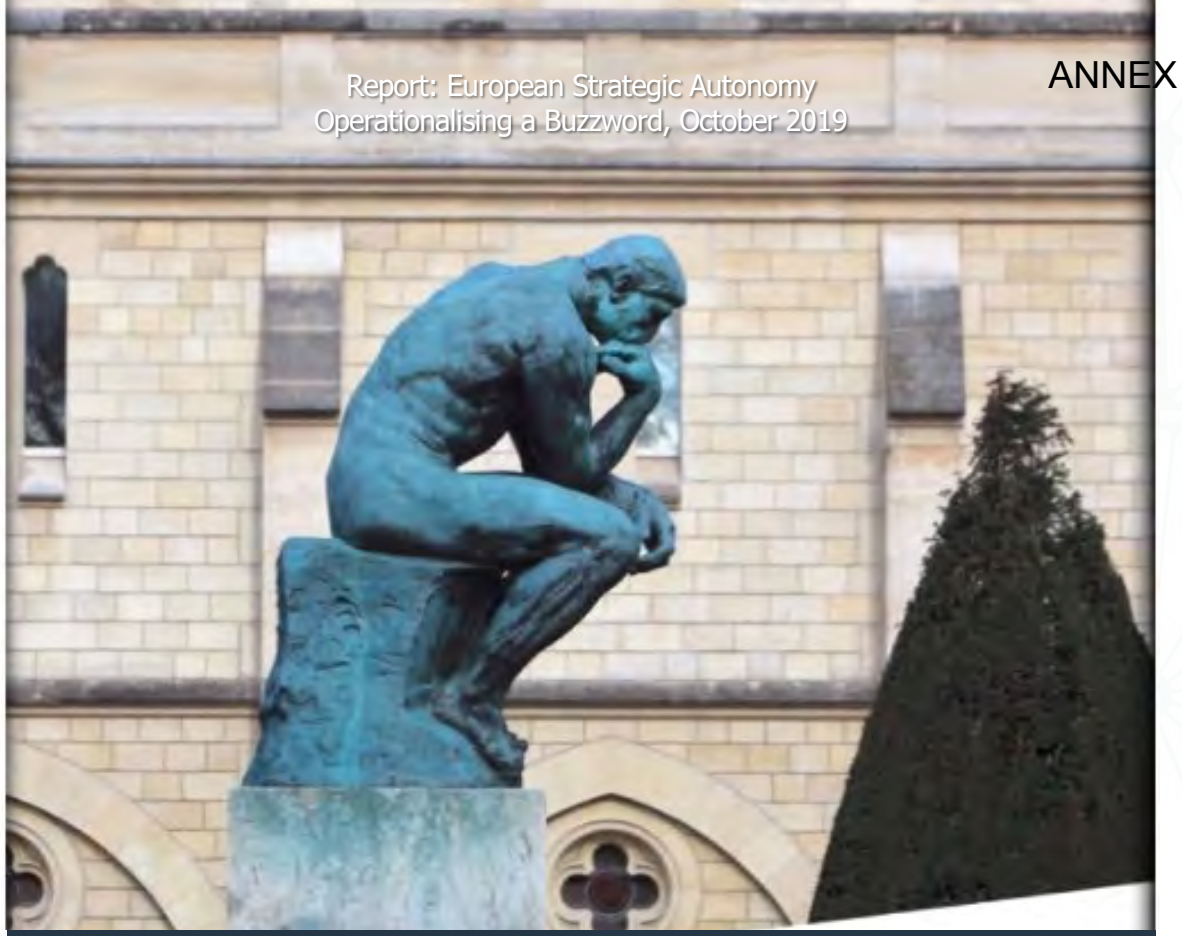
The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943



The EU Cybersecurity Challenge:

FROM ***"FRAGMENTED IN DIVERSITY"***
TO ***"UNITED IN DIVERSITY"***

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreeme[illegible]043



KOM Feb19

European strategic autonomy

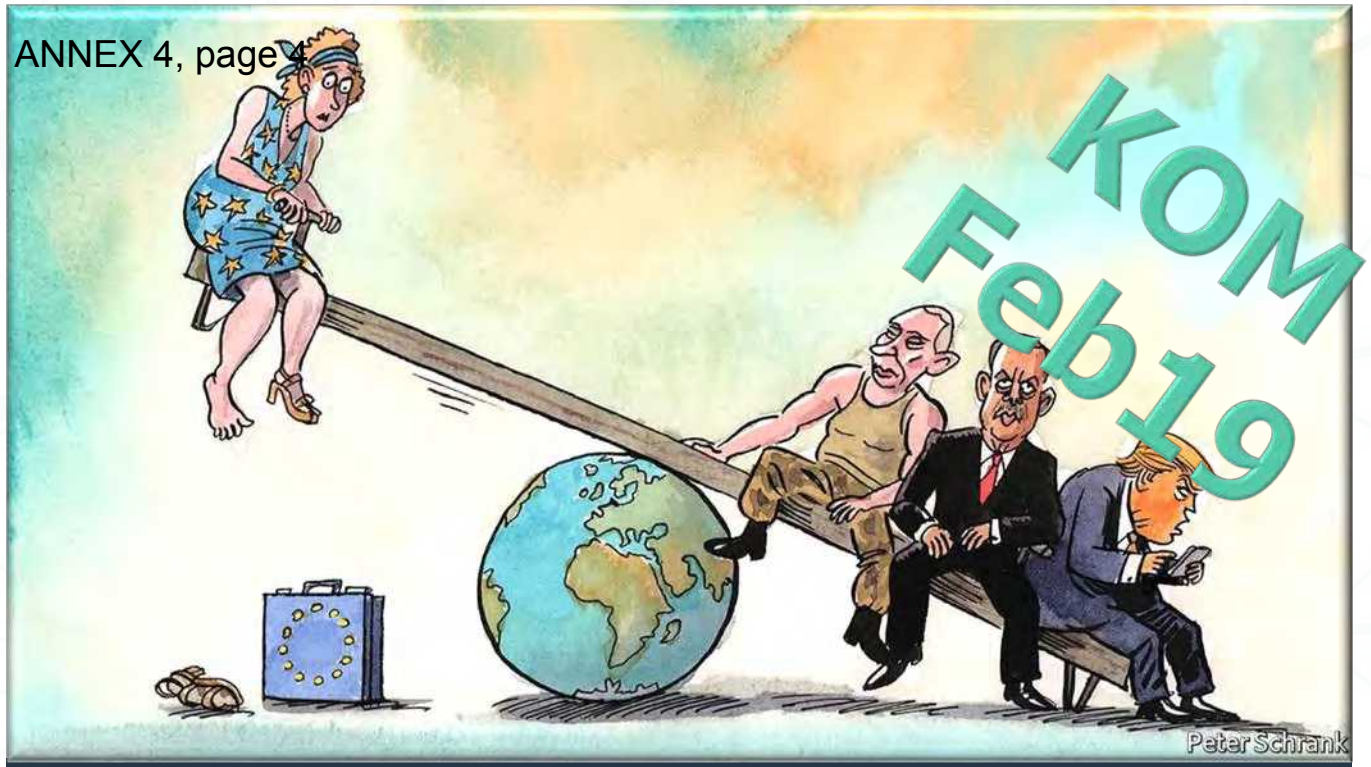
The capacity to act in four dimensions:

- Political
- Institutional
- Capabilities
- Industrial

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

STRATEGIC AUTONOMY MUST BE:

- **Sustainable**
  - **Governance model**
  - Bottom-up input to decision makers
- **Technology driven**
  - From recognized European scientific excellence to a trusted supply chain of **industrialized solutions**
- **Capability driven**
  - Autonomy to **assess a situation, make decisions** and **freedom of action to execute them**



Our strategic autonomy focus for cybersecurity

Two years ago already…

ECHO kick-off meeting in Brussels at RMA

KOM Feb 19

ECHO

KOM Feb19

Consortium Partners Presentation

National Aerospace University "Kharkiv Aviation Institute" (KhAI)

Prof. Vyacheslav Kharchenko,

Dr. Oleg Illiashenko

Department of Computer Systems, Networks and Cybersecurity

Project kick-off Meeting

Brussels, 25-26 February 2019

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

Kharkiv, Ukraine

KOM Feb19

- Kharkiv region is one of the biggest industrial, agricultural, scientific and cultural regions of Ukraine (about 3 million people)
- Kharkiv is the city of science and education Territory – 300 sq. km, population – more 1.5 millior (capital of Ukraine, 1925-1934)

Kharkiv, Ukraine

Situation today… **please support our partners and friends in Ukraine !**

Ukraine : En images, le choc après la destruction d'un immeuble d'habitation à Kharkiv

Rédaction Paris Match Belgique | Publié le 24 février 2022 | Mis à jour le 1 mars 2022

Une femme le visage en sang à Kharkiv, en Ukraine, après la destruction d'un immeuble d'habitation. WOLFGANG SCHWAN/AFP | © AFP

The City Hall building in Kharkiv: a devastating missile strike on the main square of Ukraine's second-largest city turned the regional government building into a massive fireball © Pavel Dorogov/AP

Firefighters work to extinguish a fire at the Kharkiv National University building, which city officials said was damaged by recent shelling, in Kharkiv, Ukraine March 2, 2022. REUTERS/Oleksandr Lapshyn

LVIV, Ukraine, March 3 (Reuters) - Russian shelling and attacks on civilian populations killed 34 civilians in Ukraine's eastern Kharkiv region in the past 24 hours between March 2-3, the emergency services said on Thursday.

Separately, the governor of the Ukraine-controlled eastern Donetsk region said the port city of Mariupol, one of the first targets of the Russian invasion, was without electricity or water supplies.


ECHO
EUROPEAN NETWORK OF CYBERSECURITY
CENTRES AND COMPETENCE HUB FOR
INNOVATION AND OPERATIONS

Partners

Project Coordination:
Royal Military Academy of Belgium (Wim Mees)

Project Management:
RHEA System S.A. (Matteo Merialdo)

- 16 Millions budget
- 4 years (started Feb 2019)
- 30+13 partners
- 2 new partner engagements
- 13 existing competence centres
- 19 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Main concepts:

ECHO Governance Model: Management of direction and engagement of partners (current and future)

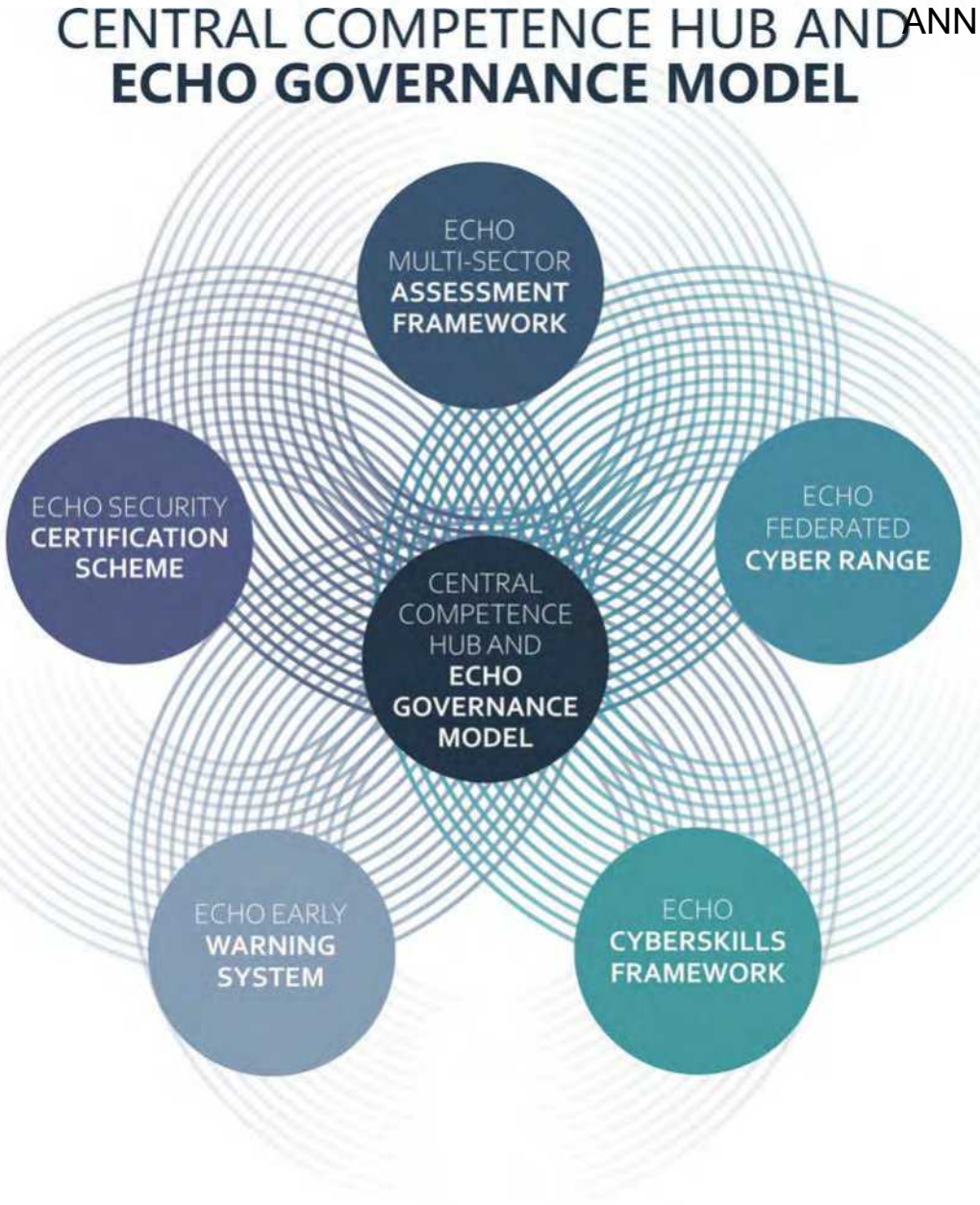
ECHO Multi-Sector Assessment Framework: Transverse and inter-sector needs assessment and **technology R&D roadmaps**

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

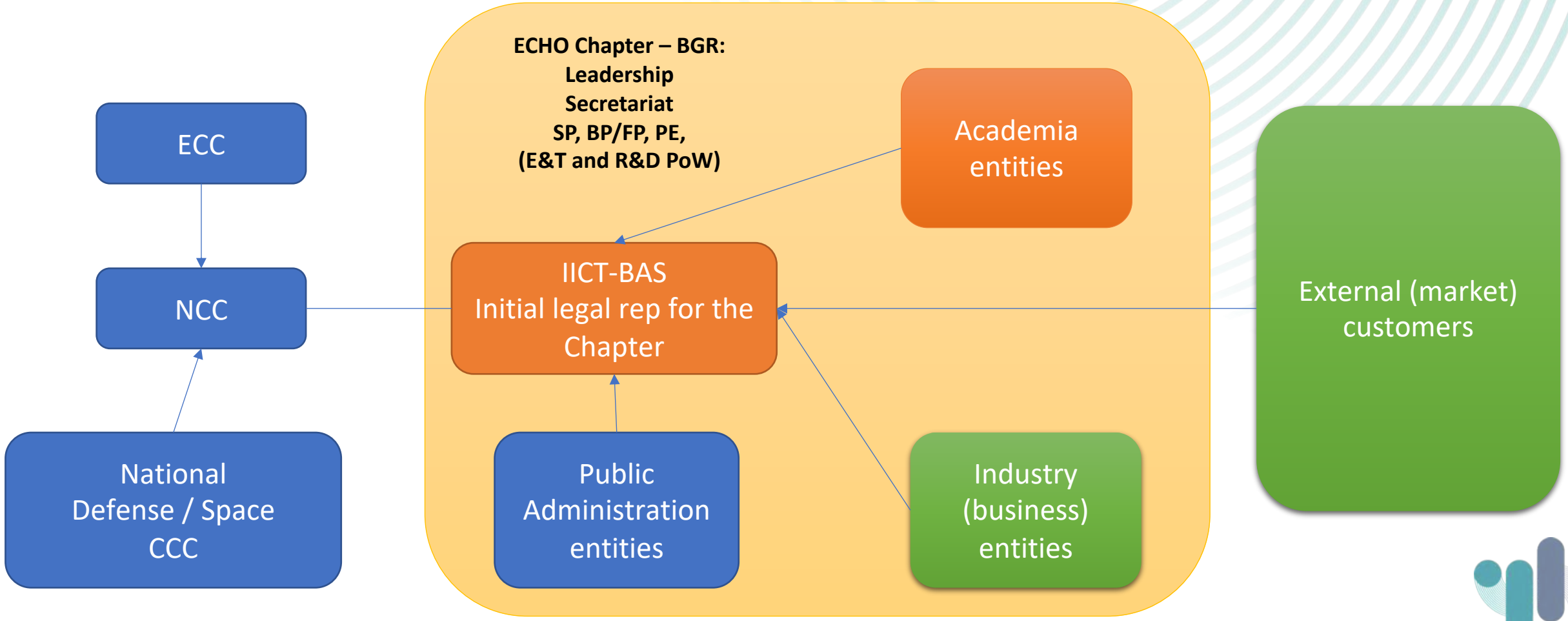
ECHO Early Warning System: Secured collaborative information sharing of cyber-relevant information



ECHO Governance Model

- Identify potentially applicable existing models
- Identify and prioritize governance needs
- Define the a possible governance model for the future **Network of Centres of Competences**
- Grow the network

Pilot in Bulgaria – envisaged structure and role of ECHO National Hub

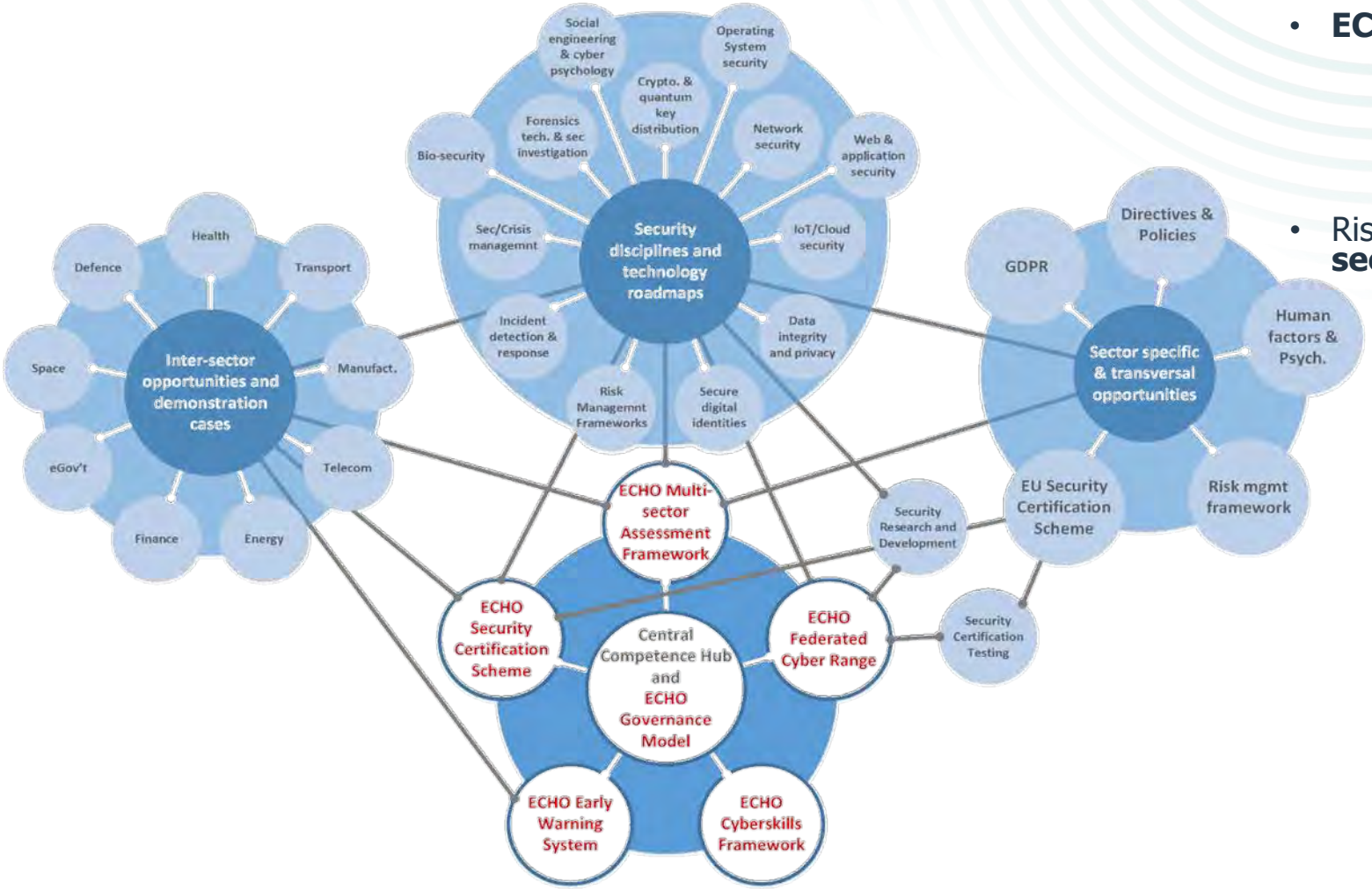


Critical Sectors

European Commission-JRC taxonomy

Audiovisual and media	Defence	Digital infrastructure	Energy	Financial
Government and public authorities	Health	Maritime	Nuclear	Public safety
Tourism	Transportation	Smart ecosystems	Space	Supply chain

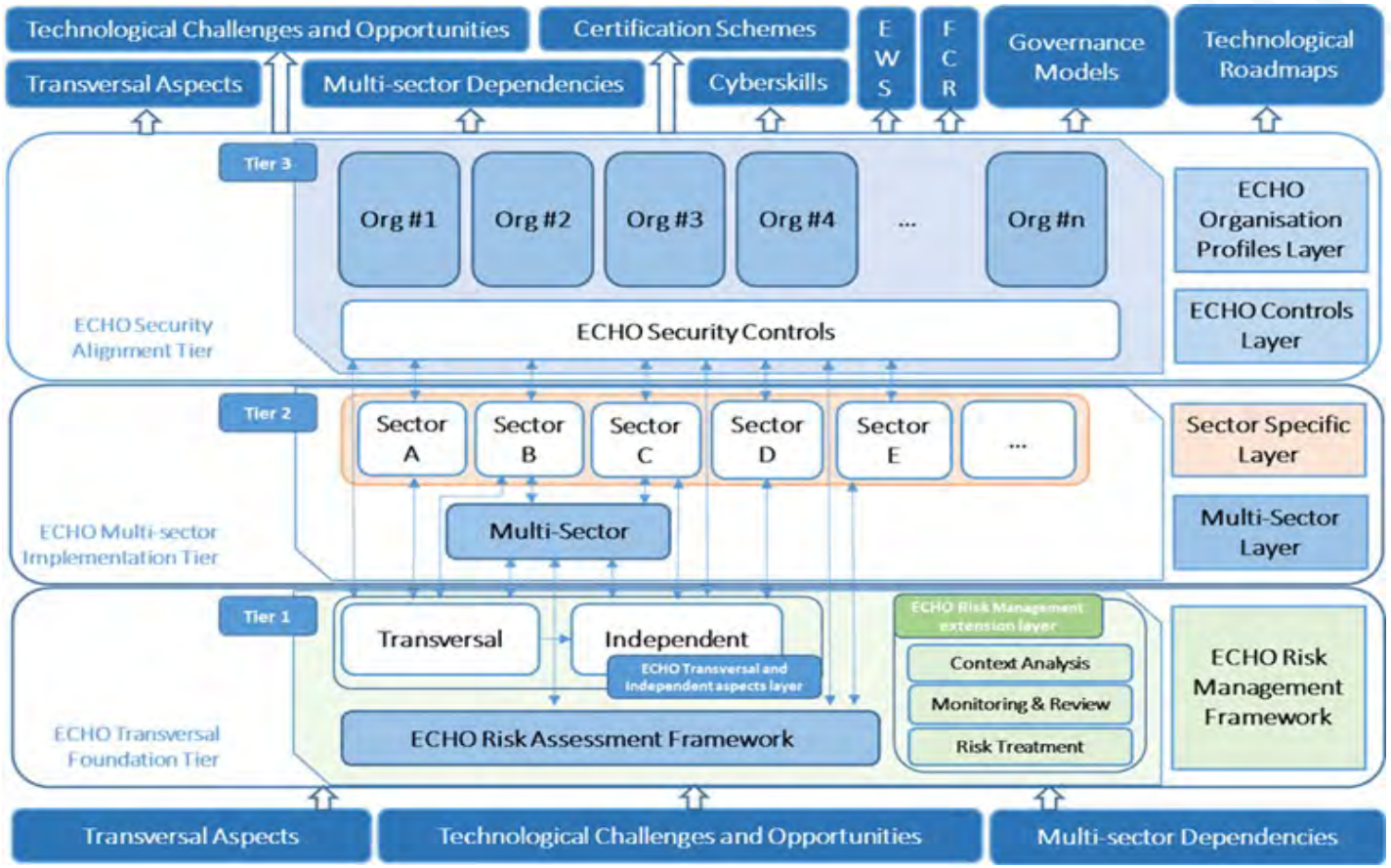
Defining technology roadmaps and assess Multisector risks



- **ECHO Multi-sector assessment framework**
  - Mechanism to define and refine **technology roadmaps** and **demonstration cases**
  - **Evaluate the risk of multi-sector scenarios**, including supply chain
- 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**

Defining technology roadmaps and assess Multisector risks

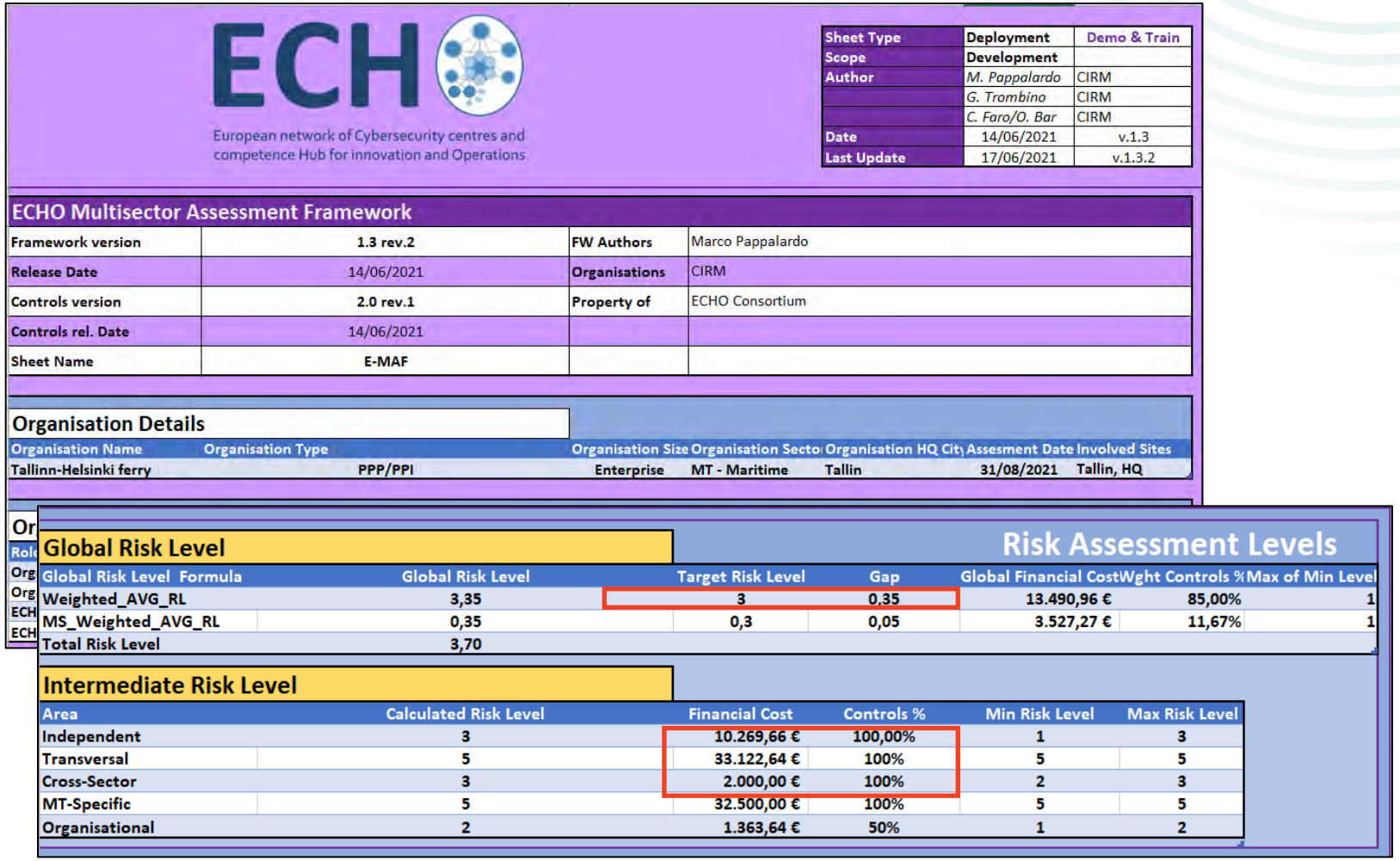
Where are we currently?



- We are ready with an **advanced prototype (1.4.x)**
- It is piloted as an Excel spreadsheet, but development of a software tool is ongoing
- Enhanced Risk Calculation
- Many single/multi sector scenarios have been developed
- Several Assessment/Examples running in ECHO domains and transport sector.
- It is being used to derive/justify **directions for** the **Skills Framework**, the **Certification Framework** and the **Technology Roadmaps**

Defining technology roadmaps and assess Multisector risks

Current improvements



ECHO

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

Sheet Type	Deployment	Demo & Train
Scope	Development	
Author	M. Pappalardo	CIRM
	G. Trombino	CIRM
	C. Faro/O. Bar	CIRM
Date	14/06/2021	v.1.3
Last Update	17/06/2021	v.1.3.2

ECHO Multisector Assessment Framework

Framework version	1.3 rev.2	FW Authors	Marco Pappalardo
Release Date	14/06/2021	Organisations	CIRM
Controls version	2.0 rev.1	Property of	ECHO Consortium
Controls rel. Date	14/06/2021		
Sheet Name	E-MAF		

Organisation Details

Organisation Name	Organisation Type	Organisation Size	Organisation Sector	Organisation HQ City	Assesment Date	Involved Sites
Tallinn-Helsinki ferry	PPP/PPI	Enterprise	MT - Maritime	Tallin	31/08/2021	Tallin, HQ

Global Risk Level — Risk Assessment Levels

Global Risk Level Formula	Global Risk Level	Target Risk Level	Gap	Global Financial Cost	Wght Controls %	Max of Min Level
Weighted_AVG_RL	3,35	3	0,35	13.490,96 €	85,00%	1
MS_Weighted_AVG_RL	0,35	0,3	0,05	3.527,27 €	11,67%	1
Total Risk Level	3,70					

Intermediate Risk Level

Area	Calculated Risk Level	Financial Cost	Controls %	Min Risk Level	Max Risk Level
Independent	3	10.269,66 €	100,00%	1	3
Transversal	5	33.122,64 €	100%	5	5
Cross-Sector	3	2.000,00 €	100%	2	3
MT-Specific	5	32.500,00 €	100%	5	5
Organisational	2	1.363,64 €	50%	1	2

- Strong Dissemination
- Risk Scoring and Prioritization
- Financial Strategies
- Automated Risk Calculation
- Improvement and Specialization of Security Control Sets
- Training Material development
- Integration of **ECHO Cybersecurity Skills Framework** in E-MAF

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Cyberskills and Training Curricula

1. Mechanism to improve the **capacity** of professionals across Europe for more effective response to cyber threats

2. Leverages a **common cyberskills reference**

3. Design modular **learning-outcome based curricula**

4. ECHO provides opportunities for **demonstration** of the gained skills **with realistic simulations** and Lessons learned feed **knowledge sharing**

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Cybersecurity Certification Scheme

1

Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)

2

Support **delivery and acceptance of technologies** resulting from technology roadmaps

- **Improved security assurance** through use of **certified products**

3

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)

4

Provides **product-oriented** cybersecurity certification schemes

- Support sector specific and inter-sector security requirements
- Leveraging on cyber ranges as testing facilities

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Technology Roadmaps

1

One of the main objectives of the ECHO project is the development of cybersecurity roadmaps as a result of **analysis** related to **current** and **emerging cybersecurity challenges**.

2

Delivery of at least 6 cybersecurity technology roadmaps including:

- **ECHO Early Warning System** (E-EWS) Roadmap
- **ECHO Federated Cyber Range** (E-FCR) Roadmap
- At least **2 additional technology innovations (E-Tools)** to be completed as part of ECHO
- At **least 2 additional technology innovations (challenges/priorities)** to be addressed by the future Cybersecurity Competence Network

3

Highlight **strategic technology-related priorities** with the goal to create the foundations for new **industrial capabilities** and assist towards the development of **innovative technologies** thus paving the way towards **EU's digital sovereignty**.

4

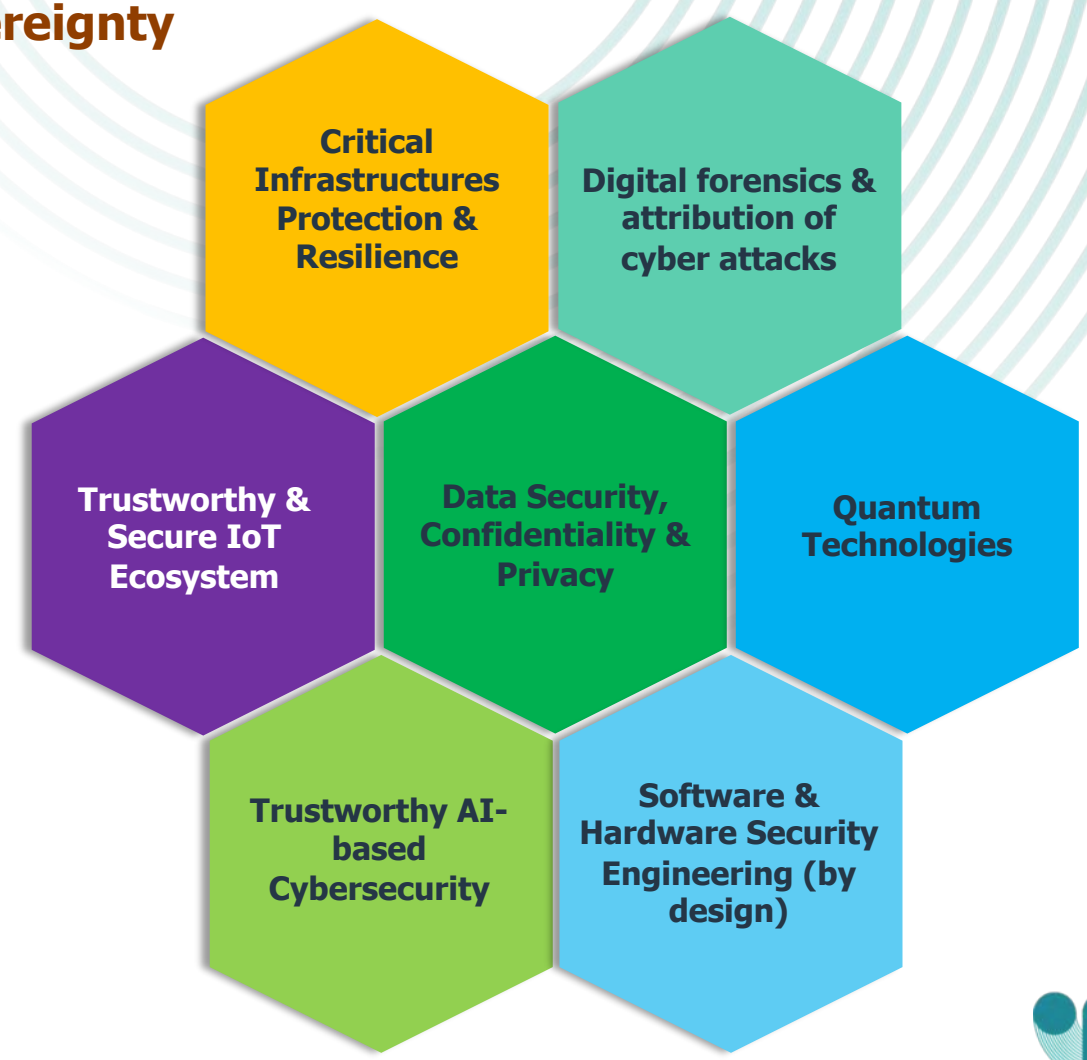
Consider the **transversal** aspects of **Education/Training** and **Certification**, while underpinned by effective **Governance** models for networked organisations that collaboratively strive to achieve these goals.

ECHO Technology Roadmaps

Current and emerging challenges: Towards EU sovereignty

Challenges identification & Priorities consolidation:

- Examined more than **140 reports** (Industrial, Academic, EU agencies etc)
- Identified **83 technical cybersecurity challenges**
- Challenges informed the **design** and **development** of **13 prototype tools & 2 technology innovation roadmaps**
- Building the foundations for future work by highlighting **priority focus areas** for **research**, **development**, **innovation,** and **prototyping**
- Closely collaborating with the other 3 pilots in order to provide a **consolidated view** of our roadmaps

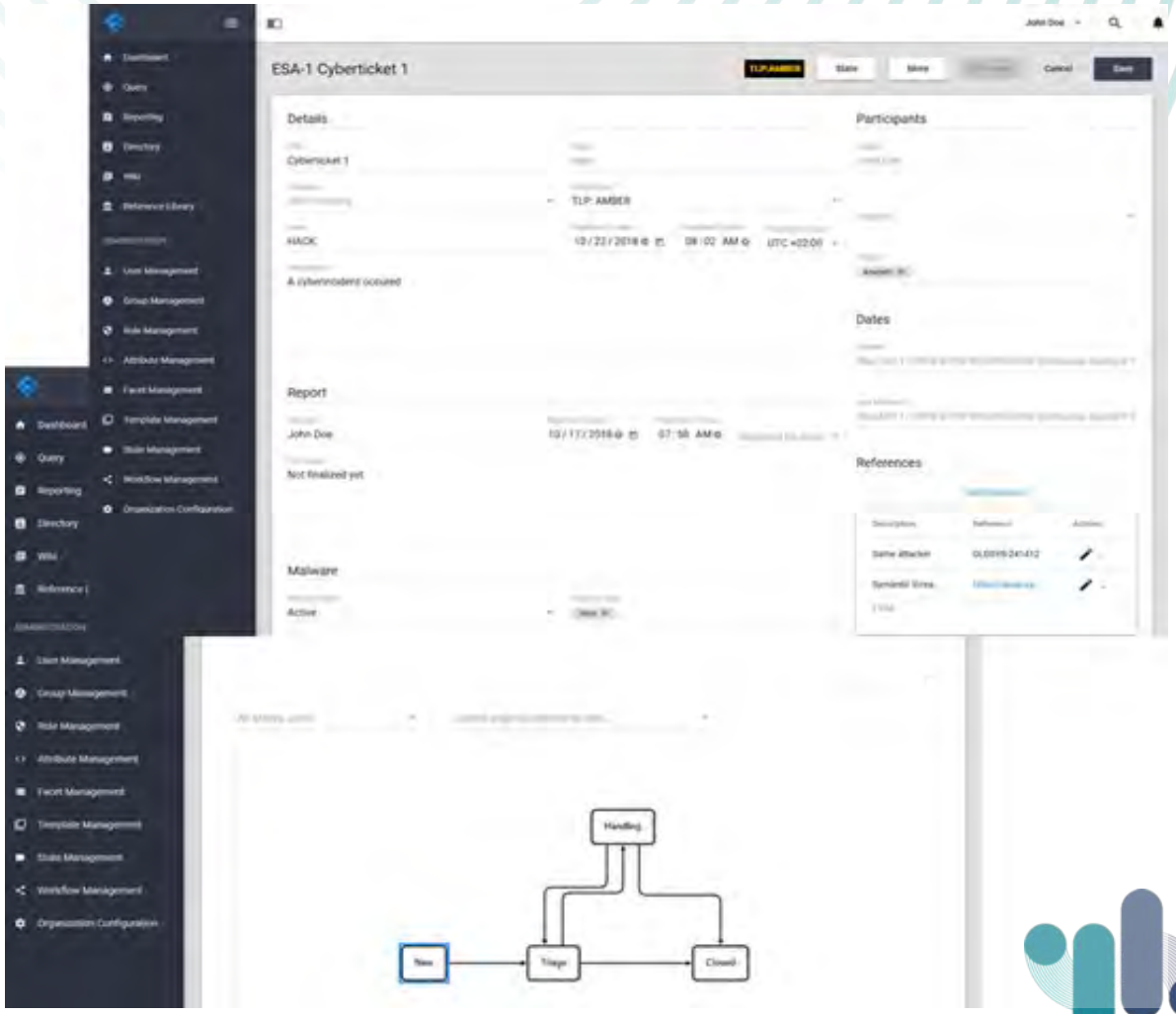


ECHO Technology Roadmaps

ECHO Early Warning System (E-EWS)

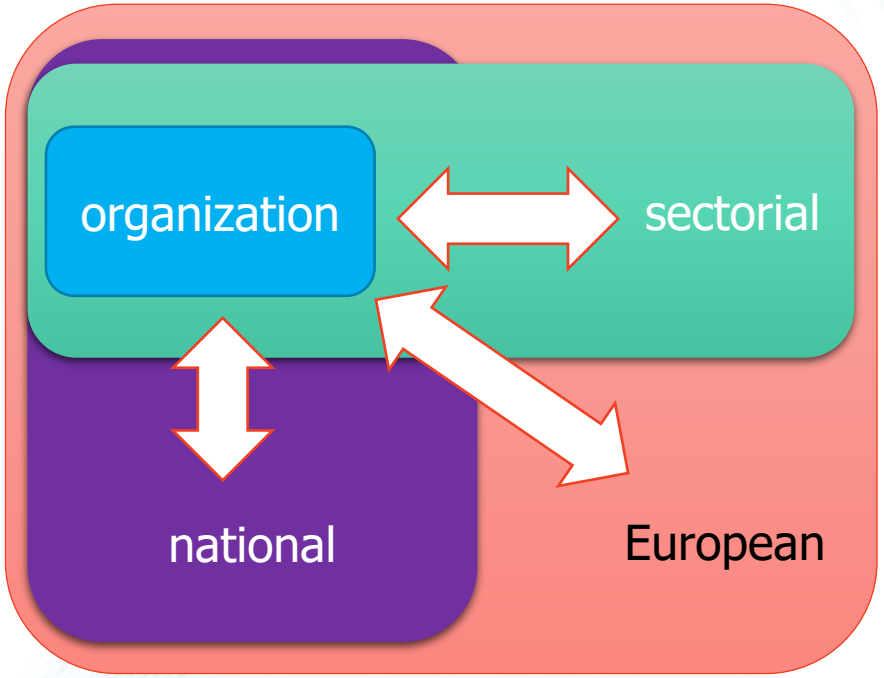
- **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
  - Tickets
  - Warnings
  - Knowledge base/Cyber Threat Intelligence
- Secure information sharing **between organizations**; across organizational boundaries and national 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)
- Multisource **threat intelligence data** gathering
- Includes sharing of **reference library** information and **incident management** coordination

- **Potentially, it could serve all the network of centers of competences!**

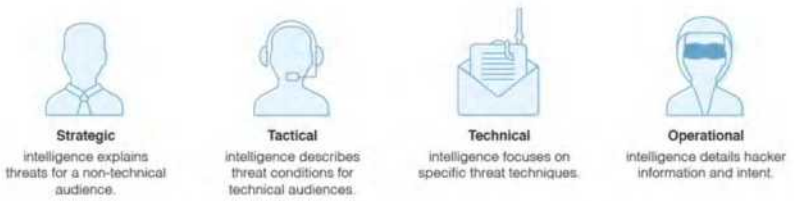


Sharing Threat Information

ECHO Early Warning System (E-EWS)



Four Types of Cyber Threat Intelligence

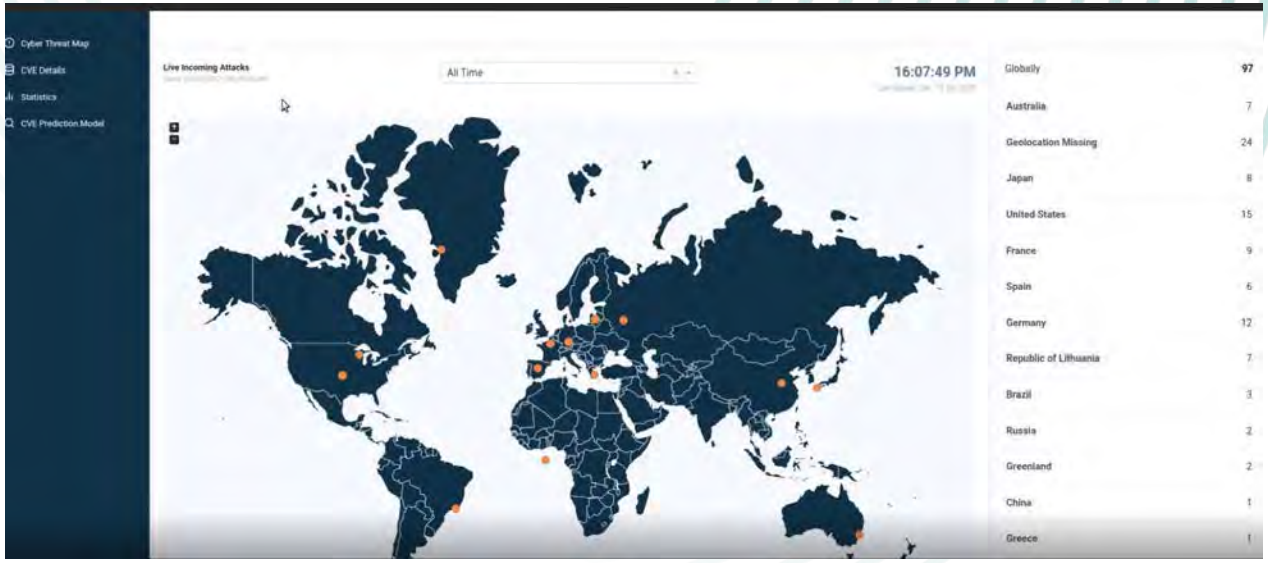


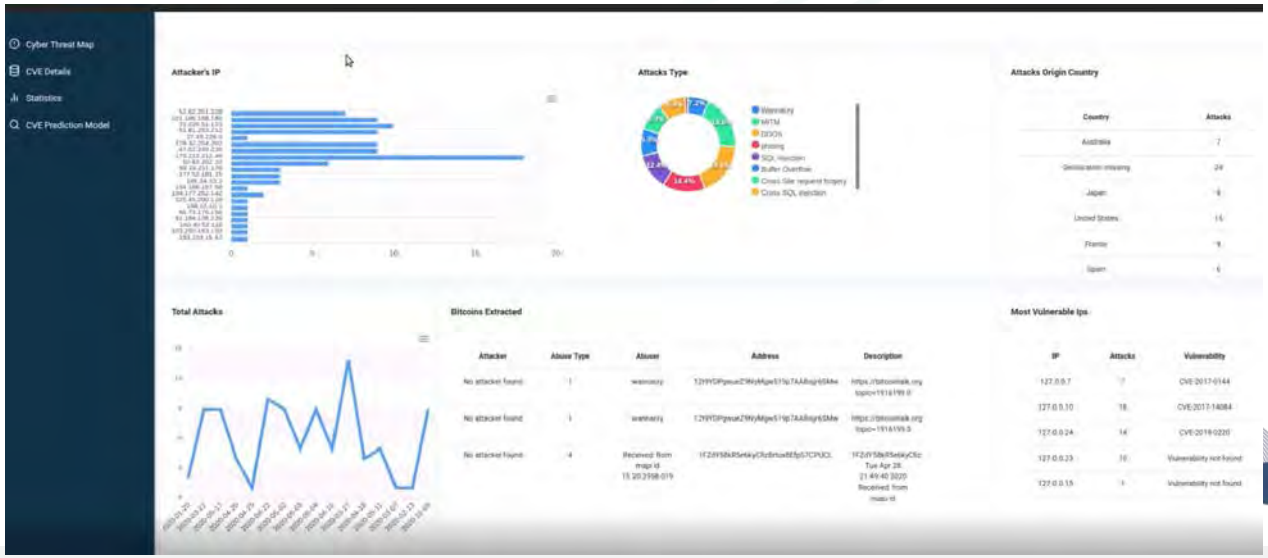
Strategic
intelligence explains threats for a non-technical audience.

Tactical
intelligence describes threat conditions for technical audiences.

Technical
intelligence focuses on specific threat techniques.

Operational
intelligence details hacker information and intent.

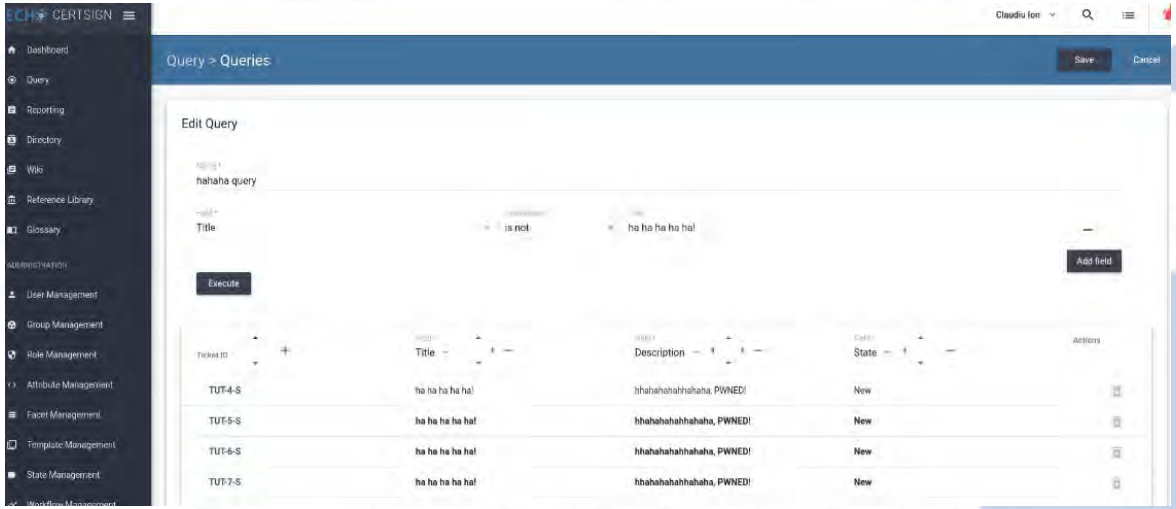


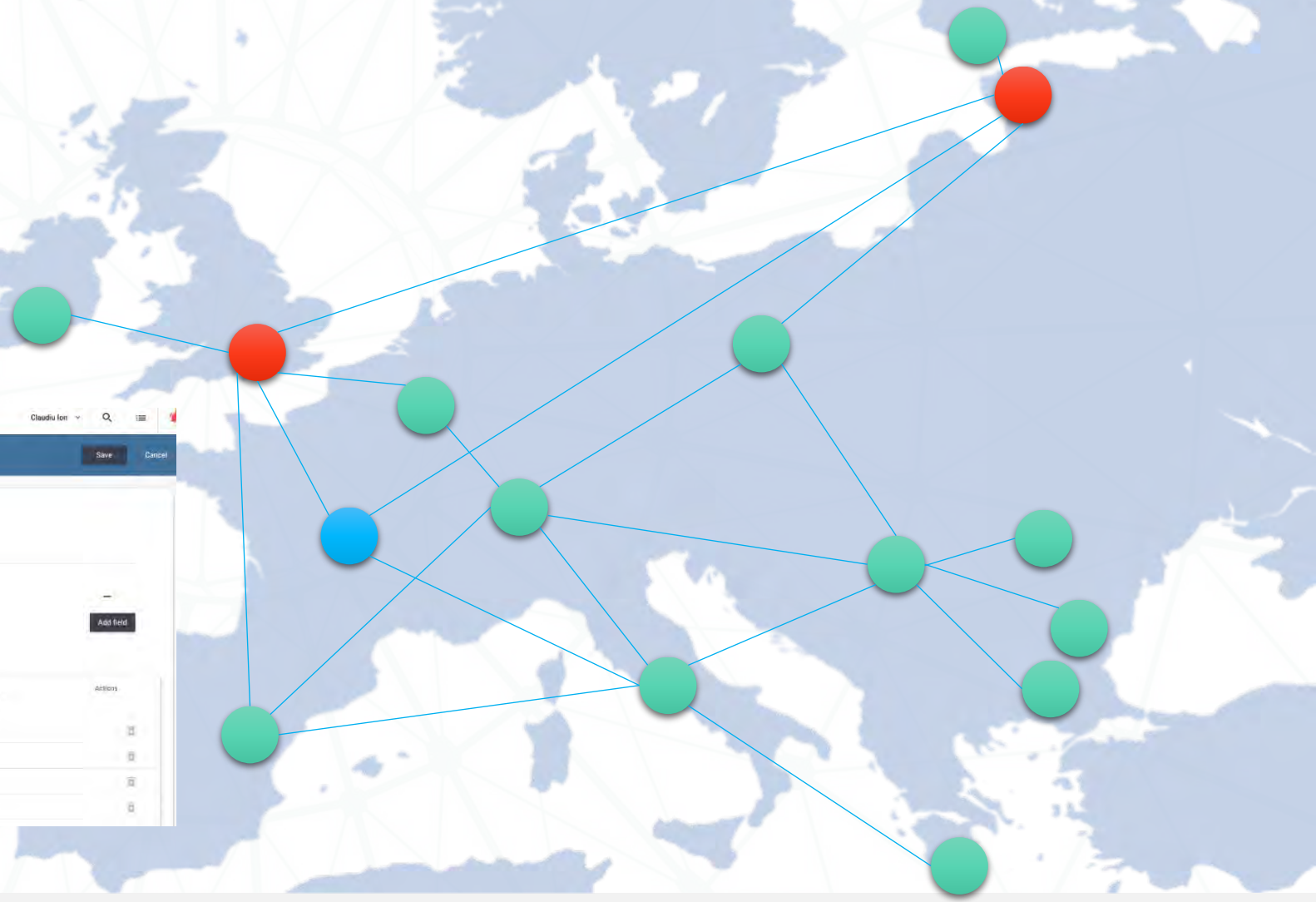


ECHO Early Warning System (E-EWS)

Where are we currently?

- Development is **complete**
- **18** ECHO organizations are already connected via E-EWS
- **6** Tabletop exercises already performed, with up to **120** participants
- The team started working to the **ECHO Demonstration cases**

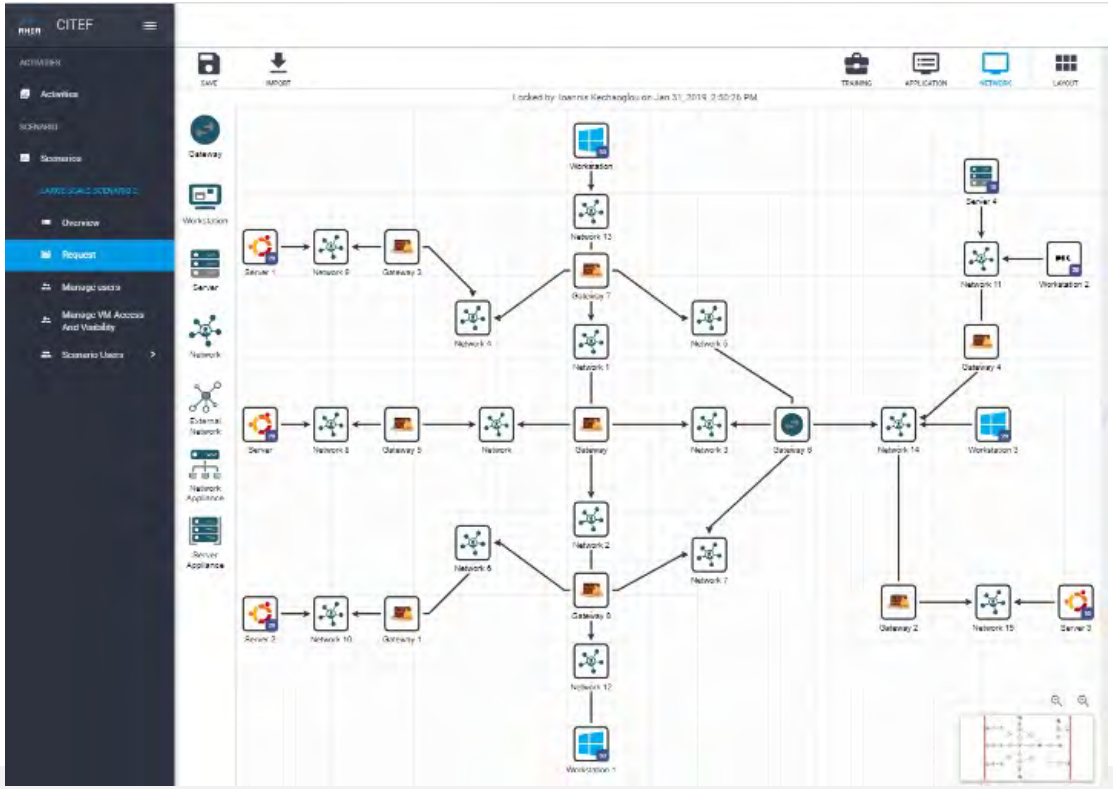




ECHO Technology Roadmaps

The ECHO Federated Cyber Range (E-FCR)

Cyber Ranges are multipurpose **virtualization environments** supporting **"security-by-design"** needs



Cyber Ranges are used to provide:

- Safe environment for **hands-on cyberskills** development
- Realistic simulation for **improved system assurance** in development
- Comprehensive means for **security test and certification** evaluation

In ECHO, we use Cyber Ranges also as virtual environments for:

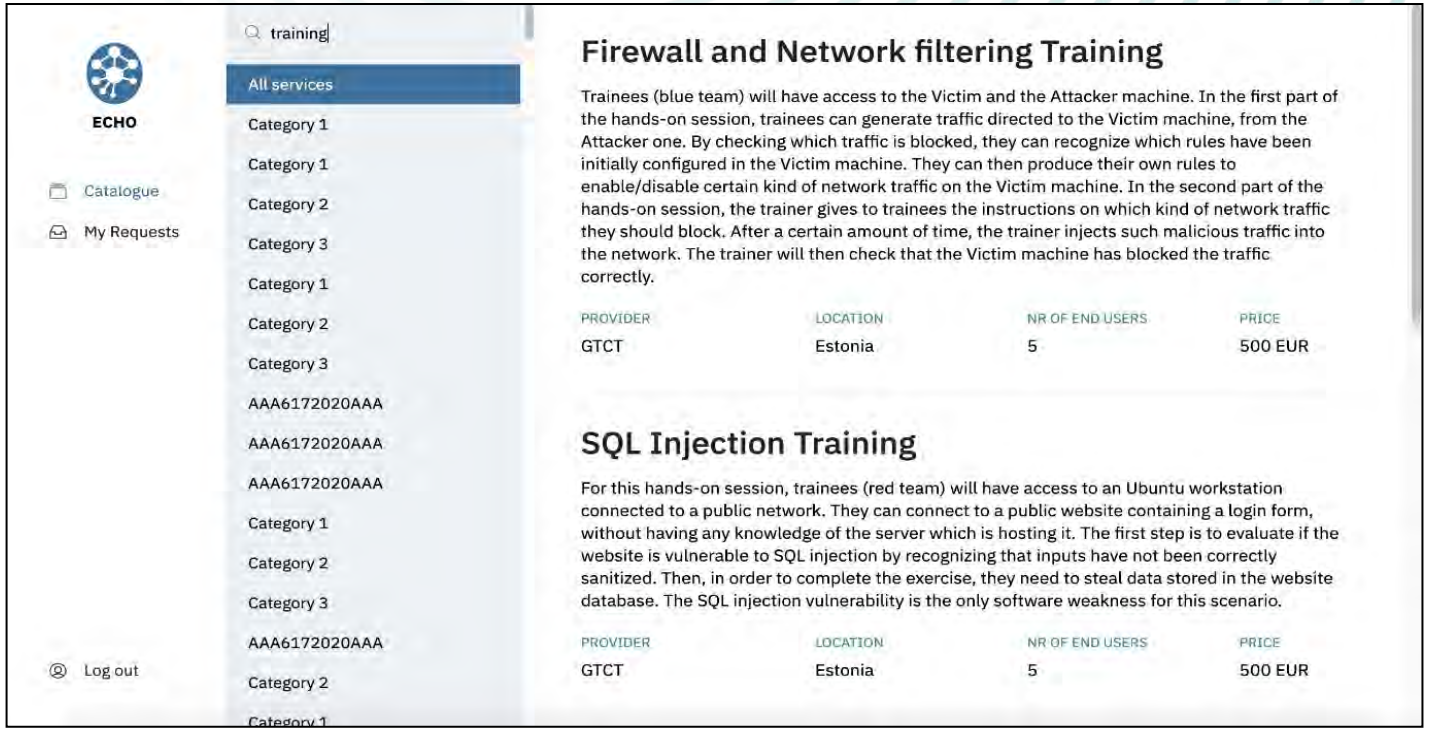
- Development and demonstration of **technology roadmaps**
- Delivery of specific instances of the **cyberskills training** curricula

ECHO Technology Roadmaps

The ECHO Federated Cyber Range (E-FCR)

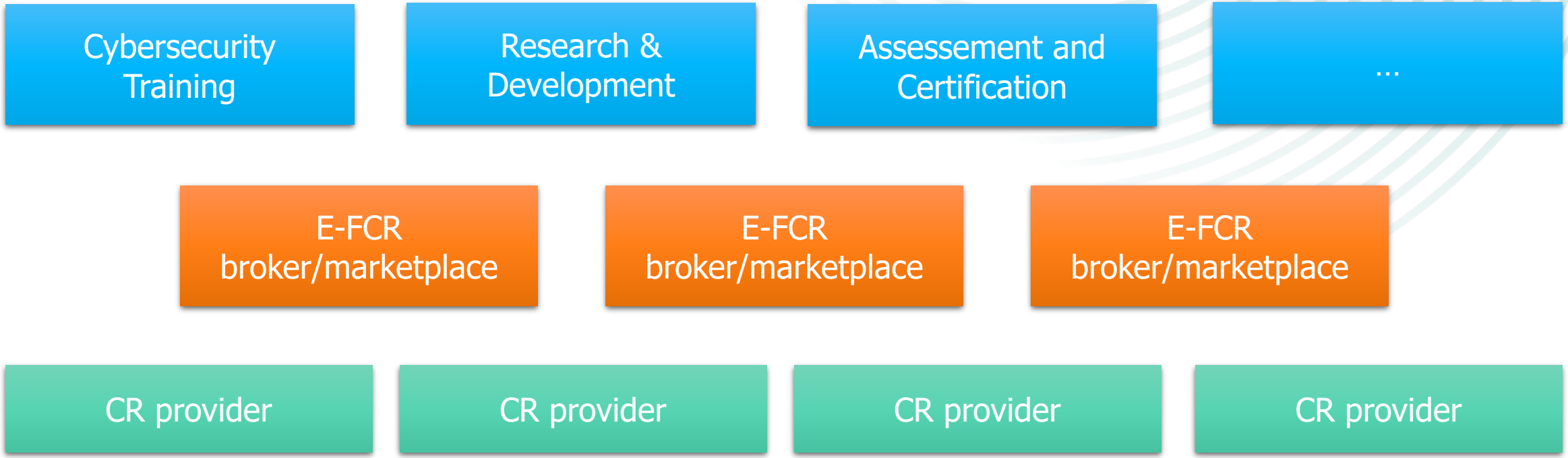
The goal of the ECHO Federated Cyber Range (E-FCR) is to:

- 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 complex emulations of **sector specific and unique technologies**



The ECHO Federated Cyber Range (E-FCR)

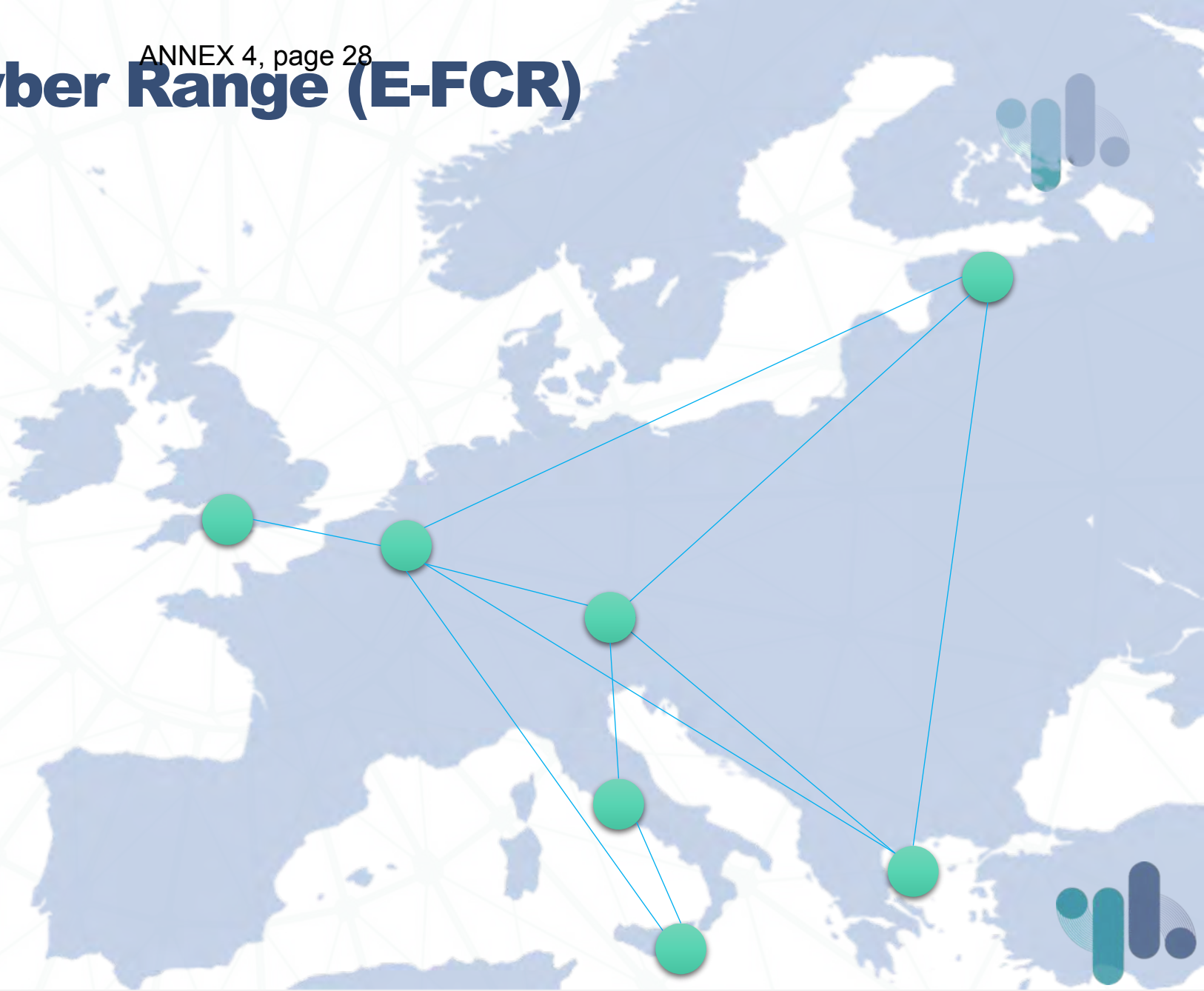
Concepts



ECHO Federated Cyber Range (E-FCR)

Where are we currently?

- Development is **complete**
- During Summer 2021, we started the first full integrations and interconnection tests, at first with 2 CRs, then 3, then 4
- The team started working to the **ECHO Demonstration cases**



The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ECHO Inter-sector Prototype tools

1

Objectives

Address most **pressing** transversal and inter-sector cybersecurity **challenges**
Cover **priority areas**
Increase **cybersecurity awareness**

2

Selection methodology

Detailed selection methodology based on **challenges**, **priority areas** covered, **innovation**, relevance, adaptability etc.

3

Development process

Scrum based development framework for integration, installation and testing of tools.

4

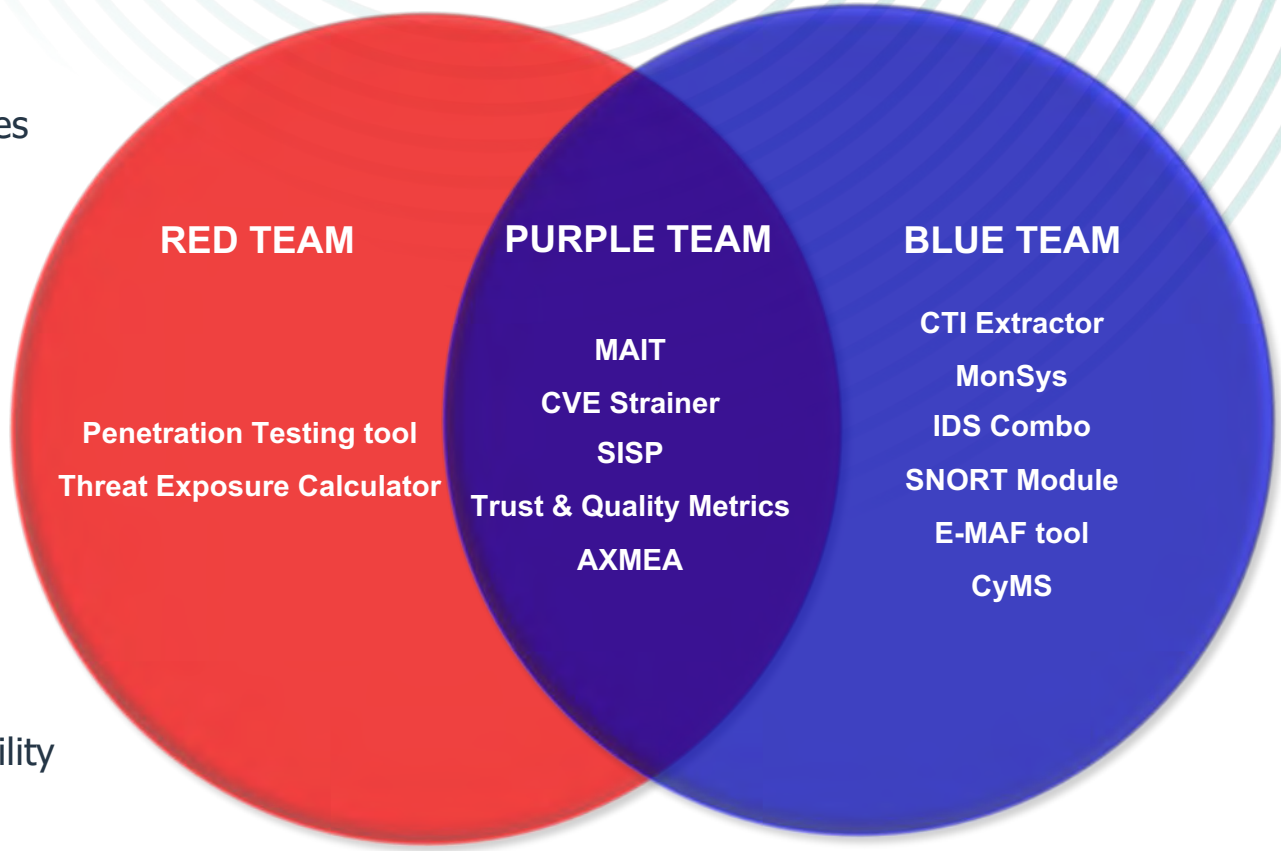
Outcomes

Innovative solutions based on **state-of-the-art** tools, techniques & methodologies
Leverage **known technologies** (Nmap, Snort, Nikto, Kali etc.)
Increase cybersecurity awareness through dedicated workshops/demonstrations

ECHO Inter-sector prototypes

Addressing the most pressing cybersecurity challenges

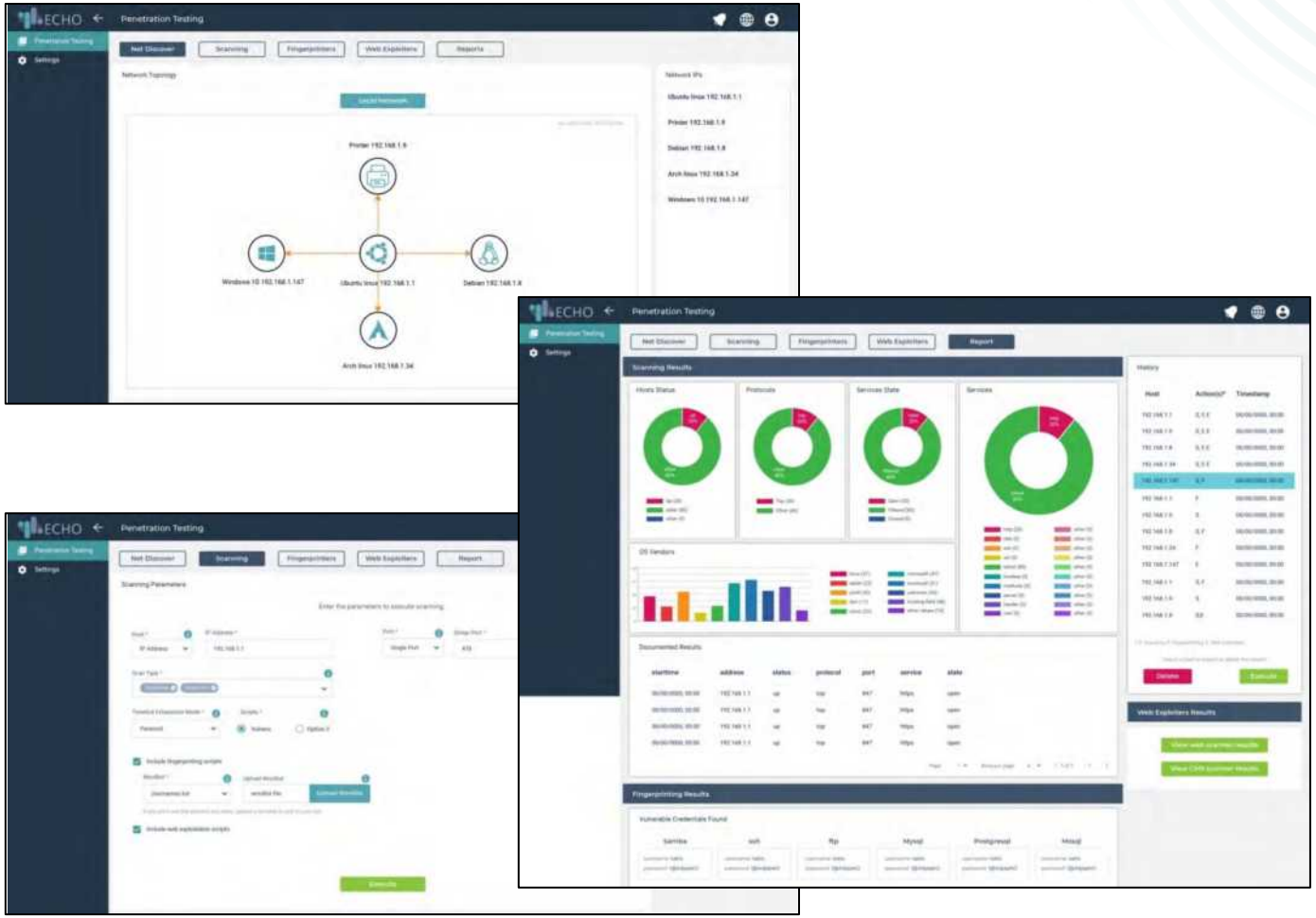
- **Tools:**
  - 38 tools initially proposed - 13 selected
  - Covering multi-domains & multiple cybersecurity challenges
- **Challenges** addressed:
  - 41 total unique challenges addressed
  - 32 transversal
  - 9 inter-sectoral
- **Priority areas** covered:
  - Maritime (CyMS)
  - Healthcare (SISP)
  - Energy (AXMEA)
  - Transversal – multiple sectors (rest)
- **Cybersecurity fields/categories:**
  - Red teaming: Penetration Testing, Network/Web Vulnerability Scanning
  - Blue teaming: Intrusion Detection Systems (IDS), SIEMs, Network Security Monitoring
  - Purple teaming: Knowledge Base, CTI Sharing, Malware Analysis, Cybersecurity/Situational Awareness

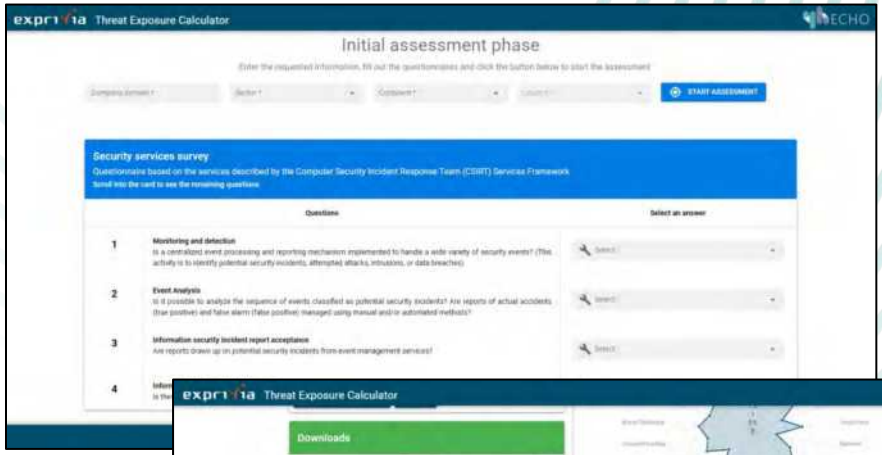


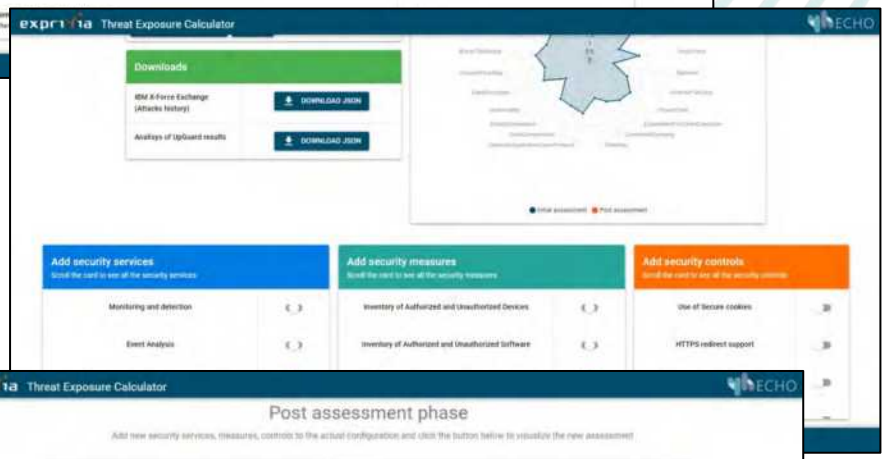
ECHO Inter-sector prototypes

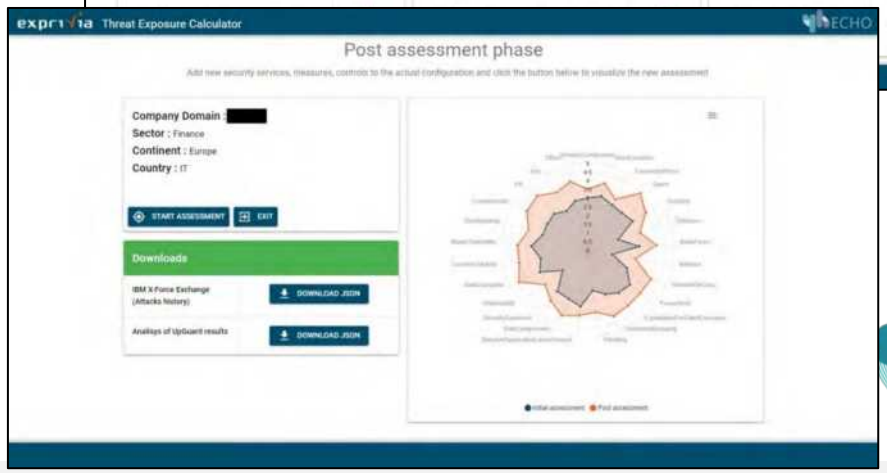
An eye on the prototypes – Red teaming

Penetration Testing tool, Threat Exposure Calculator





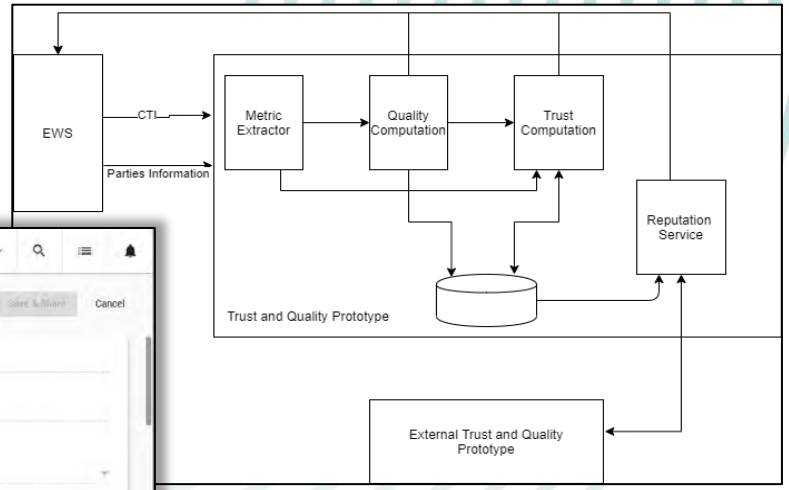


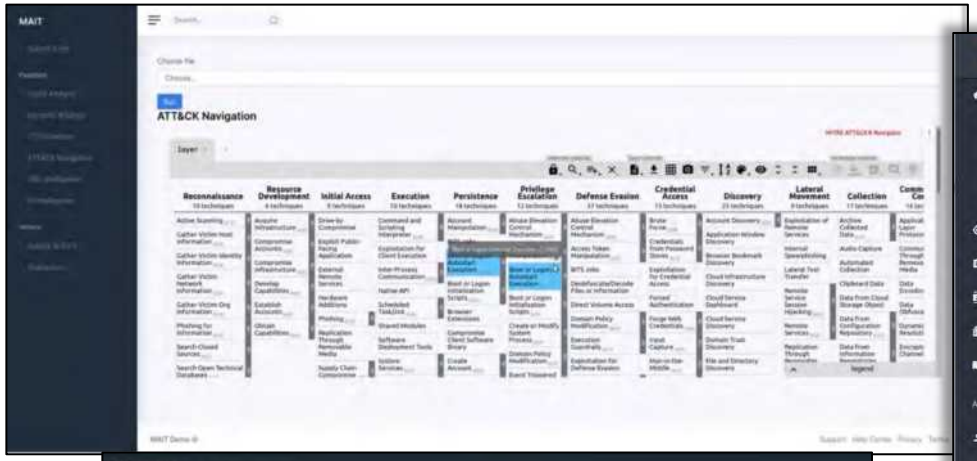


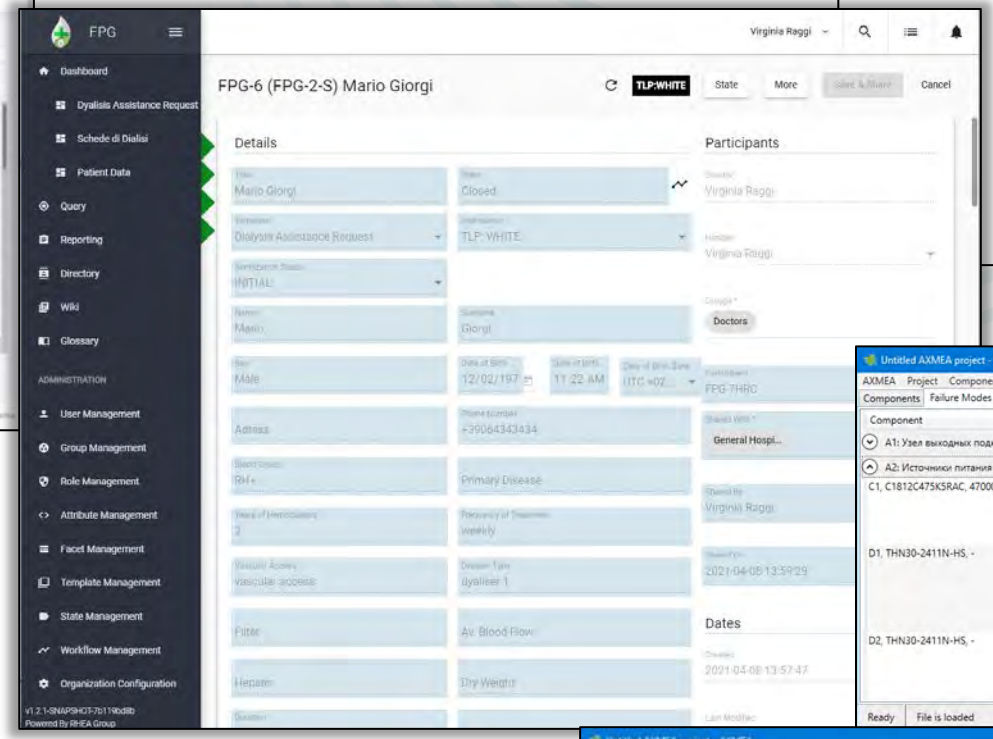
ECHO Inter-sector prototypes

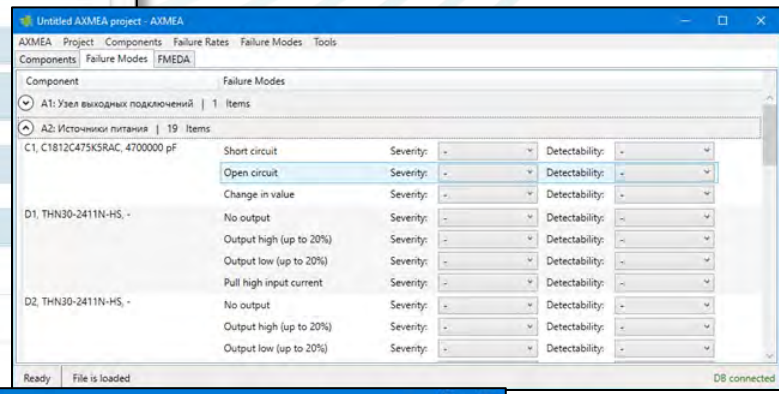
An eye on the prototypes – Purple teaming

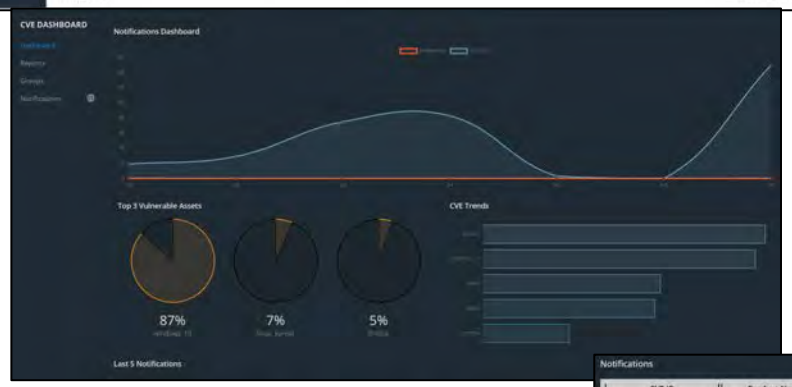
MAIT, CVE Strainer, SISP, Trust & Quality Metrics, AXMEA

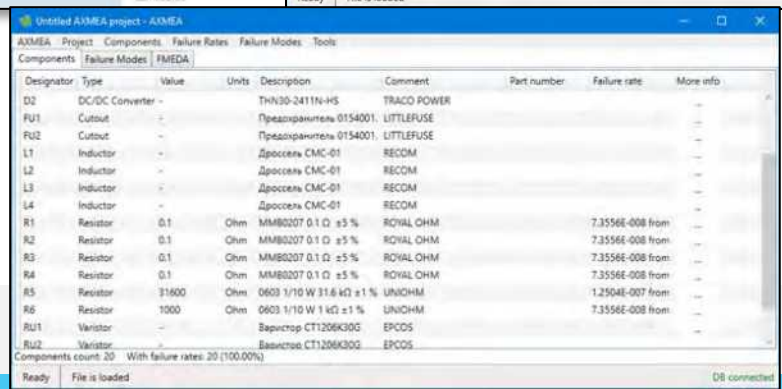








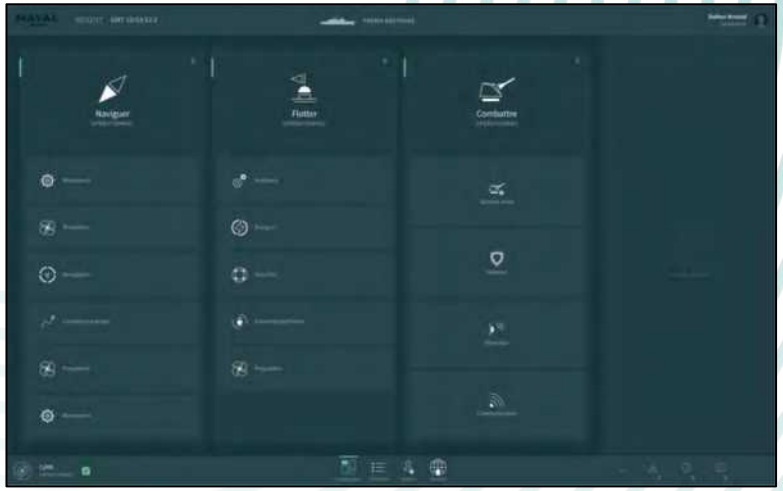


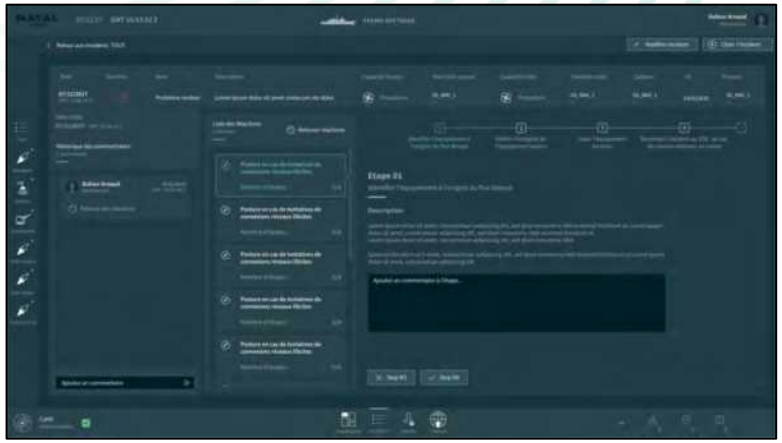


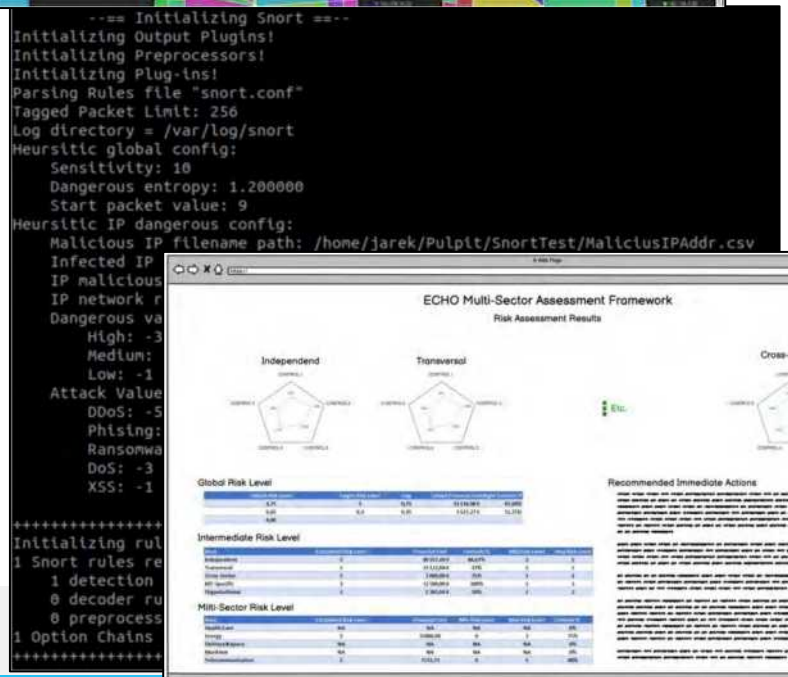
ECHO Inter-sector prototypes

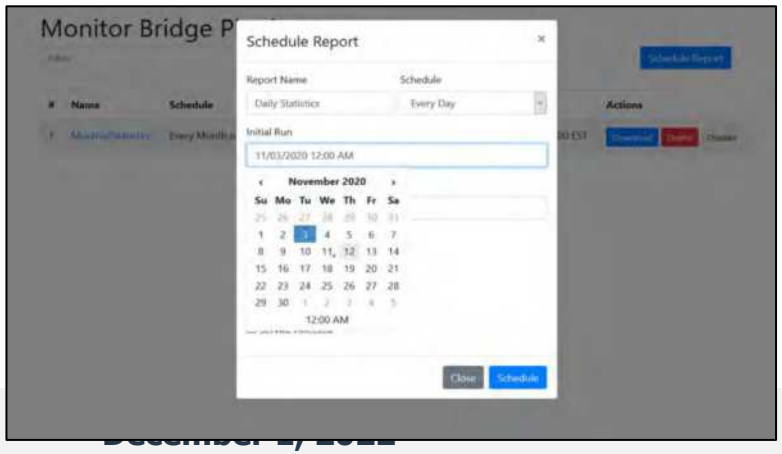
An eye on the prototypes – Blue Teaming

CTI Extractor, MonSys, IDS Combo, SNORT Module, E-MAF tool, CyMS









ECHO Inter-sector prototypes

An eye on the prototypes

Name	Leading Partner	Tool Type / Cybersecurity field
Penetration Testing Tool (PT)	CERTH	Penetration testing, Web vulnerability scanning
Cyber Threat Intelligence (CTI) Extractor	CERTH	Network Security Monitoring, SIEM/IDS, Cybersecurity awareness
Trust & Quality Metrics (TQM)	VST	Cyber Threat Intelligence Sharing
SNORT module (SM)	AGH	Network Security Monitoring, SIEM/IDS
Threat Exposure Calculator (TEC)	EXP	Web vulnerability scanning, Penetration testing, Cybersecurity awareness
Malware Analysis and Intelligence Tool (MAIT)	BU	Knowledge base, Cybersecurity awareness
Intrusion Detection System Combo (IDS Combo)	IICT	Network Security Monitoring, SIEM/IDS, Cybersecurity awareness, Knowledge base
E-MAF tool (E-MAT)	AON	Cybersecurity awareness
Cyber Management System (CyMS)	NG	SIEM/IDS
Common Vulnerability Exposure (CVE) Strainer	TBS	Knowledge base
Monitoring System (MonSys)	ESICEE	Network Security Monitoring
Secure Information Sharing Platform (SISP)	RHEA	Knowledge base, Cyber Threat Intelligence Sharing
Automated X-Modes and Effects Analysis (AXMEA)	KHAI	Knowledge base

Developed from scratch

More mature

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ANNEX 4, page 35

Demonstration cases for validation

- **Sector demonstration cases**
  - To demonstrate technologies and frameworks we developed during the project we implemented a set of complex **Demonstration Cases**
  - ECHO Demonstration Cases target **all ECHO technologies** and cover **all critical sectors** where we are involved
    - Energy
    - Maritime
    - Healthcare

ECHO Demonstration Cases

ECHO sector and multisector specific Use Cases

- Energy
- Healthcare
- Maritime

ECHO sector and multisector Cyber Ranges

- Energy
- Healthcare
- Maritime

E-EWS Reference Library Exchange	E-EWS Cyber incident coordination and response	E-FCR for cyber-skills education and training	E-FCR for cybersecurity certification of new technologies	E-FCR for R&D activities of the technology roadmaps
ECHO Early Warning System	ECHO Early Warning System	ECHO Federated Cyber Range	ECHO Federated Cyber Range	ECHO Federated Cyber Range
ECHO Cyber Ranges	ECHO Cyberskills framework	ECHO Cyberskills framework	ECHO Certification Scheme	ECHO Technology Roadmaps Prototypes
	ECHO Cyber Ranges	ECHO Cyber Ranges	ECHO Technology Roadmaps Prototypes	ECHO Cyber Ranges
			ECHO Cyber Ranges	

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Demonstration cases for validation

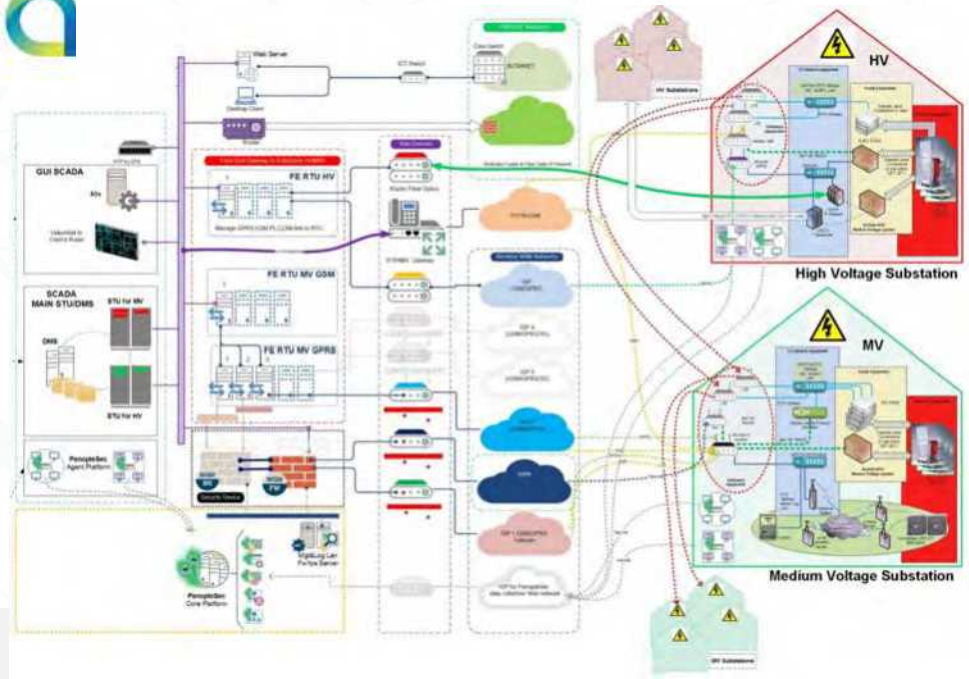
Energy Sector

The energy sector faces increasing and more sophisticated cyber threats affecting both the IT and OT side

Some use cases to be implemented in the demo case

- Attacks against the command-and-control systems of an energy provider
- Attacks to SCADA equipment/devices of an energy provider

We are creating a sector-specific cyber range emulating a C&C Centre to support the Demonstration Cases



Demonstration cases for validation

Healthcare Sector

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ICT is becoming more and more pervasive in the healthcare sector

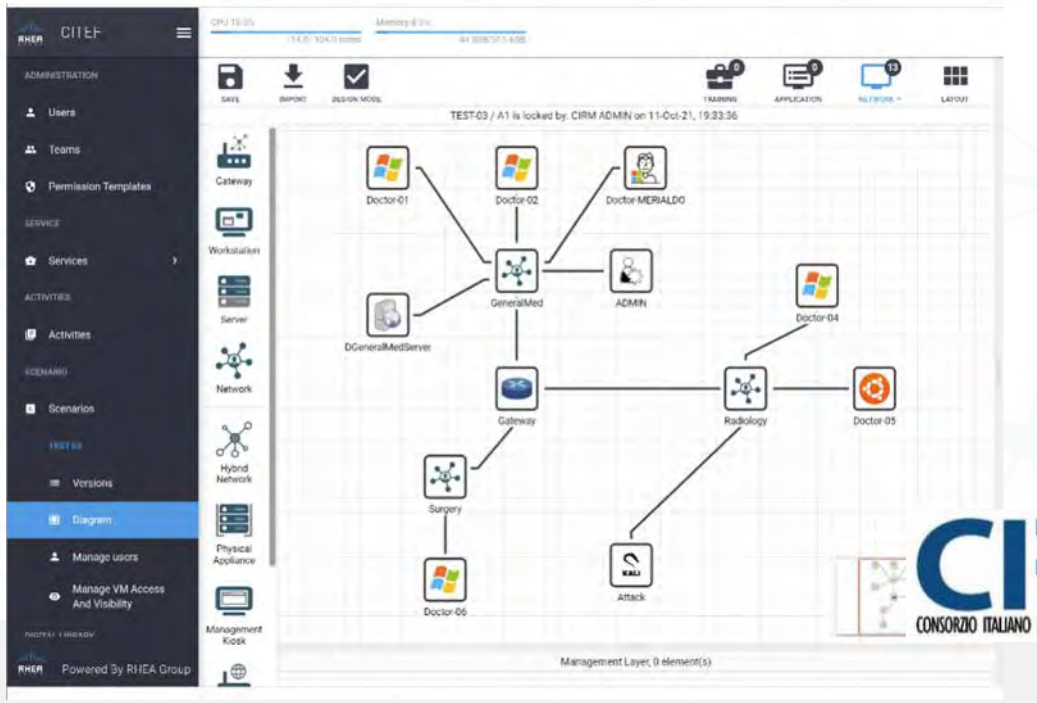
- Computerized systems for automation of diagnostic and collection of patient data
- Sensors and medical devices with IP addresses connected to the Internet (IOT)
- Multidisciplinary teams interact with patient and share sensitive data also through personal devices

Some use cases to be implemented

- Attacks against complex medical systems (blood analysis laboratory)
- Attacks against corporate IT system via ransomware

We are refining two sector-specific cyber range to support the Demonstration Cases

- Corporate hospital IT system
- Blood sample analysis lab emulation



CRM
CONSORZIO ITALIANO PER LA RICERCA IN MEDICINA

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Demonstration cases for validation

Maritime Sector

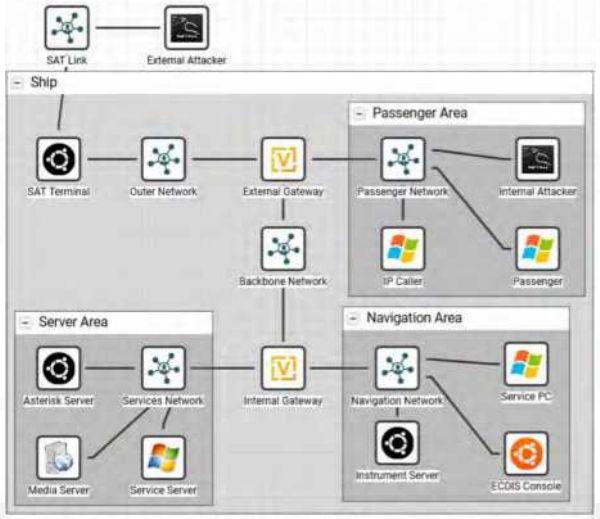
The maritime sector is already strongly digitized and it is of strategic importance

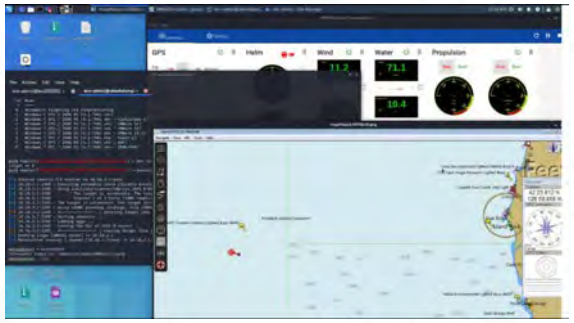
IT and OT networks are highly integrated, raising specific challenges

Some use cases to be implemented

- Attacks against ship's navigation systems via the GPS link
- Attacks against ship's OT systems

We implemented two sector-specific cyber ranges to support the demonstration cases of technologies and prototypes





ECHO ACTIVE SERVICES

ECHO Daily Bulletin and Newsletter

We implemented an engine to collect relevant **cyber security news** from thousands of sources worldwide and we constantly refine the engine to improve the news collection.

We publish the most relevant news (10/20 per day) on our website. The most relevant are spread and discussed via Social Media

When E-EWS and E-FCR will be active, they will be added to the list of ECHO Services

December 1, 2022

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Engagement Opportunities

Whilst we are still early in the Project, we are keen to begin growing our network of interested parties, stakeholders and potential new partners, and are constantly looking for **new** and **exciting opportunities** to refine and improve the project results.

https://echonetwork.eu**/join-echo/**

ECHO is interested on enlarging the number of partners, when newcomers can bring an added value to the team. As of December 2021, **13** new partners already joined the team!

Parties (**including single individuals**) interested in ECHO will be mapped into the following categories:

ECHO CLUB

- Subscription to ECHO's monthly newsletter
- Free participation in ECHO Workshops and Hackathons (up to 5 people)
- Participate in exclusive events for ECHO Club Members (up to 5 people)
- Opportunity to become an ECHO Participant

ECHO PARTICIPANT

- Subscription to ECHO's monthly newsletter
- Free participation in ECHO Workshops and Hackathons (up to 10 people)
- Participate in exclusive events for ECHO Participants (up to 10 people)
- Gain exclusive access to ECHO products and services
- Participate in dedicated surveys and studies
- Opportunity to become an ECHO Partner

ECHO PARTNER

- Subscription to ECHO's monthly newsletter
- Free and unlimited participation in ECHO Workshops and Hackathons
- Unlimited participation in exclusive events for ECHO Partners
- Gain exclusive access to ECHO products and services
- Participate in dedicated surveys and studies
- Opportunity to actively contribute to the ECHO Early Warning System
- Access to the ECHO Federation of Cyber Ranges

Get in Touch with Us and Follow us on Social Media!

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

info@echonetwork.eu

www.echonetwork.eu

https://twitter.com/**ECHOcybersec**

https://www.facebook.com/**echonetworkeurope/**

https://www.linkedin.com/in/**echo-cybersecurity**

https://www.youtube.com/channel/**UCDQBXrQhoLJ2Inf38x1X6Uw**

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

Thank You

Wim Mees

www.echonetwork.eu

CyberSec4Europe

Safeguarding European values through excellence in cybersecurity

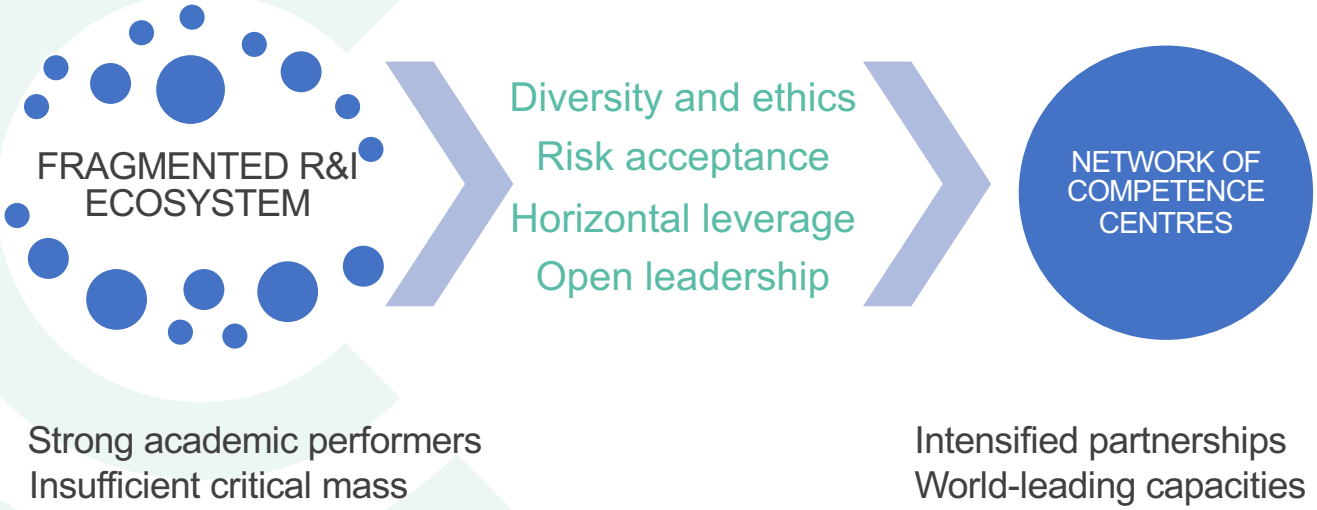
CONVERGENCE NEXT
2022-06-01, Brussels & Online

Kai Rannenberg
Goethe University Frankfurt

Kai.Rannenberg@m-chair.de

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

To change Europe's cybersecurity research and innovation landscape

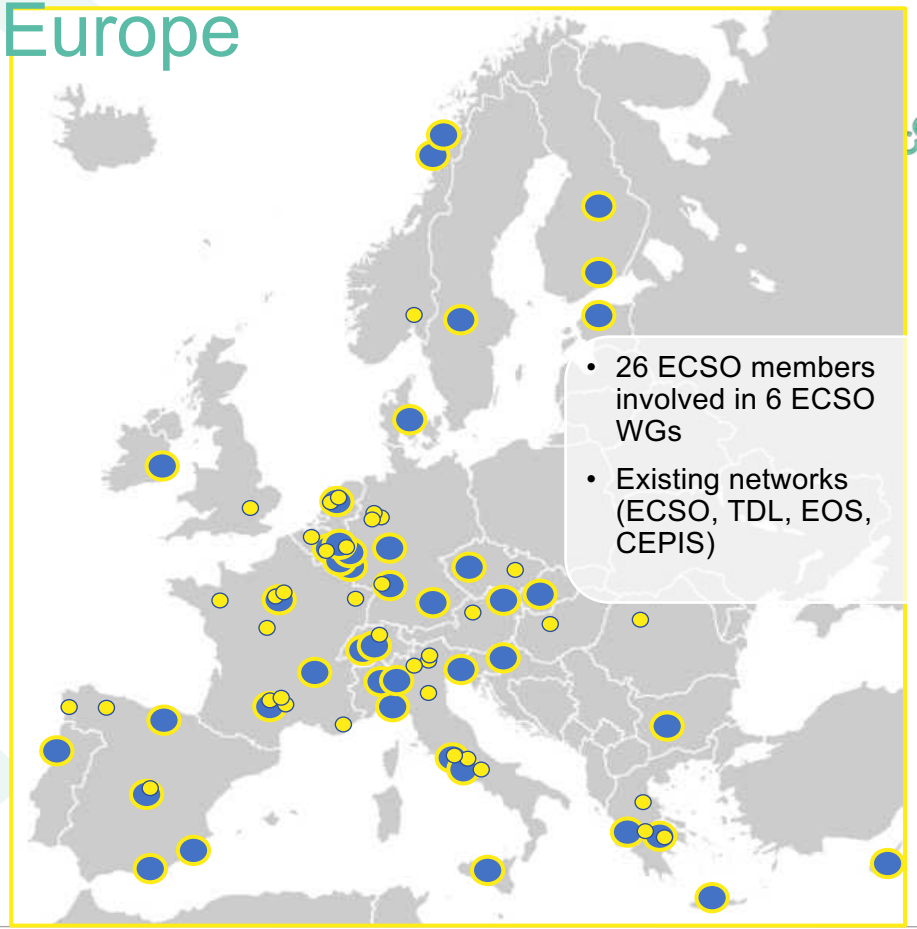


Strong academic performers
Insufficient critical mass

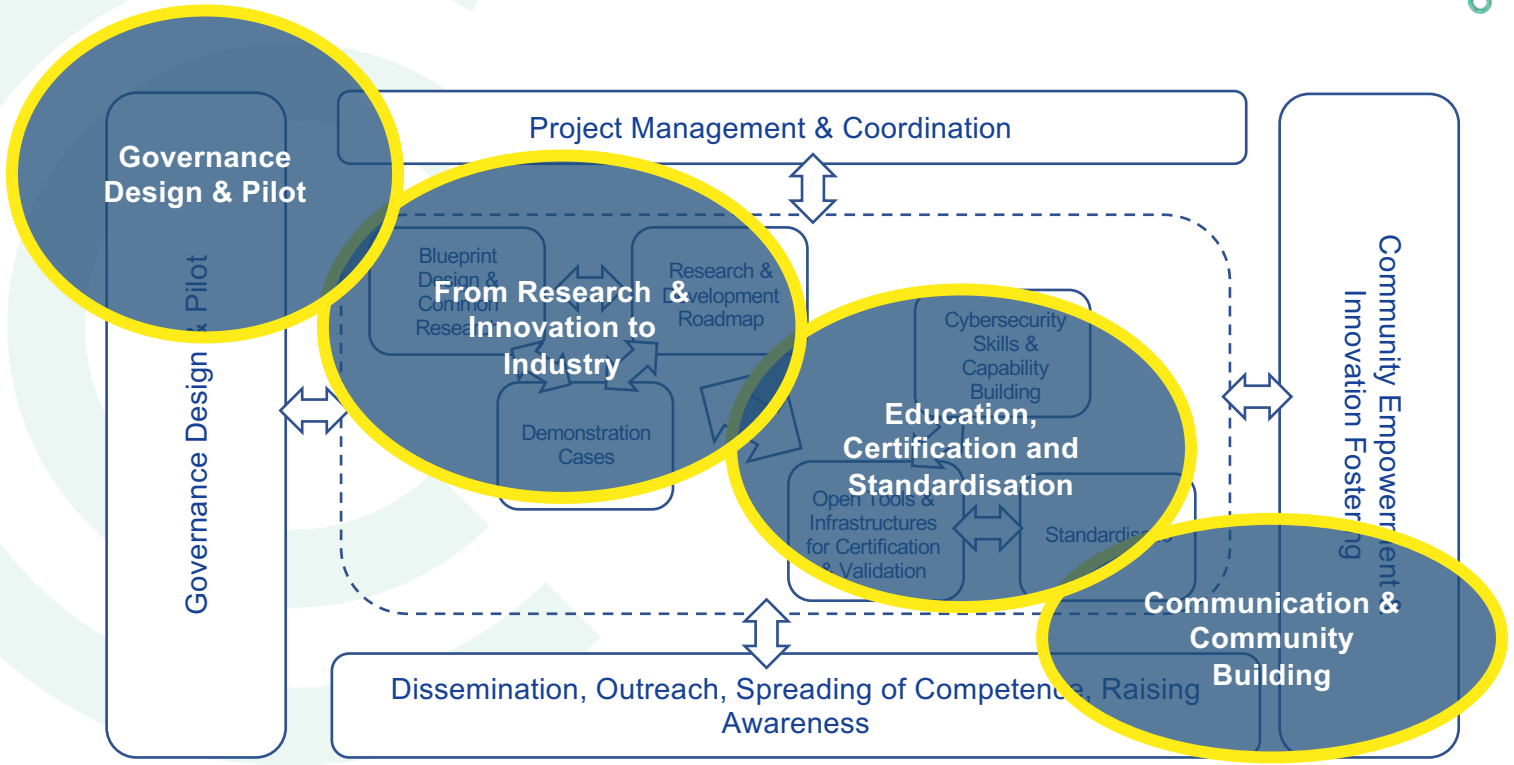
Intensified partnerships
World-leading capacities

Who are CyberSec4Europe

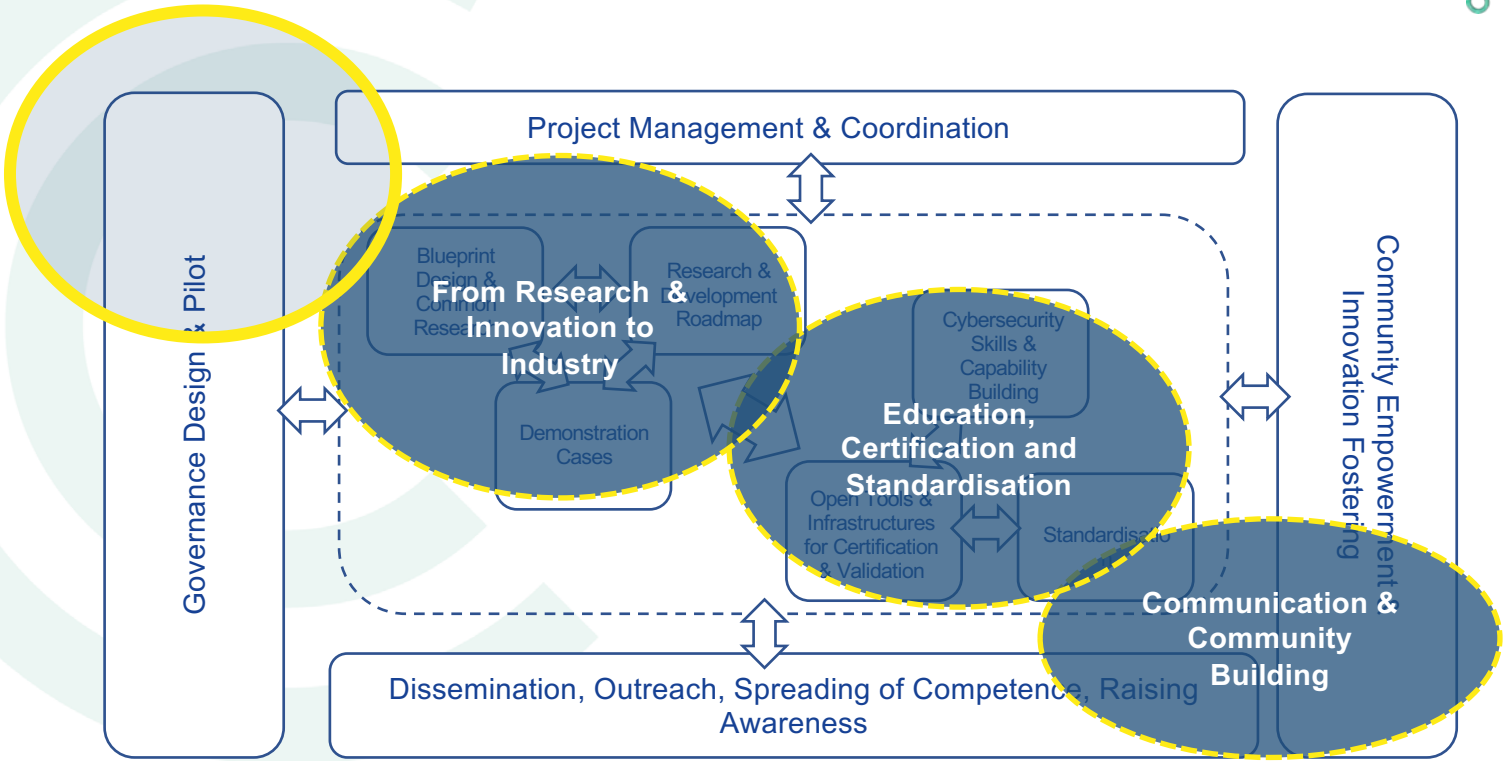
- Centres of Excellence / Universities / Research Centres / Enterprises (small and larger)
- 43 members in 22 countries
- 40+ associates in 16 countries
- Experience from over 100 cybersecurity projects in 14 key cyber domains
- 11 technology/application elements and coverage of nine vertical sectors
- One of 4 ECCC pilots



Project Architecture



Pillar I: Governance Design & Pilot



Pillar I: Governance, Design & Pilot (WP2)

Collecting stakeholder viewpoints

- If you have strong opinions: Let us know!

Assessing (best) governance practices

- Top-down vs. bottom up
- Stakeholder involvement: academia, administration, civil society (NGOs), government, industry, military, …

Governance structure (D2.1, D2.2, D2.3)

- Design: enable bottom-up advice and community-derived capabilities
- CHECK (**C**ommunity **H**ub of **E**xpertise in **C**ybersecurity **K**nowledge)

Implementation: regional & national

- Pilot regional competence hub in Toulouse
- National hub candidates in e.g. Denmark & Spain

Lessons learned and being learned: Participation and trust essential

Synergy between **top-down** and **bottom-up** structures
→ **integrating stakeholder** groups (**including citizens**)
→ efficient stakeholder **engagement** on **all societal levels**

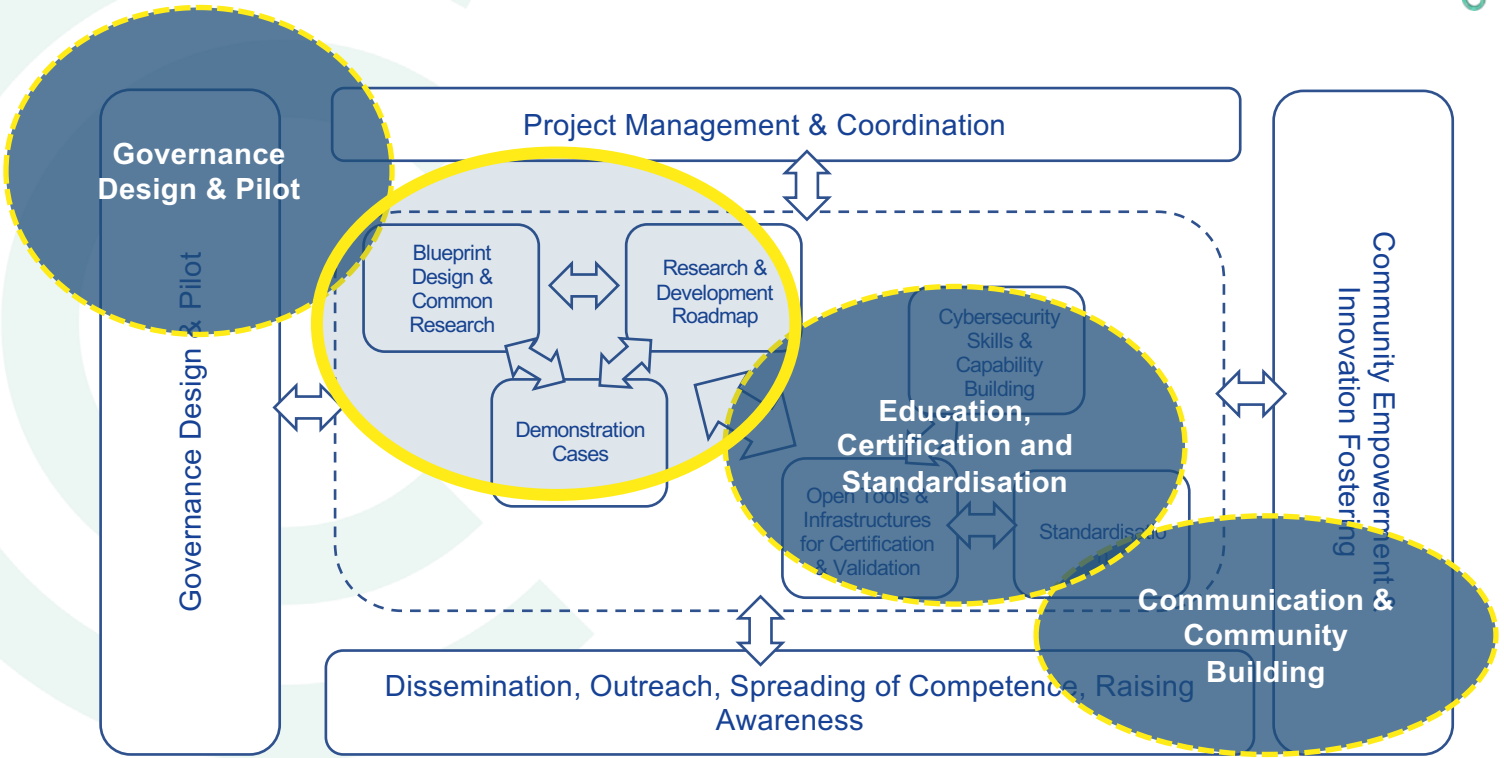
- Industry groups, local governments, CERTs → not all the same level of formality as representatives of the EC and Member States
- May be different per country (so regulation must allow this, e.g. sectoral vs regional)

Key elements of **trust** into an **organisation**

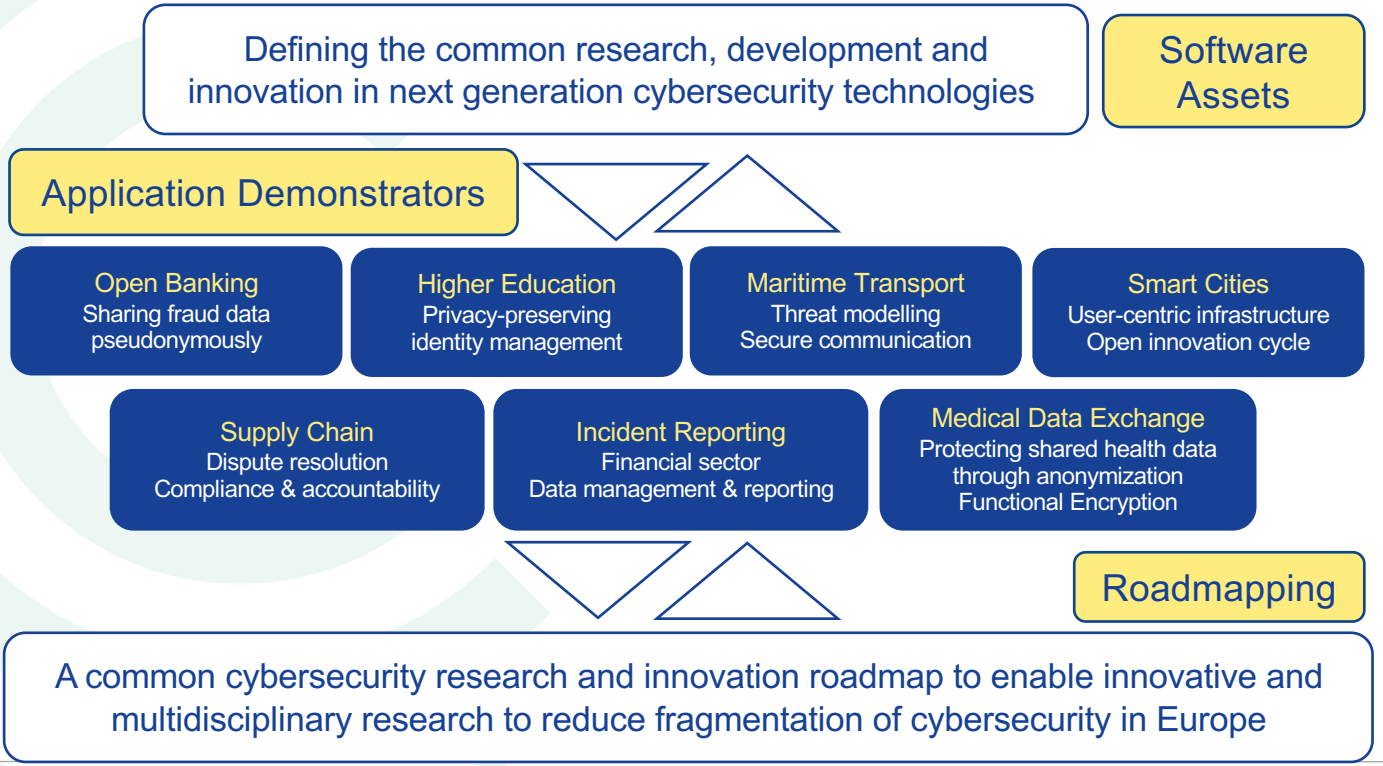
- Secured participation
- Organisational transparency

Agile, trustful, and **lively exchange** in and between **Cybersecurity Communities**

Pillar II: From Research & Innovation to Industry



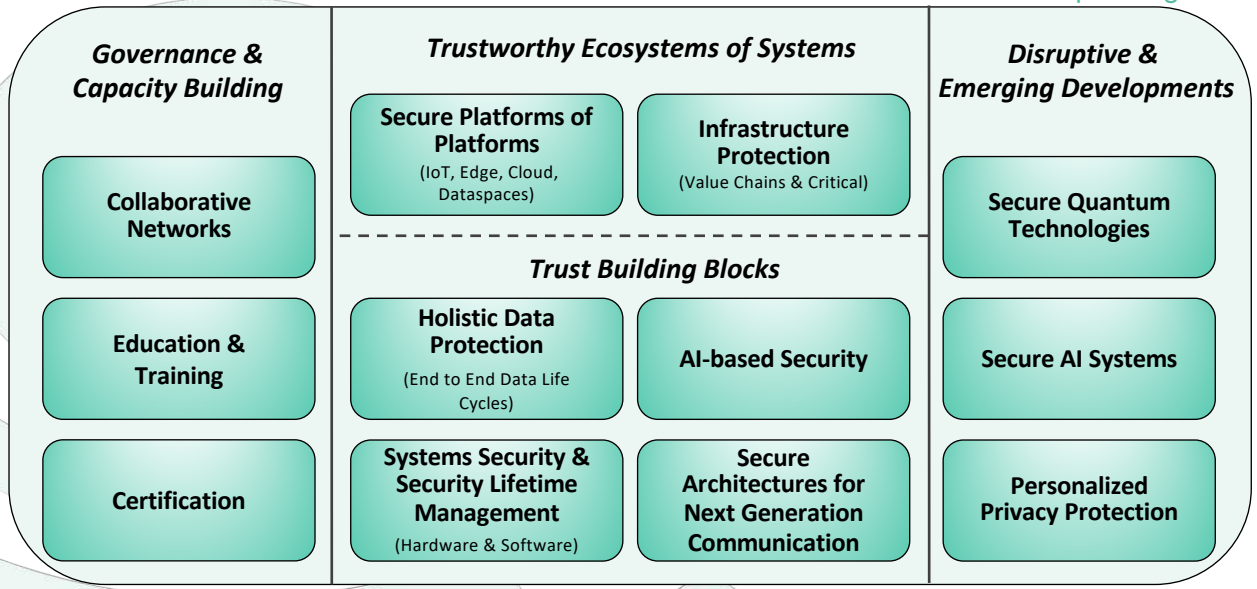
Pillar II: From Research to Innovation to Industry (WP3, WP4, WP5)



Pillar II: From Research and Innovation to Industry (WP4)

Cybersecurity research focus areas priorities: The four pilots & ECSO perspective

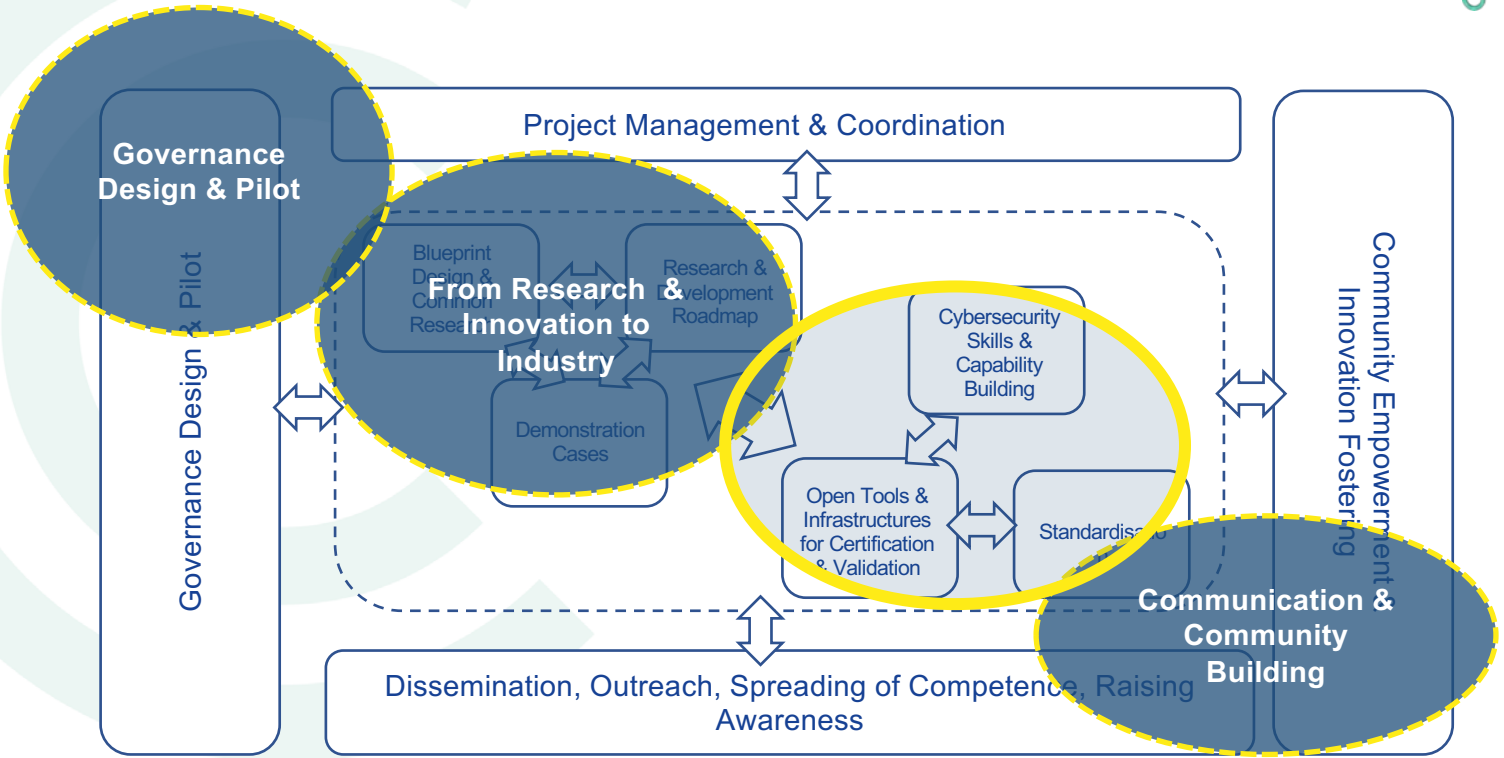
As per August 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

https://cybersec4europe.eu/heterogeneity-of-data-protection-legislation-in-the-eu/

Pillar III: Education, Certification and Standardisation



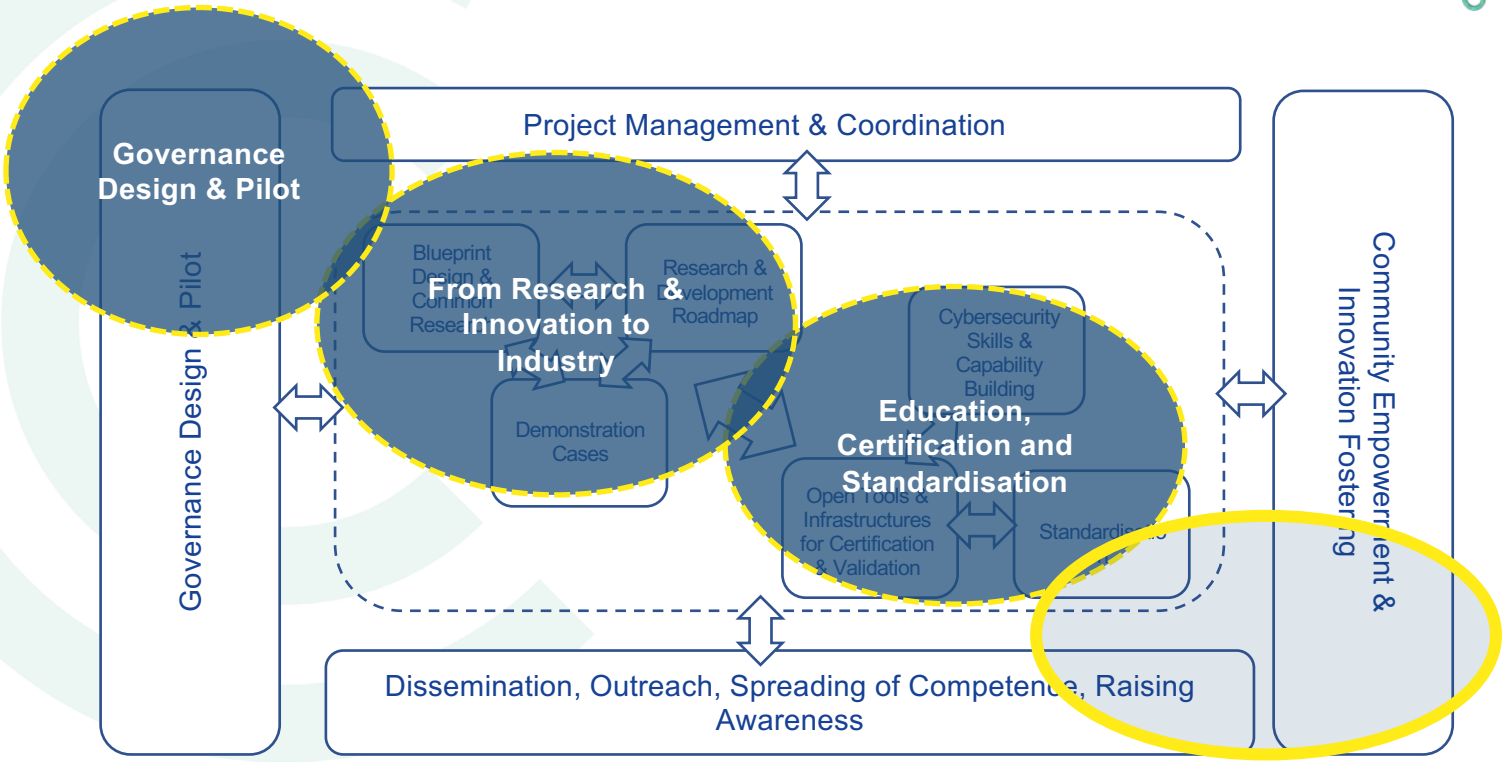
Pillar III: Education, Certification, and Standardization (WP8)

International standardisation is an important channel for global dissemination of technology and research results.

Even though standardisation is a long-term strategy with no immediate return on investment, it will be instrumental in ensuring that European companies grow in size to compete on the global market.

- Established a **liaison relationship** with ISO/IEC JTC 1/SC 27
  - WG 2 – Cryptography and security mechanisms, and
  - WG 5 – Identity management and privacy technologies
- **Project Standards Matrix** (D8.2) together with the **Standards Matrix** (currently updated again)
- Comparison of **governance structures** and **organisational principles of several SDOs** and **recommendations to the EU** for **standardisation** (D8.4)

Pillar IV: Outreach & Community Building



Pillar IV: Outreach & Community Building

Concertation events, organised by the four pilots with ECSO

- Toulouse, 2019
- CONVERGENCE, December 2020
- **CONVERGENCE NEXT, June 2022**

Featuring six collaborative focus groups plus JRC Cybersecurity Atlas

- Governance
- Education
- Roadmapping
- Threat intelligence in the financial sector
- Communications
- Cyber ranges

Upcoming events
Save the Date(s)

07-06 – 09-06	Forum International de la Cybersécurité **(FIC), Lille**
13-06 – 15-06	37th International Conference on ICT Systems Security and Privacy Protection **– IFIP SEC, Copenhagen**
29-08 – 02-09	17th **IFIP Summer School** On Privacy And Identity Management
16 September	**Evening event** on occasion of the CyberSec4Europe General Meeting**, Brussels and possibly hybrid**
01-12 – 02-12	**CyberSec4Europe Summit** Conference**, Brussels and possibly hybrid**

More at https://cybersec4europe.eu/events/

Get involved with CyberSec4Europe

Cyber Security for Europe Associates

Discover the benefits of becoming an **Associate Partner.**

Cyber Security for Europe Friends

Become a Friend of CyberSec4Europe and keep up to date with all the latest news and views from the project

Find out more about the work packages:
https://cybersec4europe.eu/work-packages

Discover and download all our public deliverables!

Summary & Outlook

- CyberSec4Europe is a **vibrant pilot community.**
- **Agile** with regard to newly arising requirements and spontaneous requests by the EU, e.g. contributions to EC concept of strategic axis and JRC Atlas cybersecurity roadmap
- Spearheaded the design of **a distributed governance model**
- Progressed research and research planning based on **real** application requirements
- Progressed education, certification and standardization initiatives
- Integrated **all** pilots, ECSO and focus groups in a single **comprehensive event**:
  - **CONVERGENCE**, 2020-12-09/11, virtual
  - **CONVERGENCE NEXT**, 2022-06-01/03, Brussels, hybrid
- Intensive *contribution* to and interaction with **ECSO**
- Implemented **principles** in **practice** (e.g. GDPR compliant open-source web conferencing)

Thank you very much for your attention!

Kai.Rannenberg@m-chair.de

BackUp Material

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

CyberSec4Europe

Safeguarding European values through excellence in cybersecurity

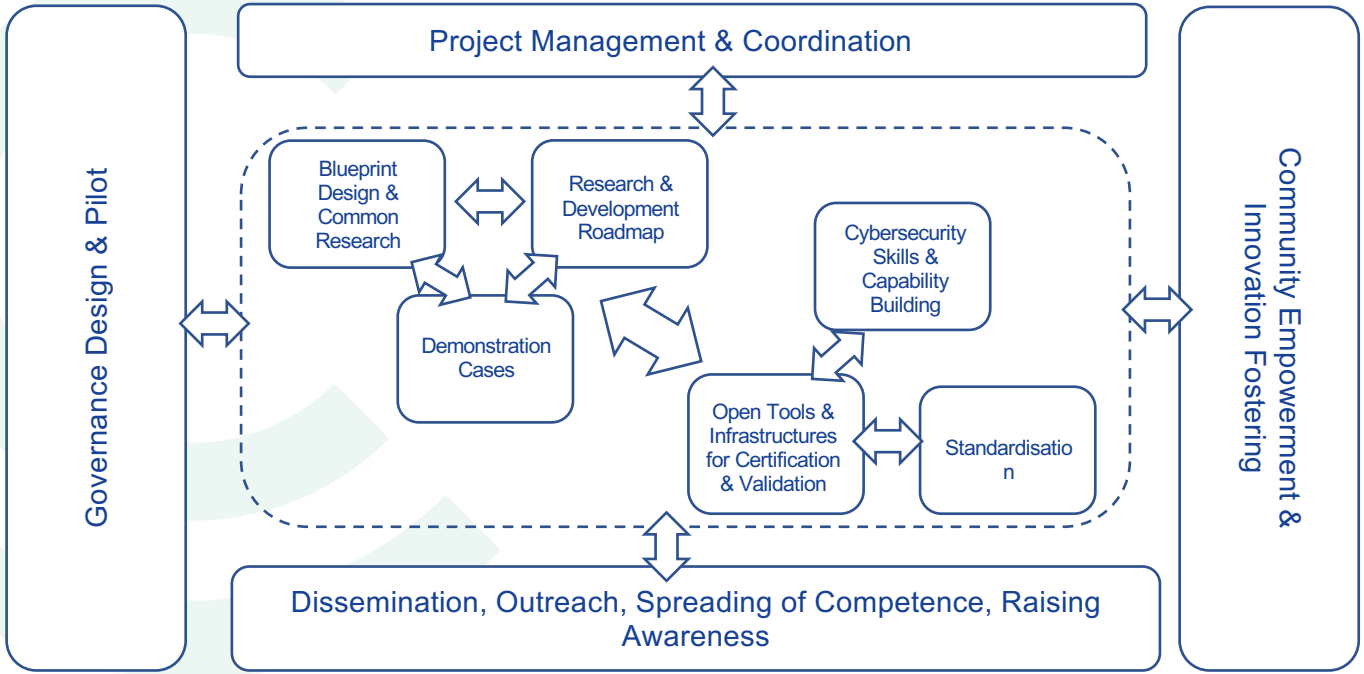
CONVERGENCE NEXT
2022-06-01, Brussels & Online

Kai Rannenberg
Goethe University Frankfurt

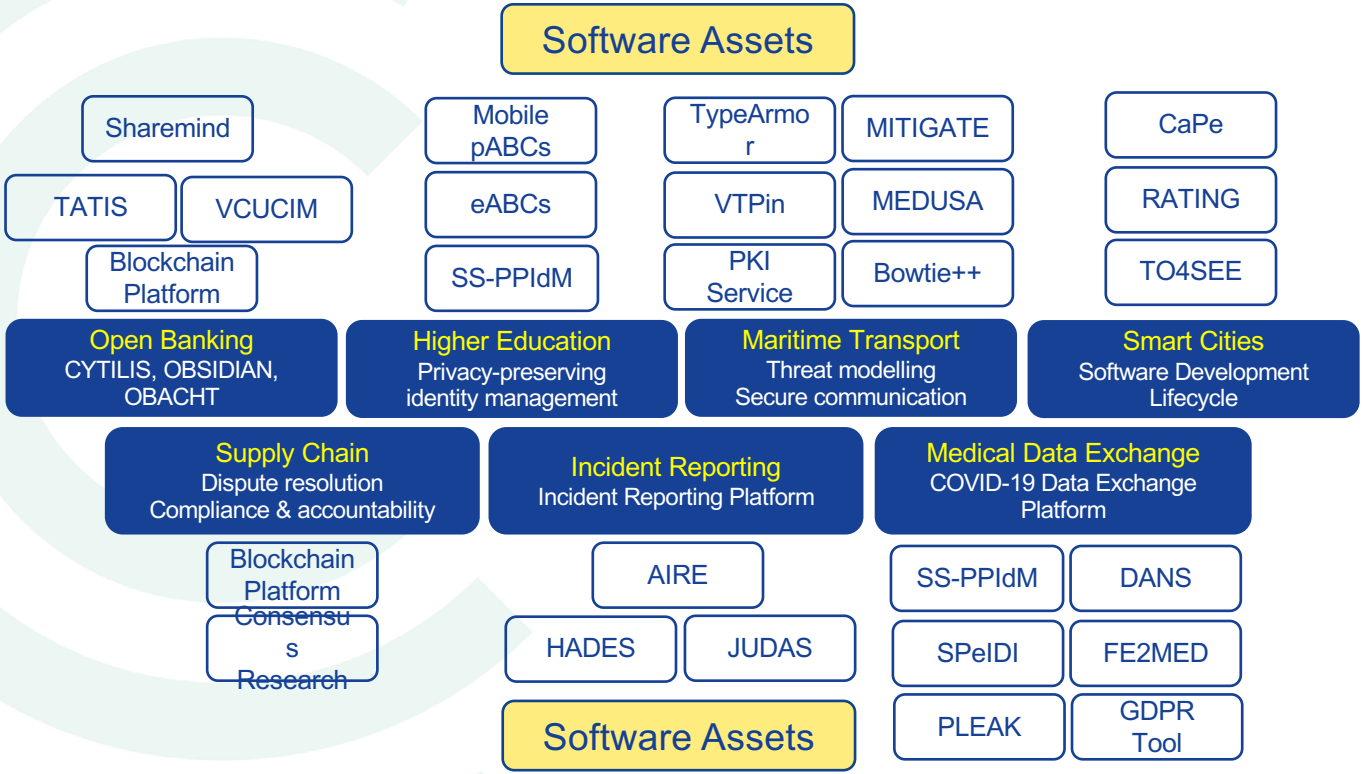
Kai.Rannenberg@m-chair.de

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

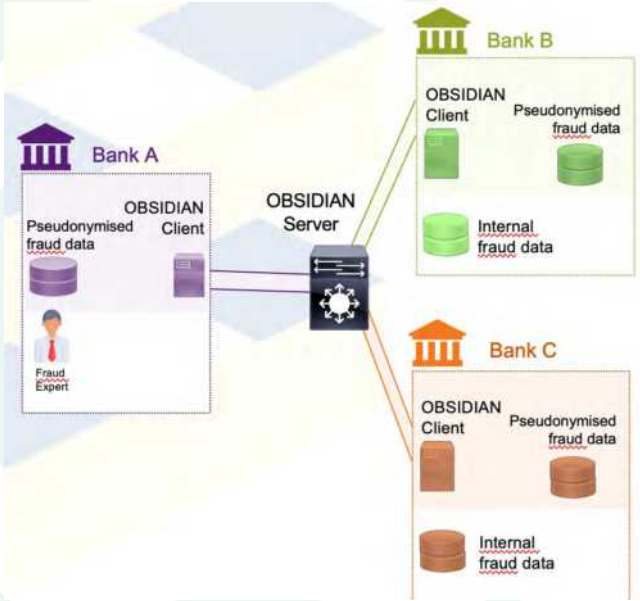
Project Architecture Details



Pillar II: From Research and Innovation to Industry
WP3, WP5: From Assets to Demonstrators



Open Banking



The OBSIDIAN server does not store fraud data and a suspected IBAN is always pseudonymised when exchanged

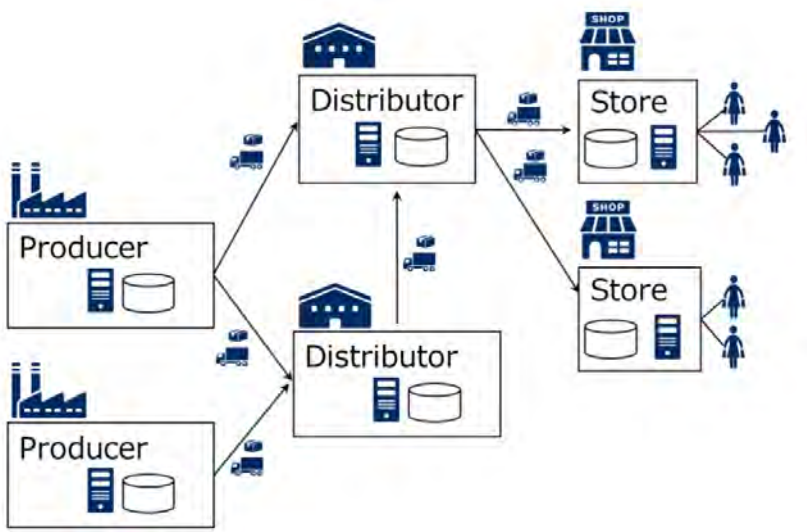
Open Banking represents a new wave in financial transactions including payments, closely related to Payment Services Directive 2 (PSD2) and the GDPR.

One of the use cases is **OBSIDIAN:**

Open Banking Sensitive Data Sharing Network for Europe

- To support the fight against fraud by sharing IBAN information between banks
- To be more effective in detecting money laundering or terrorist financing to protect the European market in an open economy

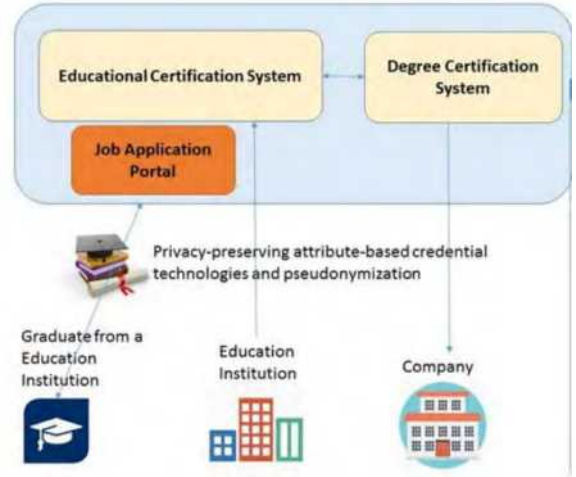
Supply Chain Security Assurance

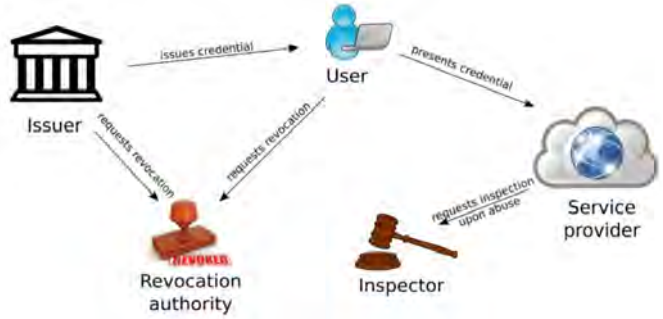


To allow involved stakeholders to secure the supply chain and trace the movement of components and goods during all stages of the supply chain and to guarantee quality and integrity of the parts and products.

The overall result of this application use case will be to provide a blueprint for supply chain solutions for multiple sectors.

Higher Education

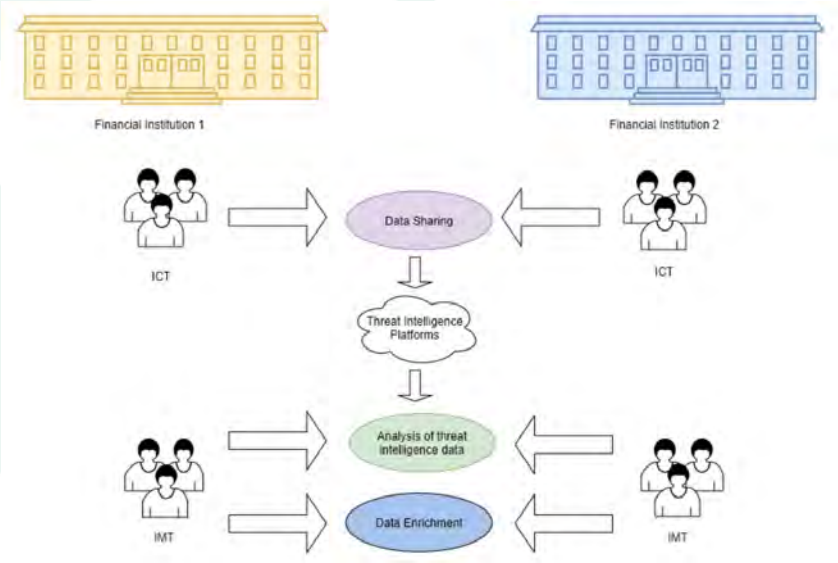




To enable an identity infrastructure to fulfil the need for strong privacy-preserving authentication with a distributed and scalable platform for privacy-preserving self-sovereign identity management.

This use case also provides transversal support to the other application use cases and empowers end-users and organisations to control their privacy and increase trust in Internet services.

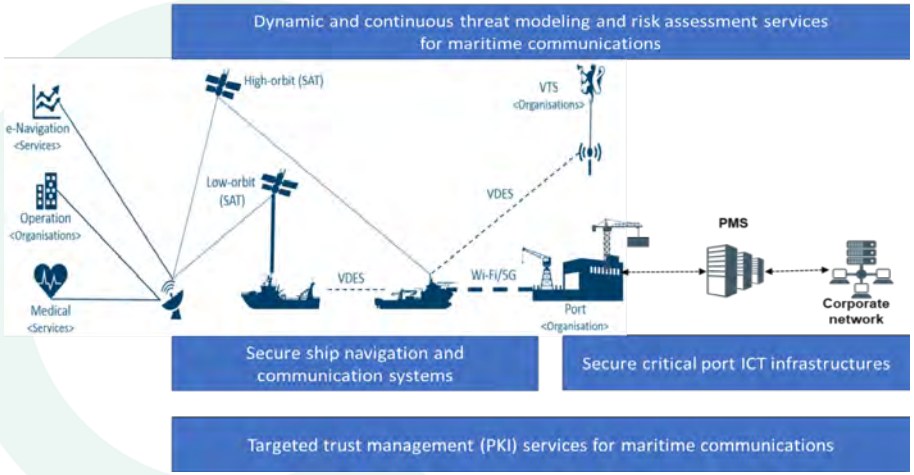
Incident Reporting



To specifically support cybersecurity information data sharing in a bi-directional way, allowing for a centralised or a de-centralised approach, i.e., a peer-to-peer approach.

To develop a platform that enables organisations or their entities to report incidents according to the different procedures and methods specified by applicable laws and regulatory bodies, such as PSD2 and the ECB (European Central Bank) Cyber Incident Reporting Framework.

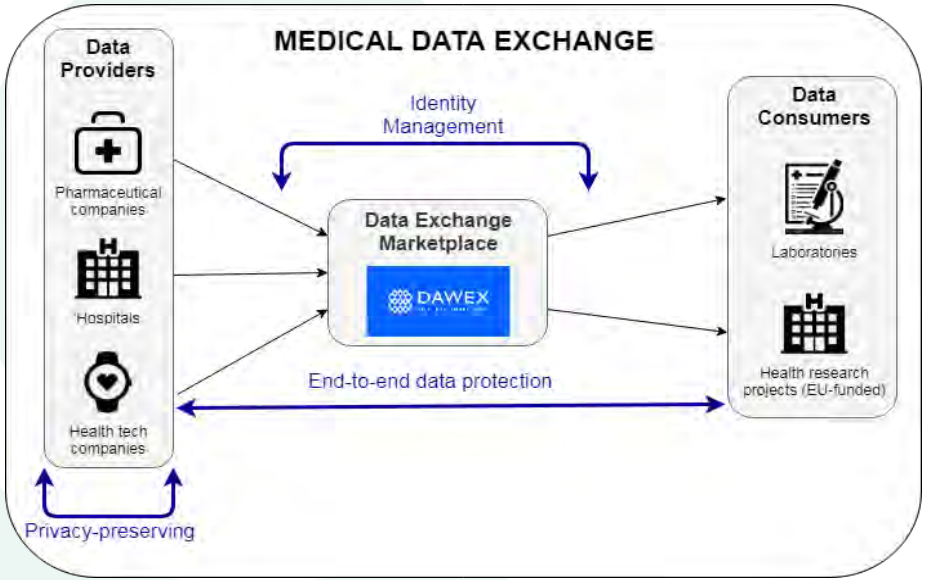
Maritime Transport



To identify the current cybersecurity challenges of the maritime sector and design and develop a threat management system capable of continuously managing cybersecurity threats against Internet-connected critical cyber infrastructures in the maritime sector.

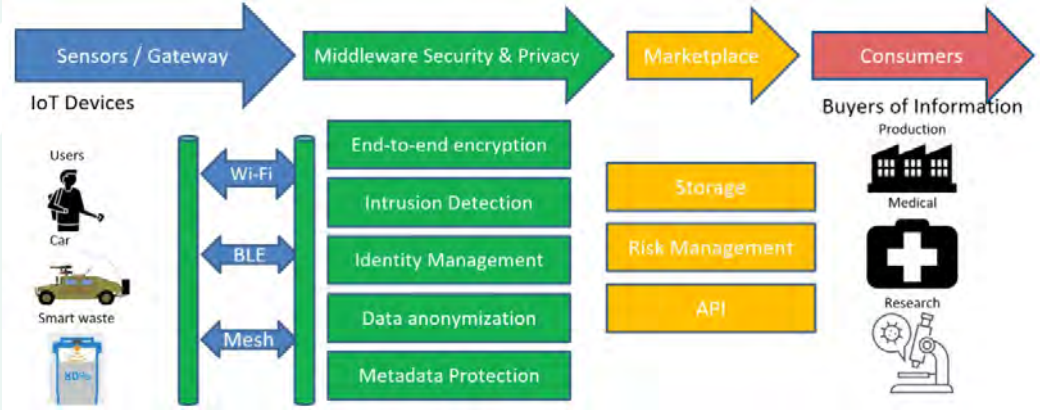
To develop several advanced threat models for the maritime environment, able to capture and assess new threats that may involve the whole maritime sector ecosystem and to assist the relevant stakeholders, such as ship operators and port operators, to be in line with the related regulations and best practices

Medical Data Exchange



To integrate and validate in a realistic environment the research outcomes on the cybersecurity and sensitive and personal data protection for medical data sharing, enhancing the multi-lateral trust among stakeholders generating and consuming data in the medical business sector. through the DAWEX data marketplace platform, improving its trustworthiness and creating new business opportunities as a result.

Smart Cities

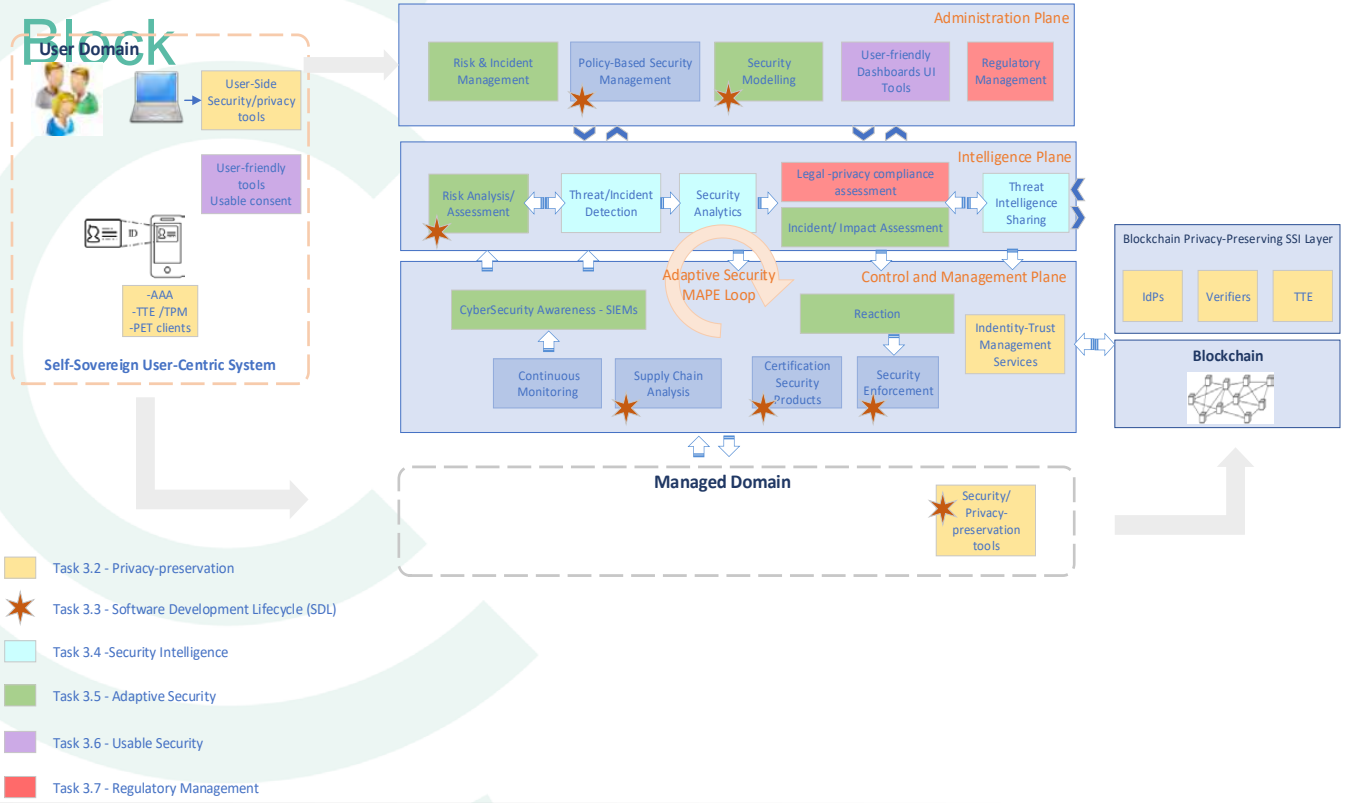


To connect the cybersecurity challenges of smart cities to "create an open smart city market based on the needs of cities and communities"

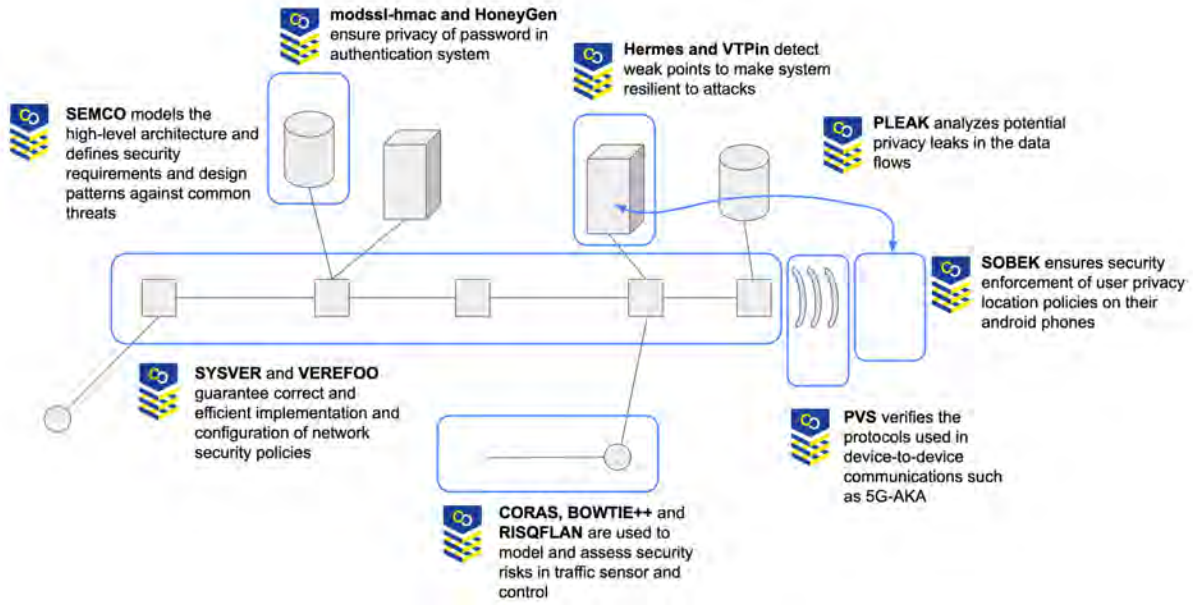
A dedicated environment enabling ideas, needs, best practices and lesson learned exchanged among cities and cities' stakeholders

To ease the identification, uptake, collaboration and deployment of cybersecurity services for smart cities, including novel business models to pool resources and decrease the individual cost supported by each city.

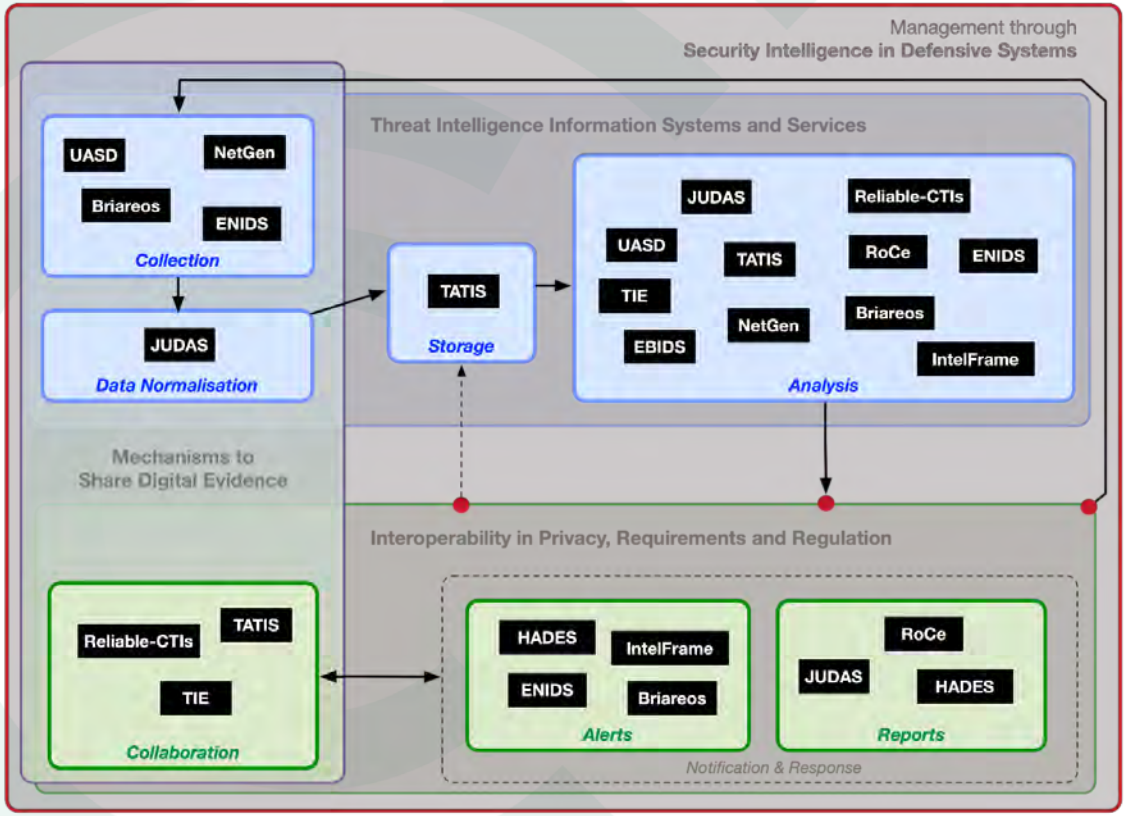
WP3
Global Architecture and Tasks Block



Assets in the Software Development Lifecycle (Task 3.3)



Assets in a Security Intelligence System (Task 3.4)



TIE: *Threat Intelligence intEgrator* **(ATOS)**
Briareos (C3P)
UASD: *Unautorized App Storage Discovery* **(CNR)**
EBIDS: *Ensemble Based Intrusion Detection System* **(CNR)**
IntelFrame: *Intelligent Machine Learning-based Intrusion Detection* **(DTU)**
TATIS: *Trustworthy APIs for Enhanced Threat Intelligence Sharing* **(KUL)**

NetGen (POLITO)
JUDAS: *JSON Users and Device Analysis Tool* **(UMA)**
HADES: *Automatic analysis of malware samples* **(UMA)**
Reliable-CTIs - *Reliable Cyber-Threat intelligent sharing* **(UMU)**
ENIDS: *Edge Network Intrusion Detection System* **(UNITN/FBK)**
RoCe: *Risk of Compromise estimation* **(UNITN)**

Pillar III: Open Tools and Infrastructures for Certification and Validation (WP7)

- Cyber Sandbox Creator
  - Virtual lab for open-source tools education and research (D7.2)
  - A lightweight virtual lab environment for cybersecurity education, testing and certification.
    - Goal: run the lab environment at a single PC using state-of-the-art free and open-source components and best practices.
    - Actively developed (version 2.0.0) and fully open-source released (version 1.0.1), including wiki and documentation.
  - Hands-on teaching: Masaryk University (CZ) – 200+ students, Slovak University of Technology (SK), The Hague University of Applied Sciences (NL)
  - Sandbox development for KYPO Cyber Range Platform (CONCORDIA)
- SECCERTS: Tool for processing of security certification reports (CC, FIPS)
  - Analysis of FIPS140-2 & Common Criteria certificates
  - Additional functionality for vulnerability assessment (affecting/affected)
    - Example: Austrian eHealth cards report affecting Estonia's EstID (ROCA vulnerability)
  - Presentation internally and also at the 2021 Spring RedHat Research Day

Pillar III: Education, Certification, and Standardization (WP6)

- Design of education and professional framework (D6.3)
  - 4 (new) job profiles defined in border-control use case → long-term cybersecurity careers
  - 2 job profiles adapted from the ECSO Minimal Reference Curriculum
  - Assessment of these 6 new profiles upcoming: fellow pilots & ECSO will be invited
- 2nd Flagship challenge exercise
  - Held January 2022, both a (new) open track and an internal track
  - **Open track** ("analysts activity")
    - 43 participants from companies and universities beyond CS4E, submitting 522 individual results
    - In/correct submissions ratio and response times show high variance in experience of participants
    - Very active participation → **reveals pushing need for these cybersecurity exercises in the IT sector**
  - **Internal track**
    - 19 participants, prepared with Cyber Sandbox Creator, again 100% positive feedback
    - Gender proportion (6 women = 24% female participants) matching current state of IT sector

Convergence 2020 documentation on cybersec4europe.eu

- Organised by the four pilots
  - **CyberSec4Europe**
  - **CONCORDIA**
  - **ECHO**
  - **SPARTA**
- Keynotes
  - **Rasmus Andresen, MEP**
  - **Wojciech Wiewiórowski, EDPS**
  - **Andreas Könen, EU German Presidency**
  - **Khalil Rouhana, EC**

Upcoming events
Save the Date(s)

29-08 – 02-09	**17th IFIP Summer School On Privacy And Identity Management 2022**
16 September	Evening event on occasion of the CyberSec4Europe General Meeting (Brussels and possibly hybrid)
01-12 – 02-12	**CyberSec4Europe Summit Conference**

More at https://cybersec4europe.eu/events/

Selected deliverables

D2.2	Internal Validation of Governance Structure
D2.3	Governance Structure v2.0
D3.12	Common Framework Handbook 2
D3.13	Updated version of enablers and components
D3.14	Cooperation with Threat Intelligence Services for deploying adaptive honeypots
D3.15	Proactive approaches for secure software development
D3.16	Security Requirements And Risks Conceptualisation
D4.4	Research and Development Roadmap 2
D5.4	Requirements Analysis of Demonstration Cases Phase 2
D6.3	Design of Education and Professional Framework
D6.4	Flagship 1
D7.2	Virtual lab for open-source tools education and research
D8.2	Project Standards Matrix (together with the Standards Matrix)
D9.8	Policy Recommendations
D10.2	CONVERGENCE 2020 Conference Documentation

All at https://cybersec4europe.eu/publications/deliverables/

EU Strategy and Investments in Cybersecurity

Martin Übelhör

Challenges in Cybersecurity

- Geopolitical contest over cyberspace
- Large increase in cybercrime
- Supply chain security (e.g. 5G)
- Expanding attack surface (e.g. IoT; hospitals, vaccine distribution)
- Threat from quantum computing breaking “legacy” crypto
- Advent of AI
- Skills shortage; awareness
- Capacity building, resilience
- Vulnerability of smaller organisations, SMEs
- Info sharing, joint analysis and response
- Commercialisation of R&D
- Uptake
- Single market
- Dual use
- (…)

THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020); 3 instruments (regulatory, investment, policy initiatives) 3 to three pillars

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

Revised Directive on Security of Network and Information Systems (NIS 2)

Cybersecurity Shield (CSIRT, SOC)

Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS

Competence Centre and Network of Coordination Centres (CCCN)

EU workforce upskilling

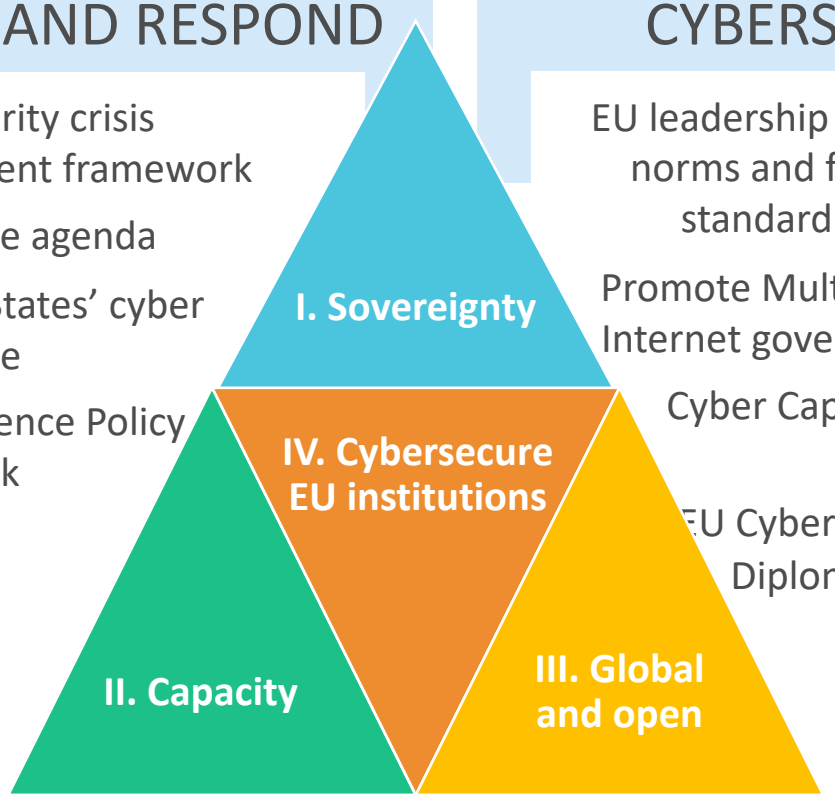
BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

Cybersecurity crisis management framework

Cybercrime agenda

Member States' cyber intelligence

Cyber Defence Policy Framework



COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

EU leadership on standards, norms and frameworks in standardisation bodies

Promote Multi-Stakeholder Internet governance model

Cyber Capacity Building Agenda

EU Cyber Dialogue and Diplomacy Network

European Commission

A EUROPEAN CYBERSECURITY TECHNOLOGY & INNOVATION ECOSYSTEM

EU Funding, Capacity-building, Community-building

European Commission

Cybersecurity knowledge and capabilities in the EU

The EU represents 26% of the global cybersecurity market

More than 660 expertise centres registered in the mapping of cybersecurity centres of expertise

CYBERSECURITY PRODUCTS AND SOLUTIONS

Up to 30% of the European demand is met by companies headquartered outside the EU.

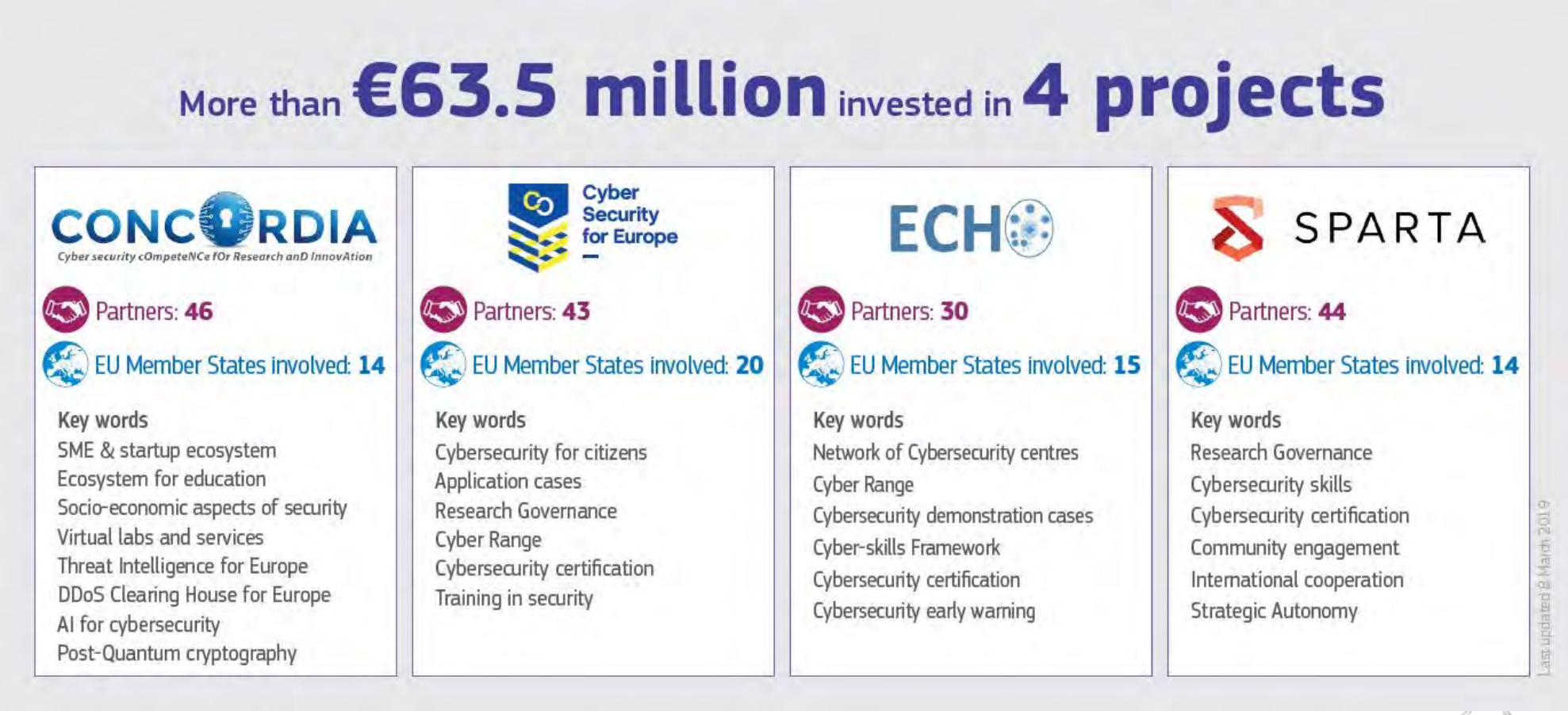
Europe is the location for the corporate headquarters of only 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas, 7% for Israel and 4% for Asia.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO has +/- 250 members

European Commission

EU pilots helping to prepare the European Cybersecurity Competence Network



European Commission

THE EUROPEAN CYBERSECURITY INDUSTRIAL, TECHNOLOGY AND RESEARCH COMPETENCE CENTRE & NETWORK

Network and Community

Mission, Objectives and Implementation

EU Cybersecurity Competence Centre and Network

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres (NCCs):

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- May receive funding, may pass on financial support
- One NCC per Member State

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors
- Provides input to the activities of the competence centre to the work programmes

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

MISSION	OBJECTIVES	IMPLEMENTATION
Strategic autonomy and global competitiveness	Cyber resilience, capabilities, knowledge and infrastructures	Strategic Agenda for research, innovation, deployment
Technological capacities and capabilities	An inclusive, resilient stakeholder ecosystem	EU funding programmes, voluntary national contributions
	Promoting research, innovation, deployment	Cooperation, Coordination; Network and Community

European Commission

Network of National Coordination Centres

- One NCC per Member State, nomainated by the Member State
- May receive EU funding
- May pass on EU funding
- Objective: national capacity building and link with existing initiatives
- Contributes to strategic tasks
- Promotes participation in cross-border projects and in cybersecurity action
- Provides technical assistance
- Coordinates the national, regional and local levels
- Asses requests by entities in the Member States
- Promotes cybersecurity educational programmes
- Advocates involvement of relevant entities

EU Cybersecurity Competence Centre and Network – tasks

Strategic Tasks

- Agenda-monitoring and priority-setting
- Technical and strategic support to industry and SMEs
- Expert advice to the Member States upon request
- Use of research results
- Support cooperation between relevant Union institutions
- Coordination of national centres through the network

Implementation Tasks

- Administration of the Network and the Community
- Deployment of ICT Infrastructure
- Annual work programme, expert advice to the EC
- Cooperation with the European Digital Innovation Hub
- Synergies of civilian and defence spheres
- Promotion of the CCC, CCN and the Community

Competence Community

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors which acts cross-sectoral and cross-department
- Management of the Community has been prepared through the pilots CONCORDIA, ECHO, SPARTA and CyberSec4Europe
- The Centre, Network and Community should help to advance and disseminate the latest cybersecurity products and services
- Exchanges with the Centre on developments in cybersecurity
- Provides input to the activities of the competence centre to the multiannual work programme and to the annual work programme
- Splits up into working groups for regular dialogue
- Supports stakeholders at their request, public-private coordination

European Cybersecurity Atlas – the digital knowledge management platform

- Enables knowledge management activity related to cybersecurity research
- Provides an up-to-date overview of stakeholders and outcomes of research projects
- Indicates pressing cybersecurity research areas which guides effective investment across the EU
- Collects of cybersecurity knowledge and establishes a cybersecurity taxonomy
- Facilitates collaboration among researchers, industry, practitioners on the national and European level

Governing Board: Working Groups

- WG1: Community membership and registration
- WG2: NCCs reference manual (NCC services catalogue)
- WG3: NCC network functioning
- WG4: Strategic Agenda (SRIA)

2021-2027 proposed EU cybersecurity funding sources

Digital Europe Programme

Horizon Europe

Co-investment by industry on project basis

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-investment by Member States (voluntary)

Network of National Coordination Centres

Capacity building projects

Collaborative R+D projects

European Commission

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

The ECCC 'Agenda': process and priorities

Proposed priority areas for cybersecurity capacity support

1. Enhance processes and tools for **risk management** and the **management of cybersecurity information**
2. Secure and resilient **hardware and software systems**, in particular for critical infrastructure protection
3. Enhance the **industrial and market uptake** of EU cybersecurity research and innovation results
4. Advanced **cyber security skills**: higher education and professional training
5. Foster the **human and social dimension of cybersecurity,** and increase awareness

The “Agenda”

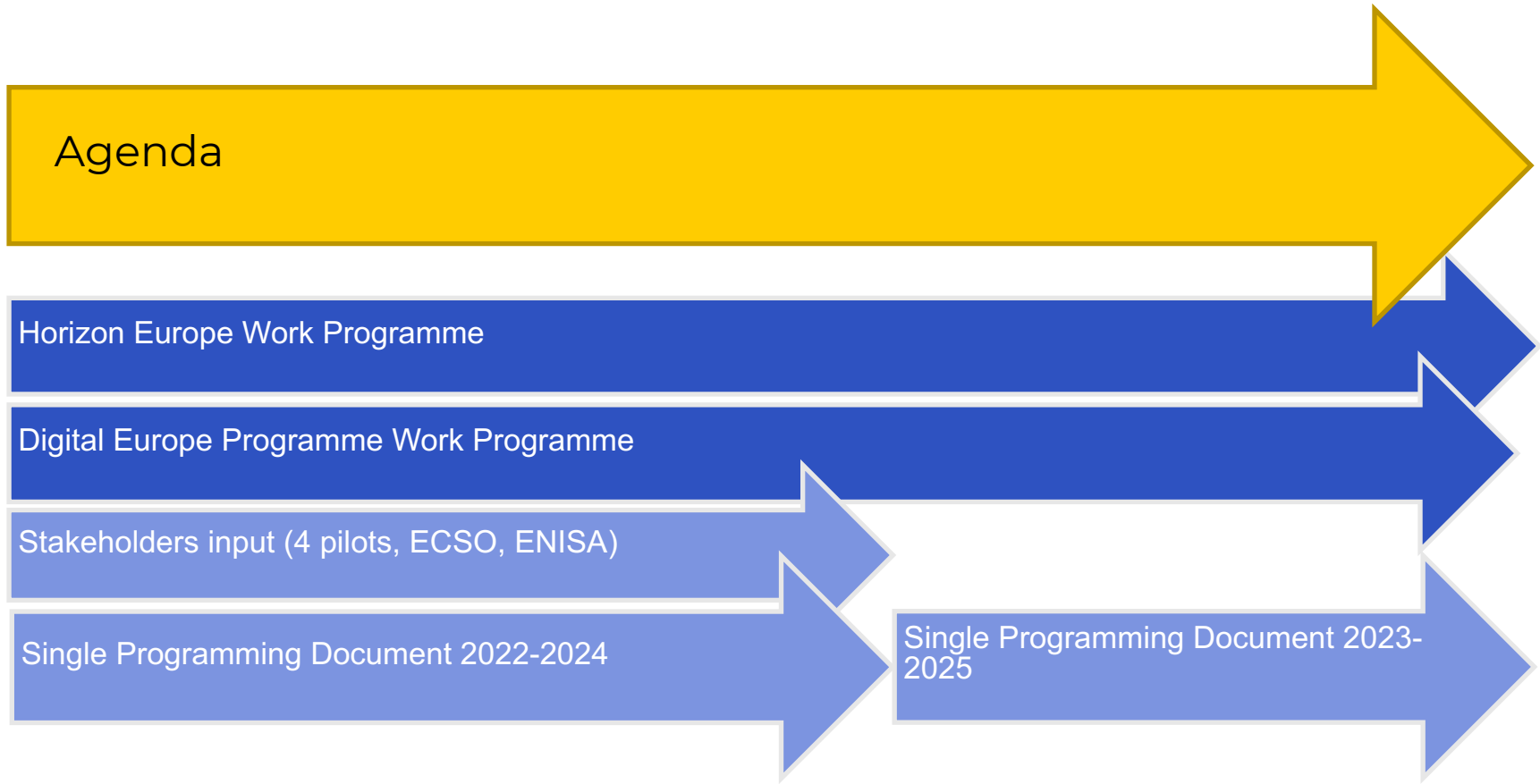
- A comprehensive and sustainable cybersecurity industrial, technology and research strategy
- sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector
- sets out strategic priorities for the Competence Centre’s activities
- (…)

(Regulation 2021/887, Article 2(8))

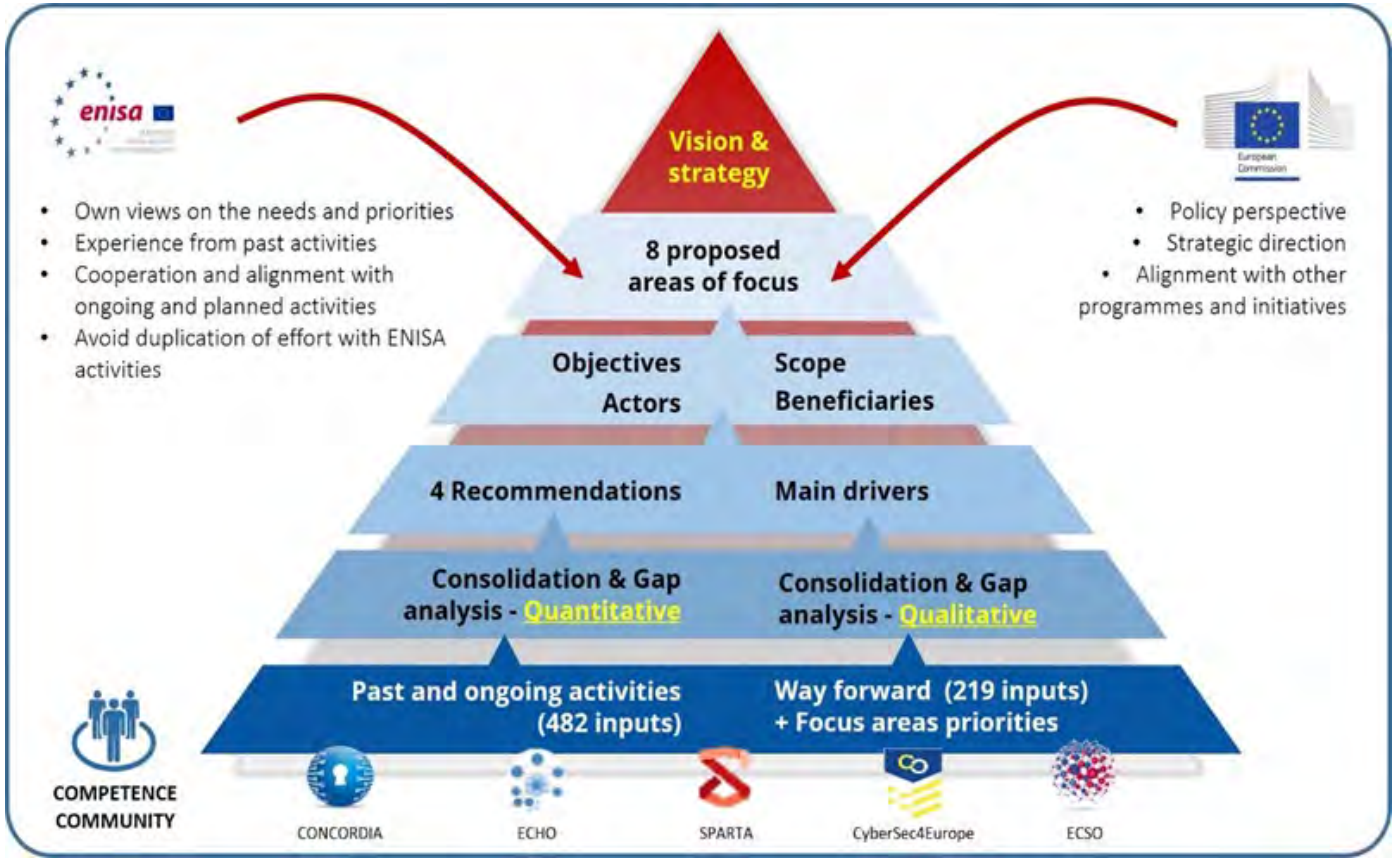
Tools and Assets

- **EU Programmes**
  - Horizon Europe programme
  - Digital Europe programme
  - Recovery and Resilience Facility
  - European Structural and Investment Funds
- **Joint Actions**, i.e. funding actions contained in the ECCC work programme, which are financed jointly by one or more Member States and the Union
- **Funding modalities:** Grants, Procurement, Prizes, procurement of innovative goods and services, etc...)
- Central management by the **ECCC/EC,** or in collaboration with **NCCs (cascading funding)**
- Approaches: **Local, regional, national, pan-EU**
- ECCC projects for **collaboration in the Competence Community**

The ECCC 'Agenda': process



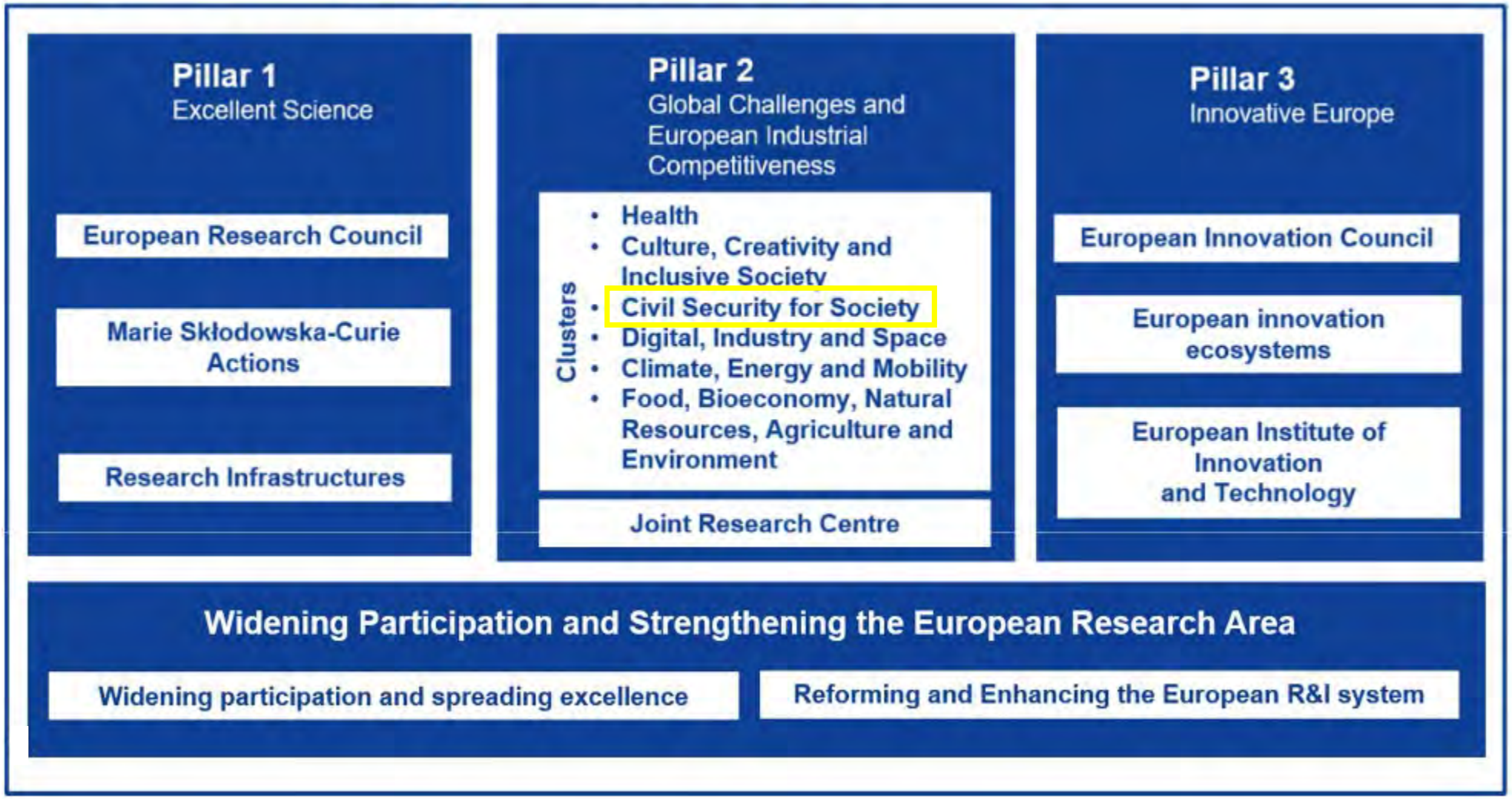
Consultation process so far



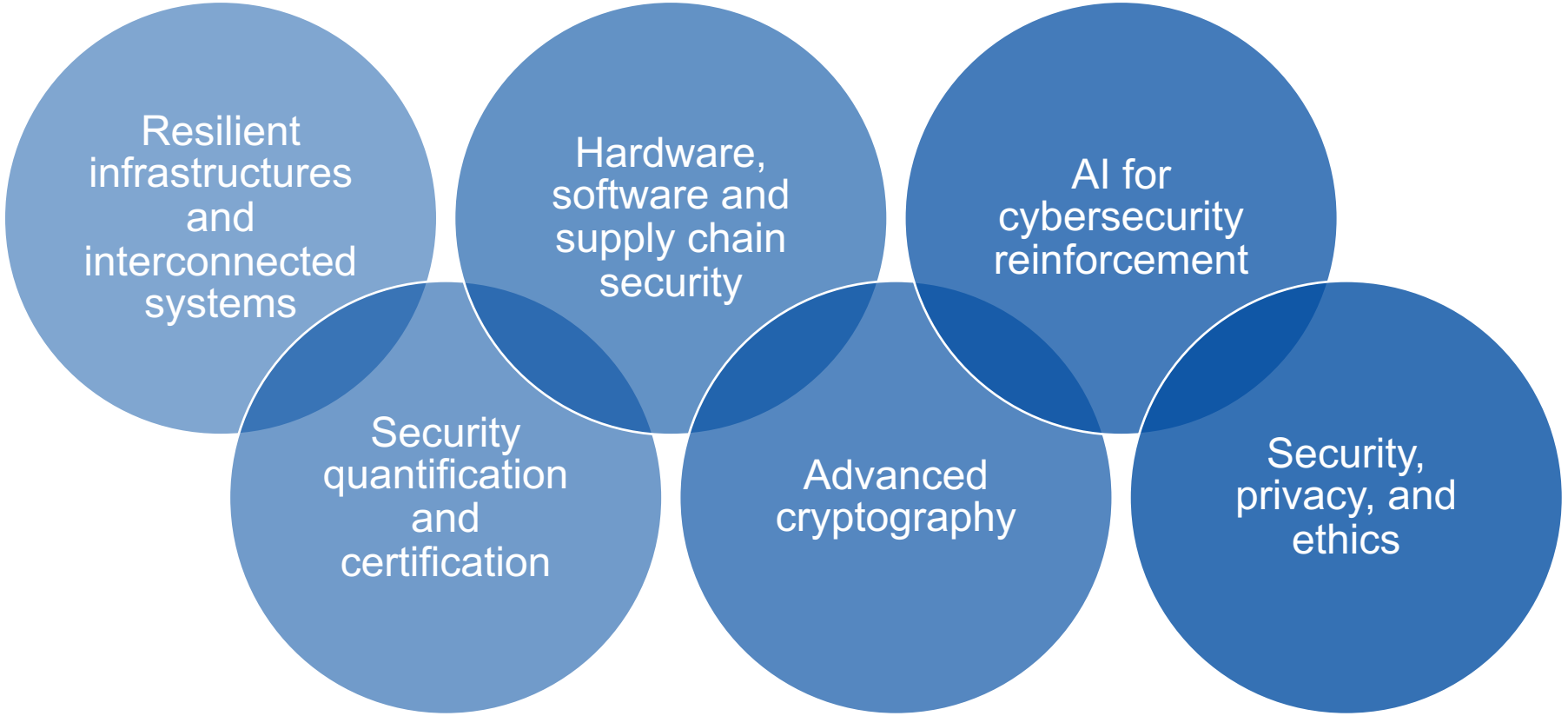
Funding priorities 2021-22

Digital Europe and Horizon Europe programmes

Horizon Europe - Structure



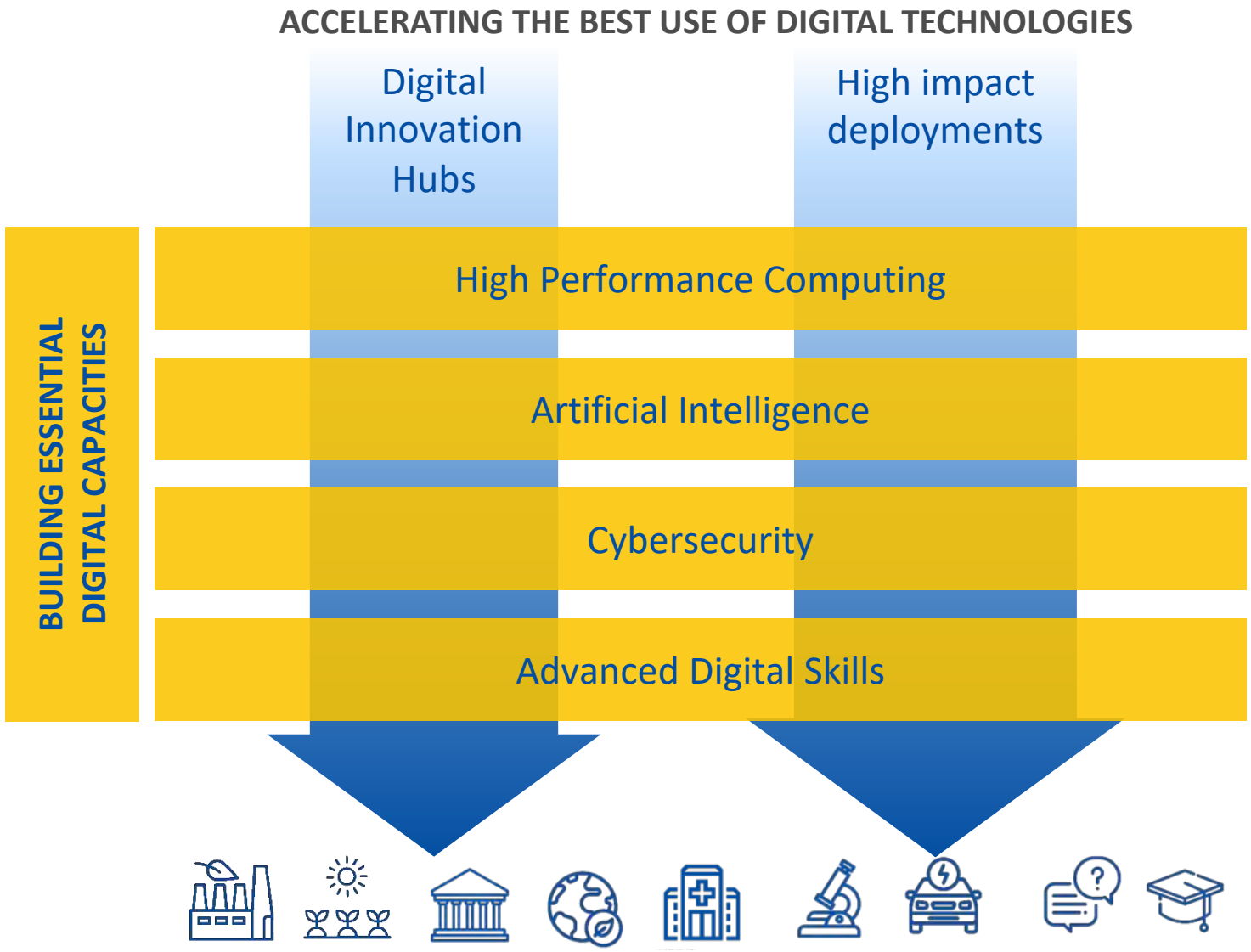
Horizon Europe – Work Programme 2021-22 (135m EUR)



European Commission

Horizon Europe – Work Programme 2021-22: Topics	Budget in mEUR	Call window
Secure and resilient digital infrastructures and interconnected systems	**42**	
Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures	21	2022
Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity	21	2021
Hardware, software and supply chain security	35	
Trustworthy methodologies, tools and data security “by design” for dynamic testing of potentially vulnerable, insecure hardware and software components	17.3	2022
Improved security in open-source and open-specification hardware for connected devices	17.7	2021
Cybersecurity and disruptive technologies	22	
Transition towards Quantum-Resistant Cryptography	11	2022
AI for cybersecurity reinforcement	11	2021
Smart and quantifiable security assurance and certification shared across Europe	18	2022
Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes		
Human-centric security, privacy and ethics	17	2021
Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data		
Total	134	

Digital Europe programme structure



European Commission

Digital Europe work programme 2021-22

- **European Cyber-shield (147m EUR)**
  - EU cybersecurity resilience, coordination and cybersecurity ranges
  - Capacity building of Security Operation Centres (SOCs)
  - Secure 5G and other strategic digital infrastructures and technology
  - Uptake of innovative cybersecurity solutions in SMEs
  - Support to the health sector cybersecurity
- **Support to implementation of relevant EU Legislation (83m EUR)**
  - Network of National Coordination Centres
  - Cybersecurity Community support
  - NIS Directive implementation and national cybersecurity strategies
  - Testing and certification capabilities
- **Secure quantum communication infrastructure (174m EUR)**
- **Skills (incl. Cyber – 166m EUR)**

Thank you

European Commission


1–3 June 2022
Brussels
CONVERGENCE NEXT
Cyber Competence Network

Governance FG
June 1, 2022

Working Together: A Way Forward

Our mission:

- Working together

- Community organization:
providing tools, platforms, and channels for the community to communicate, interact, and cooperate

CyberSec4Europe

Cyber Security for Europe

WP2 “Governance Structure and Design”

Natalia Kadenko
N.I.Kadenko@tudelft.nl

Michel van Eeten
M.J.G.vanEeten@tudelft.nl

Tobias Fiebig
T.Fiebig@tudelft.nl

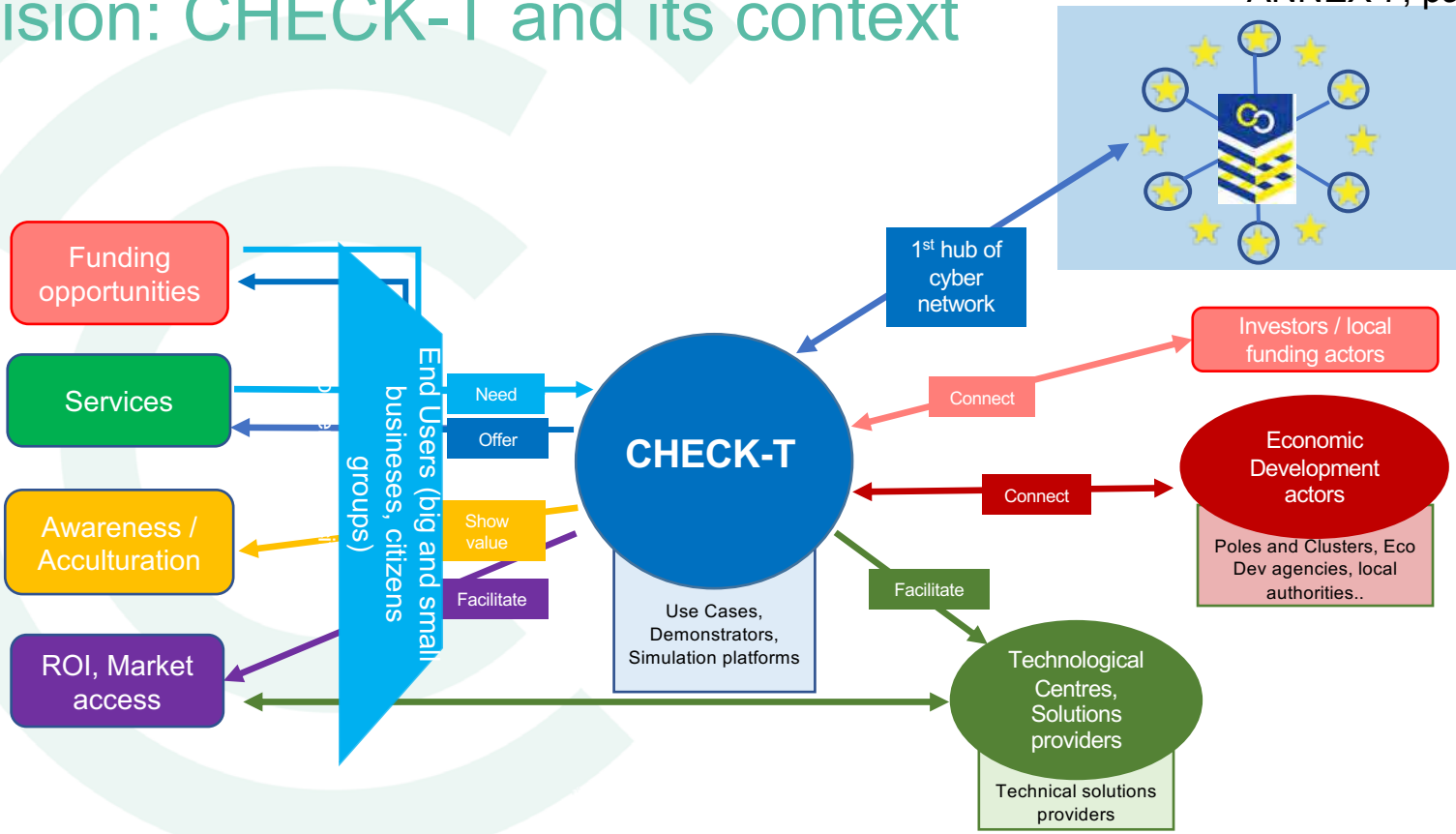
CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

CyberSec4Europe Governance Approach

Governance Challenges for European Cybersecurity Policy: Combining Stakeholder Views and European Objectives

- An outline of possible approaches to cybersecurity governance → bottom-up approach
- Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs)
- Our concept: a flexible organization, accounting for the needs of the local community and creating real added value, combined with requirements for the CHECK establishment
- Promoting the already existing and functioning structures, especially at national level, while actively pursuing the aim of a pan-European community
- Community-level **cybersecurity hubs** which should enable collaboration between industry and academia, bring market security innovations, and help build capabilities in the area
- Shortening the chain between decision-making and existing needs on the ground
- The governance model would benefit from accompanying European cybersecurity funding mechanisms in the next decade to increase funding and investment to build a pan-European community

Vision: CHECK-T and its context



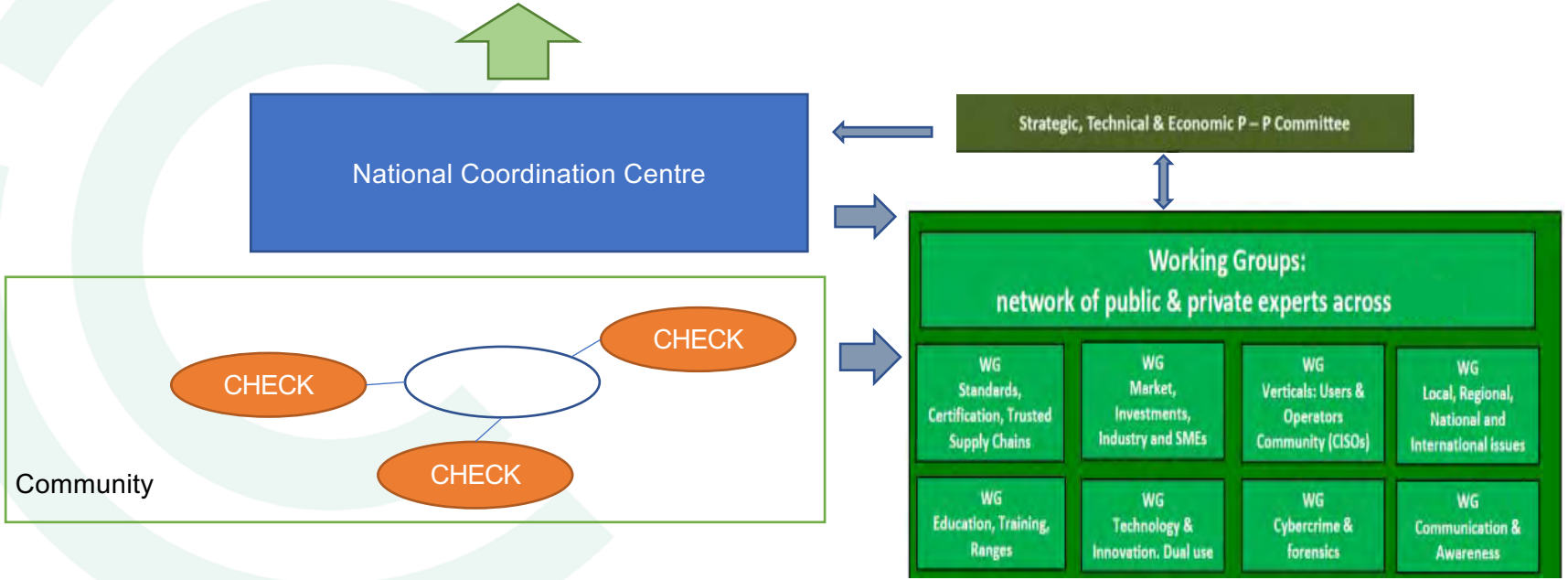
Check-M
Murcia Regional Cybersecurity Innovation Unit

- Initial work at the Region of Murcia in Spain has been launched by the University of Murcia and the regional government with the idea of creation of a Regional Cybersecurity Innovation Unit
- The objective it is to establish it as a reference center in cybersecurity within the framework of the Agenda for the Digital Transformation of Administration and Society in the Region of Murcia to promote the role of cybersecurity and its deployment in the field of Society of Knowledge, and the interrelation with similar entities at national and international level
- Based on initial interviews and contacts with the General Director of Strategy and Digital Transformation of the Murcia Government, it has been defined as a first approach of the objective of this Innovation Unit

Objectives

- Promote **collaboration** between organizations and entities in the Region of Murcia to raise awareness, disseminate and promote cybersecurity in the administration, in academia and in society in general
- Generate **synergies** between all the organizations involved for the development of collaborative projects, as well as to promote the development of new initiatives
- Create a **space for discussion** and generation of socio-ethical-legal knowledge in the area of cybersecurity
- Raise **public awareness** of the importance of cybersecurity through demonstration spaces, workshops and collaborative events

- Bottom-up approach *WG topics defined by interest from the community)
- Common interest and strategic areas (e.g. research, innovation, and capacity building in cybersecurity)
- Different focus: regional, national, sectorial
- The complexity of having large number of members under an umbrella organisation could be overcome by delegation to CHECKs, as well as sharing of the funds, tasks or risks



CHECK-NL

- **ACCSS**

- Hub of the network of all cyber security scientists in the Netherlands
- Gateway for public and private parties who want to find the right cyber security researchers in the Netherlands and conduct joint research and innovation
- Representative of cyber security scientists in the Netherlands to highlight shared positions and to provide input in policy processes where expertise on cyber security is required

- **Dcypher**

- Cybersecurity cooperation platform for research and innovation in the Netherlands
- Brings public, private parties and knowledge institutions together as well as resources and expertise to effectively engage in cybersecurity education, research, innovation for the development of concrete applications
- Stimulating knowledge development in the cybersecurity domain to give a significant impulse to the cybersecurity industry and to support the government in its role as launching customer
- Bottom-up, thematic, across Technology-Readiness Levels
- "**Looking for government support? Talk to us!**"

- The Netherlands Enterprise Agency (RVO) is the host of both the Dutch NCC and dcypher

Building The Network

Cyber Security for Europe —

43 partners

40+ associates

16 countries

Cyber Security for Europe Associates

Cyber Security for Europe Friends

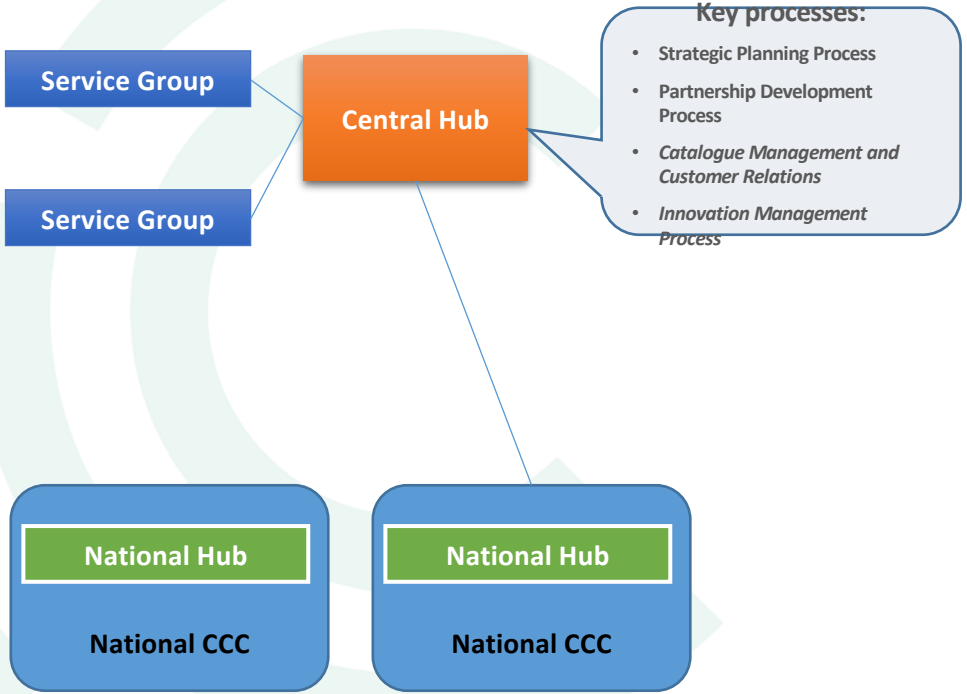
- Ten panel discussions
- Five Insights webinars
- Almost 100 published articles
- 66 openly available deliverables
- High focus on citizen-centricity and developing SME & micro-SME awareness

Innovative Governance Policy

- Bottom-up approach
- An auspicious environment for community-level research, innovation, and capacity-building in cybersecurity, shortening the chain between decision-making and existing needs on the ground
- Introducing a novel network of Community Hubs of Expertise in Cybersecurity Knowledge (CHECKs), an environment for community-level research, innovation and capacity building in cybersecurity

ECHO

ECHO's future Governance model



Progress and key decisions taken to secure ECHO sustainability:

- **CNO governance model designed and approved within ECHO –** based on extensive work to define needs and objectives, develop and assess alternatives, design process and organization, develop implementation and transition plan
- **Decision to proceed with "bottom-up" approach within last project year –** establish National Hubs and Service Groups. Pilots under way, to be completed by end 2022:
  - Pilot National Hub in Bulgaria (NH-BG)
  - Pilot Service Group Governance Consultancy Services (E-GCS)
- **Test and refine key processes and setup** – in the context of pilot NHs and SGs, to prepare for final ECHO Network decisions by end of the project

E-GCS mission is to support the sustainability of cybersecurity community in EU

E-GCS Services catalogue

Provide the solution

1. Evaluation (audit) of existing CNOs
2. Design of a CNO and its governance model
   - Needs & Objectives
   - Development of Alternatives, Assessment & Selection
   - Business Model canvas
   - Process and Organizational Design
3. Maturity Assessment of the Governance Model

Ensure implementation

1. Transition/ Change Management
   - Simulation games
   - ADKAR for Processes & Organizational elements
2. Accreditation of existing and potential partners
3. Training in governance/management of CNOs

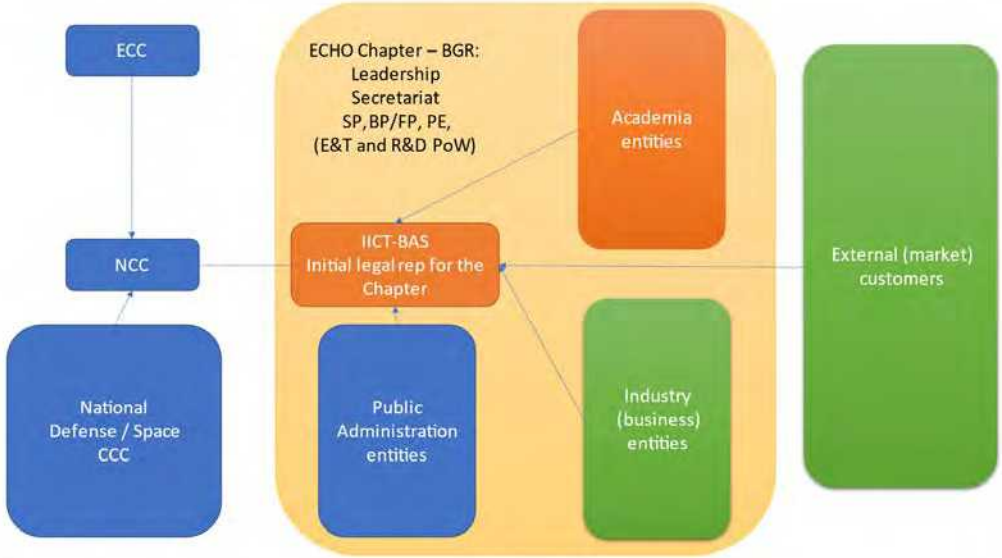
Manage relationships

1. Customer (Stakeholder) Relationship Management
2. Satisfaction assessment

Progress to set up and ensure sustainability of E-GCS:

- **E-GCS developed and tested methodology** while working on the ECHO Governance Model – included in first draft of E-GCS Services Catalogue. E-GCS exploitation strategy now being developed
- **The methodology is now being applied to establish two pilot structures** within ECHO – the E-GCS itself and NH-BG
- E-GCS is developing its Services Catalogue with the aim **to extend to potential customers and become customer-funded**:
  - Internal customers: other ECHO assets, ECHO National Hubs and Central Hub to be established
  - National-level customers, such as national authorities and policy-makers, National Coordination Centers, local cybersecurity and other technology communities
  - EU-level customers, such as cybersecurity and other technology communities and organizations, European Cybersecurity Competence Center, Cybersecurity Competence Community

Pilot National Hub in Bulgaria – E-GCS initiates the transition to a sustainable ECHO CNO after the end of the project



Progress to set up and ensure sustainability of pilot National Hub – a test case for E-GCS services:

- **National Hubs implementation kicked off in March**
- **Pilot in Bulgaria under way**, aimed to:
  - start with bilateral agreements of current ECHO partners and participants. E-GCS will facilitate the decision-making process, aims to agree on NH-BG mission and key setup parameters by Autumn 2022
  - build on the levels of Awareness and Desire recorded
  - Showcase the structure and processed on National Hub level, as well as on Service Group level

Partners

Project Coordination:
Royal Military Academy of Belgium (Wim Mees)

Project Management:
RHEA System S.A. (Matteo Merialdo)

- 16 Millions budget
- 4 years (started Feb 2019)
- 30+14 partners (+2 in the process of being signed) – academia, industry, SMEs
- 13 existing competence centres
- 19 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

CONCORDIA

How to Build, Achieve & Sustain Trusted, Hybrid Interconnected Ecosystem of Ecosystems

Arthur van der Wees, LLM

Consortium Partner, DPO and Chair Ethics Committee to CONCORDIA

Managing Director, Arthur's Legal, Strategies & Systems

Expert Advisor to Public & Private Sector (Digital Ecosystems, Data, IoT, AI, Robotics, Cybersecurity, Trust, Assurance & Accountability)

Member of EU Alliance for Industrial Data, Cloud & Edge, Souvereignty Taskforce & Cybersecurity Taskforce Lead

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

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

Two (2) Brief Governance Queries

Based on the **Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**, and the work to date by CONCORDIA and its partners:

> *Cybersecurity is an issue local, national and cross-border issue of **common interest of the EU**, and it needs to make sure that it has the **capacities to secure its economy, democracy and society**. For Europe to be prepared it needs to have a **thriving cybersecurity ecosystem**, including industrial and research communities.*

1. **Do we Really Know and Understand the Ecosystem & Communities?**
2. **For these to Thrive, How to Team up, Share and Act?**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Two (2) Brief Governance Queries

Based on the **Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**, and the work to date by CONCORDIA and its partners:

> *Cybersecurity is an issue local, national and cross-border issue of **common interest of the EU**, and it needs to make sure that it has the **capacities to secure its economy, democracy and society**. For Europe to be prepared it needs to have a **thriving cybersecurity ecosystem**, including industrial and research communities.*

1. **Do we Really Know and Understand the Ecosystem & Communities?**

2. **For these to Thrive, How to Team up, Share and Act?**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

How to Organise the European Cybersecurity Industrial, Technology and Research Competence Centre, the Network of National Coordination Centres, the EU Cybersecurity Community, and Digital Sovereign Society at large?

Contextual, Impact-based, Symbiosis of Four Intertwined Main Domains

as mentioned in the ECCC & NCC Network Regulation

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Two (2) Brief Governance Queries

Based on the **Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**, and the work to date by CONCORDIA and its partners:

> *Cybersecurity is an issue local, national and cross-border issue of **common interest of the EU**, and it needs to make sure that it has the **capacities to secure its economy, democracy and society**. For Europe to be prepared it needs to have a **thriving cybersecurity ecosystem**, including industrial and research communities.*

1. **Do we Really Know and Understand the Ecosystem & Communities?**

2. **For these to Thrive, How to Team up, Share and Act?**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

To Share, or Not to Share, that is the Trust Question

Trust and related trustworthiness are always the main enablers, also in any of the cyber/cyber-physical domains, any community and any information sharing. Does one have the appropriate level of trust in the assets, trust in its own competences, trust in the organisations and community involved, trust in the technical systems and trust in the ecosystem at large? The right level of trust both brings the courage, confidence and comfort to engage, and share.

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Trusted Threat Intelligence Sharing

Imagine you want to become a member of a sports team, a musical ensemble, an innovation hub, or interest group, to contribute, learn and otherwise engage.

With that, you want to become part of a certain community, each with its specific habits, codes and rules to set clear expectations of the members of such community as well as protect the interests of both the community and each of the members separately, as well as society and the ecosystems within the community is operating.

Imagine this is possible regarding sharing of threat intelligence **and related trusted experience sharing and engagement.**

Welcome to the world of Trusted Threat Intelligence Sharing,

Based on Trust, and co-powered by a Code of Engagement

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

EXAMPLE | Trusted Threat Intelligence Sharing

Initial Assessment Towards Code of Engagement Trusted Threat Intelligence Sharing

Draft v2022.1

1. What 2. Why 3. Purpose 4. Who 5. Access 6. Where 7. Data Classes 8. Personal Data 9. Data Flow 10. Data Life Cycle 11. Contribution 12. Use 13. Benefits 14. Transparency 15. Security 16. Privacy 17. Accountability 18. Governance 19. [*]	CTI Platform X	CTI Platform Y	Incident Clearing House Z	Ecosystem for Trusted Threat Intelligence & Code of Engagement
1. What	This is a Challenging Problem Set There is No One Solution There is No One Technical Fixture There is No One Centralised Fixture This is about Working Together, as Teams To Achieve Outcomes. This is a Team Sport			The focus of this Ecosystem for Trusted Threat Intelligence will be on three core actionable components: 1. **CTI Platform X** 2. **CTI Platform Y** 3. **Incident Clearing House Z** This focus will give the ability to jointly develop, live-pilot, iterate, improve and optimize with these three intelligence sharing platform a dynamic Code of Engagement (CoE) including without limitation its data- & impact-centric governance, organising each of these core components in general, and any specifics in particular. The CoE is intended to inform, guide, facilitate oversight, insights, trust, expectations, and understanding, and to arrange the various relationships and data flows, and set a principle-based intelligence sharing and collaboration framework to cater for trust and boost engagement & sharing. The CoE is deemed to be designed and run as a runtime oOS: an organisational living and learning operating system, which will be securely patched, optimized and upgraded with new features same as securely managed secure software.
2. Why				
3. Collective Purpose				
4. Who				
5. Access				

CONCORDIA

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Arthur van der Wees

Arthur's Legal, Strategies & Systems
vanderwees@arthurslegal.com

www.concordia-h2020.eu
contact@concordia-h2020.eu

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SPARTA

SPARTA
GOVERNANCE

SPARTA GOVERNANCE

Florent Kirchner, Thibaud Antignac (CEA)
Dirk Kuhlmann (Fraunhofer ISI)

CONVERGENCE 2022

@sparta_eu

sparta.eu

June 2022

GOVERNANCE OBJECTIVES:
STRUCTURES & PROCESSES FOR MISSION-ORIENTED R&I

- **Setup** the processes and governing instances for Cybersecurity Competence Networks
  - Hybrid organization mixing technical and non-technical activities
  - Mechanisms for continuous improvements and extensions

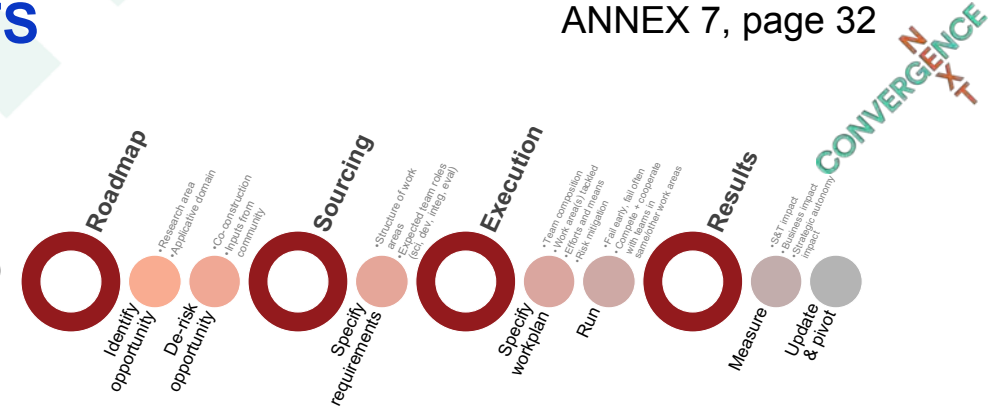
- Animate the **strategic direction at board and working group level**
  - Ensure all stakeholder groups represented interact
  - Align efforts towards common objectives

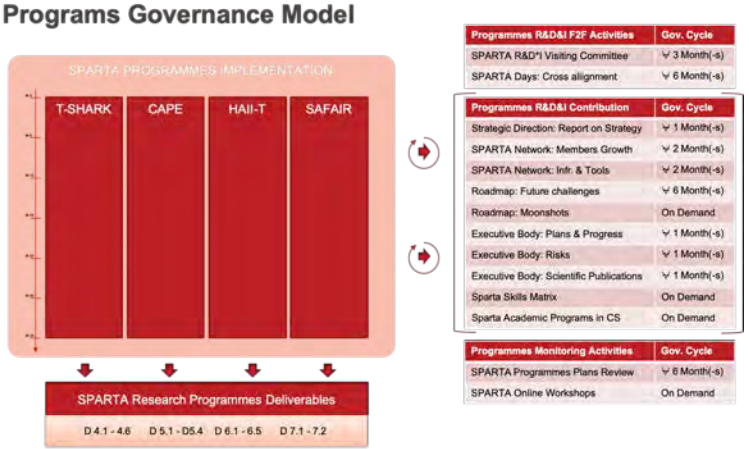
- Ensure **coordination and synchronization**
  - Look for mutualisation of efforts,
  - Comparison and sharing of practices
  - Transversal consistency of hybrid objectives

- Continuos **assessment of performance and strategic direction**
  - ECCN and NCCs, along its different dimensions
  - Make **recommendations for alignment**

GOVERNANCE INSTRUMENTS

- **Roadmap instrument**
  - Consolidated, Focus Areas (Pilots/ENISA)
  - Continuous Update (Workshops / Questionnaries)
  - Roadmap Committee and interfaces
- **Partnership instrument**
  - National CCCs, three-tier model
  - Self-selection + Partnership Committee
  - Shared resources
- **Program instrument**
  - EC Calls, coordination at national level
  - Trans-national synergies and interactions
  - Sub- and transnational “cyber regions”
    - Experimental setups
    - Synergies and interactions





GOVERNANCE: GRAVITATIONAL CENTRES

Table 1: Typology of innovation agencies

	Radical innovation Shielded from interference	**Incremental improvements** Embedded in industries	
Targeted objectives	**State-led disruptors** *Radically innovative technological breakthroughs along a narrow, focused approach* Examples: DARPA, ITRI Governance goals: design new domain-specific technologies up to the level of early stage products with key industries	**Directed Upgraders** *Incremental innovation mobilizing resources around a relatively narrow range of industries and activities, facilitating large-scale change* Examples: A*Star, CORFO Governance goals: steer technological development, attract investments in key sectors	Mission-oriented and prize- driven innovation Significant resources Targeted technology fields
Wide-ranging objectives	**Transformation enablers** *Radically innovative, large number of small-scale experiments* Examples: OCS, Sitra Governance goals: develop clusters of innovative, high-productivity, research-intensive enterprises	**Productivity facilitators** *Small-scale, incremental product and process innovations across a wide range of established industries* Examples: GTS Institutes, IRAP Governance goals: creating local networks and organizing R&D communities	Delegated innovation objectives and R&D Modest resources Maximized application fields

?

- **Priorities for operational governance of research and innovation**
  - Mission-oriented research and innovation
  - Strategic Autonomy
  - Public procurement
- **Mind the blind spots! Cyber-regions, civic society, global cooperation (including open source)**

Summary: way forward for us all

- Conducted extensive work on identifying stakeholders needs
- Mapping and understanding the community: four pilots + ECSO, continuous updates, surveys…
- Ways of (formal) community involvement
- Cyber regions, regional/sectorial hubs
- Involving underrepresented actors
- Grassroots initiatives
- Identifying common objectives
- Long-term strategic cooperation and coordination
- Trust
- Putting flesh on bare bones: What comes next?

Łukasiewicz
Instytut Technik
Innowacyjnych
EMAG

EARTO
IMPACT
DELIVERED
EARTO Working Group
Security & Defence Research

Łukasiewicz-EMAG for Cybersecurity

Artur Kozłowski D. Sc. Institute Professor

Director of the Łukasiewicz Research Network - Institute of Innovative Technologies EMAG

1 June 2022

EARTO Working Group
Security & Defence Research

Founded in 1999, EARTO (European Association of Research and Technology Organizations) promotes RTOs and represents their interest in Europe. The EARTO network counts over 350 RTOs in more than 20 countries. EARTO members represent 150.000 of highly-skilled researchers and engineers managing a wide range of technology infrastructures.

The Security & Defence Research Working Group has over 60 representatives from 31 RTO's coming from 18 countries,

The EARTO Working Group Security and Defence Research (WG S&D) has the ambition to contribute to the European Cybersecurity Competence Center & Network being a strong and stable representation of the research community and an important actor in the security and defence innovation eco-system. EARTO WG S&D members are already involved in three out of the four pilot projects, namely CONCORDIA, SPARTA and CyberSec4Europe.

These projects will end at some point in time and EARTO, being a sustainable network not depending on project life-times, can support in maintaining and furthering their results.

The EARTO WG S&D includes members with expertise in cybersecurity who are not part of any of the four pilot projects. This means we can be complementary to the current project-related networks. These members are able to provide valuable input into the future programming as well.

Łukasiewicz
EMAG

Łukasiewicz Research Network,
Third largest research network
in Europe

26 institutes

12 cities

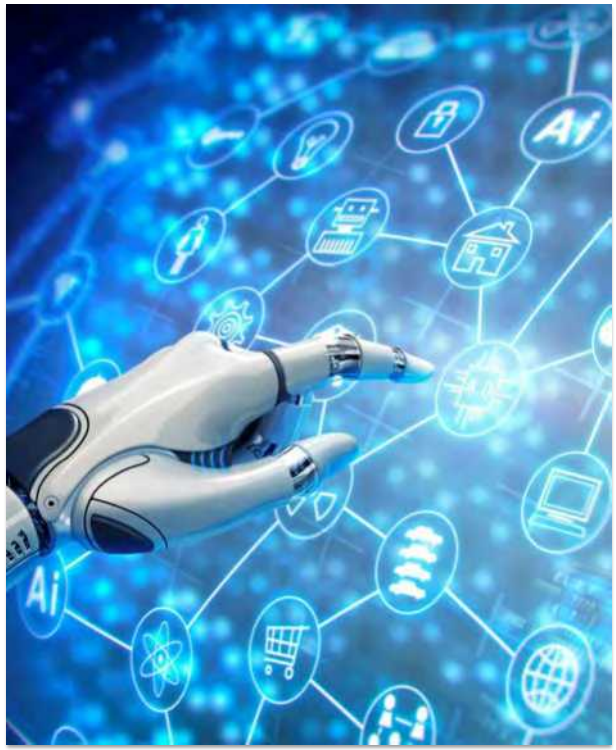
4500 scientist

4 research groups

Łukasiewicz – EMAG is a member of Łukasiewicz Research Network

Main areas of activity of Łukasiewicz-EMAG:

- **Cybersecurity**
- AI, Prediction, Decision support systems
- Digital Public Services
- IoT, Industry 4.0
- Research and certification
- Counteracting social exclusion
- Accessibility Plus
- Digital Education Center



Łukasiewicz
EMAG

Selected Examples of completed projects:

A national scheme for assessing and certifying the security and privacy of IT products and systems according to Common Criteria.

The aim of the project is:

• Development and implementation in Poland of a scheme for assessing and certifying the security and privacy of IT products for compliance with the recognized ICT security assessment standard: PN - ISO / IEC 15408 Information technology - Security techniques - Criteria for assessing IT security, commonly known as "Common Criteria". The standard contains a number of requirements for the construction and assessment of security of IT products. These security features are characterized by a reasonable level of confidence in the effectiveness and efficiency of security measures, which is confirmed in the course of independent assessment by licensed assessment laboratories.

KSO3C

Cybersecurity Assessment and Certification System - lightweight certification programs.

• Development and implementation of a lightweight Cybersecurity Assessment and Certification System.

•Development and implementation of Rapid Cybersecurity Assessment and Certification Programs in the field of IoT, IIoT, Data Processing Centers / Clouds, and Industrial Automation Components (IACS).

•Expansion of Łukasiewicz-EMAG Laboratories to perform tests under the newly created Certification Programs (IIoT, IACS).

Łukasiewicz
EMAG

Cybersecurity: projects and services

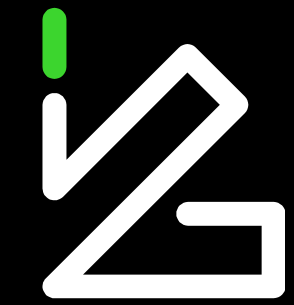
Regional Center for Cyber Security.

The goals of the project are:

- Development of a hardware and software solution used at the client point - the point of connection of the entity's internal IT network to the public network (client part - local),
- Development of an organizational system and software for the operation of regional cybersecurity centers integrating client devices from a given area (regional part),
- Development of mechanisms for integrating RegSOC regional centers with the central entity - CSIRT NASK and NPC (National Cyber Security Platform).

Services:

- Security Operation Center SOC service (CUBE)
- Risk analyzers
- Monitoring of computer equipment for end stations along with ongoing analysis of events and incidents
- Cybersecurity audit compliant with regulatory requirements
- Security evaluation of IT products (ITSEF)
- Certification
- Vulnerability scan
- Cybersecurity training (also within Łukasiewicz network)



40-189 Katowice, Poland
ul. Leopolda 31
www.emag.lukasiewicz.gov.pl
emag@emag.lukasiewicz.gov.pl
Director:
artur.kozlowski@emag.lukasiewicz.gov.pl
Head of Cybersecurity:
michal.chrobak@emag.lukasiewicz.gov.pl
International Cooperation:
mateusz.skowronski@emag.lukasiewicz.gov.pl
martyna.dudzicz@emag.lukasiewicz.gov.pl

CyberSec4Europe

Research results sessions

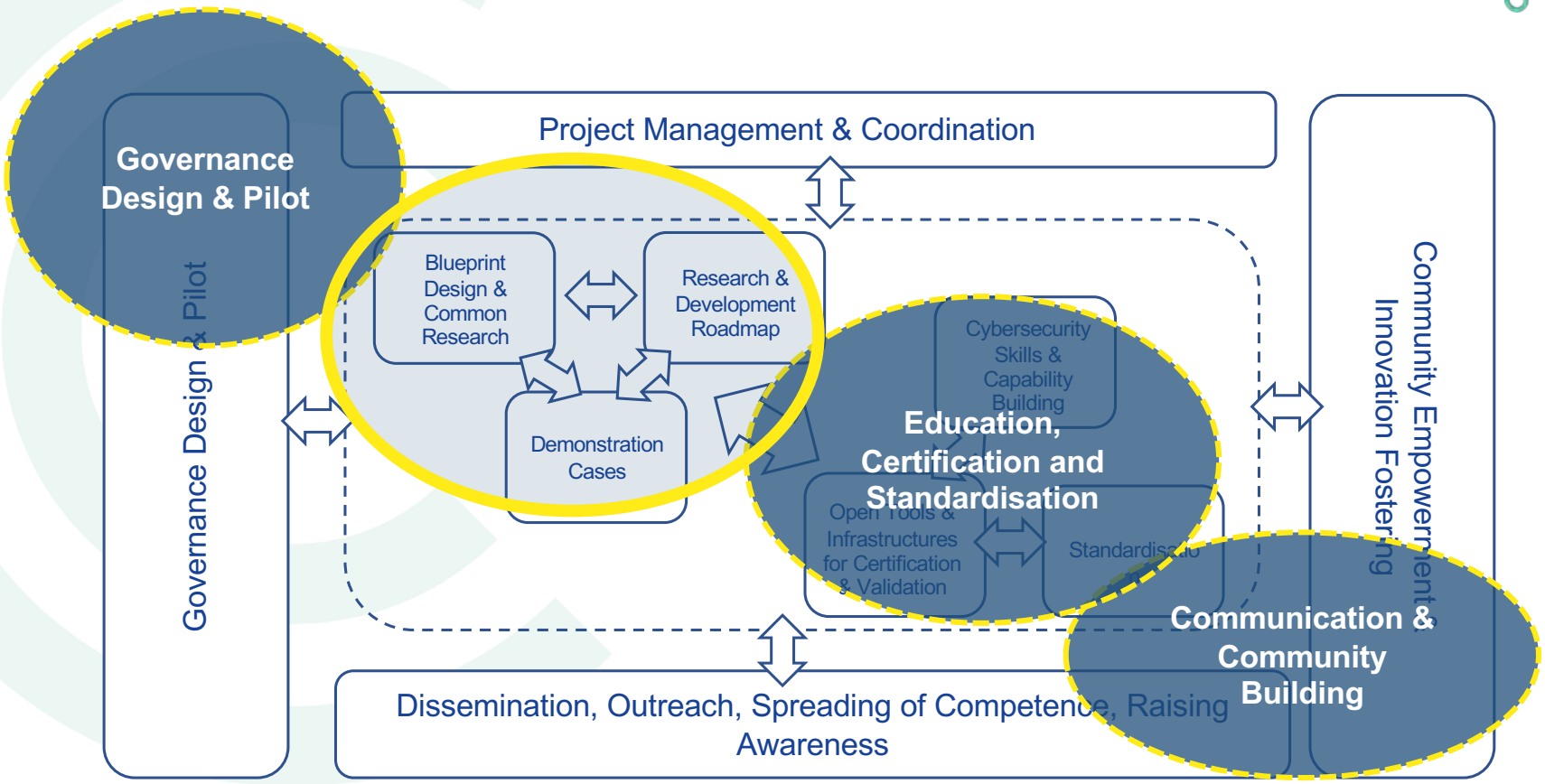
CONVERGENCE NEXT
2022-06-01, Brussels & Online

Antonio Skarmeta
Universidad de Murcia

skarmeta@um.es

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

From Research & Innovation to Industry



From Research and Innovation to Industry

- CyberSec4Europe research and innovation on
  - Privacy-preserving IdM, strong AAA and secure & private communications (T3.2)
  - Usability aspects of security assets (T3.6)
  - Certification frameworks and continuous monitoring (T3.8)
  - Automated tools for verification and enforcement of security policies in software (T3.3)
  - GDPR compliance for use in SMEs (T3.7)
  - Methodology for the individualized evaluation of requirements (T3.7)
  - Advanced threat intelligence services for deploying adaptive security solutions (T3.4)
- Update of the **functional cybersecurity architecture** based on the research work, considering
  - 75 assets from WP3/WP5
  - 18 of them in the process of integration with vertical demonstrators

CyberSec4Europe Research areas

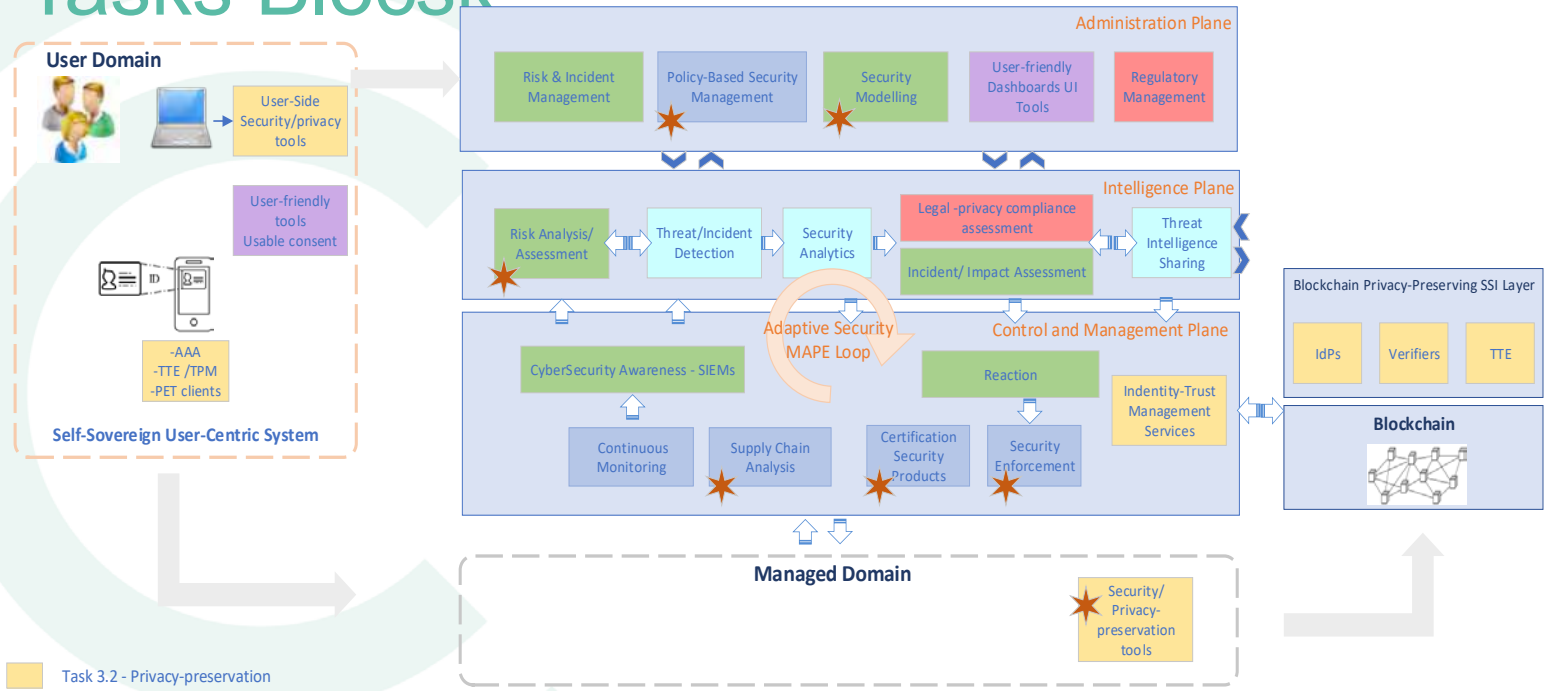
Blueprint design & common research

1. Common framework design
2. Research and integration on cybersecurity enablers and underlying technologies
3. SDL - software development lifecycle
4. Security intelligence
5. Adaptive security
6. Usable security
7. Regulatory sources for citizen-friendly goals
8. Conformity, validation and certification
9. Continuous scouting
10. Impact on society

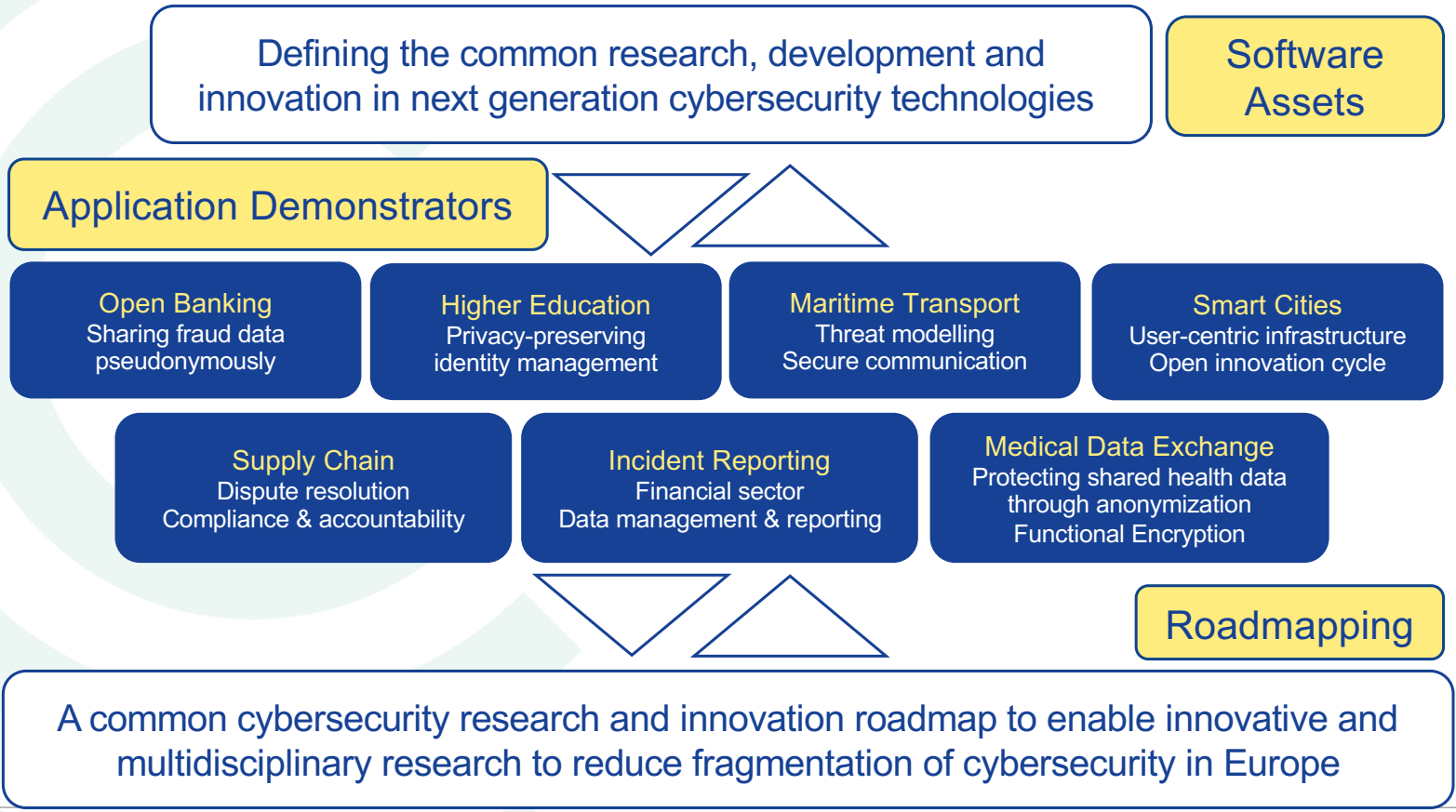
Demonstration cases

1. e-Commerce
2. Supply chain security assurance
3. Privacy-preserving identity management
4. Incident reporting
5. Maritime transport
6. Medical data exchange
7. Smart cities

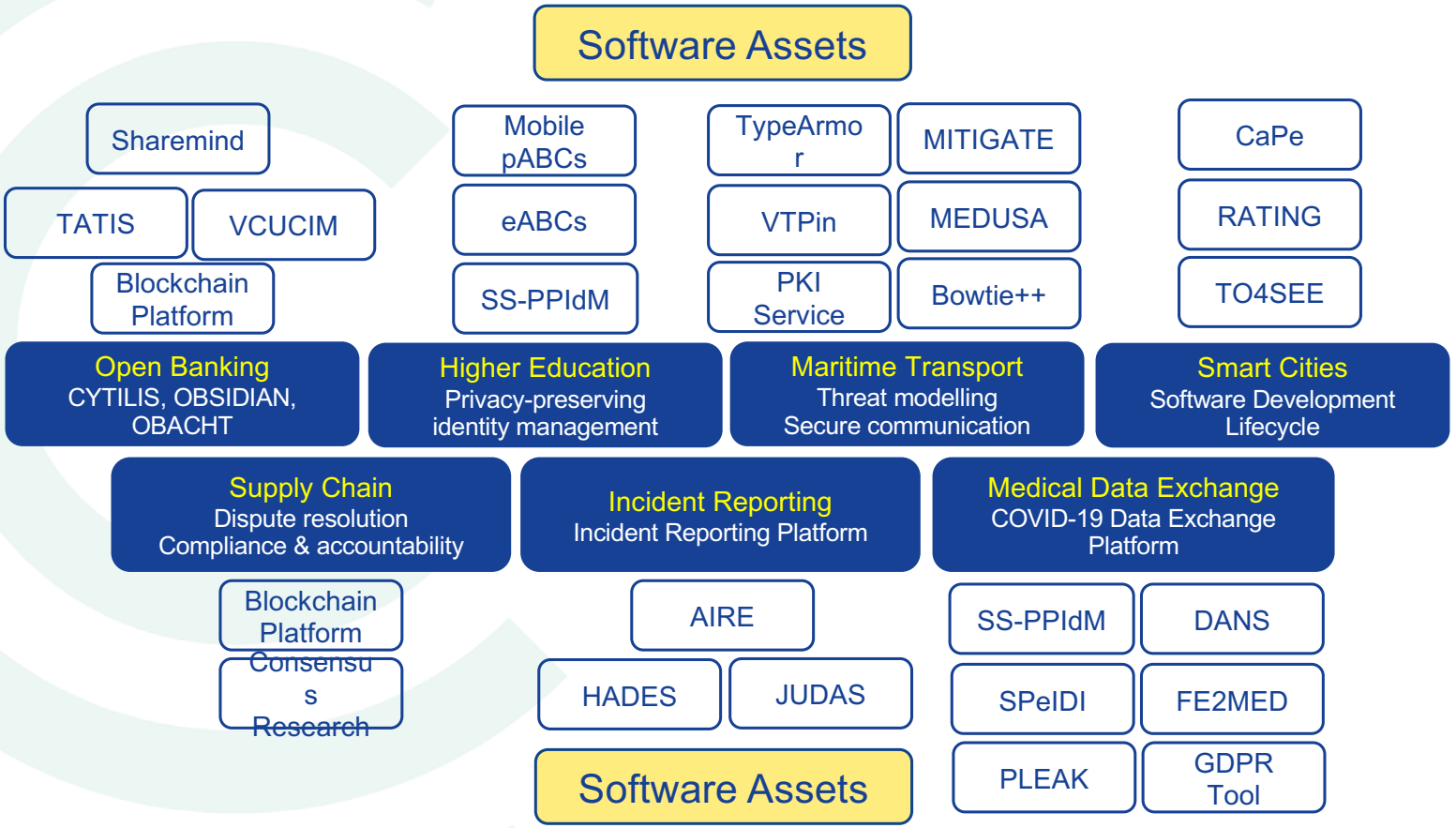
WP3 Global Architecture and Tasks Blocsk



From Research to Innovation to Industry



From Research and Innovation to Industry WP3, WP5: From Assets to Demonstrators

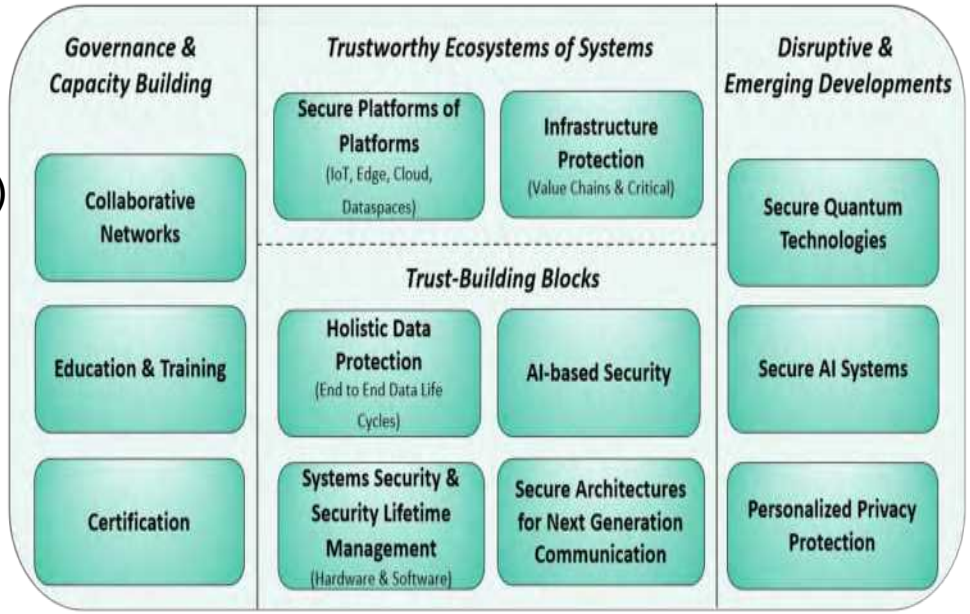


CyberSec4Europe
GitHub - cs4ewp3/wp3

- Introduction to each task and a link to each task's folder.
- On each folder:
  - Summary of task's goals.
  - Resources (videos & papers)
  - Assets
  - Cybersecurity Research and Areas Priority tables
- An also a grouping of assets per building block as defined in the common roadmap

Cybersecurity Research Focus Areas Priorities: The 4 Pilots & ECSO Perspective

As per August 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

GitHub Structure – Cybersecurity Research Areas Priority

https://github.com/cs4ewp3/wp3/blob/main/README.md#cybersecurity-research-and-areas-priority

- Governance and Capacity Building

(CS4E 2021, CS4E D3.9, CS4E D3.10, CS4E D3.3, CS4E D3.9, CS4E D3.11, CS4E D3.6)

- TrustWorthy Ecosystems of Systems

(CS4E 2021, CS4E D3.2, CS4E D3.11, CS4E D3.9, CS4E D3.3)

- Trust-building Blocks

(CS4E D3.18, CS4E 2021)

- Disruptive Emerging Development

(CS4E 2021, CS4E D1.30, CS4E D3.2)

▼ table groups

---	Governance and Capacity Building	Trustworthy Ecosystems of Systems	Trust-Building Blocks	Disruptive Emerging Develpment
PTASC	-	✔	-	-
ARGUS	-	-	✔	-
GDPR compliant user experience	-	-	✔	✔
Interoperability and cross-border compliance	✔	-	-	-
Edge Privacy (UMA)	-	✔	-	✔
Asset 6	✔	-	-	✔
Password-less AuthN	-	✔	✔	-
SS-PP-IdM	-	-	✔	✔
CryptoVault	-	-	✔	-
GENERAL_D	-	✔	✔	✔
pp-FL	-	-	✔	✔
Sharemind	-	-	✔	✔
PLEAK DP analysers	-	-	✔	-
SOBEK	---	---	✔	---
HERMES	---	---	✔	---

GitHub Structure - Cybersecurity Research Areas Priority

https://github.com/cs4ewp3/wp3/blob/main/README.md#cybersecurity-research-and-areas-priority

▼ table groups

---	Governance and Capacity Building	Trustworthy Ecosystems of Systems	Trust-Building Blocks	Disruptive Emerging Develpment
PTASC	-	✔	-	-
ARGUS	-	-	✔	-
GDPR compliant user experience	-	-	✔	✔
Interoperability and cross-border compliance	✔	-	-	-
Edge Privacy (UMA)	-	✔	-	✔
Asset 6	✔	-	-	✔
Password-less AuthN	-	✔	✔	-
SS-PP-IdM	-	-	✔	✔
CryptoVault	-	-	✔	-
GENERAL_D	-	✔	✔	✔
pp-FL	-	-	✔	✔
Sharemind	-	-	✔	✔
PLEAK DP analysers	-	-	✔	-
SOBEK	---	---	✔	---
HERMES	---	---	✔	---

▼ table subgroups

---	Collaborative Networks	Education & Training	Certification	Secure Platforms of Platforms	Infrastructure Protection	Holistic Data Protection	b Se
Conceptual Framework & Guidelines	---	✔	---	---	---	---	---
Conceptual Framework & Guidelines	---	✔	---	---	---	---	---
Criteria for Serious Game Evaluation	---	✔	---	---	---	---	---
PTASC	---	---	---	✔	✔	---	---
ARGUS	---	---	---	---	---	✔	---
GDPR compliant user experience	---	---	---	---	---	✔	---
Interoperability and cross-border compliance	✔	---	---	---	---	---	---
Edge Privacy (UMA)	---	---	---	✔	---	---	---
Asset 6	---	✔	---	---	---	---	---
Password-less	---	---	---	✔	✔	---	---

Cybersecurity Research and Areas Priority

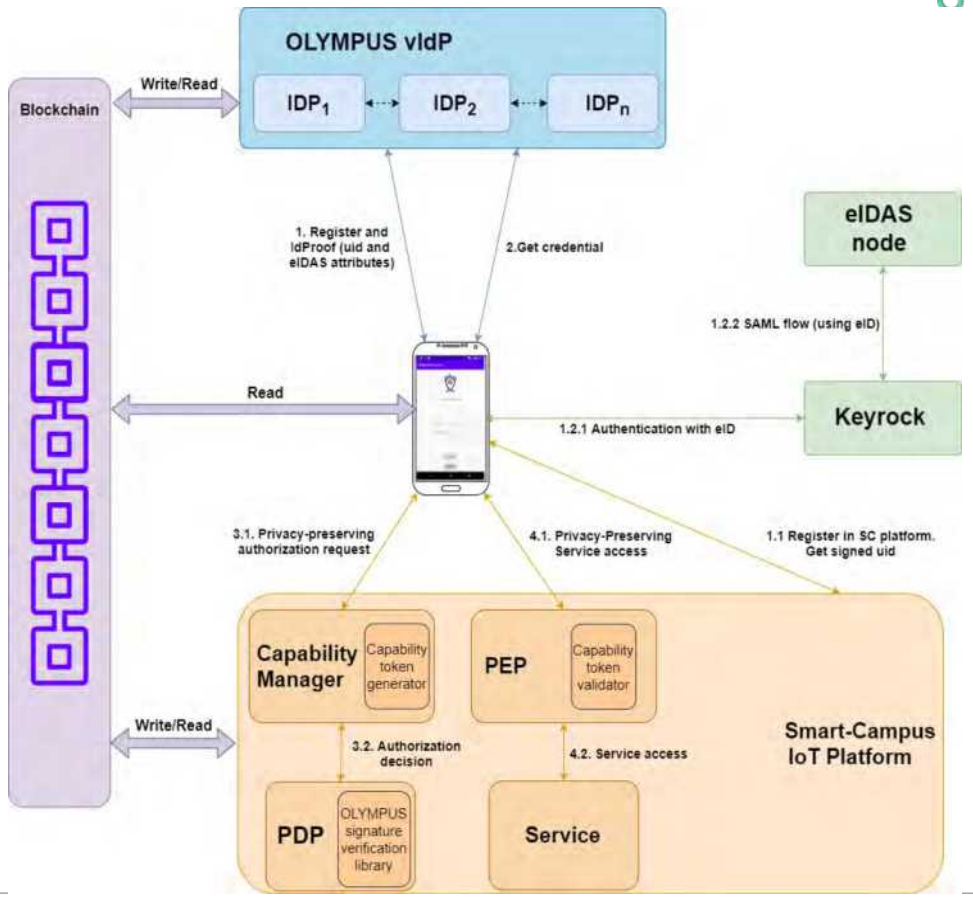
▸ table groups

▸ table subgroups

---	Governance and Capacity Building	Trustworthy Ecosystems of Systems	Trust-Building Blocks	Disruptive Emerging Develpment
Collaborative Networks	Interoperability and cross-border compliance, TIE (ATOS), Analysis of interoperability and cross-border compliance issues	-	-	-
Education & Training	Conceptual Framework & Guidelines, Conceptual Framework & Guidelines, Criteria for Serious Game Evaluation, Asset 6, HATCH, CyberSecurity Awareness Quiz, LEECH, HAMSTERS	-	-	-
Certification	PVS, CSA	-	-	-
Secure Platforms of Platforms	-	PTASC, Edge Privacy (UMA), Password-less AuthN, GENERAL_D, Sharemind	-	-
Infrastructure Protection	-	PTASC, Password-less AuthN, GENERAL_D, SOBEK, HERMES, Brianeos (C3P), EBIOS (CNR), ENOS (FBK), HADES (UMA), IntelFrame (DTU), IUDAS (UMA), NatGen (Polito), RoCe (UNITN), TATIS (KUL), TIE (ATOS), CSA	-	-
Holistic Data	-	-	ARGUS, GDPR compliant user experience, SS-PP-IdM, GENERAL_D, pp-FL, PP-CTI (UMU), TATIS (KUL), TIE (ATOS), Privacy-preserving IdM, DPIA template, HATCH,	-

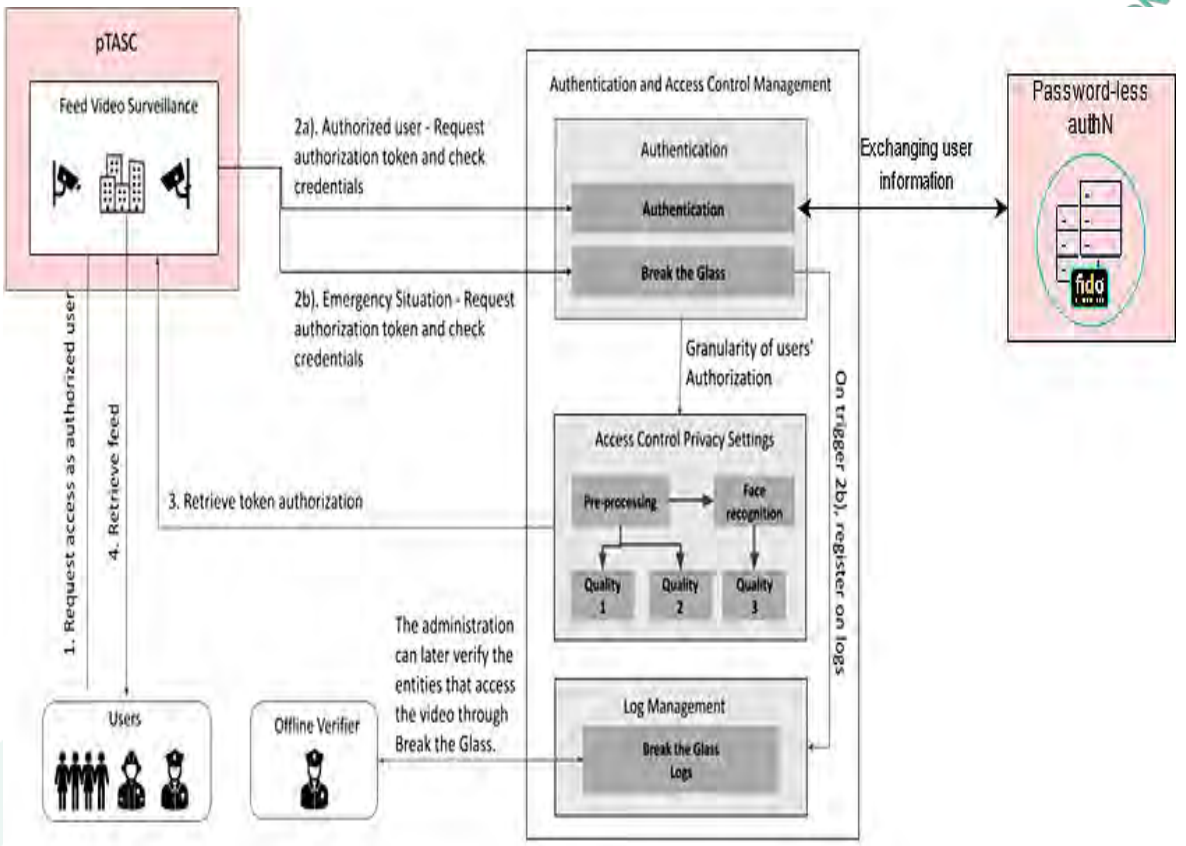
Identity Management in Smart-city

- **Pp-SS-IdM:** to manage user identities and authentication It relies on distributed p-ABCs to offer privacy-preserving (minimal disclosure and unlinkability) and authentication (presentation of attributes) linked to eIDAS.
- The asset proposes a trust framework based on Blockchain to complement the usage of credentials.



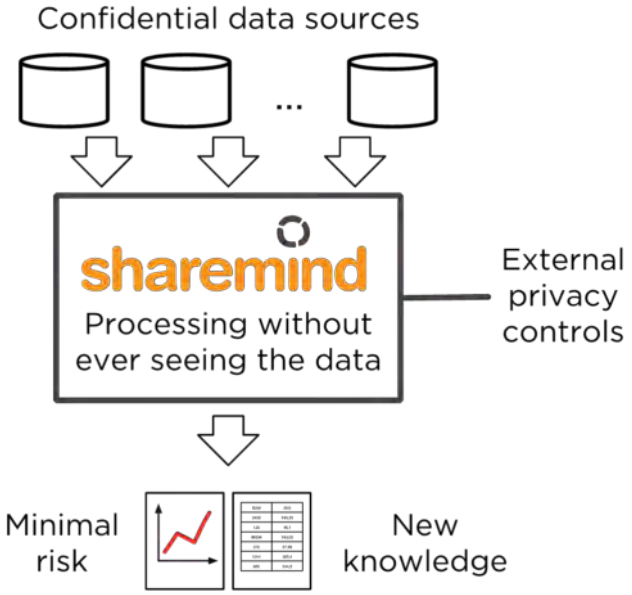
Advanced AAI

- **PTSAC:** Manage device Identity, control the data exchanged by the video-surveillance cameras. Devices' provisioning process using PTASC
- **Argus:** cloud storage solution that acts as a proxy to the existing public cloud infrastructures by performing all the necessary authentication, cryptography, and erasure coding.
- **Password-less authentication** based on FIDO 2 strengthen the user authentication process by implementing a two-factor authentication approach with biometric
-



Data protection

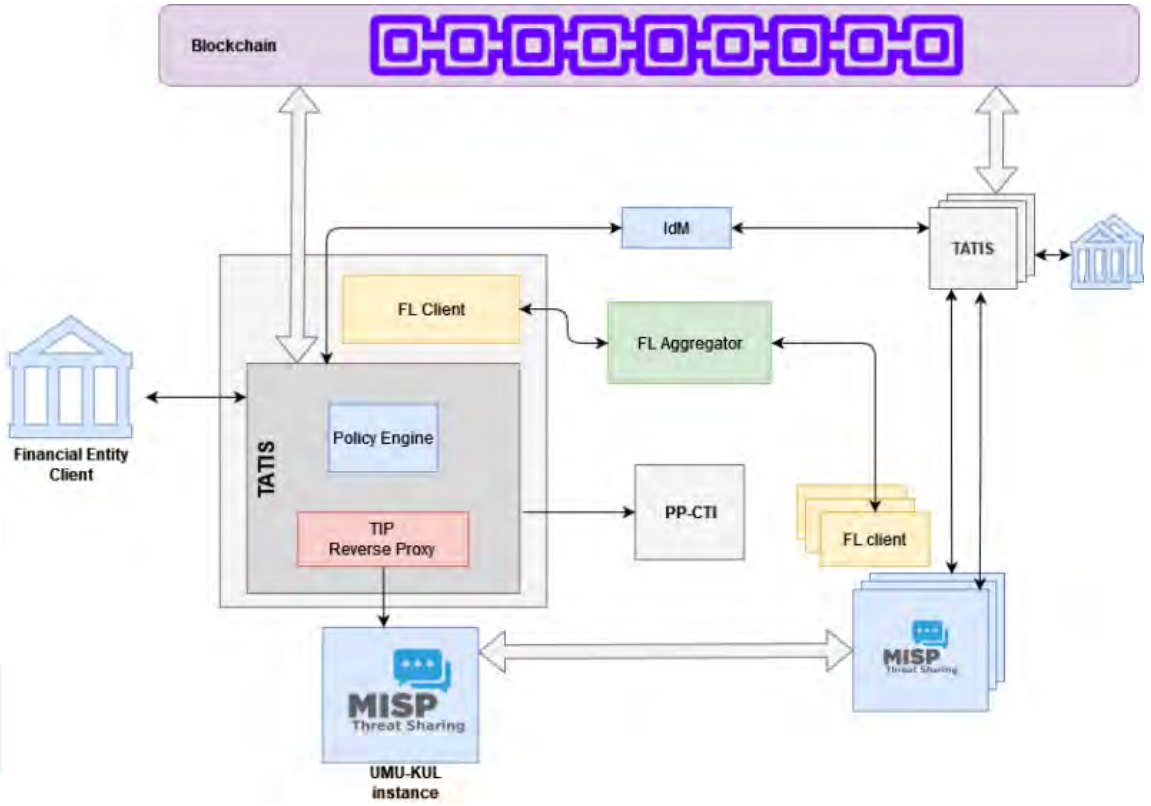
- **Sharemind MPC**[1] uses secret sharing and secure multi-party computation to protect confidential data at rest, in transit and in use. Sharemind MPC overview and documentation https://docs.sharemind.cyber.ee/
- Allows the banks to secret-share details about potentially fraudulent transactions and compute the following KPI-s using secure multiparty computation
- The system allows each bank to secret-share basic transaction data (IBAN/hash, data and amount) and computes the reputation information and KPI-s from secret-shared data using secure multiparty computation.



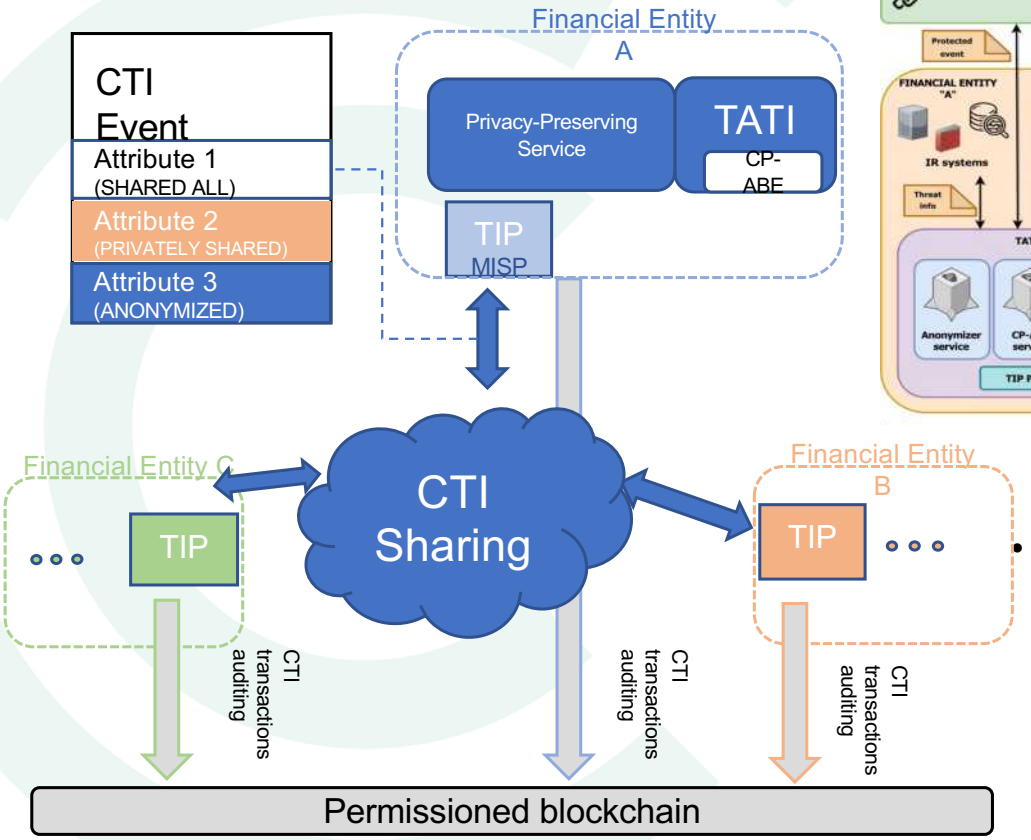
Privacy-preserving Incident Reporting

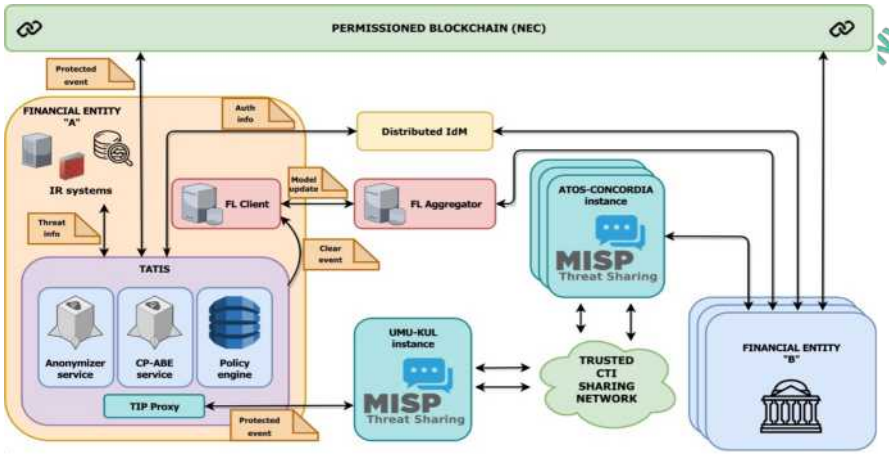
Involved WP3 assets:

- **TATIS :** this asset is used as a proxy to the MISP instance. TATIS enhances the CTI haring platform to share indicators of compromise in a trustworthy manner.
- **PP-CTI:** this asset is used to apply PETs to the shared information and will investigate, integrate and adapt privacy-preserving solutions, anonymity techniques within CTI systems.
- **Pp-FL**: this asset employs privacy-preserving federated learning for incident detection
- **Blockchain Platform:** novel scalable consensus protocols



Cross-Pilot: A Privacy-Preserving and Confidential CTI Sharing Approach





WP3 Assets

- **Application of CP-ABE schema** to enable access control of certain attributes
- **Privacy-preserving module** is reponsible to support PETs mechanisms, such as k-anonymity.
- **Permissioned blockchain** to audit CTI-related transactions between organizations
- **CTI sharing network** is agnostic to TIPs by using standards format (ie STIX+TAXII or MISP format)

Conclusion

- **Multiple collaborations** on research papers and asset interaction at intra- and inter-task level
- **Instantiation of assets** for demonstration scenarios
- **A github** with results and mapping to the research roadmap topic
- **Collaboration** with verticals, CONCORDIA and ECHO based on WP3 assets
- Contribution to the **joint pilot research roadmap** based on the work on scouting for new cybersecurity trends

Thank you very much for your attention!

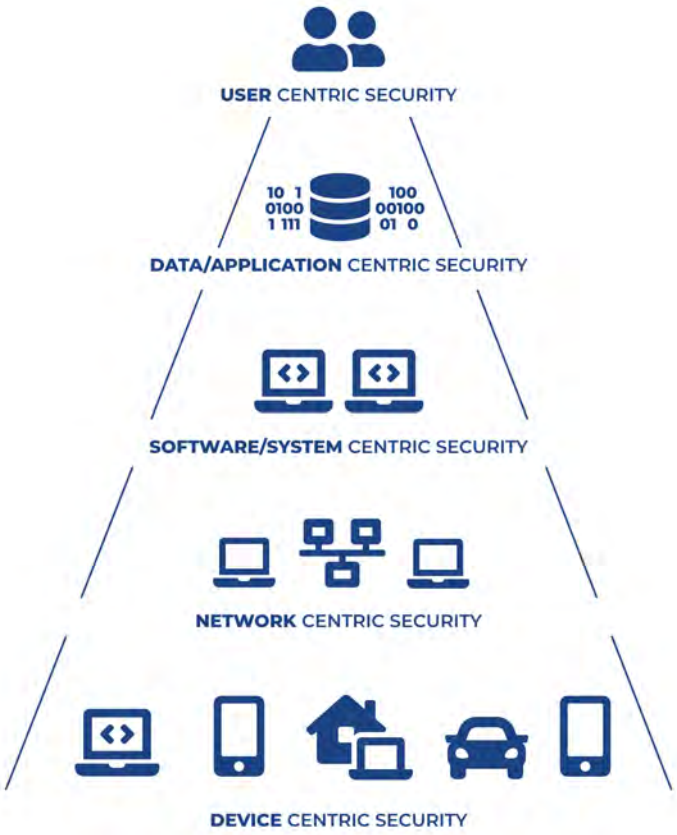
Kai.Rannenberg@m-chair.de


1–3 June 2022
Brussels
CONVERGENCE NEXT
Cyber Competence Network

Convergence Next 2022 – Research (WP1)

Antonio Ken Iannillo (University of Luxembourg)
Jürgen Schönwälder (Jacobs University Bremen)

WP1 Research Tasks



T1.5: User-centric security

T1.4: Application/Data-centric security

T1.3: System/Software-centric security

T1.2: Network-centric security

T1.1: Device-centric security

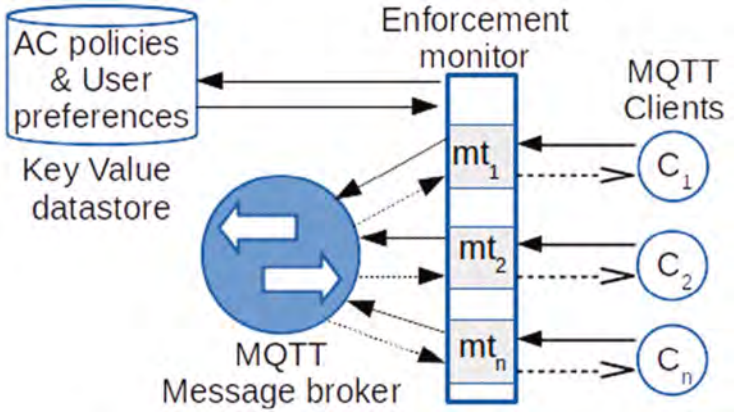
T1.1 Device-centric Security

Jürgen Schönwälder (JUB)
T1.1 Leader

- Research activities
  - Hardware assisted security mechanisms (FORTH)
  - Efficient cryptographic primitives (JUB, UP, ISI)
  - Trustworthy IoT systems and IoT protocols (UMIL, UZH, UI, CUT)
  - Device analytics for detecting anomalies (BGU, ICL)
  - Blockchain technologies applied to IoT scenarios (UZH, BGU)

T1.1 Attribute Based Access Control for MQTT

- Problem
  - Sensor data sent to cloud services via MQTT
  - Limited user-controlled access control facilities
- Approach
  - Decentralized access control in bridged environments
- Outcomes
  - Attribute Based Access Control (ABAC) framework for MQTT
  - Experiments show a reasonably low enforcement overhead



T1.1 Some Publication Highlights (2021)

- P. Colombo, E. Ferrari, E.D. Tümer (UI):
  Regulating Data Sharing across MQTT Environments.
  Elsevier Journal of Network and Computer Applications 174, January 2021
  doi:10.1016/j.jnca.2020.102907
- C.A. Ardagna, R. Asal, E. Damiani, N.E. Ioini, M. Elahi, C. Pahl (UMIL):
  From Trustworthy Data to Trustworthy IoT: A Data Collection Methodology Based on Blockchain.
  ACM Transactions on Cyber-Physical Systems, 5(1), January 2021
  doi:10.1145/3418686
- S. Harush, Y. Meidan, A. Shabtai (BGU):
  DeepStream: Autoencoder-based Stream Temporal Clustering and Anomaly Detection.
  Elsevier Computers & Security, July 2021
  doi:10.1016/j.cose.2021.102276

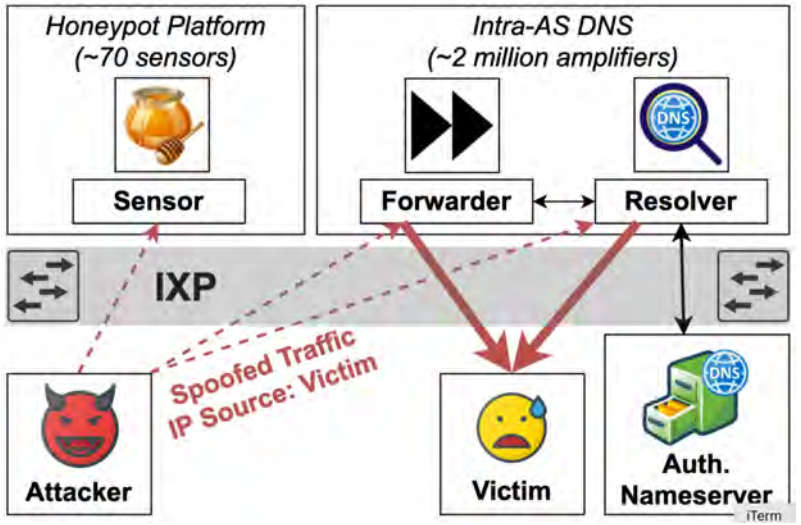
T1.2 Network-centric Security

- Research activities
  - Distributed denial of service attacks (UT, SIDN)
  - Analysing encrypted network traffic (FORTH, Flowmon, MUNI)
  - Software-defined networking (BADW-LRZ, UZH)

Mattijs Jonker (UT)
T1.2 Leader

T1.2 Tracing DNS DDoS Amplification

- Problem
  - DNS amplification is widely used for DDoS attacks
  - Studies rely on honeypots located at network edges
- Approach
  - Use complementary data sources
  - IXPs located in the core network
  - Honeypots located at the edge of the network
  - DNS scanners actively probing DNS services
- Observations
  - Different vantage points observe mostly disjoint sets of attacks
  - Attackers are able to detect new abusable amplifiers quickly and adapt quickly
  - US government domains breaking DNSSEC key rollover practices exacerbate the amplification potentials



T1.2 Some Publication Highlights (2021)

- R. Sommese, G. Akiwate, M. Jonker, G.C. Moura, M. Davids, R.v. Rijswijk-Deij, G.M. Voelker, S. Savage, K.C. Claffy, A. Sperotto (UT):
  Characterization of Anycast Adoption in the DNS Authoritative Infrastructure.
  Network Traffic Measurement and Analysis Conference (TMA '21), September 2021 (best paper award)
- M. Nawrocki, M. Jonker, T.C. Schmidt, M. Wählisch (UT):
  The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core.
  Proceedings of the ACM Internet Measurement Conference, November 2021
  doi:10.1145/3487552.3487835
- E. Papadogiannaki, S. Ioannidis (FORTH):
  A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures.
  ACM Computing Surveys, 54(6), July 2021, doi:10.1145/3457904

T1.3 Network-centric Security

- Research activities
  - Security by design (ULANC)
  - Dynamic malware analysis (UL, JUB)
  - System security validation and zero-days (ULANC, UL)
  - UAV Resilience (ICL)

Jean-Yves Marion
(UL)
T1.3 Leader

T1.3 Packed Malware Analysis

- Problem
  - Packed malware
  - Obfuscators hide APIs used by malware

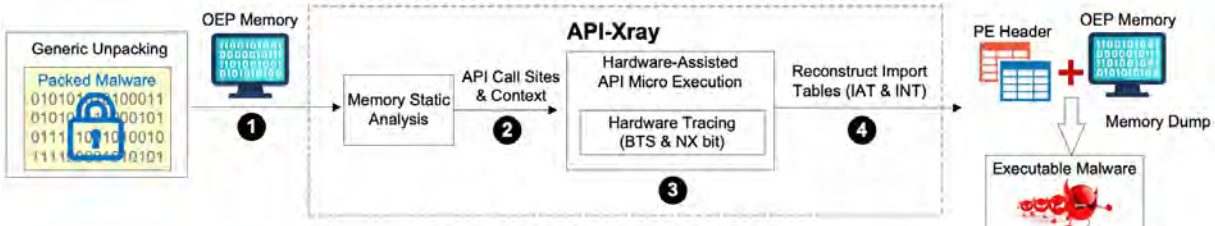


Figure 3: The Overview of API-Xray.

- Approach
  - Reconstruction of Windows import tables via API Micro Execution
  - Implementation of API-Xray producing standard Windows PE files
- Observations
  - Successfully rebuilt 155,811 executable malware programs
  - Improved the detection rate for 7,514 unknown or new malware variants

T1.3 Some Publication Highlights (2021)

- N. Coppik, O. Schwahn, N. Suri (ULANC):
  Fast Kernel Error Propagation Analysis in Virtualized Environments.
  IEEE Conference on Software Testing, Verification and Validation (ICST), April 2021
  doi:10.1109/ICST49551.2021.00027

- B. Green, R. Derbyshire, M. Krotofil, W. Knowles, D. Prince, N. Suri (ULANC):
  PCaaD: Towards automated determination and exploitation of industrial systems.
  Elsevier Computers & Security, 110, November 2021
  doi:0.1016/j.cose.2021.102424

- B. Cheng, J. Ming, E. Leal, H. Zhang, J. Fu, G. Peng, J.-Y. Marion (UL):
  Extracting Executable Payloads From Packed Malware: Import Table Reconstruction via Hardware-Assisted API Micro Execution.
  USENIX Security, August 2021

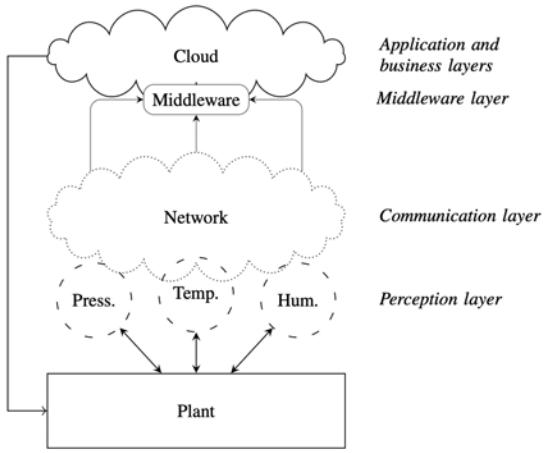
T1.4 Data/Application-centric Security

Vassilis Prevelakis (TUBS)
T1.4 Leader

- Research activities
  - Protection of (big) data (UI, TUBS)
  - Protection of cloud services (UL, UM, OsloMET, UMIL, TELENOR)
  - Application behavioural analysis (FORTH, UL, UM, TUBS, OsloMET, TELENOR)

T1.4 Assurance-based Risk Management Framework

- Problem
  - Risk management frameworks of the 1990s are limited
  - Intrinsic complexity of modern IoT plus Cloud systems
- Approach
  - Risk management process integrated with assurance techniques
  - Assurance techniques monitor the correct behavior of the target system
  - Flow networks compute risk mitigation and the residual risk for the organization
- Application
  - Evaluated in a simulated industry 4.0 scenario
  - Detection of discrepancies between *believed* and *actual* risk mitigations



T1.4 Some Publication Highlights (2021)

- F. Daidone, B. Carminati, E. Ferrari (UI):
  Blockchain-based Privacy Enforcement in the IoT Domain.
  IEEE Transactions on Dependable and Secure Computing, September 2021
  doi:10.1109/TDSC.2021.3110181

- M. Anisetti, C.A. Ardagna, N. Bena, A. Foppiani (UMIL):
  An Assurance-Based Risk Management Framework for Distributed Systems.
  IEEE International Conference on Web Services, September 2021
  doi:10.1109/ICWS53863.2021.00068

- M. Sestak, M. Hericko, T. Welzer Druzˇovec, M. Turkanović (UM):
  Applying k-vertex cardinality constraints on a neo4j graph database.
  Elsevier Future Generation Computer Systems, 115, February 2021
  doi:10.1016/j.future.2020.09.036

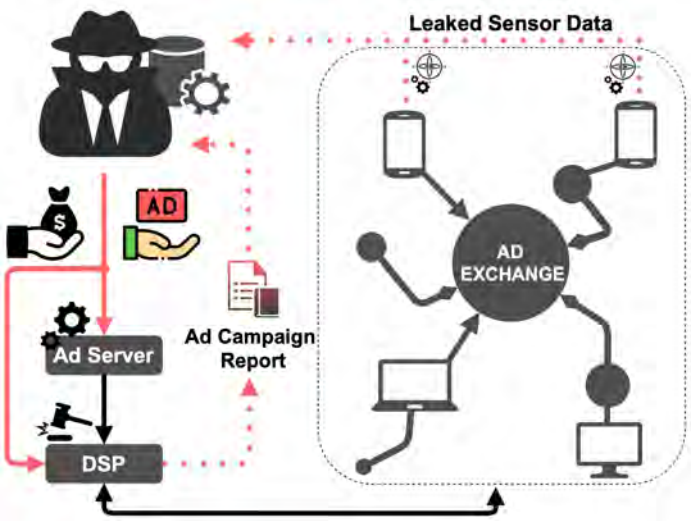
T1.5 User-centric Security

- Research activities
  - Privacy protection and risk evaluation (FORTH, SnT, UI, ICL, UMIL, TID)
  - Identity management (SnT, UZH, UP)
  - Social networks and fake news (FORTH, CUT, TID, UM)

Michael Sirivianos (CUT)
T1.5 Leader

T1.5 Misusing Mobile Sensors for Data Exfiltration

- Motivation
  - Mobile sensors leak sensitive data
  - WebView has limited access control
  - Can advertisements be used deliver attacks?
- Discoveries
  - Advertising ecosystems can deliver stealthy attacks
  - Affects all Android apps that contain in-app advertisements using WebView
  - Flaws in Android enable persistent data exfiltration
  - Apps in the Android Play Store already leak data from motion sensors



T1.5 Some Publication Highlights (2021)

- M. Diamantaris, S. Moustakas, L. Sun, S. Ioannidis, J. Polakis (FORTH):
  This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration.
  ACM SIGSAC Conference on Computer and Communications Security (CCS '21), November 2021, doi:10.1145/3460120.3485366

- F. Mo, H. Haddadi, K. Katevas, E. Marin, D. Perino, N. Kourtellis (ICL,TID):
  PPFL: Privacy-Preserving Federated Learning with Trusted Execution Environments.
  ACM Conference on Mobile Systems, Applications, and Services, MobiSys '21, June 2021 doi:10.1145/3458864.3466628 (best paper award)

- E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, E.P. Markatos (TID):
  User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users.
  Proceedings of the Web Conference 2021, WWW '21, April 2021. doi:10.1145/3442381.3450056

Summary and Outlook

- Research activities are developing well covering many different aspects
- Strong links to activities in other CONCORDIA work packages
- Experience with COVID in 2021
  - Limited impact on the research itself (work often does not requiring access to labs)
  - Bigger but highly varying impact on the individuals doing research
  - Difficult to create spaces for creative moments within a project
- In case of further questions, contact us:
  - wp1-taskleaders@concordia-h2020.eu
  - wp1-leader@concordia-h2020.eu

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

ECHO Research results sessions and demonstrations

Peter Hagstrom

Security Services, Manager at RHEA
ECHO WP5 Leader

RHEA Group

Convergence 2022

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Cybersecurity Challenges for the EU

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

- Lack of effective means **to assess multi-sector technology requirements** across security disciplines
- Lack of effective means to **assess dependencies between different industrial sectors**
- Lack of **realistic simulation environments** for technology research and development, or efficient security test and certification

- Lack of an **up-to-date cyberskills framework** as a foundation for cybersecurity education and training
- Lack of effective **means to share knowledge and situational awareness** in a secure way with trusted partners
- These gaps **are particularly relevant for EU**

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943


ECHO
EUROPEAN NETWORK OF CYBERSECURITY
CENTRES AND COMPETENCE HUB FOR
INNOVATION AND OPERATIONS

Partners

Project Coordination:
Royal Military Academy of Belgium (Wim Mees)

Project Management:
RHEA System S.A. (Matteo Merialdo)

- 16 Millions budget
- 4 years (started Feb 2019)
- 30+14 partners (+2 in the process of being signed)
- 13 existing competence centres
- 19 nations
- 9 industrial sectors
- 13 security disciplines
- 5 demonstration cases
- 6 technology roadmaps
- 3 multi-sector scenarios

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

Main concepts:

ECHO Governance Model: Management of direction and engagement of partners (current and future)

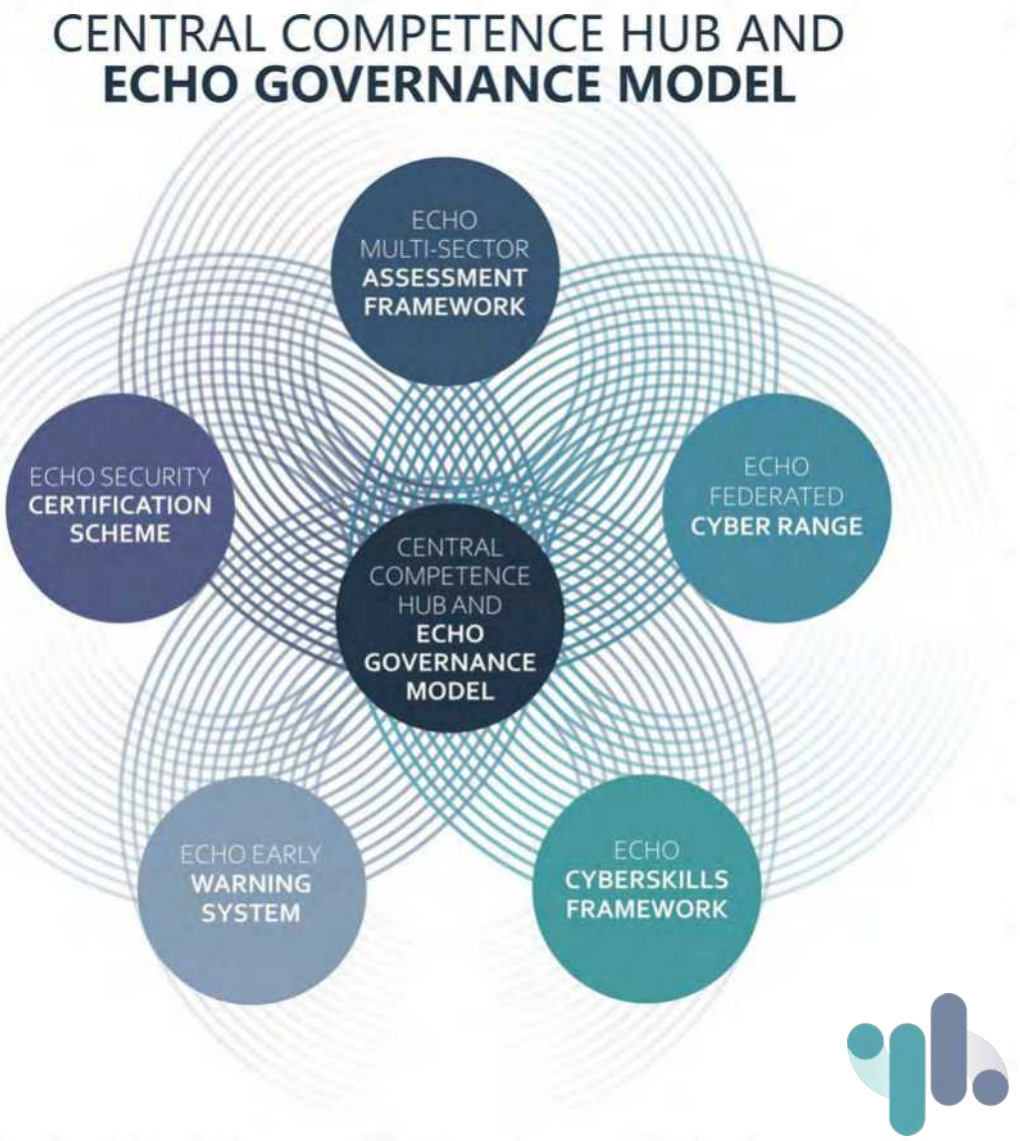
ECHO Multi-Sector Assessment Framework: Transverse and inter-sector needs assessment and **technology R&D roadmaps**

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 Multi-sector Assessment Framework

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

Evaluate the risk of **multi-sector scenarios**, including **supply chain**

2

Mechanism to define and refine **technology roadmaps** and **demonstration cases**

3

Risk based method to analyse multi-sector security needs:

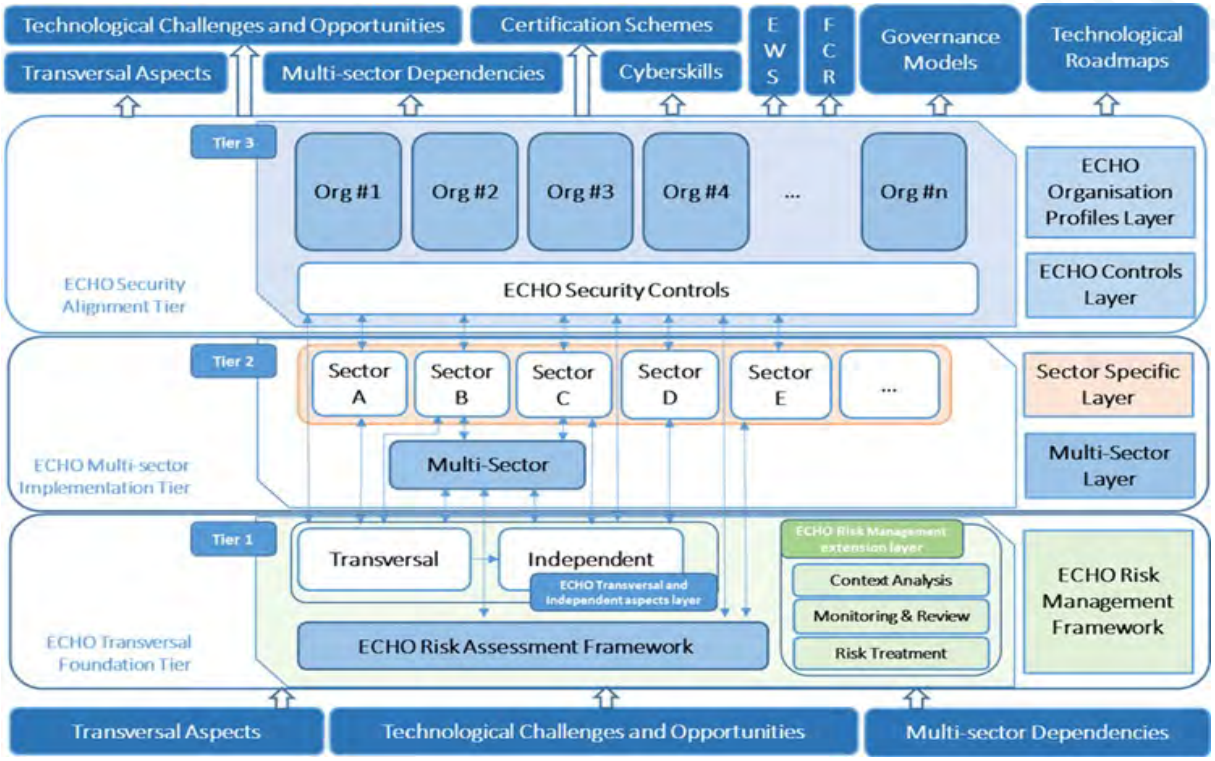
- **Inter-sector** and **transversal opportunities** and **dependencies**
- **Contributions** to **technology roadmaps**

4

ECHO identified **6 technology roadmaps** and developed **4 technology innovations** on these roadmaps, including E-FCR and E-EWS

ECHO Multi-sector Assessment Framework

Where are we currently?



- We are ready with an **advanced prototype (1.5.x)**
- It is piloted as an Excel spreadsheet and a **software tool**
- Enhanced Risk Calculation
- Many single/multi sector scenarios have been developed
- Several Assessment/Examples running in ECHO domains and transport sector.
- It is being used to derive/justify **directions for** the **Skills Framework**, the **Certification Framework** and the **Technology Roadmaps**

ECHO Cyberskills and Training Curricula

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

Mechanism to improve the **capacity** of professionals across Europe for more effective response to cyber threats

2

Leverages a **common cyberskills reference**

3

Design modular **learning-outcome based curricula**

4

ECHO provides opportunities for **demonstration** of the gained skills **with realistic simulations** and Lessons learned feed **knowledge sharing**

ECHO Training Curricula

Where are we currently?

With the E-CSF, we developed **4 training curricula**: Maritime, Energy, Healthcare, Transversal

Modular e-Learning platform (LMS) – knowledge building

Cyber Range Lab Demo – from knowledge to skills

Tabletop Exercise – skills building

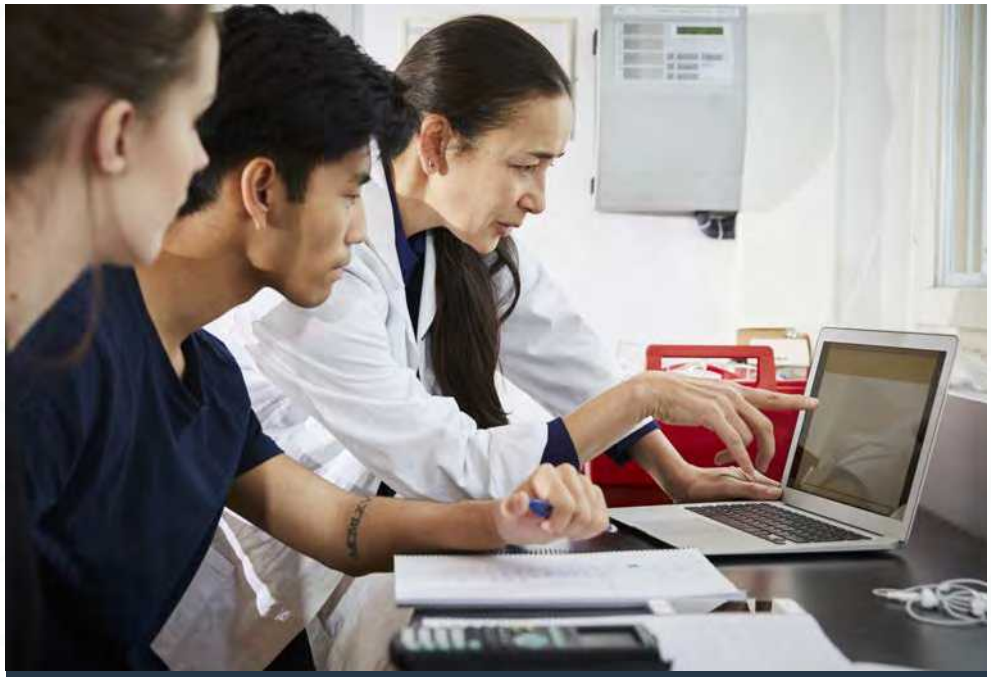
Cyber Range Exercise – skills building

Assessment at each stage, incl. Customer needs

ECHO
Federated Cyber Range
Marketplace

Service Offer

Delivered via Federated schools during 2021 and 2022, involving 80 students so far



ECHO Cybersecurity Certification Scheme

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)

2

Support **delivery and acceptance of technologies** resulting from technology roadmaps

- **Improved security assurance** through use of **certified products**

3

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)

4

Provides **product-oriented** cybersecurity certification schemes

- Support sector specific and inter-sector security requirements
- Leveraging on cyber ranges as testing facilities

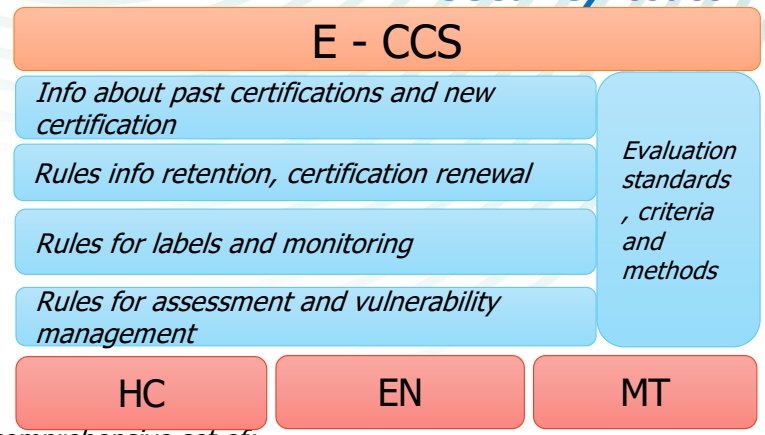
ECHO Cybersecurity Certification Scheme

ECHO CCS is a *product oriented* cybersecurity certification *scheme*, supporting security requirements for *sector specific* and inter-sector *security* issues.

Where are we currently?

E-CCS has been completed and is based on the **Common Criteria-based EU candidate Cybersecurity Certification Scheme (EU-CC)**

- It is a **horizontal** scheme for ICT **products**
- It covers **assurance levels** substantial and high
- **All the elements** of a EU scheme requested in **Cyber Security Act** are defined:
  - Evaluation standards, criteria and methods
  - Rules for labels, monitoring, assessment and vulnerability management
  - Rules info retention, certification renewal
  - Info about past certifications and new certification
- Possibility to establish **Protection Profiles (PP)** for specific security requirements



ECHO is running a "simulated certification" for at 2 of the ECHO Prototypes, following the E–CCS and leveraging the ECHO Federated Cyber Ranges and several ECHO Cyber Ranges

CYBERSECURITY CERTIFICATION SCHEME is a *comprehensive set of:*

- ✓ *rules,*
- ✓ *technical requirements,*
- ✓ *standards and procedures*

defined at EU level applying to the certification of Information and Communication Technology (ICT) products and services falling under the scope of that specific scheme.

We can:

1. **Customize** the general rules and procedures proposed in EU-CC wrt a specific sector
2. Establish a **methodology** to enable sector specific PP to be quickly designed
   - We provide a baseline consisting of SECTOR SPECIFIC SECURITY PROBLEM DEFINITION

ECHO Technology Roadmaps

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

One of the main objectives of the ECHO project is the **development of cybersecurity roadmaps** as a result of **analysis** related to **current** and **emerging cybersecurity challenges**.

2

Delivery of at least **6 cybersecurity technology roadmaps** including:

- **ECHO Early Warning System** (E-EWS) Roadmap
- **ECHO Federated Cyber Range** (E-FCR) Roadmap
- At least **2 additional technology innovations (Prototypes)** to be completed as part of ECHO
- At **least 2 additional technology innovations (challenges/priorities)** to be addressed by the future Cybersecurity Competence Network

3

Highlight **strategic technology-related priorities** with the goal to create the foundations for new **industrial capabilities** and assist towards the development of **innovative technologies** thus paving the way towards **EU's digital sovereignty**.

4

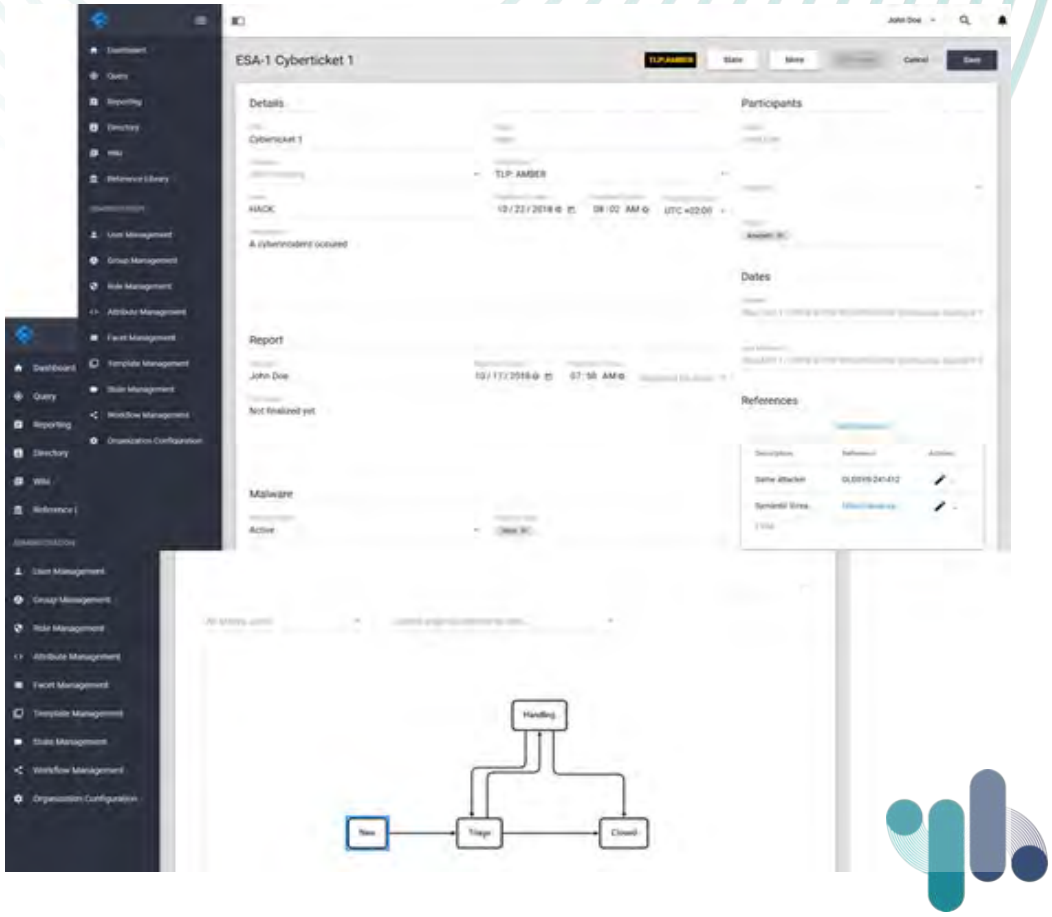
Consider the **transversal** aspects of **Education/Training** and **Certification**, while underpinned by effective **Governance** models for networked organisations that collaboratively strive to achieve these goals.

ECHO Technology Roadmaps

ECHO Early Warning System (E-EWS)

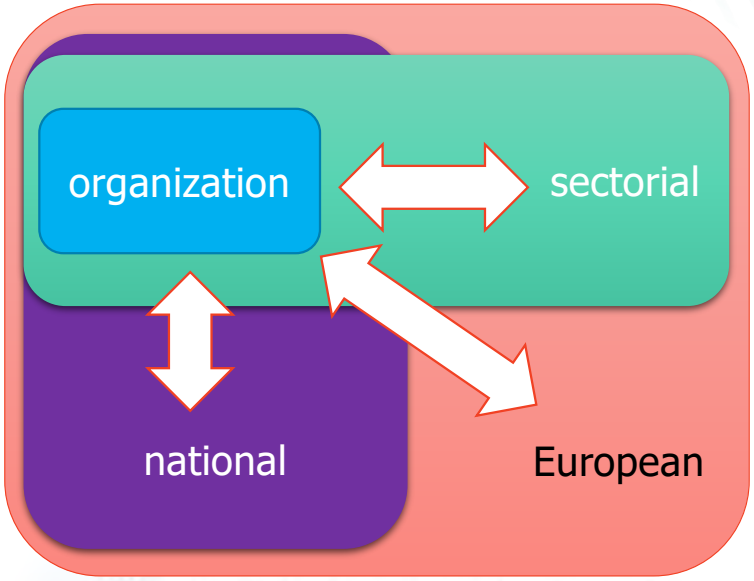
- **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
  - Tickets
  - Warnings
  - Knowledge base/Cyber Threat Intelligence
- Secure information sharing **between organizations**; across organizational boundaries and national 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)
- Multisource **threat intelligence data** gathering
- Includes sharing of **reference library** information and **incident management** coordination

- **Potentially, it could serve all the network of centers of competences!**

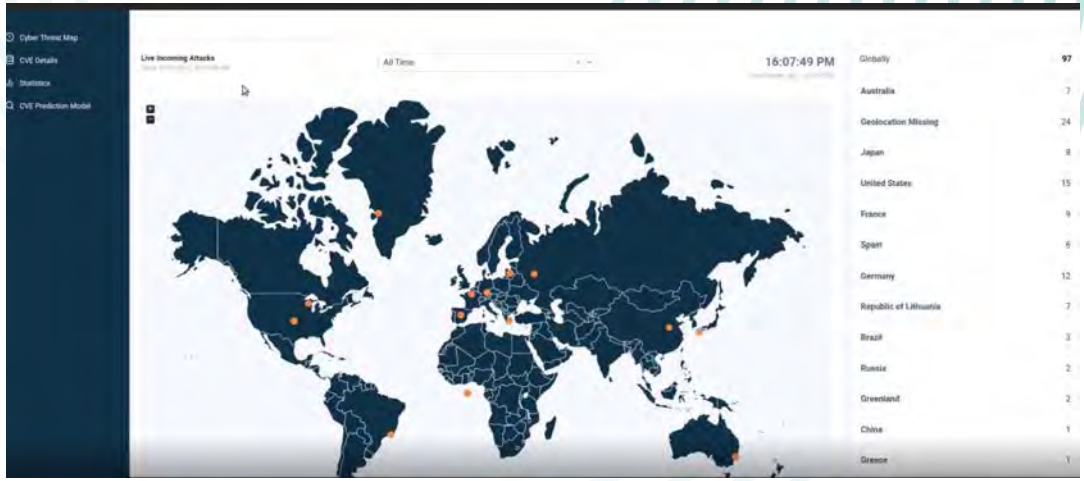


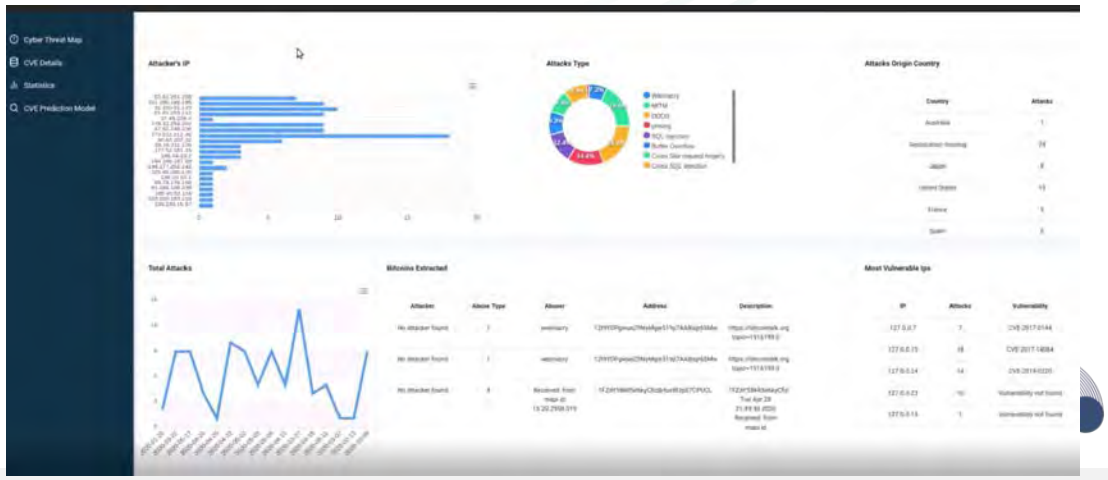
Sharing Threat Information

ECHO Early Warning System (E-EWS)



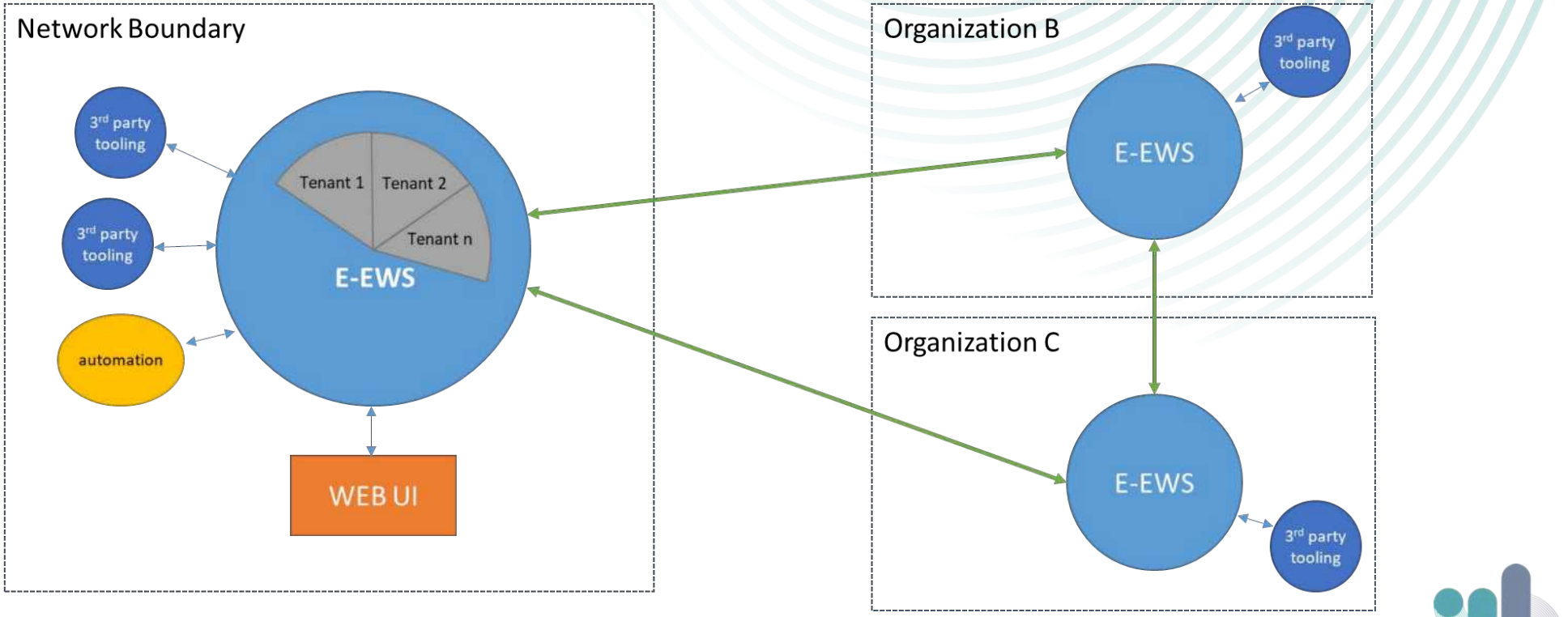
Four Types of Cyber Threat Intelligence





ECHO Early Warning System (E-EWS)

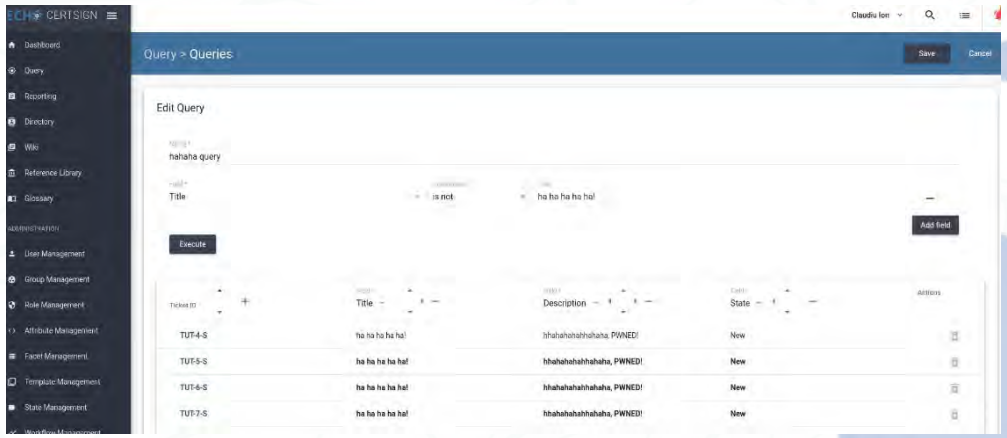
Distribution



ECHO Early Warning System (E-EWS)

Where are we currently?

- Development is **complete,** actually in **validation**
- **22** ECHO organizations are already connected via E-EWS
- **7** Tabletop exercises already performed, with up to **120** participants
- The team is currently working on the **ECHO Demonstration cases**



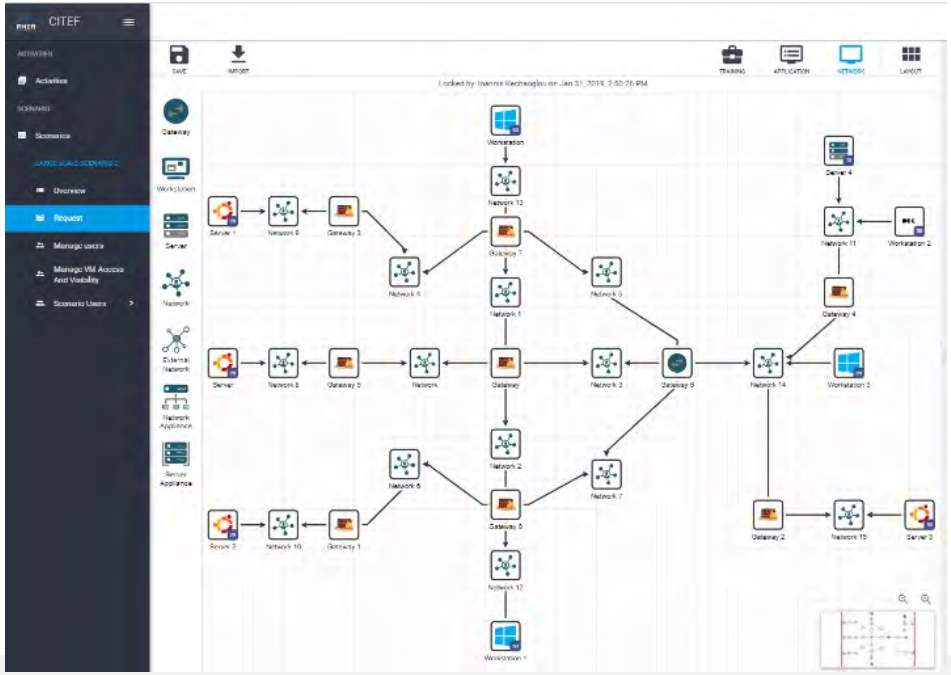
ECHO Early Warning System (E-EWS)

Play video #1 - 20210830 E-EWS Video - v2.mp4

ECHO Technology Roadmaps

The ECHO Federated Cyber Range (E-FCR)

Cyber Ranges are multipurpose **virtualization environments** supporting **"security-by-design"** needs



Cyber Ranges are used to provide:

- Safe environment for **hands-on cyberskills** development
- Realistic simulation for **improved system assurance** in development
- Comprehensive means for **security test and certification** evaluation

In ECHO, we use Cyber Ranges as virtual environments for:

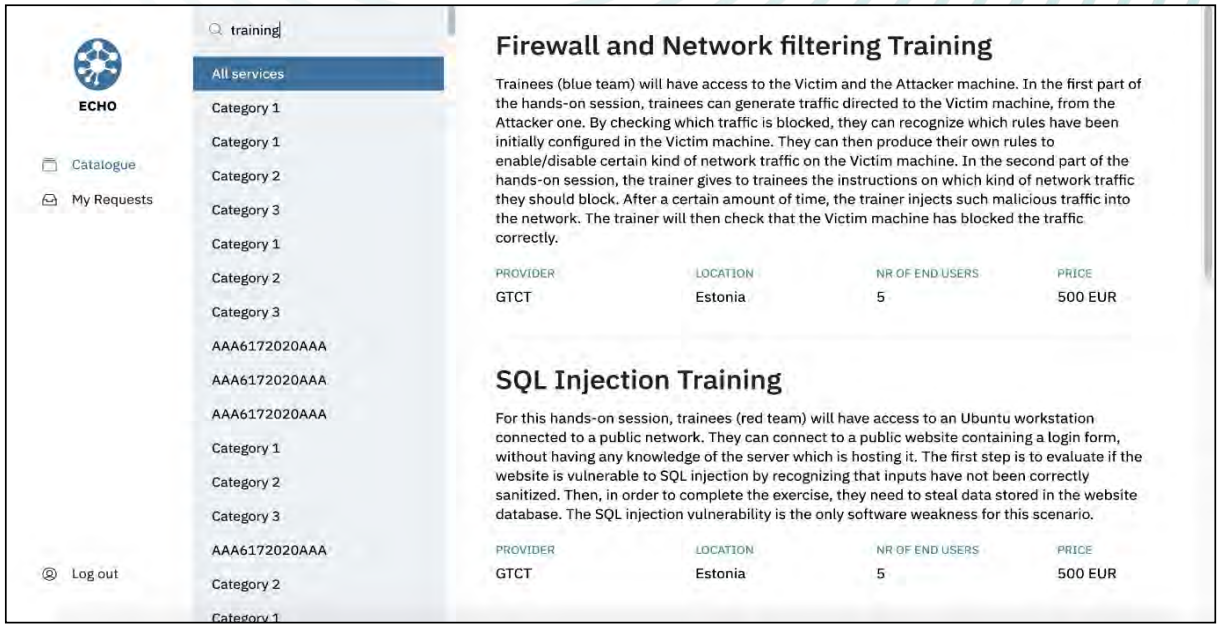
- **R&D, Testing** and **demonstration** of **technology roadmaps**
- Delivery of specific instances of the **cyberskills training** curricula

ECHO Technology Roadmaps

The ECHO Federated Cyber Range (E-FCR)

The goal of the ECHO Federated Cyber Range (E-FCR) is to:

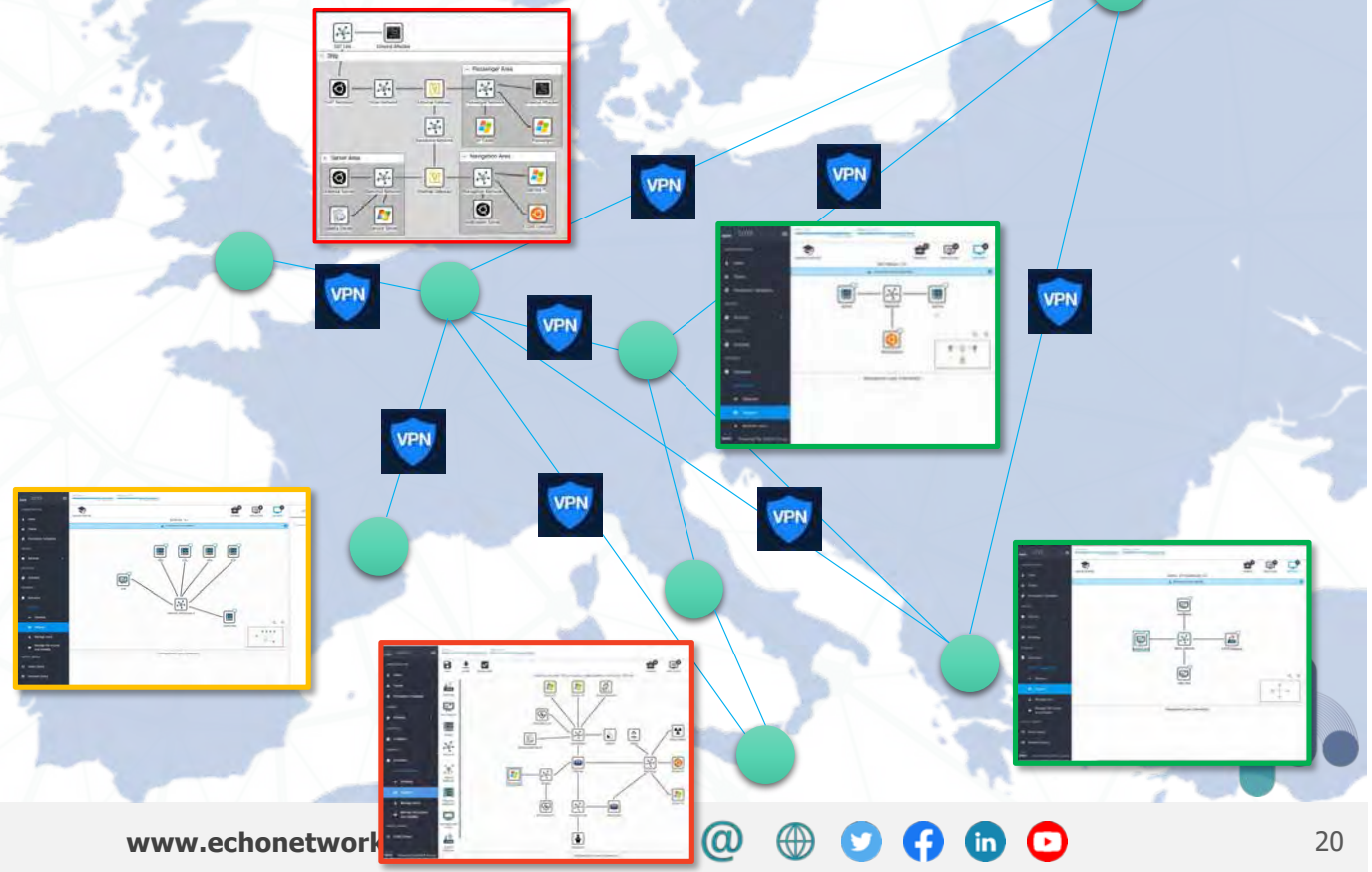
- Interconnect existing and new cyber range capabilities through a convenient **portal** and **VPN connections**
- Portal operates as a **broker** among cyber ranges
- A **marketplace** enable content providers to sell cyber range contents to a wider market
- Enables access to complex emulations of **sector specific and unique technologies**



ECHO Federated Cyber Range (E-FCR)

Where are we currently?

- Development is **complete,** actually in **validation**
- We actually federated **9** different cyber ranges
- We federated ranges for **training**, **testing** and **R&D**
- The team is working on the **ECHO Demonstration cases**



ECHO Inter-sector Prototype tools

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

Objectives

Address most **pressing** transversal and inter-sector cybersecurity **challenges**
Cover **priority areas**
Increase **cybersecurity awareness**

2

Selection methodology

Detailed selection methodology based on **challenges**, **priority areas** covered, **innovation**, relevance, adaptability etc.

3

Development process

Scrum based development framework for integration, installation and testing of tools.

4

Outcomes

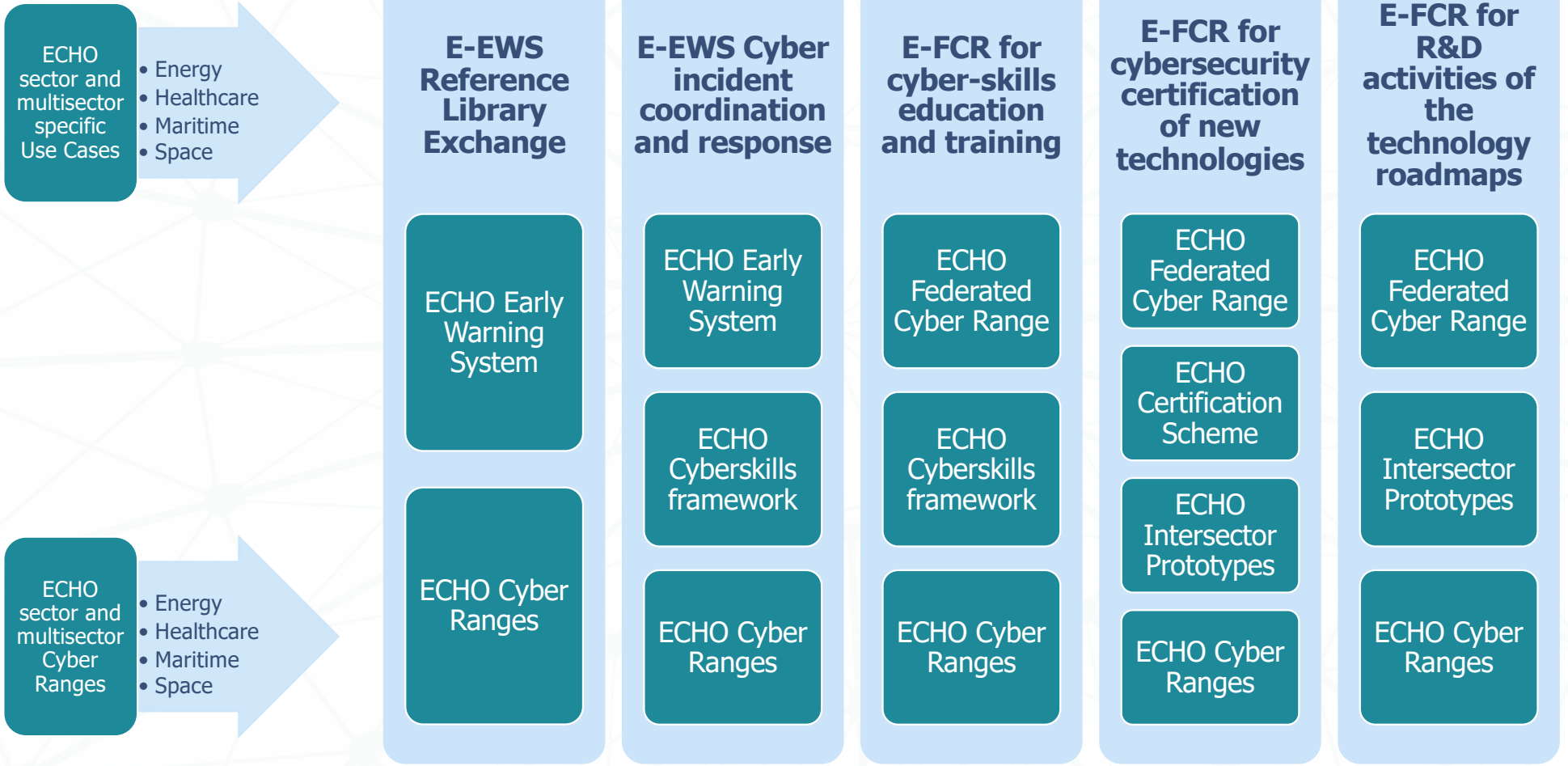
14 Iinnovative solutions based on **state-of-the-art** tools, techniques & methodologies
Leverage **known technologies** (Nmap, Snort, Nikto, Kali etc.)
Increase cybersecurity awareness through dedicated workshops/demonstrations

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

- **Sector demonstration cases**
  - To demonstrate technologies and frameworks we developed during the project we implemented a set of complex **Demonstration Cases**
  - ECHO Demonstration Cases target **all ECHO technologies** and cover **all critical sectors** where we are involved
    - Energy
    - Maritime
    - Healthcare
    - Space

Demonstration cases for validation

ECHO Demonstration Cases



Demonstration scenario

Energy Sector

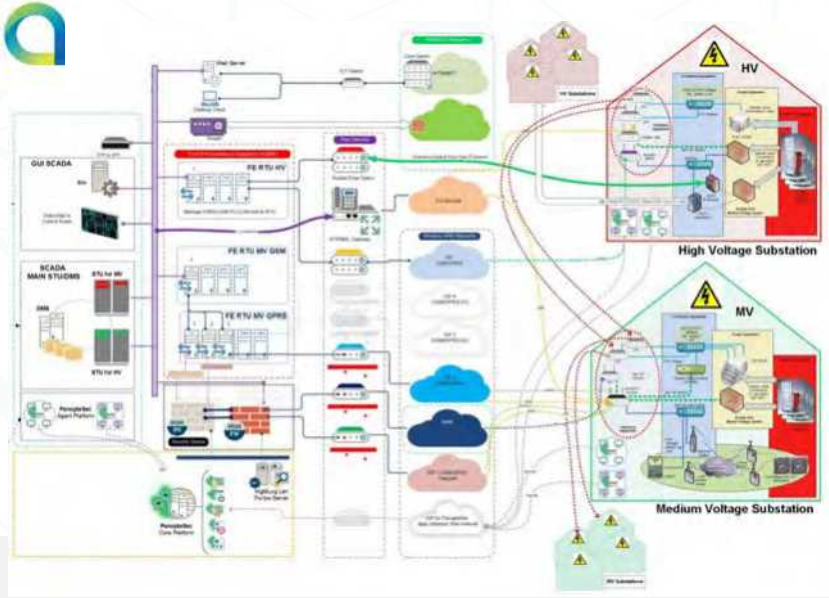
The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

The energy sector faces increasing and more sophisticated cyber threats affecting both the IT and OT side

Some use cases to be implemented in the demo case

- Attacks against the command-and-control systems of an energy provider
- Attacks to SCADA equipment/devices of an energy provider

We implemented a sector-specific cyber range emulating a C&C Centre to support the Demonstration Cases



Demonstration scenario

Healthcare Sector

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

ICT is becoming more and more pervasive in the healthcare sector

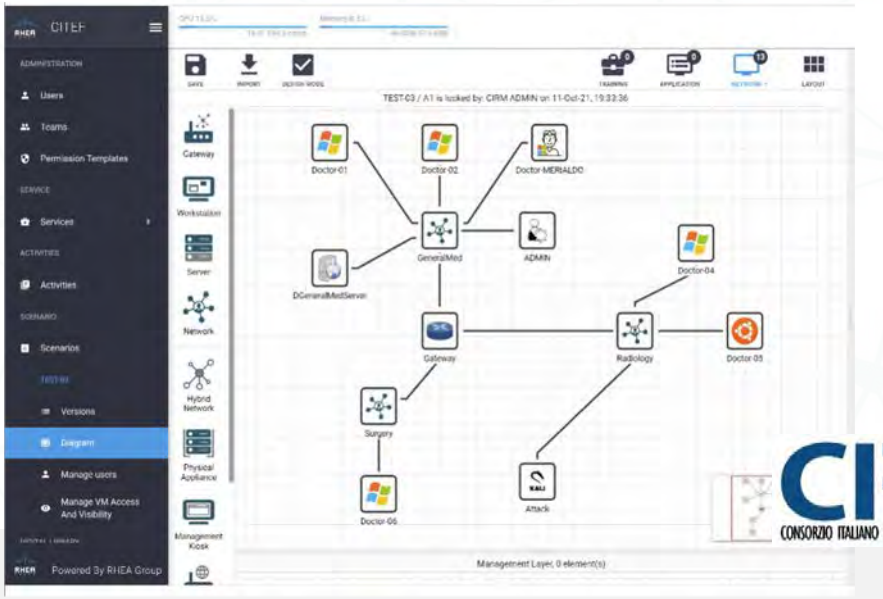
- Computerized systems for automation of diagnostic and collection of patient data
- Sensors and medical devices with IP addresses connected to the Internet (IOT)
- Multidisciplinary teams interact with patient and share sensitive data also through personal devices

Some use cases to be implemented

- Attacks against complex medical systems (blood analysis laboratory)
- Attacks against corporate IT system via ransomware

We implemented two sector-specific cyber range to support the Demonstration Cases

- Corporate hospital IT system
- Blood sample analysis lab emulation



CRM
CONSORZIO ITALIANO PER LA RICERCA IN MEDICINA

Demonstration scenario

Maritime Sector

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

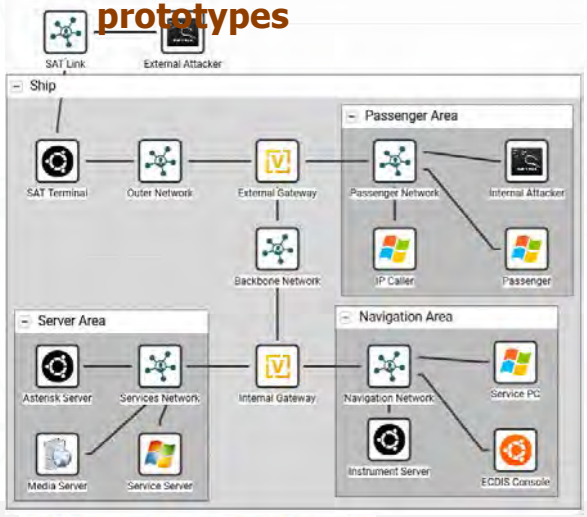
The maritime sector is already strongly digitized and it is of strategic importance

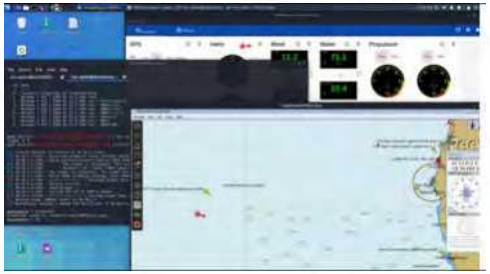
IT and OT networks are highly integrated, raising specific challenges

Some use cases to be implemented

- Attacks against ship's navigation systems via the GPS link
- Attacks against ship's OT systems

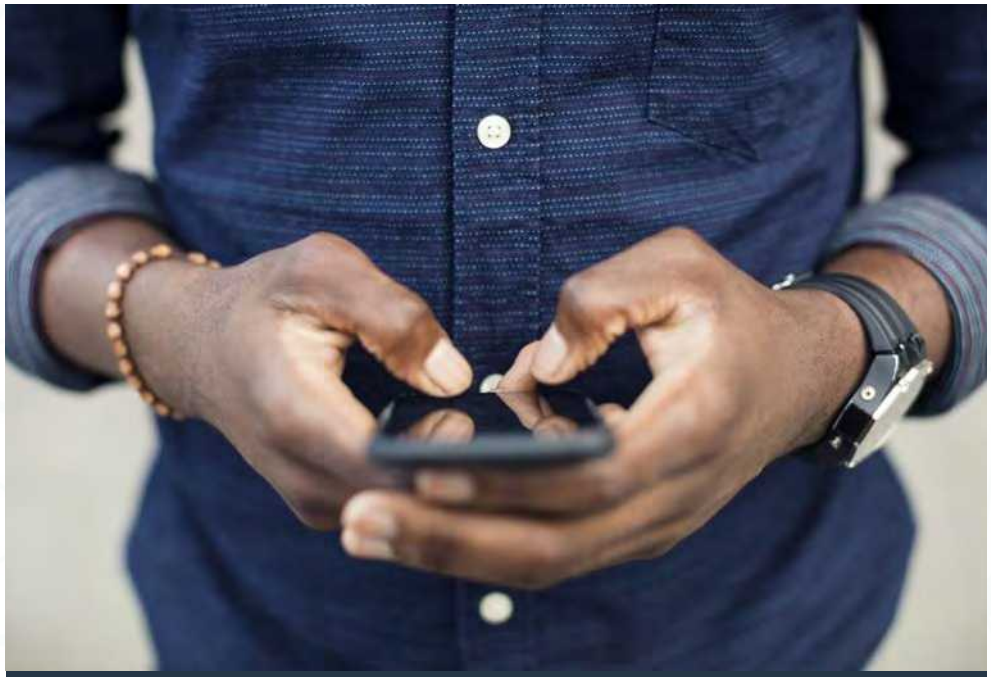
We implemented two sector-specific cyber ranges to support the demonstration cases of technologies and prototypes





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, training
  - 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..), **potentially at EU level**
- 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



Get in Touch with Us and Follow us on Social Media!

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

info@echonetwork.eu

www.echonetwork.eu

https://twitter.com/**ECHOcybersec**

https://www.facebook.com/**echonetworkeurope/**

https://www.linkedin.com/in/**echo-cybersecurity**

https://www.youtube.com/channel/**UCDQBXrQhoLJ2lnf38x1X6Uw**

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

Thank You

Matteo Merialdo
www.echonetwork.eu

1–3 June 2022
Brussels

CONVERGENCE NEXT

Cyber Competence Network

SPARTA

Research Results - SPARTA
June 2, 2022

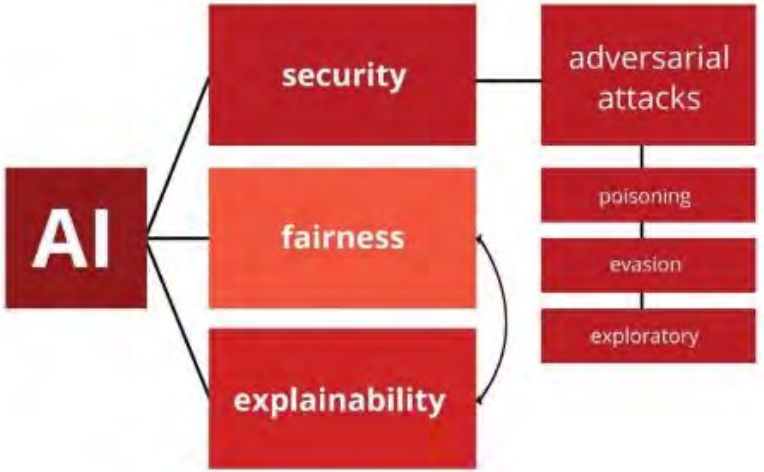
SPARTA PROGRAM
SAFAIR - CONTEXT

- **How to trust AI?**
  - A lot of advances in recent years
  - Much more widespread
  - Started to be used in industrial context
  - Sometimes in safety critical systems

- Apart from achieving good accuracy, there are many challenges that need to be discussed to effectively apply AI in critical applications

SAFAIR - GOALS

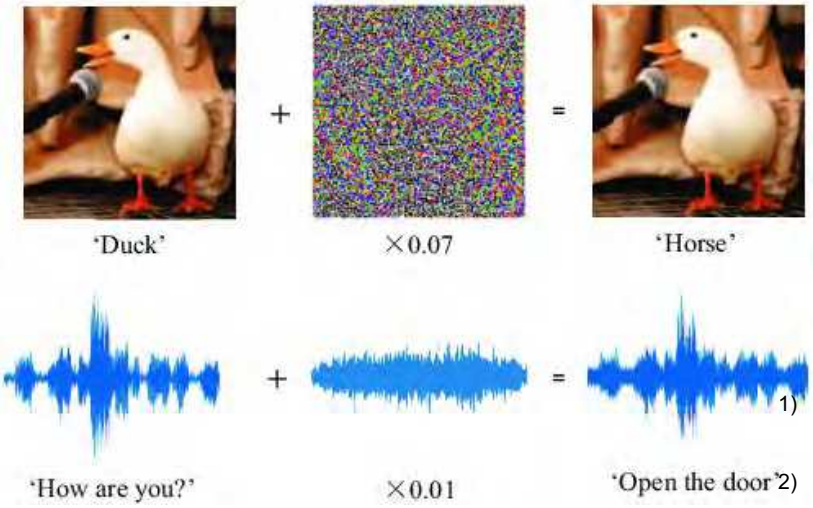
- **Main goals**
  - Robustness against attacks
  - Explainability
  - Fairness
- **Not forgetting**
  - Awareness
  - Legal framework



ROBUSTNESS

- **What is an adversarial attack?**
  - Perturbed input that induce classification error
  - Often imperceptible

2)



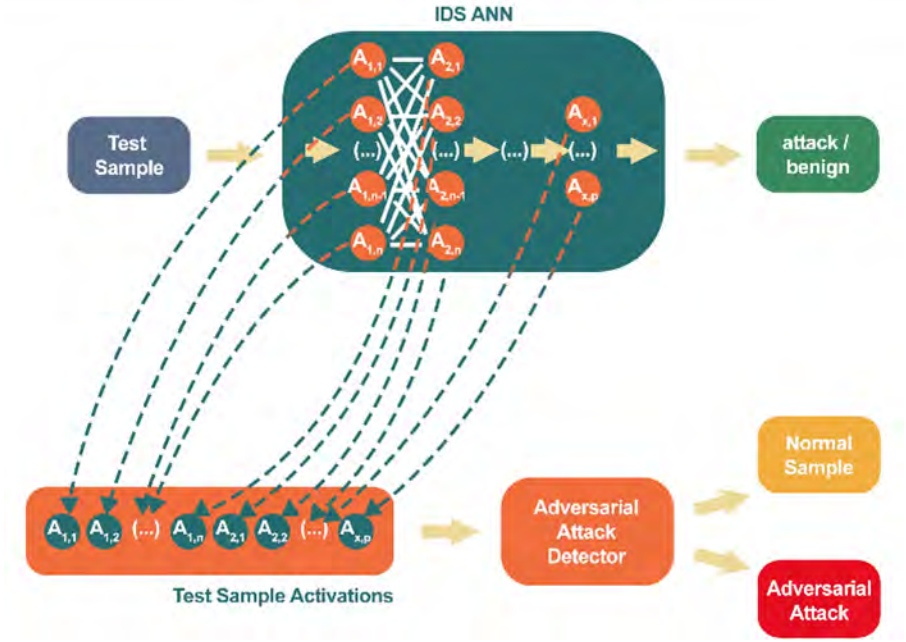
1)

1) T. Gu, K. Liu, B. Dolan-Gavitt and S. Garg, "BadNets: Evaluating Backdooring Attacks on Deep Neural Networks," in *IEEE Access*, vol. 7, pp. 47230-47244, 2019. doi: 10.1109/ACCESS.2019.2909068

2) Gong, Yuan & Poellabauer, Christian. (2018). An Overview of Vulnerabilities of Voice Controlled Systems.

ROBUSTNESS - DEMO

- **Intrusion detection system**
  - AI system to detect intrusion based on network info
  - Intercepting adversarial attacks on IDS
    - 4 adversarial attacks tested
    - Detection method implemented
    - Model keeps a good accuracy



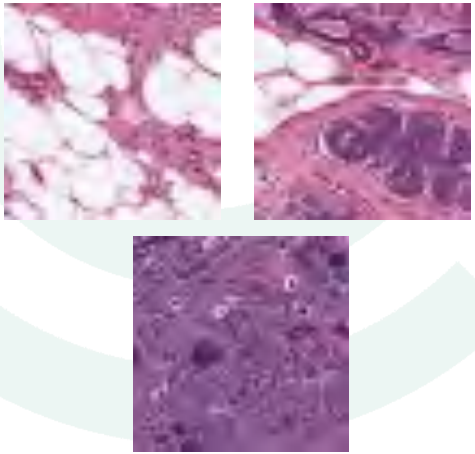
ROBUSTNESS - DEMO

- **Intrusion detection system**

Video itti-adv-training.mp4

ROBUSTNESS

- **Healthcare Image defense**
  - How to protect a breast cancer detection AI from attacks
  - Specific defenses were implemented

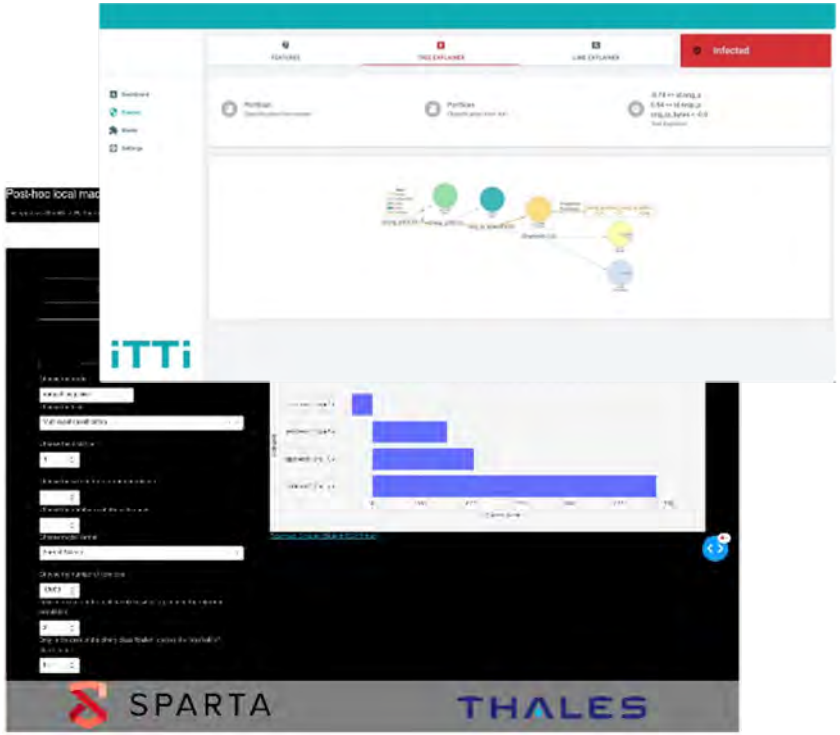


Other applications on:

- PDF malware detection
- Face reidentification
- Graph Anomaly Detection

EXPLAINABILITY

- **What to explain?**
  - Most AI systems are black boxes
  - Explain the decision to human user in understandable terms
- **Why?**
  - Provide trust in the decision
  - Enhance the utility of the AI system
  - Help model acceptation



EXPLAINABILITY - DEMO

- **Hybrid Oracle-Explainer**
  - **State-of-the-art XAI System** based on Surrogate type approach.
  - **ORACLE** delivers high quality predictions thanks to the deep learning architecture.
  - **EXPLAINER**, adopting combination of micro aggregation with shallow decision trees provides simple visualizations.
  - Whole system, because of it modular nature maintains **flexibility and openness** for further improvements.

EXPLAINABILITY - DEMO

- **Hybrid Oracle-Explainer**

Video itti-explanability.mp4

FAIRNESS

- **What does fairness means for an AI system?**
  - Fairness in AI is mainly ethically and legally motivated.
  - AI system is supposed to be fully objective, is it not?

  - In practice, the fairness of AI-driven decisions depends highly on the data provided as the input to learning algorithms.
  - This data can be (and often is) biased due to several reasons:
    - bias of human operators providing this data as input, resulting e.g. in biased labeling of samples,
    - data unbalance/misrepresentation of e.g. specific minority groups,
    - historical bias (discrimination)

FAIRNESS - DEMO

Video thales-fairness.mp4

SAFAIR – Additional results

- AI Threat Knowledge Base (also evaluated by experts)
- SAFAIR AI Contest
- Study of the implication of GDPR to AI systems
- Fairness in “The Artificial Intelligence Act”


1–3 June 2022
Brussels
CONVERGENCE NEXT
Cyber Competence Network

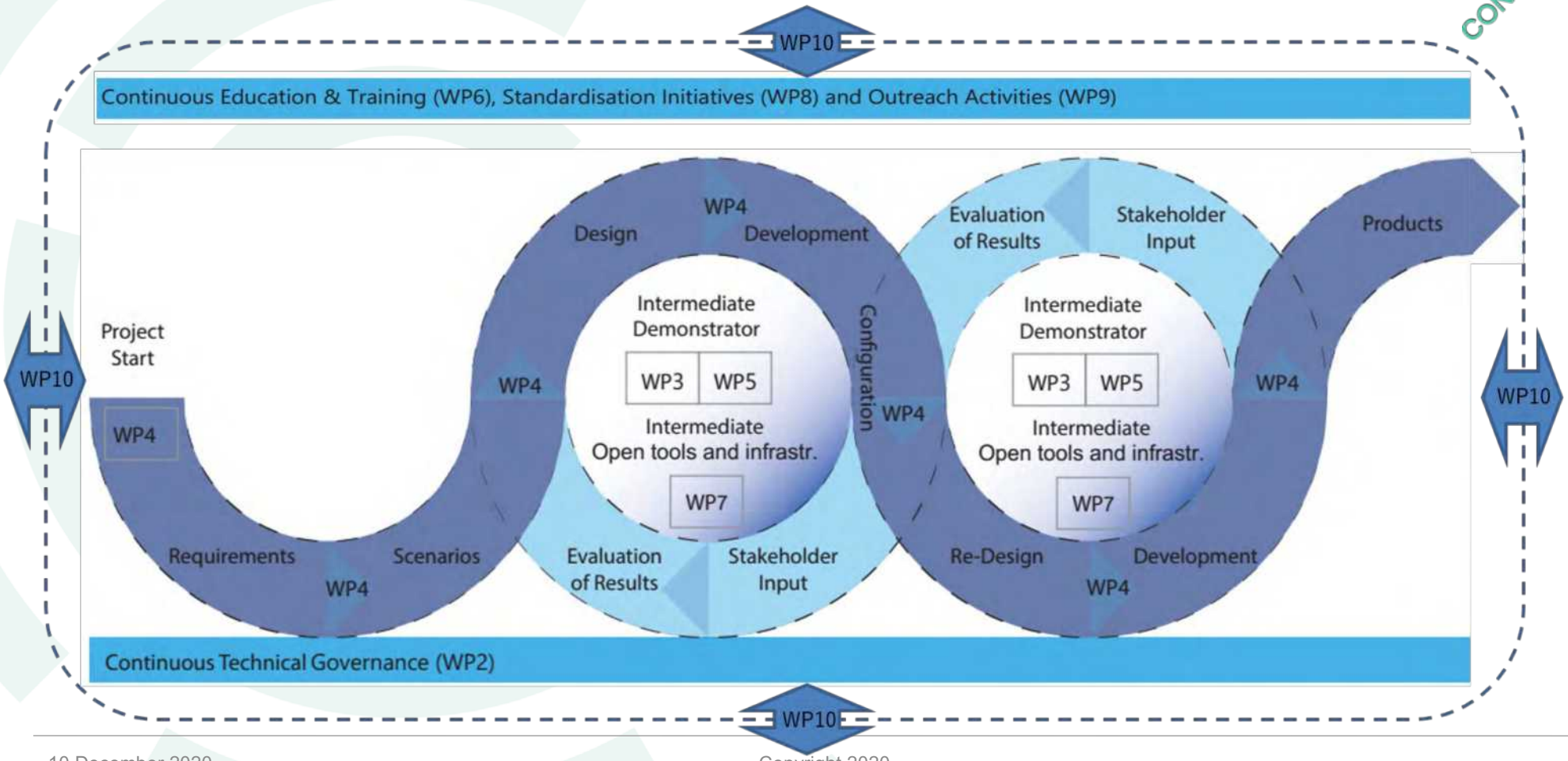
CyberSec4Europe Work Package 5 Demonstration Cases

Alessandro Sforzin
NEC Laboratories Europe GmbH
alessandro.sforzin@neclab.eu

WP5 Goals

- To **identify** and **analyze** cybersecurity industrial **challenges** in the project's selected sectors.
- To translate those challenges into demonstration cases.
- To **implement**, **test**, and **validate** said demonstration cases.
- To **provide requirements** that guide research, technology development, and design in WP3.
- To **collaborate** closely with **WP3** and **WP4** to define common security and privacy building blocks and demonstrate how they can improve cybersecurity in a variety of vertical sectors, such as health, smart cities, finance, e-commerce, transport, and supply chain.

WP5 Role Within CyberSec4Europe



WP5 At a Glance

Work Package 5 – Demonstration Cases

David Goodman
david@trustindigitallife.eu

Open Banking
Sharing fraud data pseudonymously

Stephan Krenn
Stephan.Krenn@ait.ac.at

Higher Education
Privacy-preserving identity management

Panayiotis Kotzanikolaou
pkotzani@unipi.gr

Maritime Transport
Threat modelling
Secure communication

Vincenzo Savarino
vincenzo.savarino@eng.it

Smart Cities
User-centric infrastructure
Open innovation cycle

Supply Chain
Dispute resolution
Compliance & accountability

Martin Wimmer
martin.r.wimmer@siemens.com

Incident Reporting
Financial sector
Data management & reporting

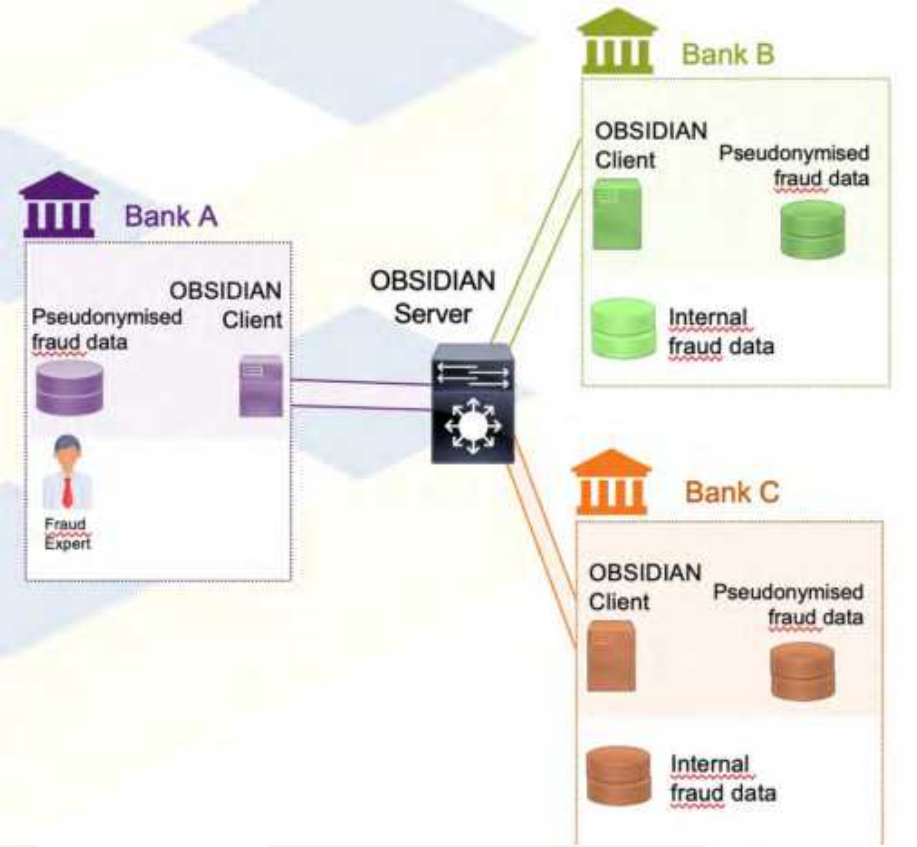
Susana Gonzalez Zarzosa
susana.gzarzosa@atos.net

Medical Data Exchange
Protecting shared health data through anonymization

Juan Carlos Perez Baun
juan.perezb@atos.net

WP5 Tasks

T5.1: Open Banking



Open Banking represents a new wave in financial transactions including payments, closely related to Payment Services Directive 2 (PSD2) and the GDPR.

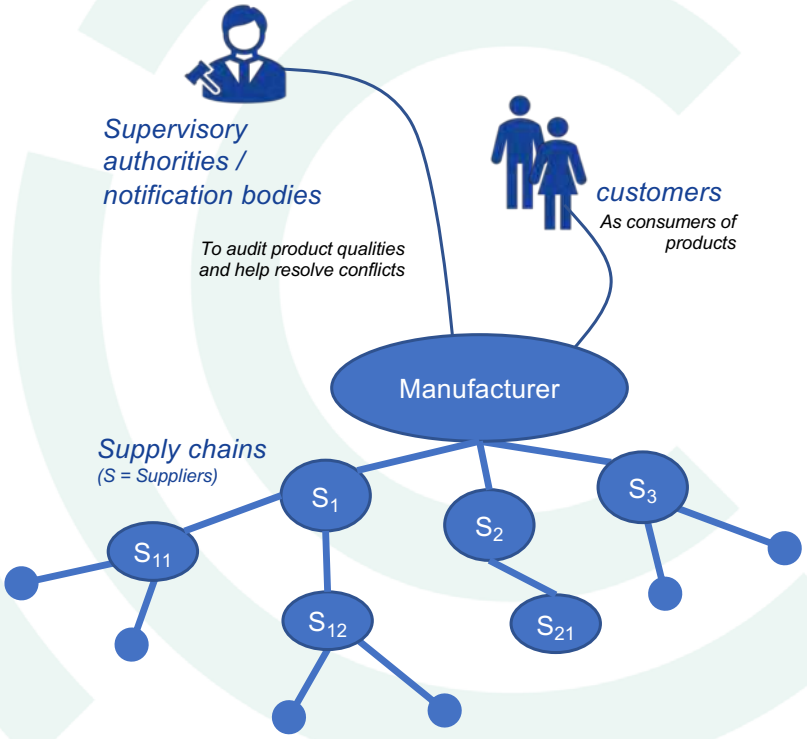
One of the use cases is **OBSIDIAN:**

Open Banking Sensitive Data Sharing Network for Europe

- To support the fight against fraud by sharing IBAN information between banks
- To be more effective in detecting money laundering or terrorist financing to protect the European market in an open economy

The OBSIDIAN server does not store fraud data and a suspected IBAN is always pseudonymized when exchanged

T5.2: Supply Chain Security Assurance



Supply Chain Security Demonstrator is about

- … securing highly distributed, cross-organizational business processes, focusing on
  - guaranteeing workflow compliance and ensuring non-repudiation
  - identifying and resolving disputes
- … demonstrating security architectures and processes that allow building up trust between business partners without the need (and/or possibility) to rely on a trusted 3rd party

The Demonstrator illustrates

- … How to ensure accountability of actions through an immutable audit log by using a blockchain architecture
- … The enforcement of business process compliance through a Petri Nets based workflow layer in combination with smart contracts
- … the secure sharing of confidential information via private channels and data storage

T5.3: Privacy-Preserving Identity Management

General

Existing online authentication mechanisms often lead over-identification of users

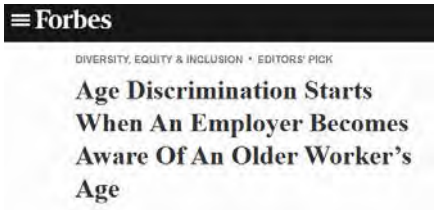
- E.g., there is no need to identify a user if only a age limit needs to be checked

Privacy-preserving identity management …

- … lets the user decide which information to disclose
- … guarantees unlinkability of actions by the same user
- … avoids re-identification of a user
- … gives the relying party cryptographic authenticity guarantees

Demonstration Use Case

There is a trade-off between privacy and authenticity in job application processes



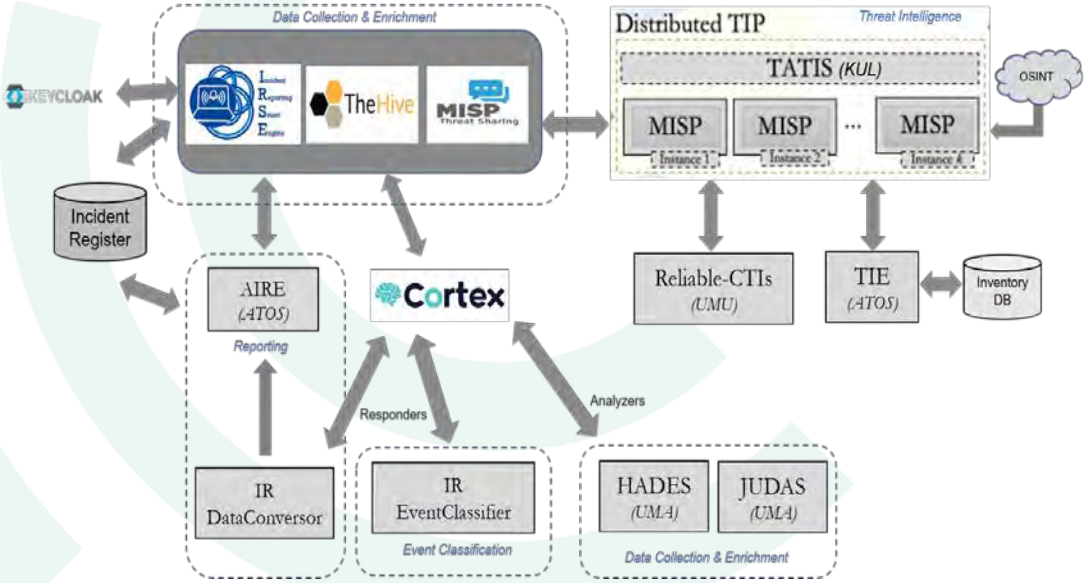
- Fake university degrees have been a problem in many countries, and should thus be detected
- But anonymity in the application processes decreases discrimination (e.g., age, sex, …)

CyberSec4Europe is thus developing and validating a privacy-preserving job application portal

T5.4: Incident Reporting in the Financial Sector

Demonstrator Goal:

Platform that enables financial entities to comply with mandatory incident reporting to the Supervisory Authorities according to the different procedures and methods specified by applicable regulatory bodies.



Use Cases:

- IR-UC1: Data Collection, Enrichment and Classification
- IR-UC2: Managerial Judgement
- IR-UC3: Data conversion and reporting preparation
- IR-UC4: Data Sharing for Threat Intelligence Analysis

Regulations supported:

- EBA-PSD2 (Payment Service Directive)
- ECB-SSM (European Central Bank)
- NIS (operators of Essential Services)
- eIDAS (Trust Service Providers)
- TARGET2 (TARGET2 critical participants)
- GDPR

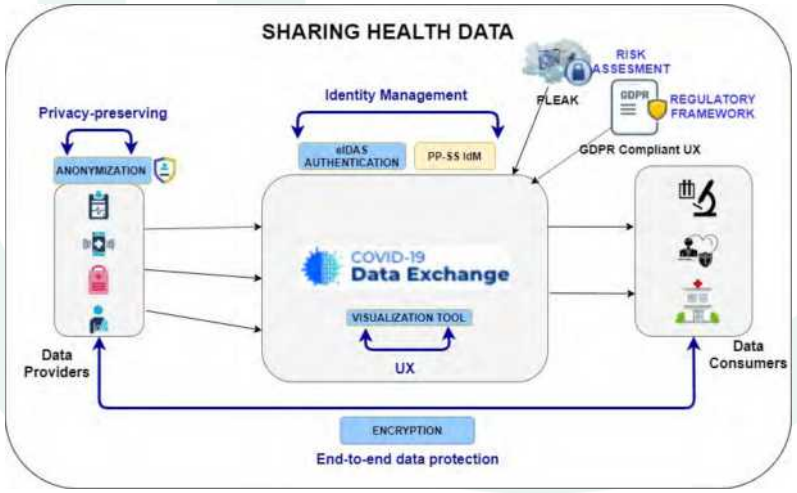
T5.6: Medical Data Exchange

GOAL

CREATE A TRUSTED ENVIRONMENT FOR SHARING DATA

- Providing security measures when data are shared
- Preserving user data privacy at any moment
- Being compliance with EU laws and regulations.
- Improving the data access control
- Generating new business opportunities

CHALLENGES



- Securing data by **functional encryption** tools: **FE2MED**
- Preserving user data privacy by **anonym.** tools: **DANS**
- Privacy analysis tool**: PLEAK**
- Secure access to DEP by **strong authentication mechanisms: eIDAS network**
- Compliance with regulations → **GDPR tool**
- Improve user experience → **Data visualization tool**
- New business opportunities → **COVID-19 DEP**

SOLUTIONS

T5.7: Smart Cities

Objectives

1)Create **a user centric infrastructure** to support **sensor, urban data platform** and other digital infrastructures for **identity** and **personal data exchange and reuse in public services**, in compliance with **GDPR**;

2) Setup an **Open Innovation Cycle** that will drive city stakeholders from cyber security **risks and needs assessment** to the identification of the related solutions.

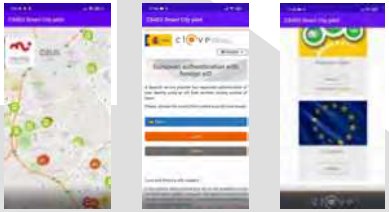
Challenges

- Trusted Digital Platform
- Cyber threat intelligence and analysis platform
- Cyber competence and awareness program
- End User trusted data management and Privacy by Design
- Interoperability between legacy and new systems
- Logging and monitoring

Application Cases

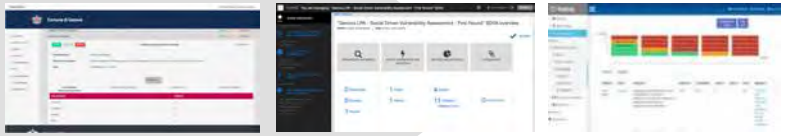
Murcia

- Extending the security and privacy aspects in Smart City Data Platform



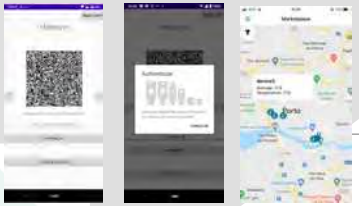
Genova

- User Centric Privacy Consent Management
- Assessment and prevention of cyber security attacks
- Estimating attack impacts



Porto

- Anonymization and privacy-preserving models for sensor network platform



T5.5 – Maritime Transport

Thank You!

Alessandro Sforzin
alessandro.sforzin@neclab.eu

Maritime Transport CyberSec4Europe

Cyber Competence Network

Cyber Security for Europe

Maritime Transport

Maritime Transport is a complex activity, engaging all the **structures, modes** and **equipment** required for the carriage of passengers or goods via sea.

Maritime transport is seen as the driving force of international trade and the backbone of globalization.

Attack Surface-Services to be Protected

Critical Services

- Ship accommodation
- Management of water transport infrastructure
- Information,accommodation, screening and boarding of passengers
- Vessel traffic services
- Passenger transport
- Transport of freight and dangerous goods
- Route planning
- Ship maintenance

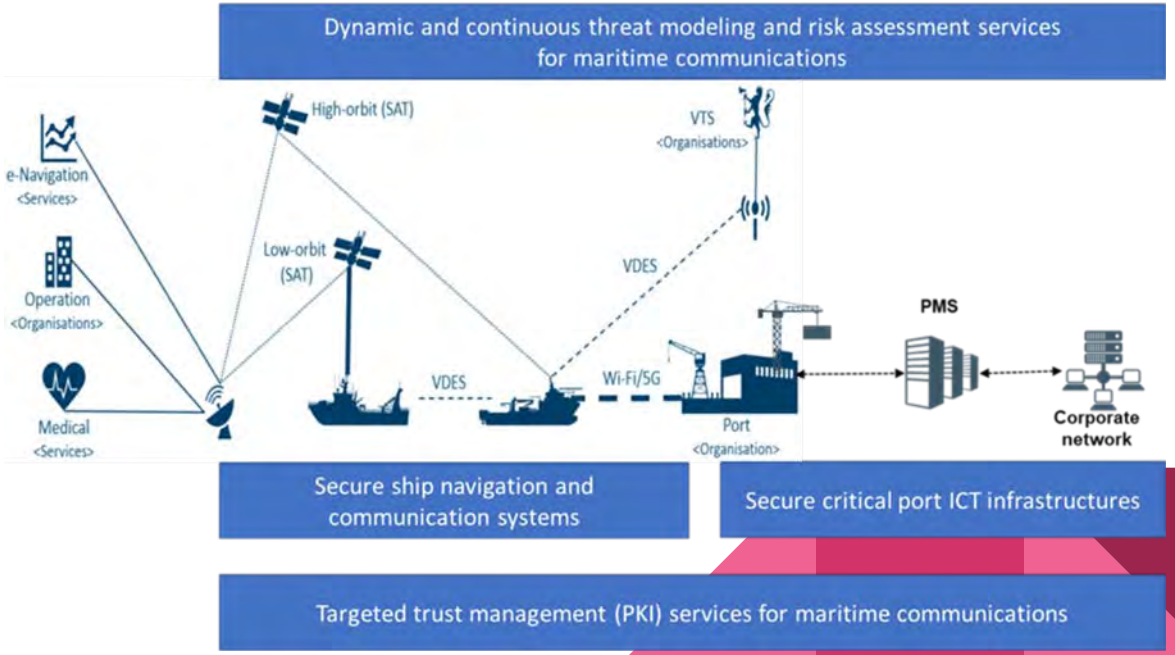
Known Threats

- GPS spoofing
- Unauthorized access to on-board mobile devices
- Manipulation of bill of lading
- Signal jamming
- Targeted access to automated terminal infrastructures
- Spear phishing
- DoS Supply chain attacks
- IoT attacks

Goals of the Maritime Transport

The effective protection of the maritime transport that arises from the interconnections and interdependencies of a set of maritime entities, such as port authorities, ministries and maritime companies in the business of cargo and passenger transfer.

- Manage security threats and risks
- Harden the security of the involved systems
- Secure the communications between the various maritime systems



Security Services and Use Cases Developed

Threat modeling and risk analysis for maritime transport services: this UC describes the functionalities related with the threat modeling and risk assessment services.

Maritime system software hardening: it describes the process of software hardening for critical maritime systems.

Secure maritime communications : it describes various maritime communications that require security services such as confidentiality, integrity and authentication.

Trust infrastructure for secure maritime communication: it describes the functionalities related with the design of a trust infrastructure, required to support system and communication security for the maritime sector.

Maritime Transport Service Demonstration

Secure Maritime Communications

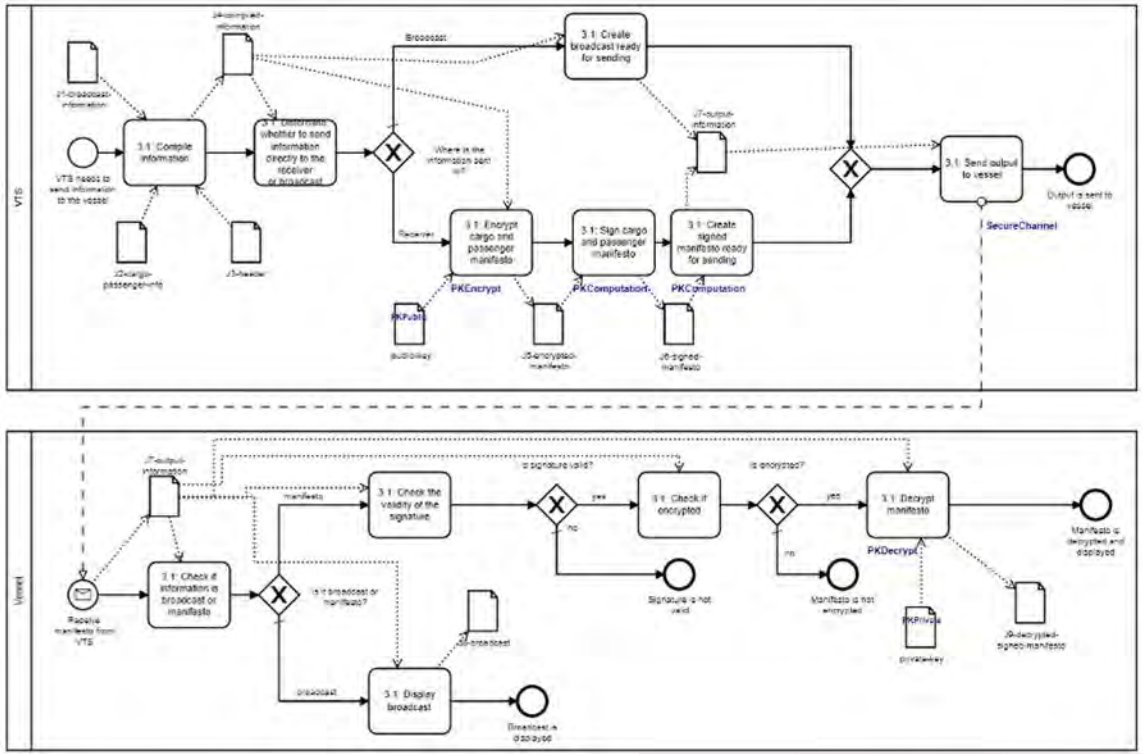
Currently there are no cryptographic authentication, authorisation or integrity measures in place in maritime communications.

- AIS does not easily allow for cryptography (messages are too small)
- VDES is the new standard which can accommodate crypto

We have implemented a VDES ready communications prototype that connects to a PKI and allows for cryptographically secure communications

Secure Maritime Communications Prototype

- Privacy- and security-by-design
- We use PE-BPMN, visibility tables and leakage analysis
- White-box penetration testing



Generated visibility tables and leakage analysis

#	J1-broadcast-information	J2-cargo-passenger-info	J3-header	J4-compiled-information	J5-encrypted-manifesto	J6-signed-manifesto	J7-output-information	J8-broadcast	J9-decrypted-signed-manifesto	private-key	public-key
VTS	O	O	O	V	H	H	H	-	-	-	O
Vessel	-	-	-	-	-	-	H	V	V	O	-
	I	I	I	I	I	I	D				I
Shared over	-	-	-	-	-	-	S	-	-	-	-

V (Visible) – contents of this data object are fully visible to the stakeholder;

H (Hidden) – the stakeholder has the data object, but the object has a form of protection on it;

"-" – the stakeholder does not see this data object in the process;

D (Direct dependency) – data A is an input to a task that produces data B, meaning that B directly depends on A;

I (Indirect dependency) – dependency between A and C, meaning that C indirectly depends on A

	J1-broadc…	J2-cargo-passenger-info.data	J3-header.header
J8-broadcast.data	if	if	always
J8-broadcast.header	never	never	always
J9-decrypted-signed-manifesto.data	if	if	never
J9-decrypted-signed-manifesto.header	never	never	always

Hardening Maritime Systems

- Maritime systems utilize native components, which are written in C/C++, and thus suffer from memory corruption vulnerabilities
- These vulnerabilities, if successfully exploited, can lead to severe consequences that threaten vessels' normal operation
- In the vertical, we apply *hardening* to these components for protecting them from exploitation

Control Flow Integrity (CFI)

- Control-flow hijacking attacks exploit memory corruption vulnerabilities to divert program execution away from the intended control flow
- Common objectives of such attacks include arbitrary code execution, privilege escalation, and exfiltration of sensitive information
- CFI restricts the set of possible control-flow transfers to those that are strictly required for correct program execution
- Enforcing CFI, for example, prevents code-reuse techniques, such as ROP, because they would cause the program to execute control-flow transfers, which are illegal under CFI

Example – Building OpenSSL with CFI

- OpenSSL is an open-source framework for building applications that use applied cryptography
- It is widely used by Internet servers, including the majority of HTTPS websites
- Exploiting OpenSSL leads to severe consequences
  - Remember the Heartbleed Bug!
- For this vertical, we offer a *hardened* version of OpenSSL based on CFI for preventing memory corruption attacks
- CFI-enabled OpenSSL protects the communication of the PKI service used by the vertical from memory corruption attacks

CFI Checks

- As shown, each target contains a single jump to the *hardened* implementation of each function

```
0000000000465198 <pkey_main>:
  465198:       e9 c3 4f fd ff          jmpq   43a160 <pkey_main.cfi>
  46519d:       cc                      int3
  46519e:       cc                      int3
  46519f:       cc                      int3

00000000004651a0 <pkeyparam_main>:
  4651a0:       e9 0b 56 fd ff          jmpq   43a7b0 <pkeyparam_main.cfi>
  4651a5:       cc                      int3
  4651a6:       cc                      int3
  4651a7:       cc                      int3

00000000004651a8 <pkeyutl_main>:
  4651a8:       e9 b3 58 fd ff          jmpq   43aa60 <pkeyutl_main.cfi>
  4651ad:       cc                      int3
  4651ae:       cc                      int3
  4651af:       cc                      int3

00000000004651b0 <prime_main>:
  4651b0:       e9 db 66 fd ff          jmpq   43b890 <prime_main.cfi>
  4651b5:       cc                      int3
  4651b6:       cc                      int3
  4651b7:       cc                      int3
```

Research Output

- Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator

  (Conference: IC3 '21: 2021 Thirteenth International Conference on Contemporary Computing)

- Modelling Human Tasks to Enhance Threat Identification in Critical Maritime Systems

  (Conference: PCI 2021: 25th Pan-Hellenic Conference on Informatics)

- An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector

  (Sensors 2022,MDPI)

- A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems

  (Computer Security. ESORICS 2021 International Workshops)

Research Applications

“A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems”

- **CVE-CWE-CAPEC Graph Database:**
- **CVSS Vector Translator**

1–3 June 2022
Brussels

CONVERGENCE NEXT

Cyber Competence Network

Pilots Overview

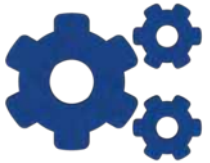
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

CONCORDIA's Service Board

CONCORDIA DEVELOPS

Developing of vertical industrial pilots and cross sectoral pilots using innovative cybersecurity tools

INDUSTRY PACT



CYBERSECURITY TOOL

CONCORDIA DEVELOPS

- CONCORDIA focuses on five industrial fields
  - Telecom
  - Finance and insurance
  - E-Mobility / E-Charging
  - E-Health
  - Vehicular Communication Systems

CONCORDIA DEVELOPS

CONCORDIA Industrial Impact

Threat Intelligence

DDoS Clearing House

CONCORDIA DEVELOPS

- Telecom
- Finance and insurance
- E-Mobility / E-Charging
- E-Health

01

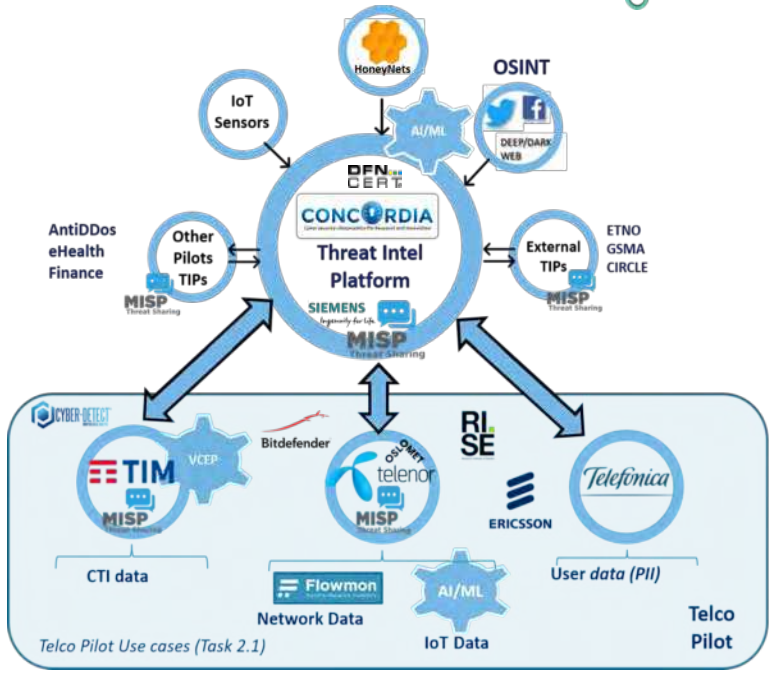
Telco Pilot

Telenor, OsloMet, Ericsson, TIM

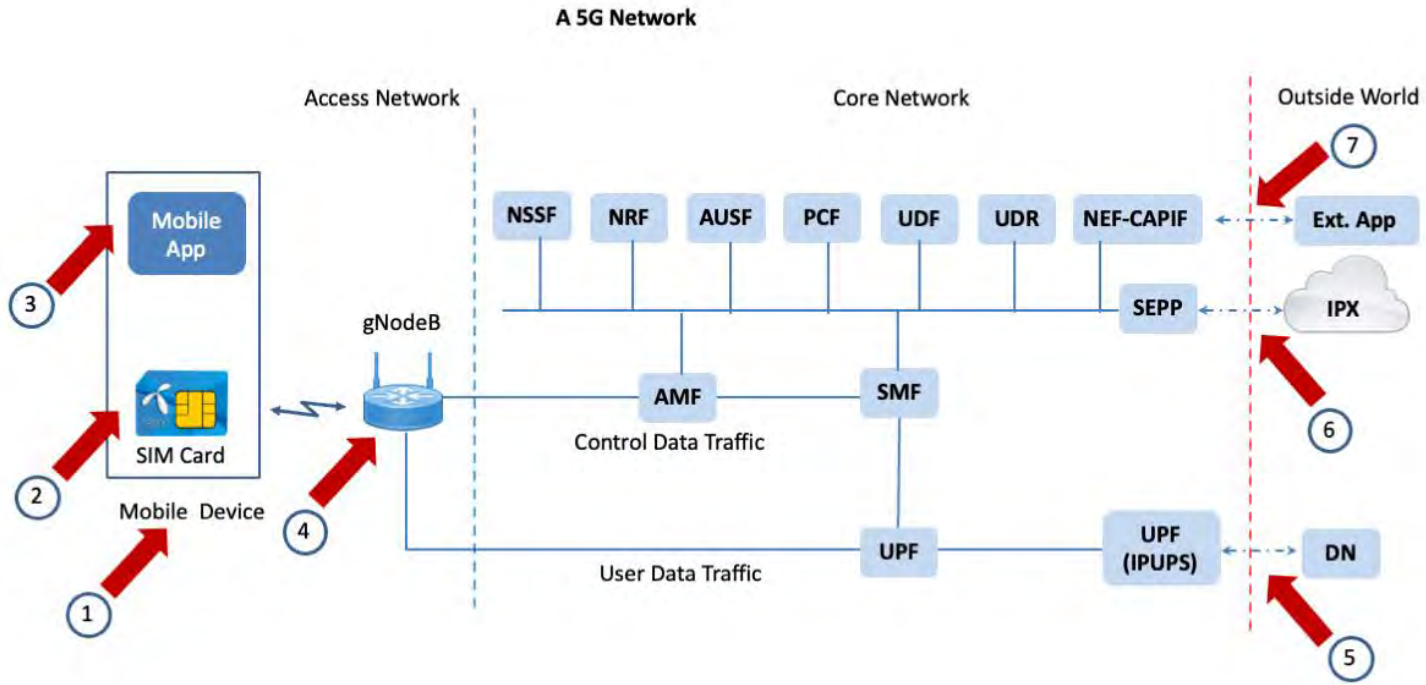
CONCORDIA
Mobile Threat Modelling Framework

Main Objective

- Extend and enhance the Concordia Threat Intelligence Platform with 3 use cases;
- From a telecom operator/ mobile network perspective, how to do this efficiently?



Threats in 5G



Threat Modelling

- The activity aiming at **identifying**, **understanding** and making simple **descriptions** or **models** of the potential threats and attack vectors that a system could be exposed for such that risk analyses, detection methods, countermeasures, and mitigation strategies can be developed.

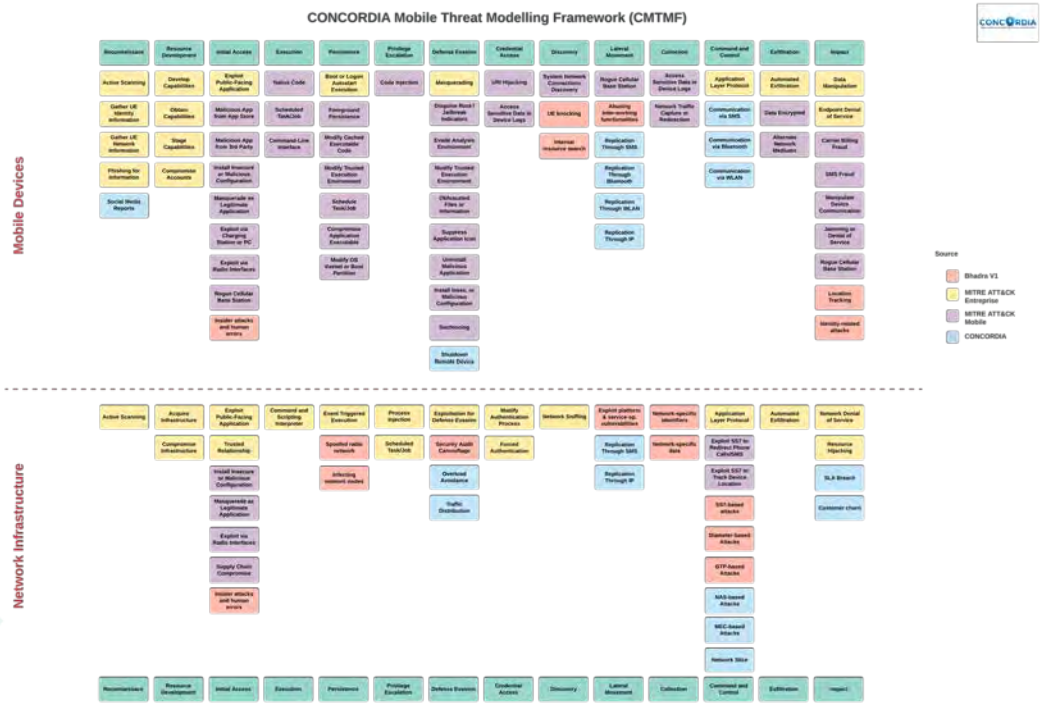
- The **attack-centric approach** (focus on attacks and attackers) is most appropriate for the threat modelling of mobile networks and the MITRE ATT&CK is selected as fundament for this work.

Beyond MITRE ATT&CK

- 5G networks are not only subject to the same cyber threats as regular enterprise networks but are also exposed to the ones brought by its capability of providing connectivity to billions of IoT devices ranging from primitive sensors to advanced medical equipment requiring ultra-reliable and low-latency connections. Potential attackers to 5G networks have different behaviours, tactics and techniques that require extensions to the current MITRE ATT&CK framework.

CONCORDIA Mobile Threat Modelling Framework

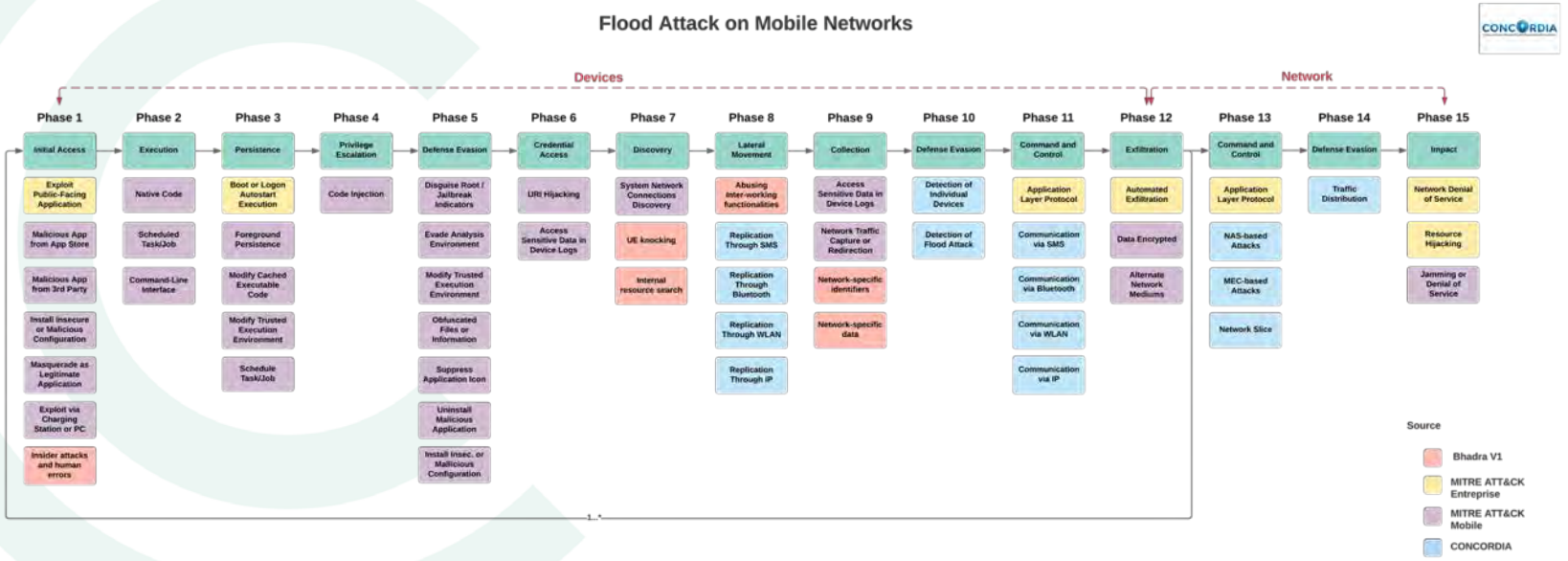
- To address this urgent need in the mobile networks, the Concordia Mobile Threat Modelling Framework (**CMTMF**) has been developed, which is a compatible combination of the enterprise, mobile and ICS (Industrial Control Systems) matrices of the MITRE ATT&CK framework.



CMTMF Features

- Like MITRE ATT&CK matrices, CMTMF is composed by **tactics** and **techniques**;
- However, **no tactic is unique**, instead we document an attack by **phases**;
- Attacks can be recursive as they spread to multiple devices, so we use **loops** to showcase this behaviour;
- An attack documented with CMTMF will reflect which effects it has had on **devices** as well as and alongside with the **operator's network infrastructure**;

Use Case: Flood Attack



Video: CMTMF Implementation in MISP Demo

Automated Processing of Threat Intelligence Information

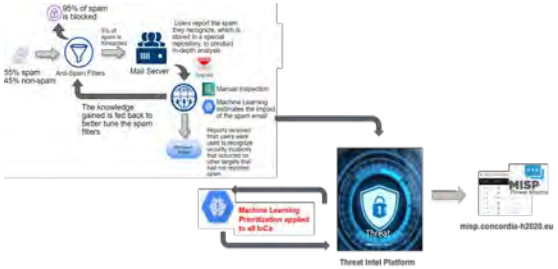
Automated Processing of TI Information

Description:

Provide an automated mechanism based on Machine Learning to help CTI analysts with the task of Indicator of Compromise prioritization to allow the consumption of most critical indicators.

Motivation

Cyber Threat Intelligence (CTI) analysts submerged by indicators, need tools for automatic analysis, validation and prioritization of different types of indicators in order to consume the most critical for our organization.



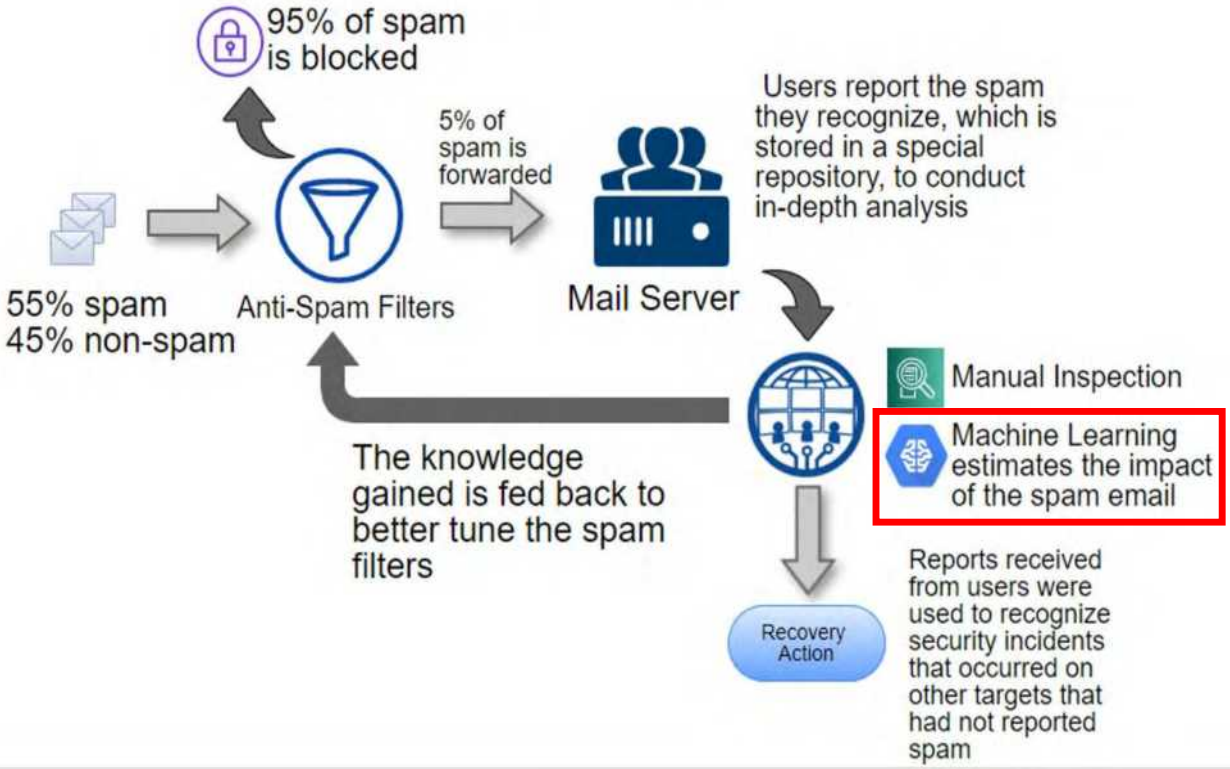
SoTA

State-of-the-art solutions: existing solutions for the triage of incident response indicators, not specifically for indicators from external heterogenous sources with different degrees of contextualization

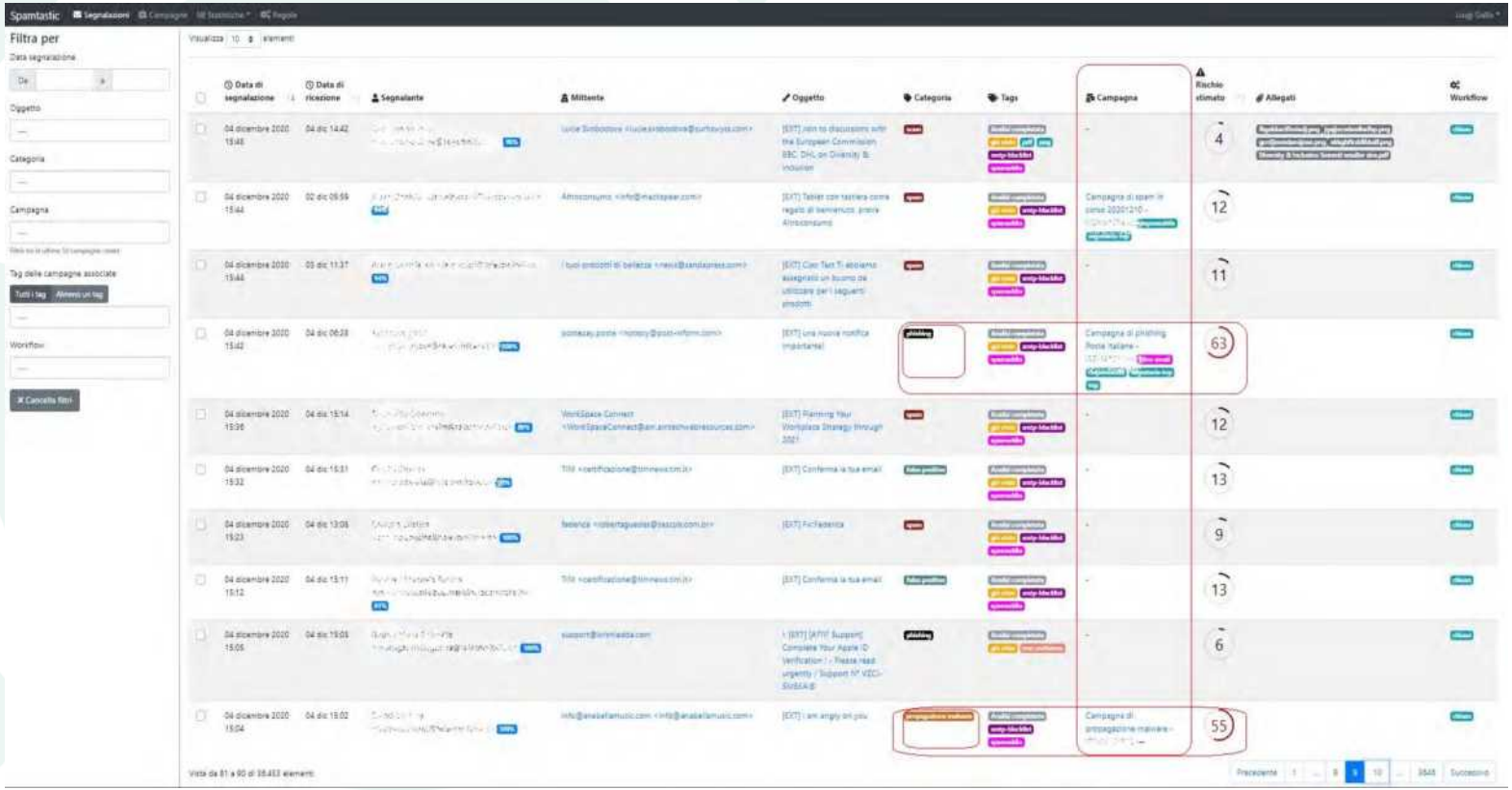
Automated Processing of TI Information

- Collaborative ML-based framework for analysis and classification of SPAM messages
- Paper published: "*2 Years in the anti-phishing group of a large company*" in "*Elsevier Computers and Security*" Journal, 2021
- Apply ML-based prioritization to all Threat Intelligence indicators of compromise

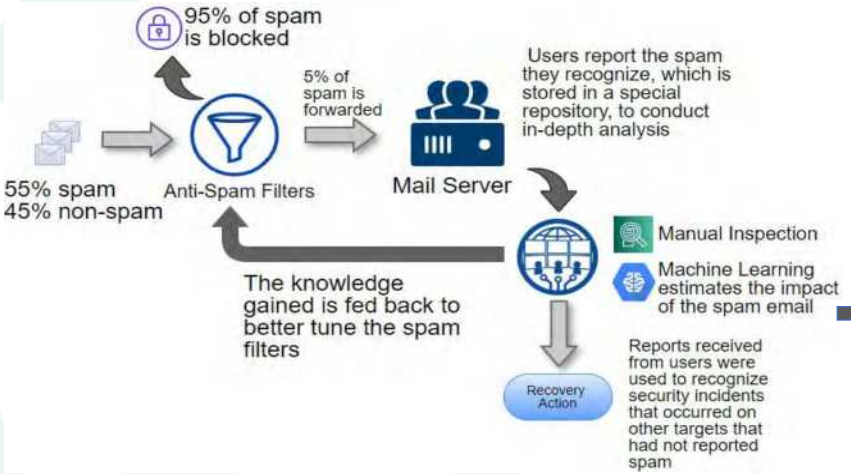
Automated Processing of TI Information: Scenario



Automated Processing of TI Information



Automated Processing of TI Information



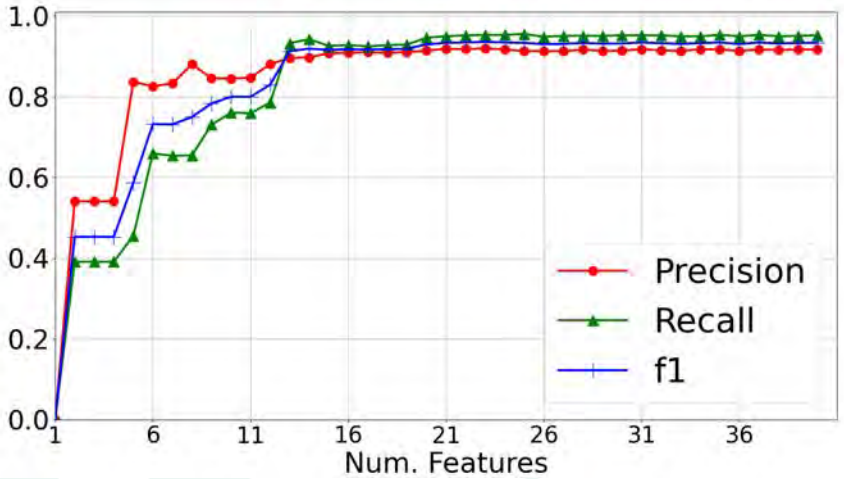
Prototype implementation of ML-based IoC prioritization for consumption

Threat Intel Platform

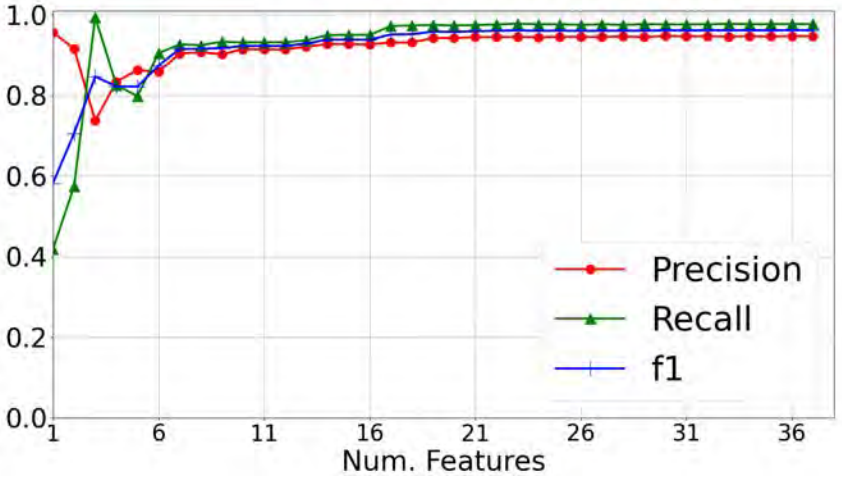
Machine Learning Prioritization applied to all IoCs

misp.concordia-h2020.eu

Performance



(a) Hash indicators



(b) Network indicators

02

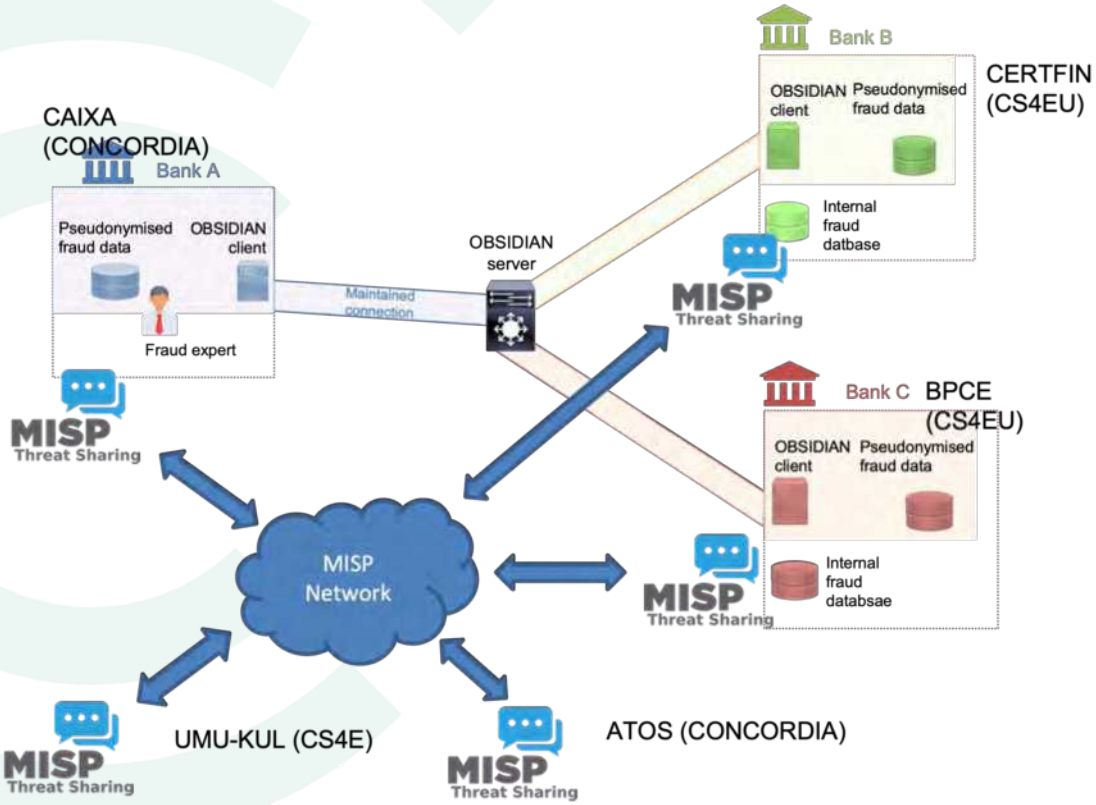
Financial Pilot

CAIXABANK

Financial cross-pilot

- The financial sector is a strategic and critical area in Europe, where cybersecurity plays a key role.
- Data sharing between financial entities on incidents and alerts is limited and managed by national regulations and company-specific policies.
- Both CONCORDIA and CyberSec4EU are addressing the needs of the financial sector, using CTI as one of the solutions.
- Regulations and GDPR are strong requirements in this work.

Integrated Scenario



03

Automotive Pilot

CRF, Efacec, Politecnico di Torino

Transport E-Mobility Sector

SoTA

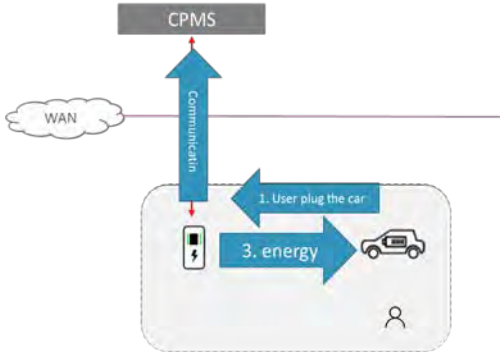
The actual configuration of EVCS is a simple system, where EV driver authenticate own person to the EVCS, then EVSE will make a hardware handshake where it will check the details of the EV, maximum power and voltage. After the protocol and physical handshake, it will deliver the energy to the car, in a process is dependent of the EV and EVSE technology.

Achievements:

A new cyber secured PnC system was developed in the EFACEC's laboratory.

This PnC system is developed with self made CPMS Software to take in account:

- Look for inter-operability
- Follow cyber security
- Implement recommended for the use case (15118-2 , OCPP 1.6+)



Monitoring and Certification of inbound logistics for the EV battery

SoTA

State-of-the-art solutions are based on limited interactions between the supply chain members: each company manages its information system and adopts its conventions and methodologies to ensure the quality of services and products offered to clients.

Achievements:

Assessment of different Blockchain infrastructures in order to define their characteristics, applicability, and impacts on the Supply Chain and Logistics networks.

The indicators used for the technical assessment are:

- Parallelism: number of different memory locations to read/write to;
- Size: dimension of the transaction in kB;
- Repetitions: number of read/writes per transaction.

	Resiliency	Scalability	Industrial adoption	Speed (TPS)	Community
Fabric (Raft)	4	5	5	5	5
GoQuorum (Raft)	3	5	2	4	4
GoQuorum (IBFT)	5	3	4	4	4
Besu (IBFT2)	5	3	2	3	4
Sawtooth (Raft)	3	5	1	2	3/4
Sawtooth (PBFT)	5	1	3/4	2	3/4

04

E-Health Pilot

Infineon

Paradigm Shift

	In the past	In the future
Aging society	In **hospitals**, IT-systems and medical devices must be protected	In **smart home: secure** data acquisition and **secure** data transmission to hospitals, clinics and family doctor´s;
Ambulance services	Vehicle for **transportation**	Vehicle for • 1st **patient analyzing** and • 1st **aid treatments** („mobile hospital on 4 wheels“)

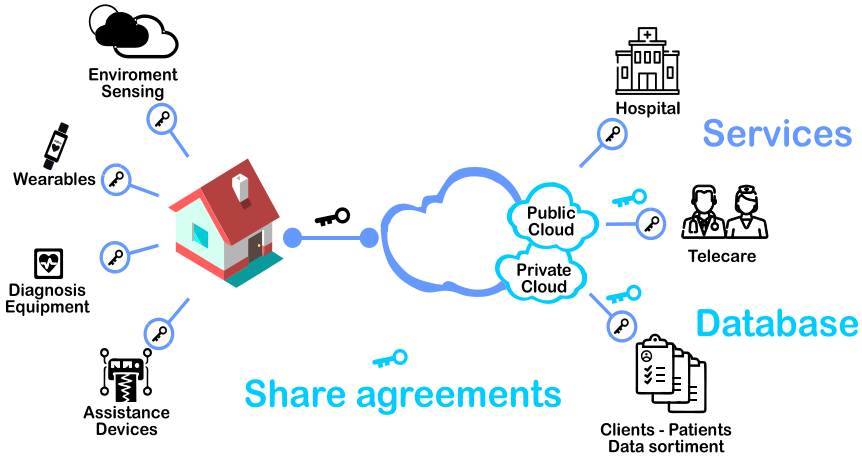
Key inputs for CONCORDIA:

- Impact for smart home: creeping transition from **health-tech** (healthcare) to **wearables** (wellness)
- Impact for emergency: shifting from **stationary** medical products to **smart and mobile** medical products

Remote health service from home

Security aspects:

- on **device** level
  - medical devices, wearables, mobile phones …
- on **person/patient data**
  - e.g. client authentication
- on **IT/network**
  - LAN
- on **Web, Cloud** connection/services
  - e.g. remote data sharing



Thank you!

concordia-h2020.eu

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

ECHO Verticals

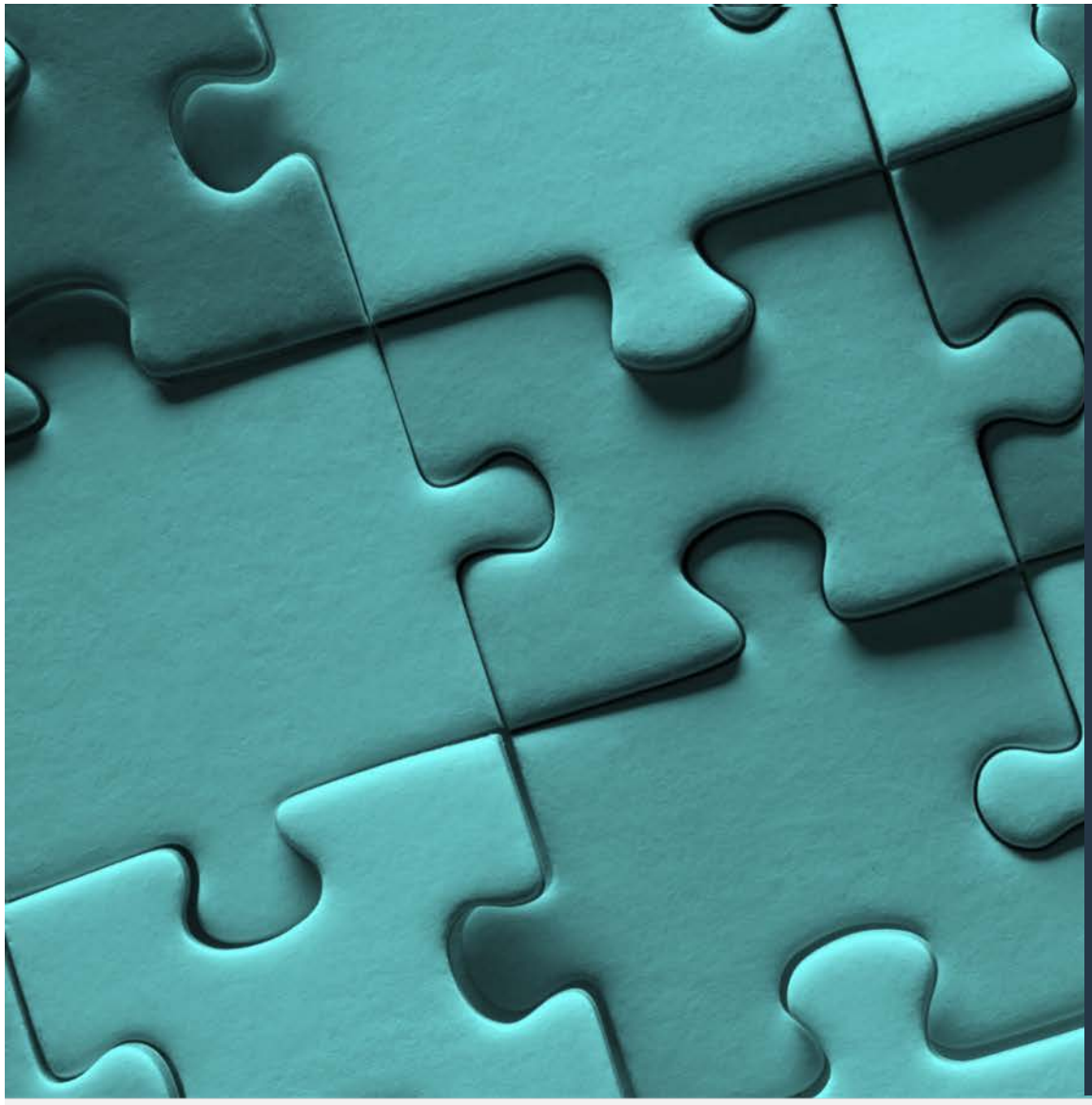
José María TORRES

Security Services, Project Manager at TELESPAZIO BELGIUM
PM of TPZB ECHO Activities and ECHO T7.2 Coordinator

ECHO

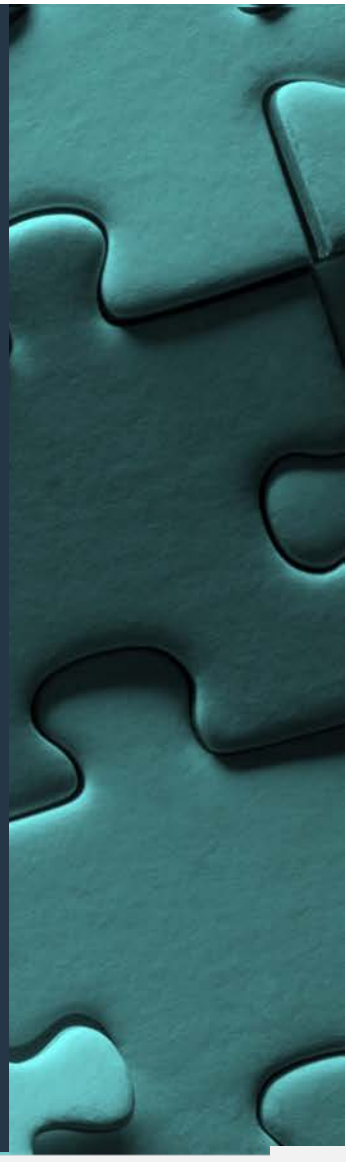
CONVERGENCE NEXT, 1 June 2022

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943



The EU Cybersecurity Challenge:

FROM ***"FRAGMENTED IN DIVERSITY"***
TO ***"UNITED IN DIVERSITY"***



Main concepts:

ECHO Governance Model: Management of direction and engagement of partners (current and future)

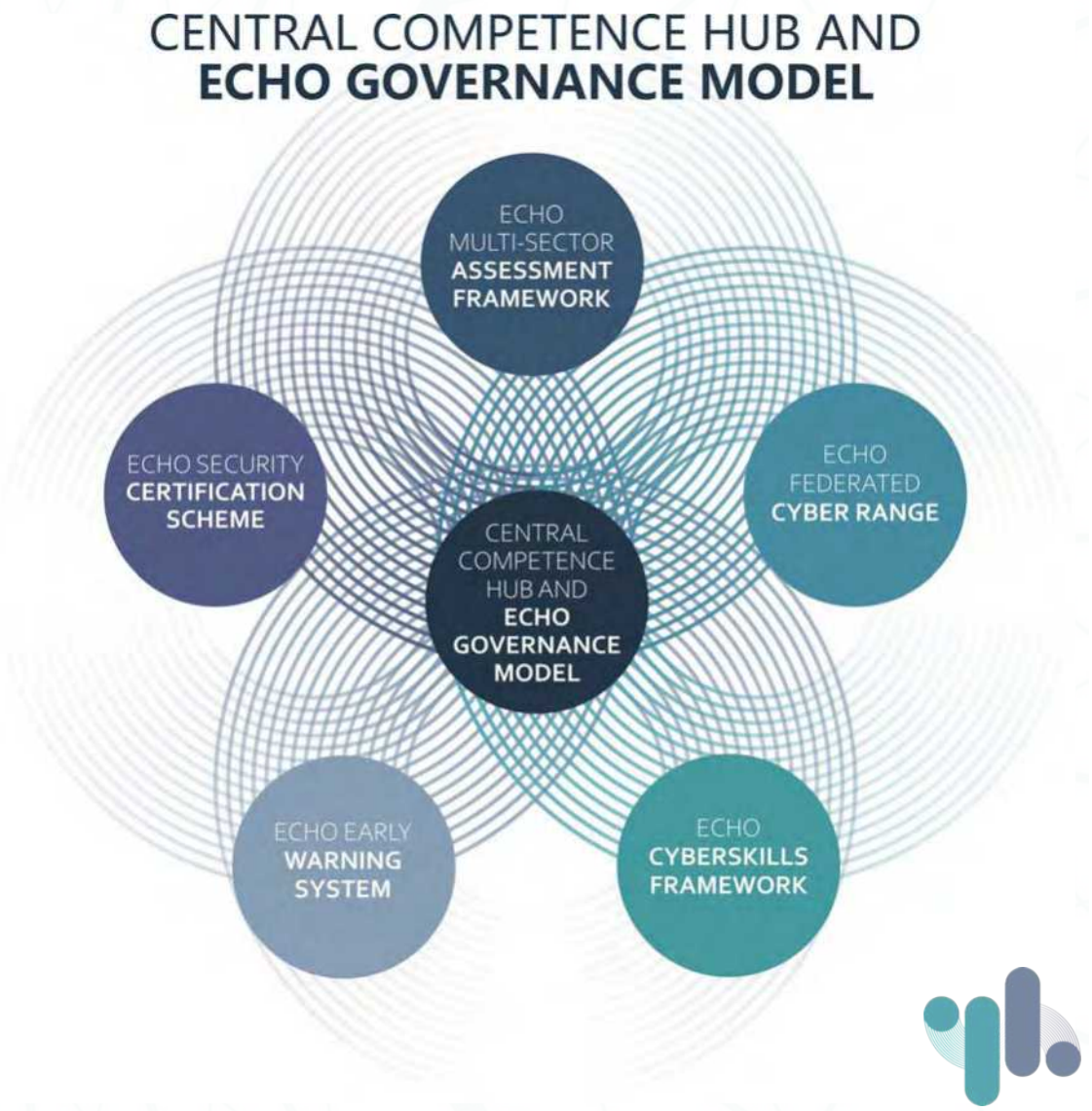
ECHO Multi-Sector Assessment Framework: Transverse and inter-sector needs assessment and **technology R&D roadmaps**

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



Critical Sectors

European Commission-JRC taxonomy

Audiovisual and media	Defence	Digital infrastructure	Energy	Financial
Government and public authorities	Health	Maritime	Nuclear	Public safety
Tourism	Transportation	Smart ecosystems	Space	Supply chain

ECHO Technology Roadmaps

Led by CERTH/ITI - Notis Mengidis

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

One of the main objectives of the ECHO project is the development of cybersecurity roadmaps as a result of **analysis** related to **current** and **emerging cybersecurity challenges**.

2

Delivery of at least 6 cybersecurity technology roadmaps including:

- **ECHO Early Warning System** (E-EWS) Roadmap
- **ECHO Federated Cyber Range** (E-FCR) Roadmap
- At least **2 additional technology innovations (E-Tools)** to be completed as part of ECHO
- At **least 2 additional technology innovations (challenges/priorities)** to be addressed by the future Cybersecurity Competence Network

3

Highlight **strategic technology-related priorities** with the goal to create the foundations for new **industrial capabilities** and assist towards the development of **innovative technologies** thus paving the way towards **EU's digital sovereignty**.

4

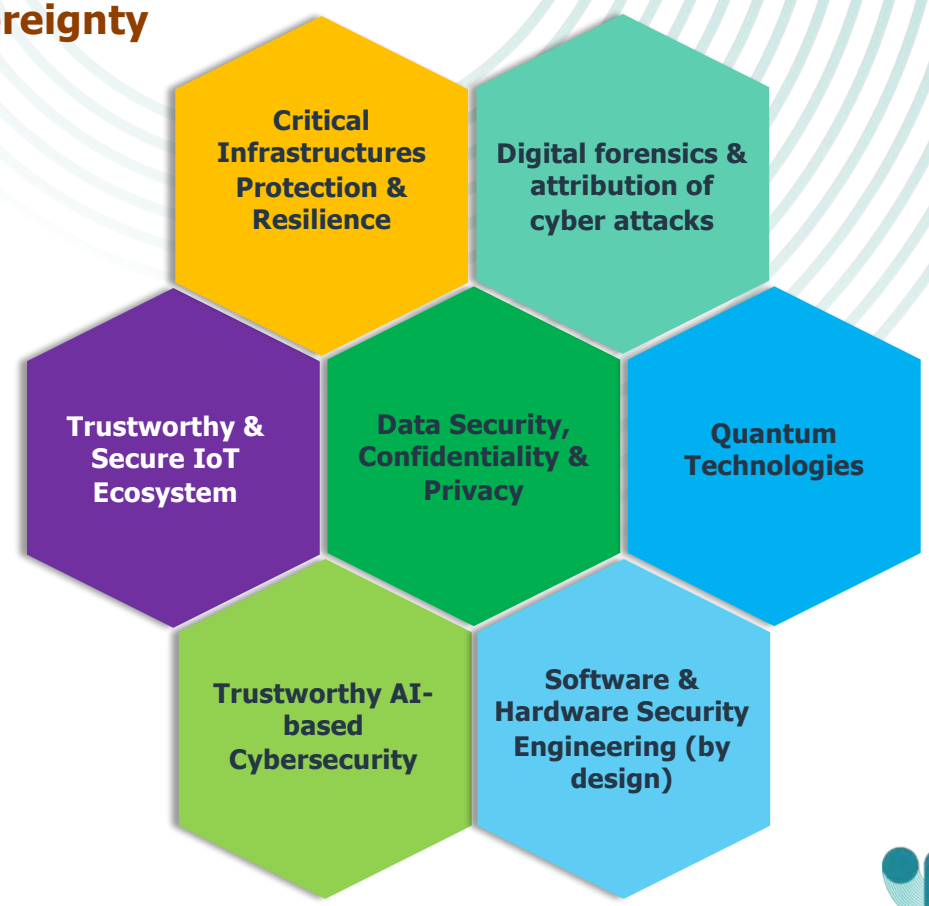
Consider the **transversal** aspects of **Education/Training** and **Certification**, while underpinned by effective **Governance** models for networked organisations that collaboratively strive to achieve these goals.

ECHO Technology Roadmaps

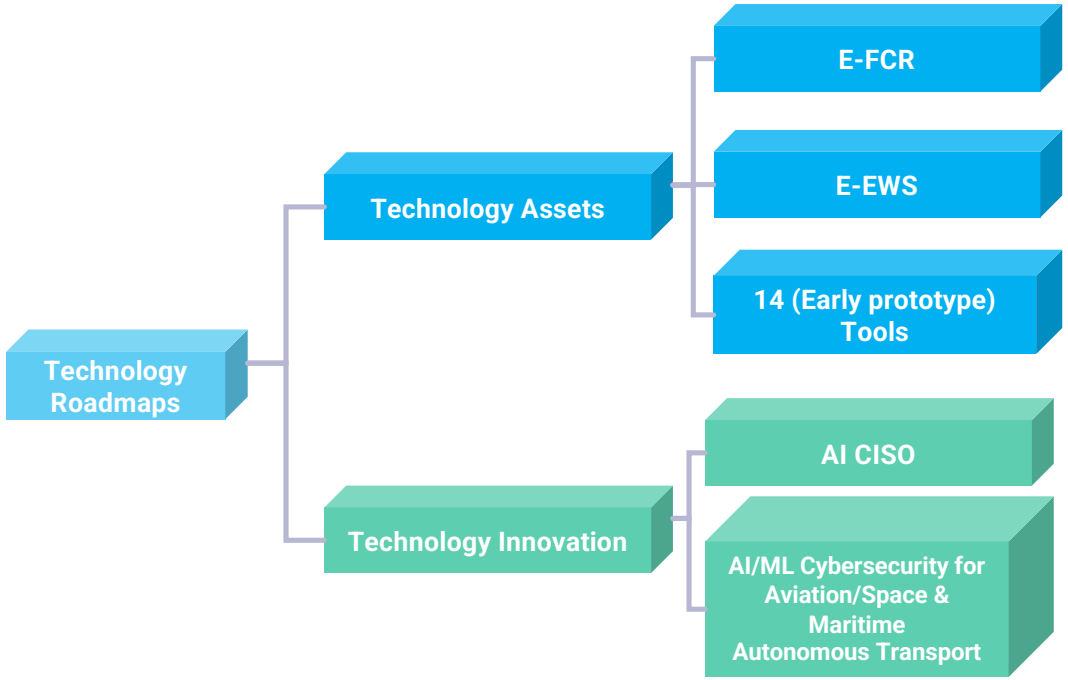
Current and emerging challenges: Towards EU sovereignty

Challenges identification & Priorities consolidation:

- Examined more than **140 reports** (Industrial, Academic, EU agencies etc)
- Identified **83 technical cybersecurity challenges**
- Challenges informed the **design** and **development** of **14 prototype tools & their respective roadmaps + 2 technology innovation roadmaps (E-EWS and E-FCR) + 2 innovation roadmaps** (AI CISO and AI/ML Cybersecurity for Aviation/Space and Maritime Autonomous Transport)
- Building the foundations for future work by highlighting **priority focus areas** for **research**, **development**, **innovation,** and **prototyping**
- Closely collaborating with the other 3 pilots in order to provide a **consolidated view** of our roadmaps



WP4 – T4.2 Technology Roadmaps



ECHO Federated Cyber Range (E-FCR)

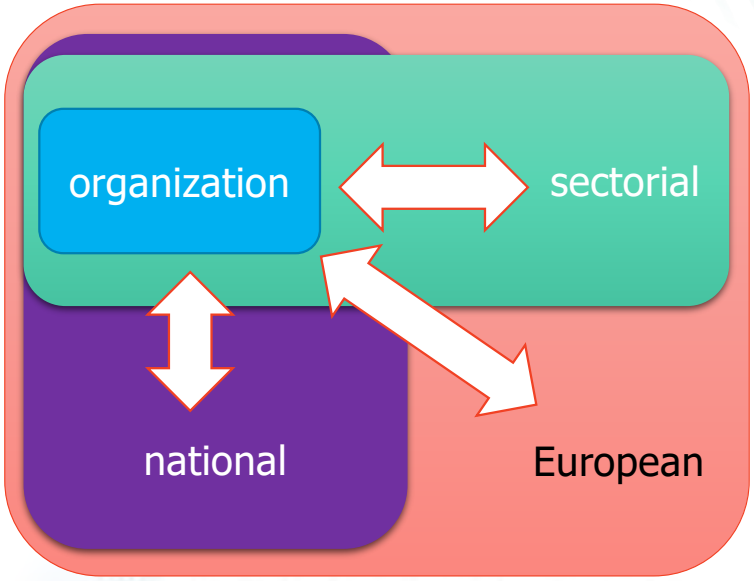
interconnects cyber range capabilities through a portal that operates a broker and enables access to emulations of complex realities and inter-sector dependencies and a marketplace enabling the provision of cyber range content to a wider market.

ECHO Early Warning System (E-EWS)

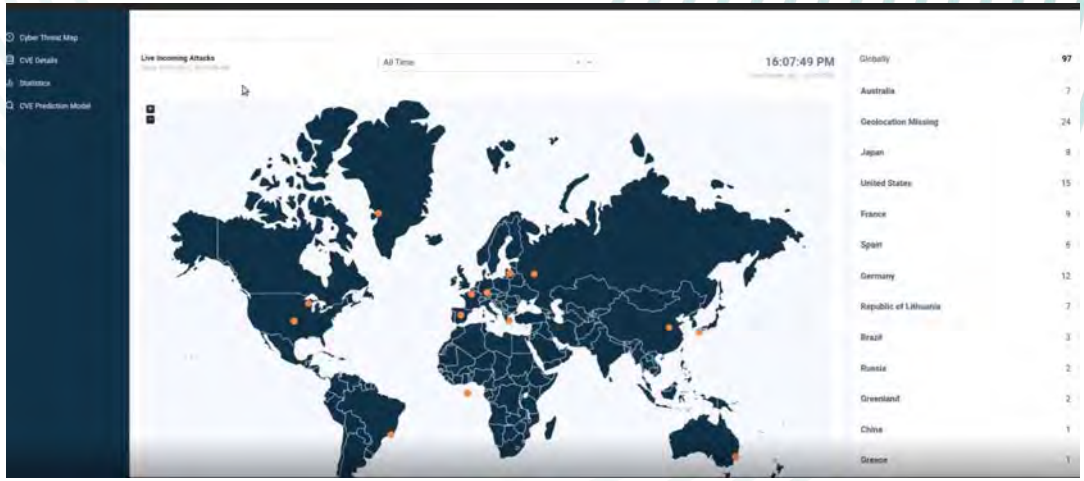
provides the infrastructure needed to support trusted and secure information sharing among across a network of competence centres and their respective constituents.

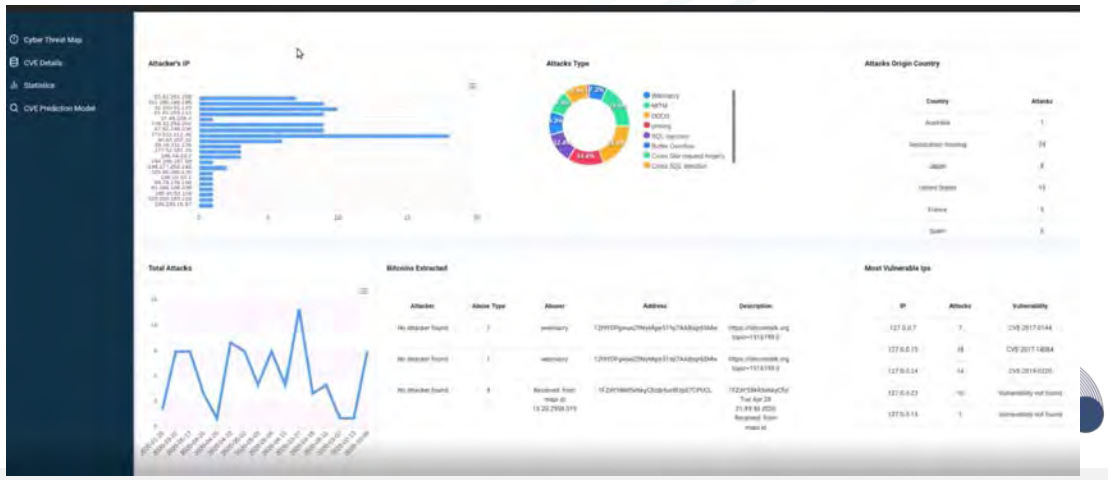
Sharing Threat Information

ECHO Early Warning System (E-EWS)



Four Types of Cyber Threat Intelligence

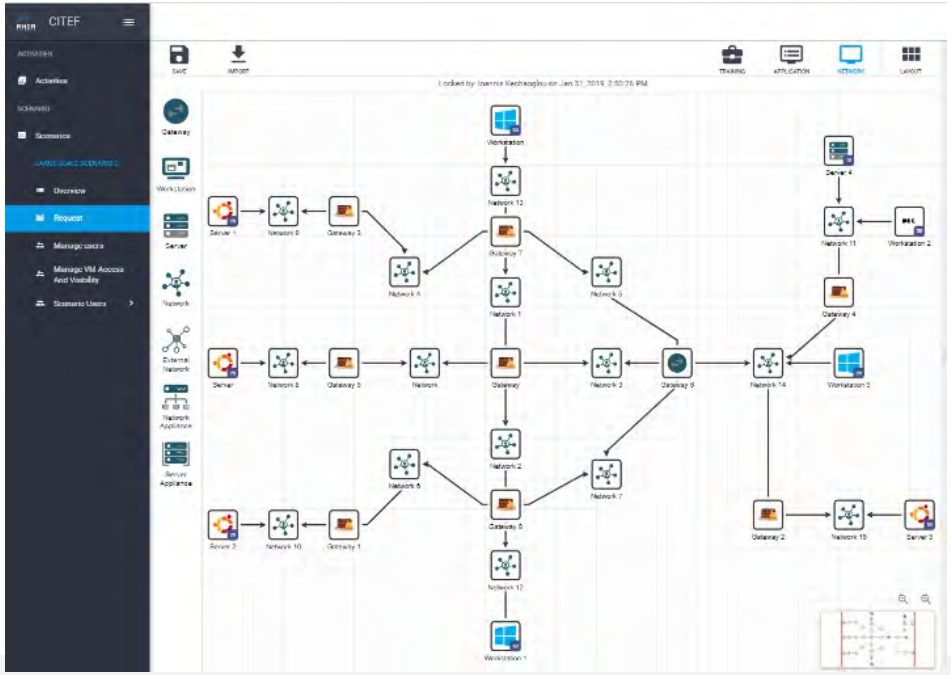




ECHO Technology Roadmaps

The ECHO Federated Cyber Range (E-FCR)

Cyber Ranges are multipurpose **virtualization environments** supporting **"security-by-design"** needs



Cyber Ranges are used to provide:

- Safe environment for **hands-on cyberskills** development
- Realistic simulation for **improved system assurance** in development
- Comprehensive means for **security test and certification** evaluation

In ECHO, we use Cyber Ranges also as virtual environments for:

- Development and demonstration of **technology roadmaps**
- Delivery of specific instances of the **cyberskills training** curricula

ECHO Inter-sector Prototype tools

Led by CERTH/ITI - Antonis Voulgaridis

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

1

Objectives

Address most **pressing** transversal and inter-sector cybersecurity **challenges**
Cover **priority areas**
Increase **cybersecurity awareness**

2

Selection methodology

Detailed selection methodology based on **challenges**, **priority areas** covered, **innovation**, relevance, adaptability etc.

3

Development process

Scrum based development framework for integration, installation and testing of tools.

4

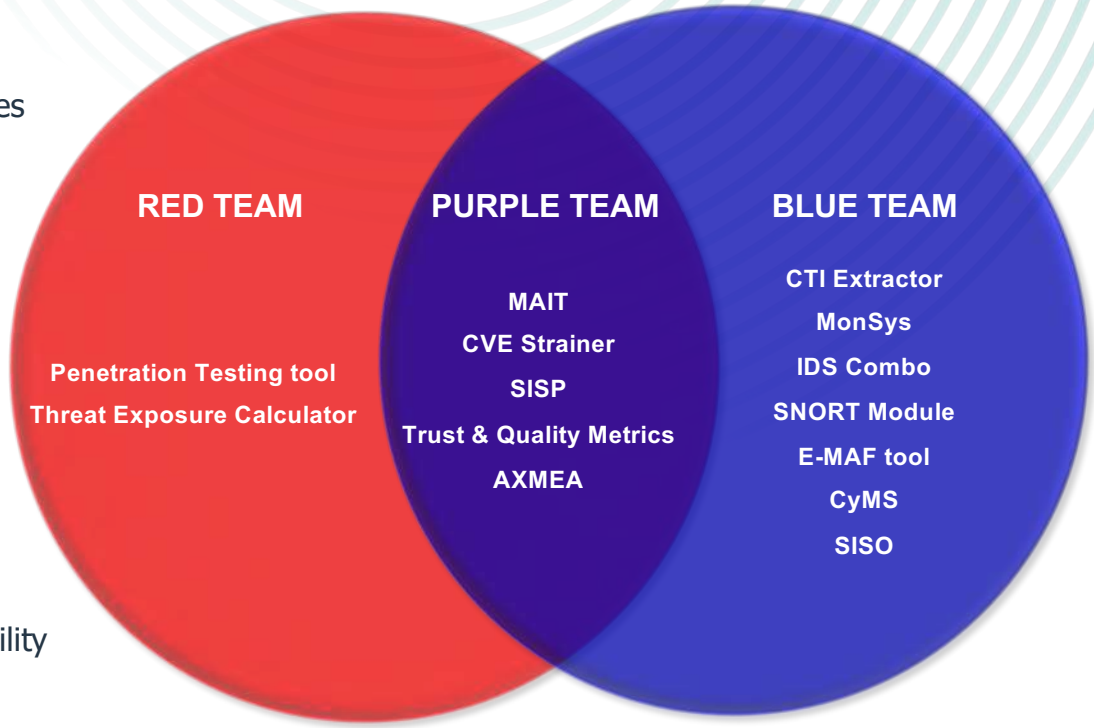
Outcomes

Innovative solutions based on **state-of-the-art** tools, techniques & methodologies
Leverage **known technologies** (Nmap, Snort, Nikto, Kali etc.)
Increase cybersecurity awareness through dedicated workshops/demonstrations

ECHO Inter-sector prototypes

Addressing the most pressing cybersecurity challenges

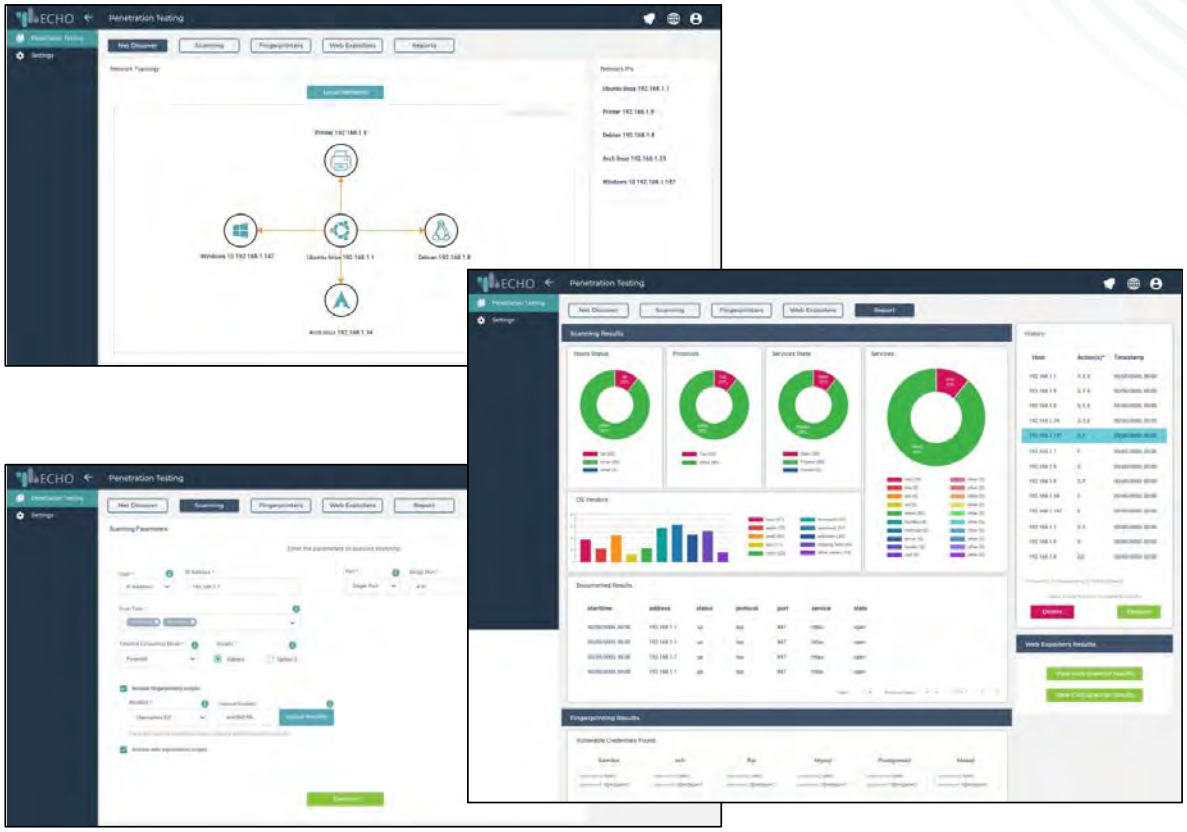
- **Tools:**
  - 39 tools initially proposed - 14 selected
  - Covering multi-domains & multiple cybersecurity challenges
- **Challenges** addressed:
  - 41 total unique challenges addressed
  - 32 transversal / 9 inter-sectoral
- **Priority areas** covered:
  - Maritime (CyMS)
  - **Healthcare (SISP)**
  - Energy (AXMEA)
  - Space (SISO)
  - Transversal – multiple sectors (rest)
- **Cybersecurity fields/categories:**
  - Red teaming: Penetration Testing, Network/Web Vulnerability Scanning
  - Blue teaming: Intrusion Detection Systems (IDS), SIEMs, Network Security Monitoring
  - Purple teaming: Knowledge Base, CTI Sharing, Malware Analysis, Cybersecurity/Situational Awareness

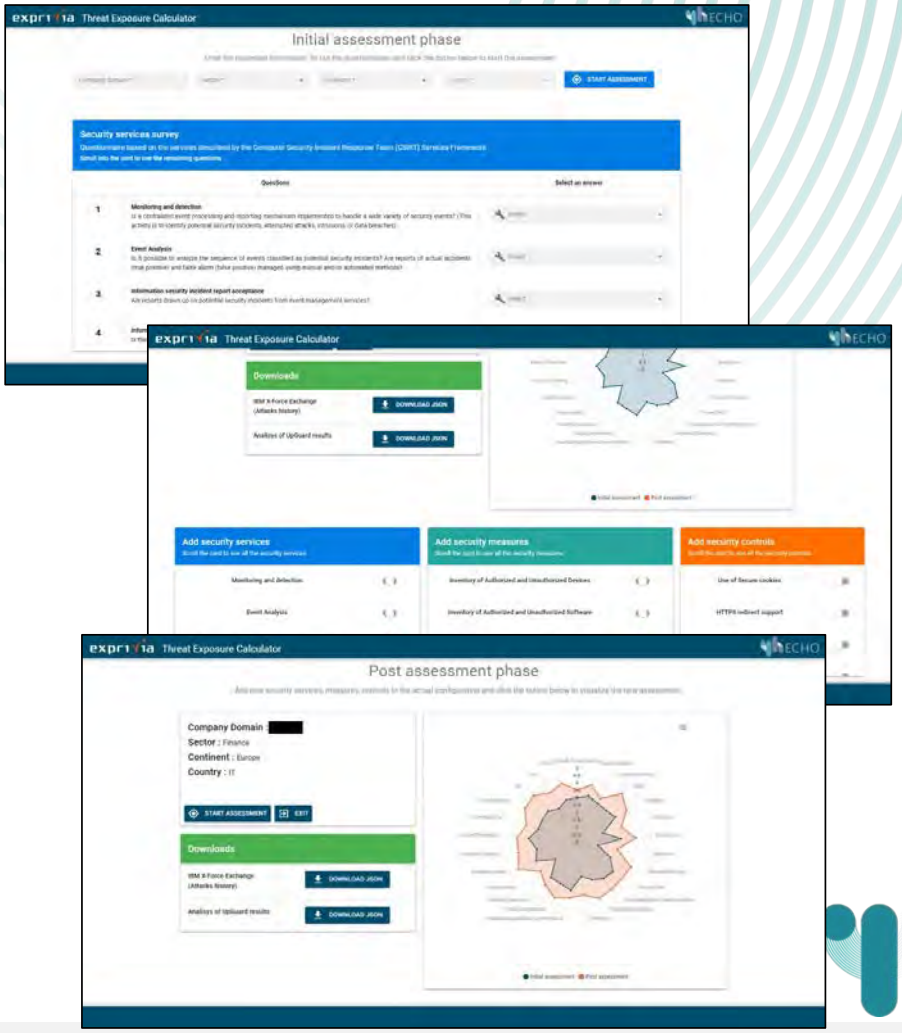


ECHO Inter-sector prototypes

An eye on the prototypes – Red teaming

Penetration Testing tool, Threat Exposure Calculator

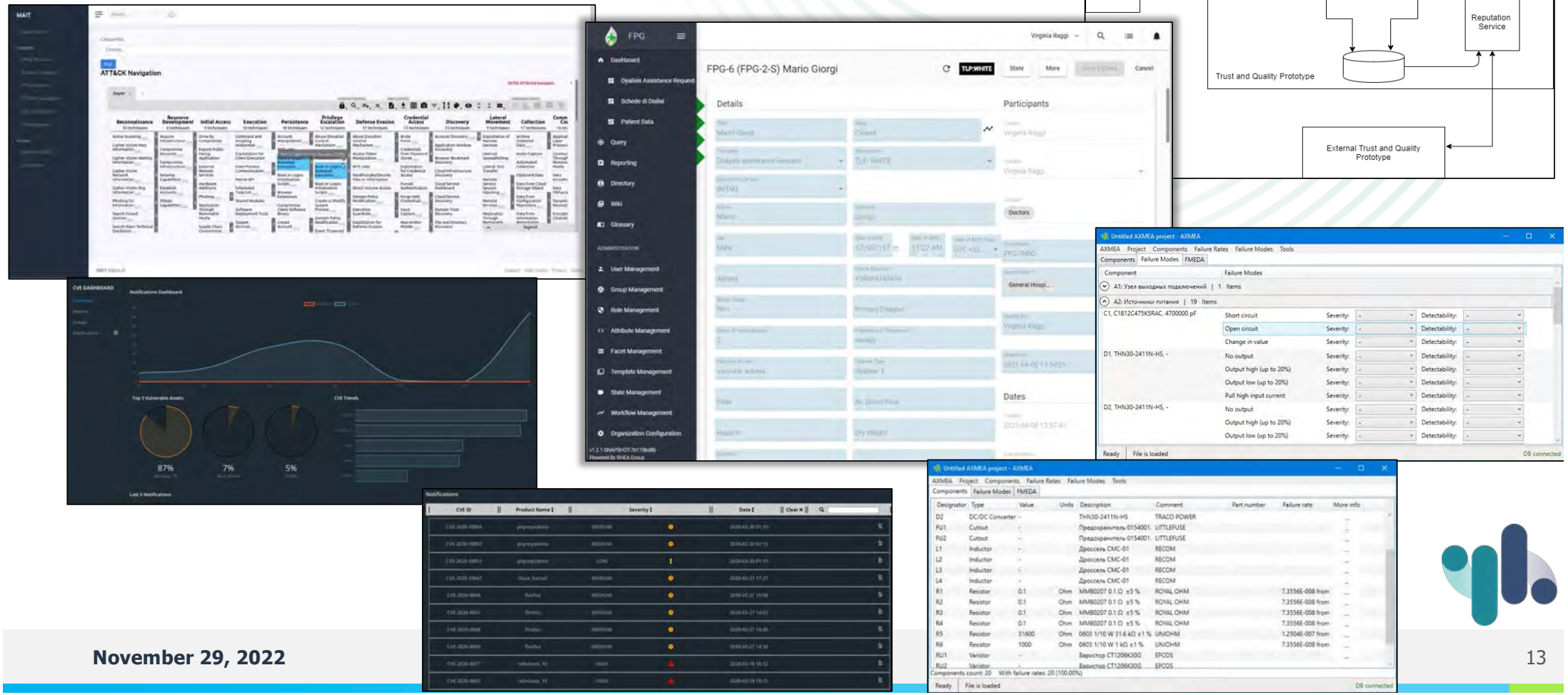




ECHO Inter-sector prototypes

An eye on the prototypes – Purple teaming

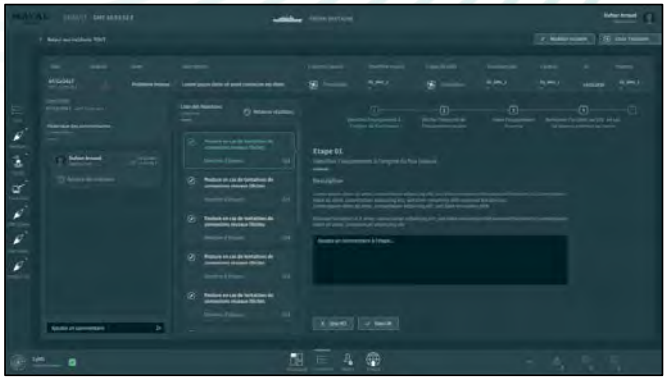
MAIT, CVE Strainer, SISP, Trust & Quality Metrics, AXMEA

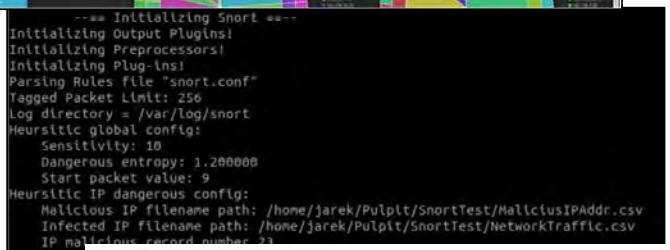


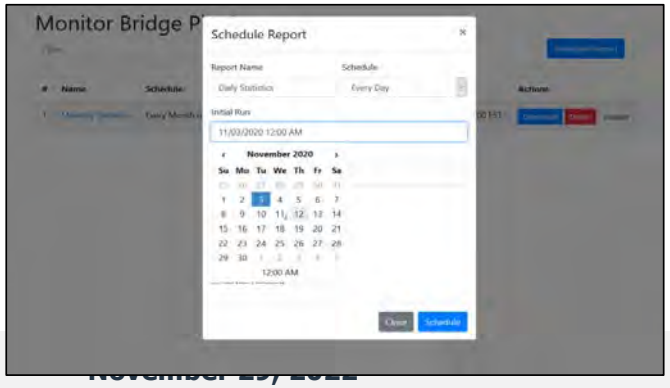
ECHO Inter-sector prototypes

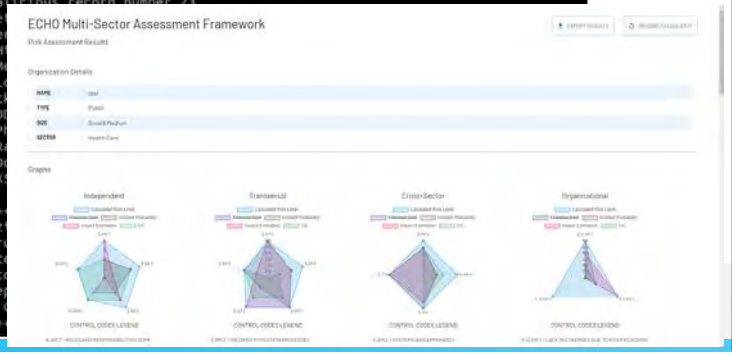
An eye on the prototypes – Blue Teaming

CTI Extractor, MonSys, IDS Combo, SNORT Module, E-MAF tool, CyMS, SISO









ECHO Inter-sector prototypes – Video SISO

ECHO Inter-sector prototypes – Video SISP

ECHO Inter-sector prototypes

An eye on the prototypes

Name	Leading Partner	Tool Type / Cybersecurity field	Challenges Addressed
Penetration Testing Tool (PT)	CERTH	Penetration testing, Web vulnerability scanning	12
Cyber Threat Intelligence (CTI) Extractor	CERTH	Network Security Monitoring, SIEM/IDS, Cybersecurity awareness	11
Trust & Quality Metrics (TQM)	VST	Cyber Threat Intelligence Sharing	3
SNORT module (SM)	AGH	Network Security Monitoring, SIEM/IDS	4
Threat Exposure Calculator (TEC)	EXP	Web vulnerability scanning, Penetration testing, Cybersecurity awareness	6
Malware Analysis and Intelligence Tool (MAIT)	BU	Knowledge base, Cybersecurity awareness	6
Intrusion Detection System Combo (IDS Combo)	IICT	Network Security Monitoring, SIEM/IDS, Cybersecurity awareness, Knowledge base	8
E-MAF tool (E-MAT)	AON	Cybersecurity awareness	5
SIEM IDS for Space Operations (SISO)	VST	SIEM/IDS	6
Cyber Management System (CyMS)	NG	SIEM/IDS	6
Common Vulnerability Exposure (CVE) Strainer	TBS	Knowledge base	4
Monitoring System (MonSys)	ESICEE	Network Security Monitoring	5
Secure Information Sharing Platform (SISP)	RHEA	Knowledge base, Cyber Threat Intelligence Sharing	7
Automated X-Modes and Effects Analysis (AXMEA)	KHAI	Knowledge base	6

Developed from scratch

More mature

ECHO Inter-sector prototypes

Increase cybersecurity awareness through dedicated workshops/demonstrations

Demonstration Cases - *Ongoing*

- DC#4: CyMS, SISP
  Demonstration of the E-FCR to support certification activities following the E-CCS for the ECHO products
- DC#5: PenTest, CyMS, MonSys, SISO
  Demonstration of E-FCR capabilities for technology experimentation, research and development

Objectives

- Showcase ECHO assets capabilities (E-FCR, E-CCS)
- Thorough testing via extended scenarios
- Continuous R&D

Demonstration Workshops

- WC#1: PenTest, SISP, SnortModule – **19/04/22**

Testing the resilience of a health-related app while deployed IDS detecting the activity

- WC#2: PenTest, SISO, CVE Strainer, TEC **14/06/22**

Identifying vulnerabilities in space-related system providing user notifications and risk assessment calculation

- WC#3: CTI Extractor, MAIT, TQM **28/07/22 TBC**

Analyzing malware from CTI collected from honeypots. Information shared and evaluated through E-EWS

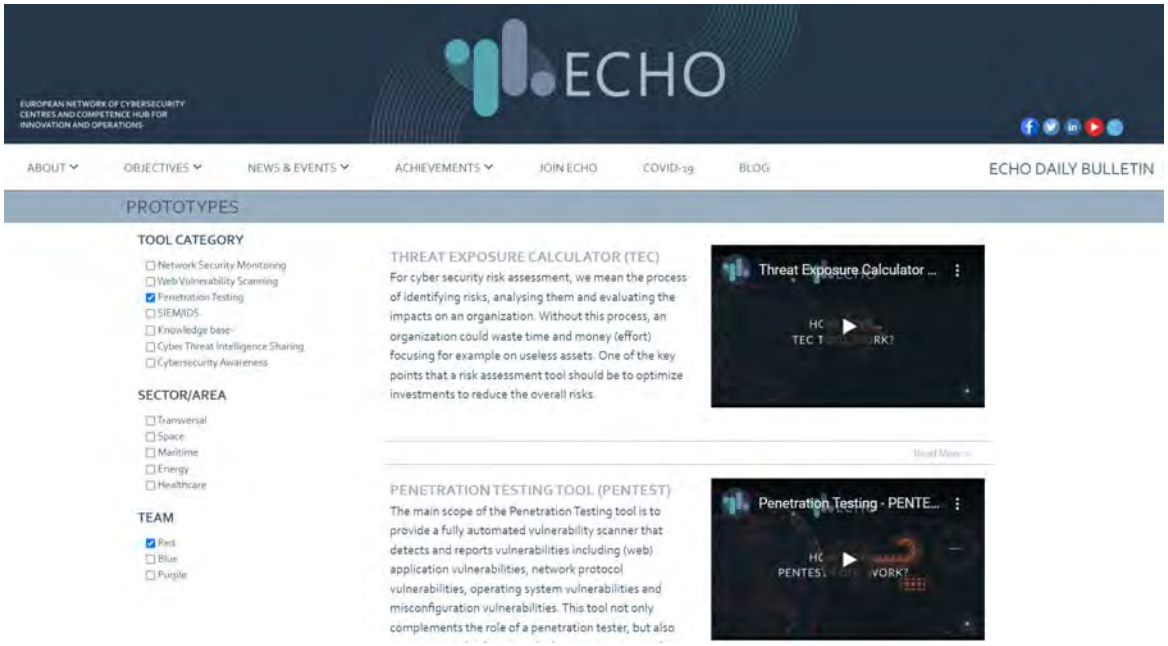
Objectives

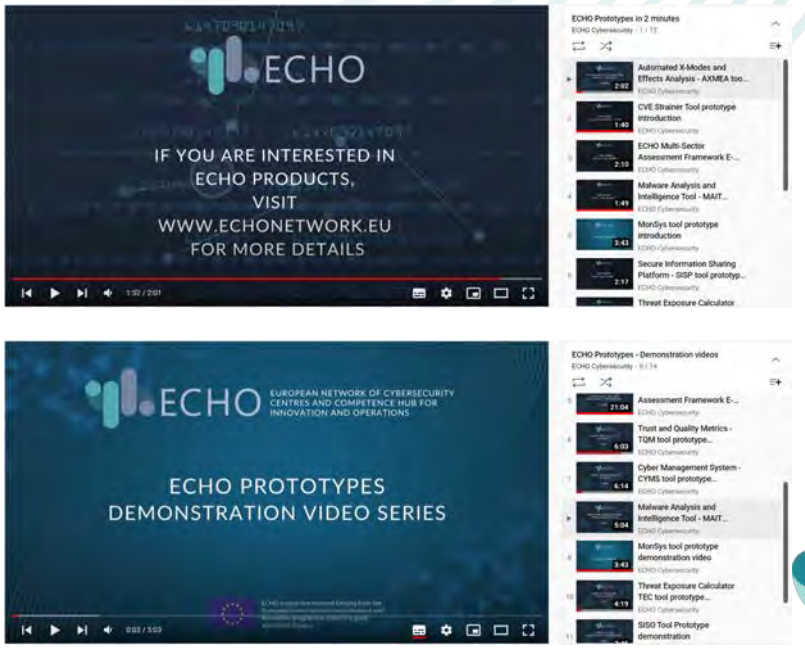
- Show full functionality of tools both as standalone tools but also in storylines interconnecting "compatible" ones
- Get feedback from users
- Improve and adapt

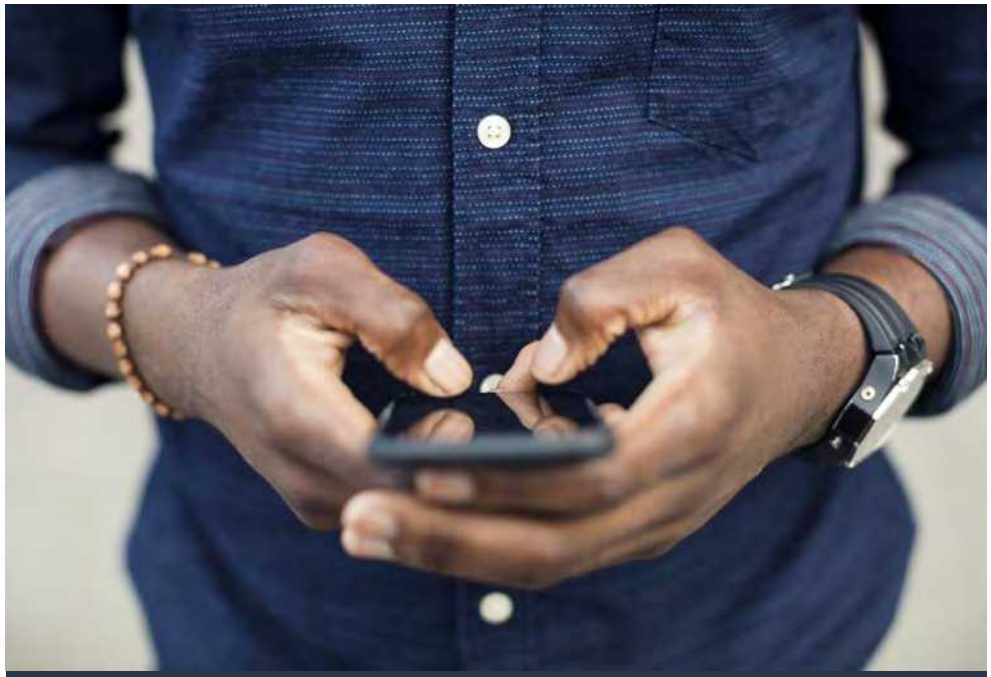
ECHO Inter-sector prototypes

Dissemination

- Dissemination through ECHO's website, public workshops and newsletters
  - Teaser demos + Short description + categorization uploaded on ECHO's website
  - Technical demos uploaded on ECHO YouTube channel







Get in Touch with Us and Follow us on Social Media!

The ECHO Project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement №830943

info@echonetwork.eu

www.echonetwork.eu

https://twitter.com/**ECHOcybersec**

https://www.facebook.com/**echonetworkeurope/**

https://www.linkedin.com/in/**echo-cybersecurity**

https://www.youtube.com/channel/**UCDQBXrQhoLJ2lnf38x1X6Uw**

https://www.youtube.com/watch?**v=2S2sJfJ1VyQ**

https://echonetwork.eu/**echo-workshop-it-development-and-cybersecurity/**

ECHO

EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

Thank You

Matteo Merialdo
www.echonetwork.eu

SPARTA

High-Assurance Intelligent Infrastructure Toolkit (HAII-T)

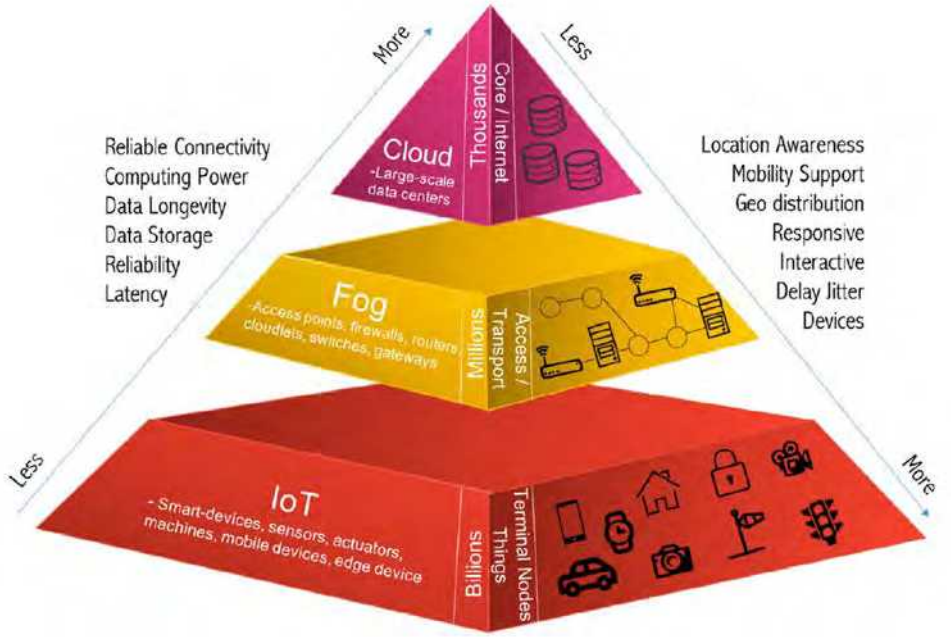
Program presentation

Gabriele Costa
CONVERGENCE NEXT (Brussels)
@sparta_eu
sparta.eu

2nd, June 2022

INTRODUCTION
PROGRAM OBJECTIVES

Develop a foundation for **secure-by-design Intelligent Infrastructures**, built on truly reliable approaches, **addressing multiple cybersecurity facets**.



SCOPE & OBJECTIVES
WP OVERVIEW

Duration: M01-M36

WP Lead: CINI

Partners involved: INRIA, TUM, UNILU, BUT, CNIT, FTS, IMT, JR, UTARTU, KTU, LIST, UNAMUR

Tasks structure:

#	Title	Lead	Date
T6.1	Securing Operating System Software	INRIA	M01-M36
T6.2	Hardening Legacy Components	TUM	M01-M36
T6.3	Secure Orchestration of the II	CINI	M01-M36
T6.4	Resilience-by-design of II	UNILU	M01-M36
T6.5	Privacy-by-design	BUT	M01-~~M24~~ **M36**

EVENTS AND MILESTONES
WP OVERVIEW

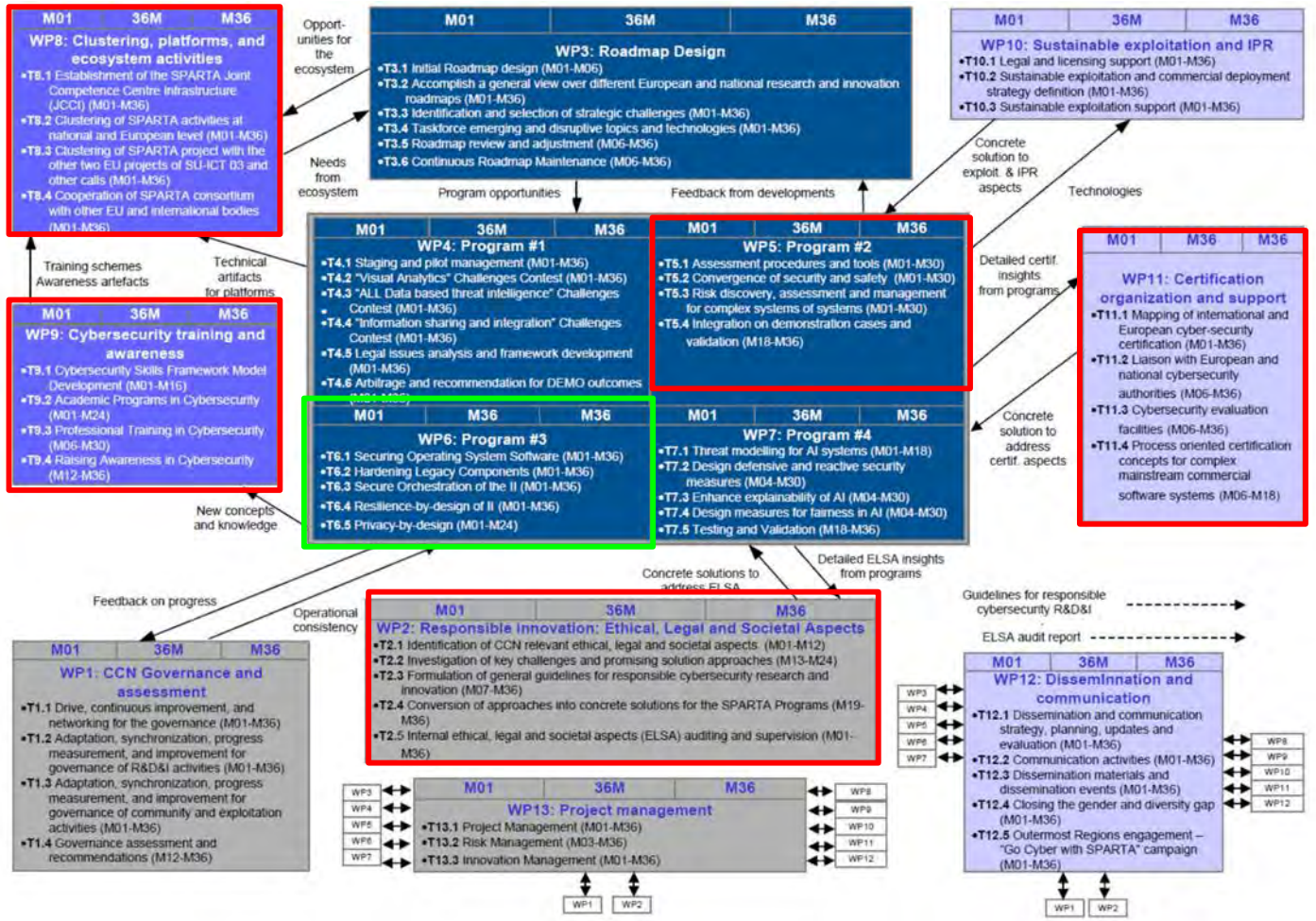
- Four deliverables (D6.1-4) including two demonstrators
- 3 annual strategic meetings
  - 2019 physical (Lucca)
  - 2020 virtual
  - 2021 hybrid (Graz)

GOVERNANCE
INTERACTION WITH OTHER WPs

Agenda

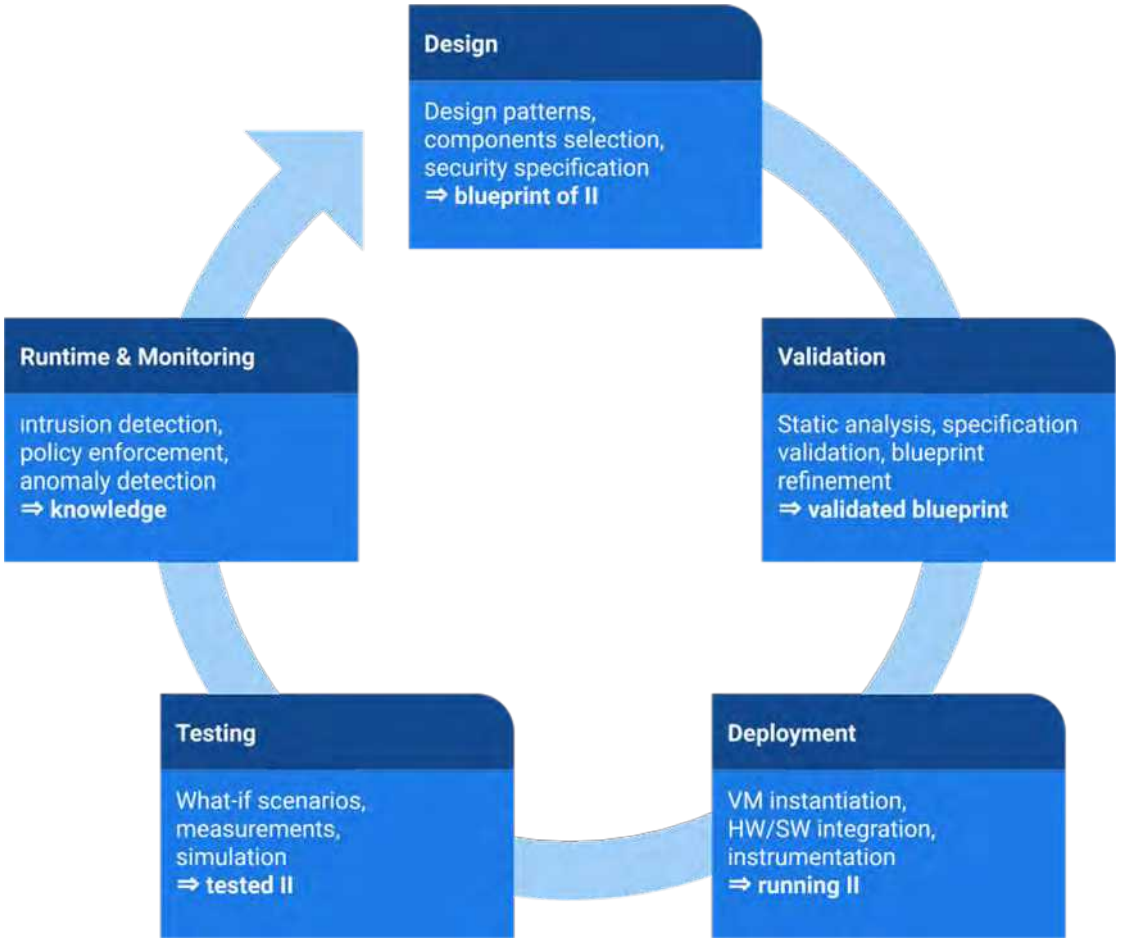
Interaction with other WPs:

- WP2: **ELSA**
- WP5: **Automated Verification**
- WP9 on **Training** and **Simulation Environments**
- WP11 on **Certification**
- WP8: platforms & ecosystem
- WP10: OS software exploitation

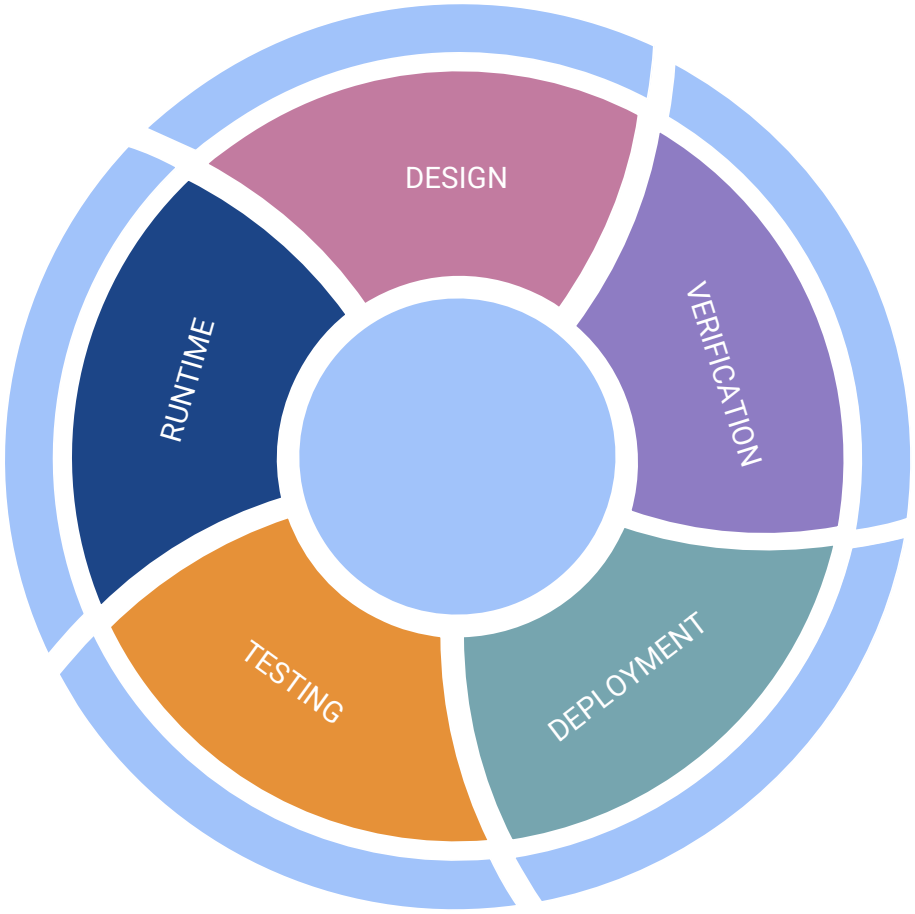


SECURE ORCHESTRATION
SECURING THE II LIFECYCLE

- Support all the phases of the lifecycle of an Intelligent Infrastructure
- Rely on extensible, state-of-the-art orchestration technologies
- Embed methodologies developed in WP6



SECURE ORCHESTRATION
WP6 CONTRIBUTIONS MAPPING

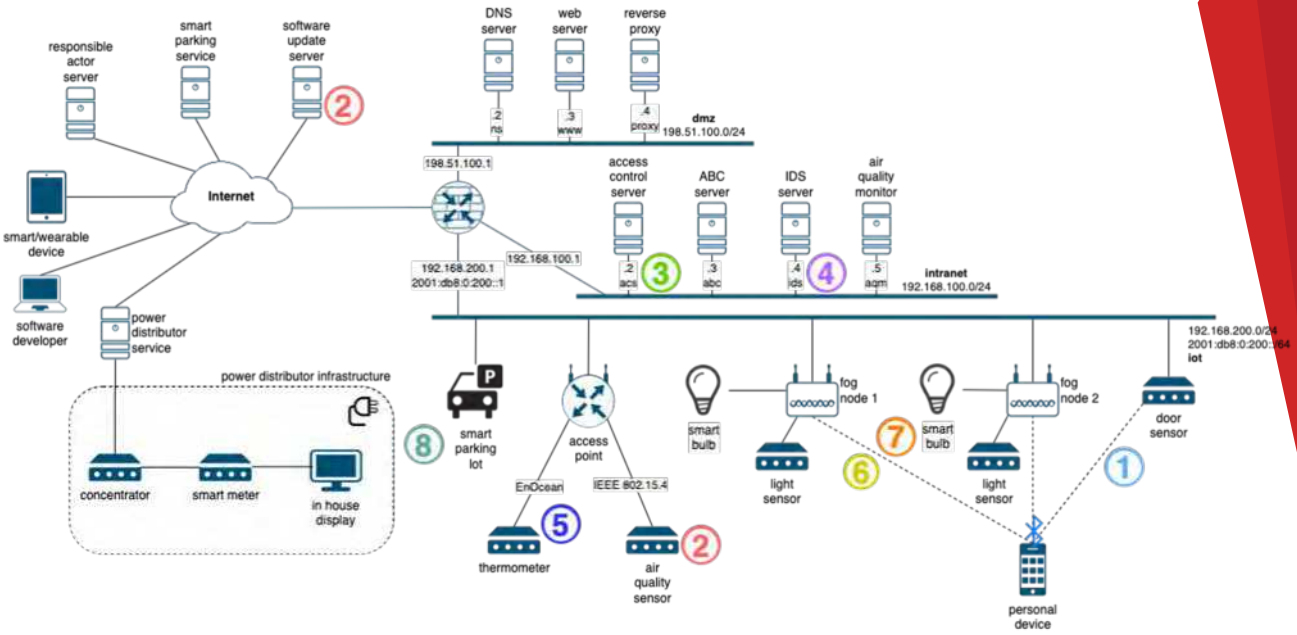


Task	Technology
T6.1	New IoT crypto primitives
	Low-power, secure networks
	Secure OS software supply chain
T6.2	Defenses against data-oriented attacks though virtualization
	Defenses against code-oriented attacks though hardware-based monitoring
	Defenses against fault injection attacks for present and future devices
T6.3	Security orchestration framework
	Formal verification of protocols
	Formal evidence language
	Security orchestration for Fog computing
	II key components classification
T6.4	Intrusion detection
	Fault and intrusion tolerance
T6.5	Privacy-preserving management and regulation
	Privacy-enhancing technologies
	Privacy evaluation techniques and methods

OUTCOMES
CASE STUDY

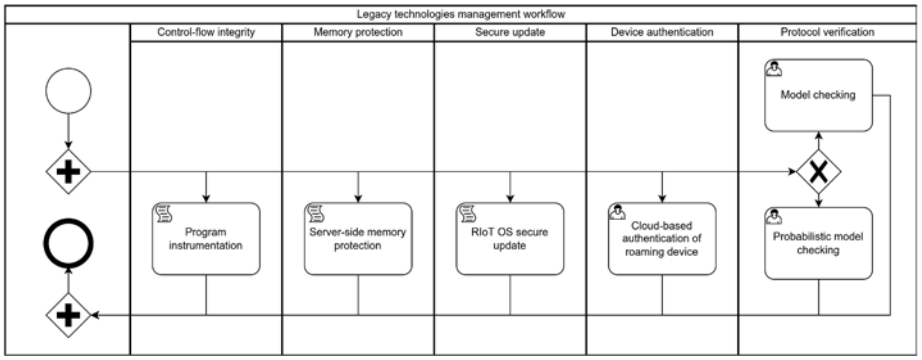
Inspired by a real smart building

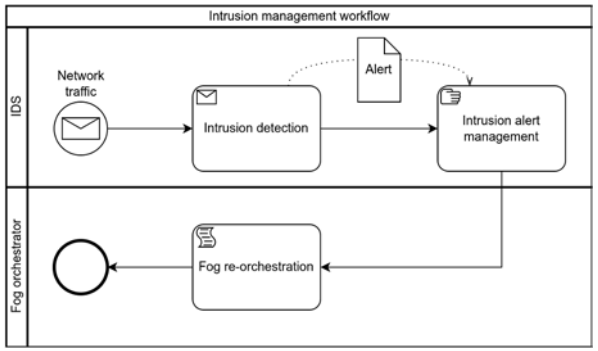
- Part of the Savona Polygeneration Microgrid (University of Genova)
- Not yet a “digital twin”, but ...
- Decorated with 8 security scenarios
- A publicly available asset!
  - Computers & Security (to appear)

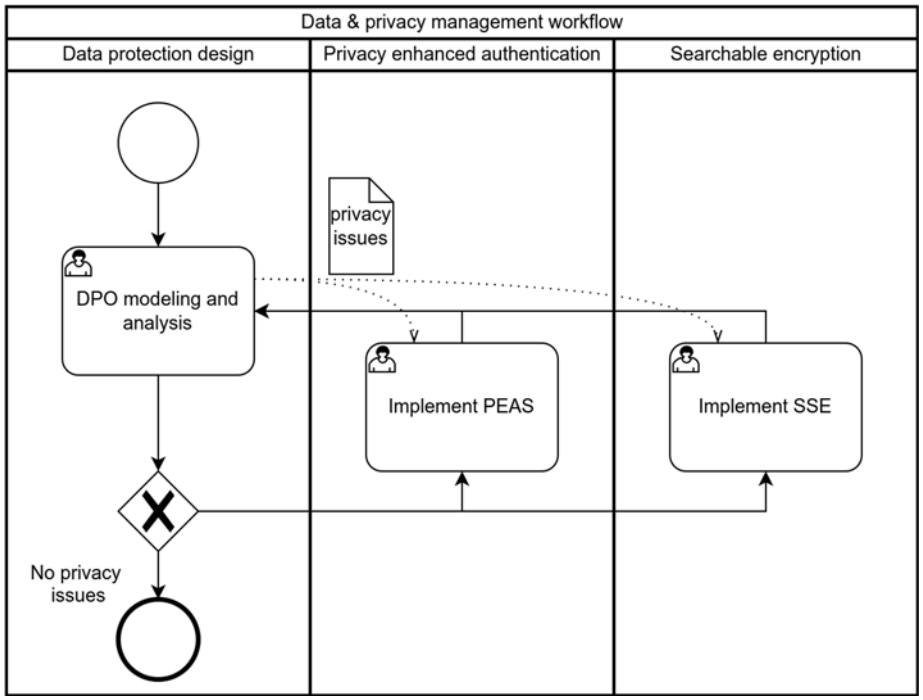


OUTCOMES
INTEGRATION INSPIRING PRINCIPLE

- **HAll-T combines security technologies in arbitrary security workflows**
- Three already implemented, support for custom ones provided







CONCLUSION
LESSON LEARNED

No silver bullets in security

- Rarely a security concern can be solved with a single technology
- Effective security mechanisms are often domain-specific
- Our implementation follow the SxD inspiring principles
    - Customized security processes can be reviewed and maintained over time

SPARTA

THANK YOU!

@sparta_eu | sparta.eu

June 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

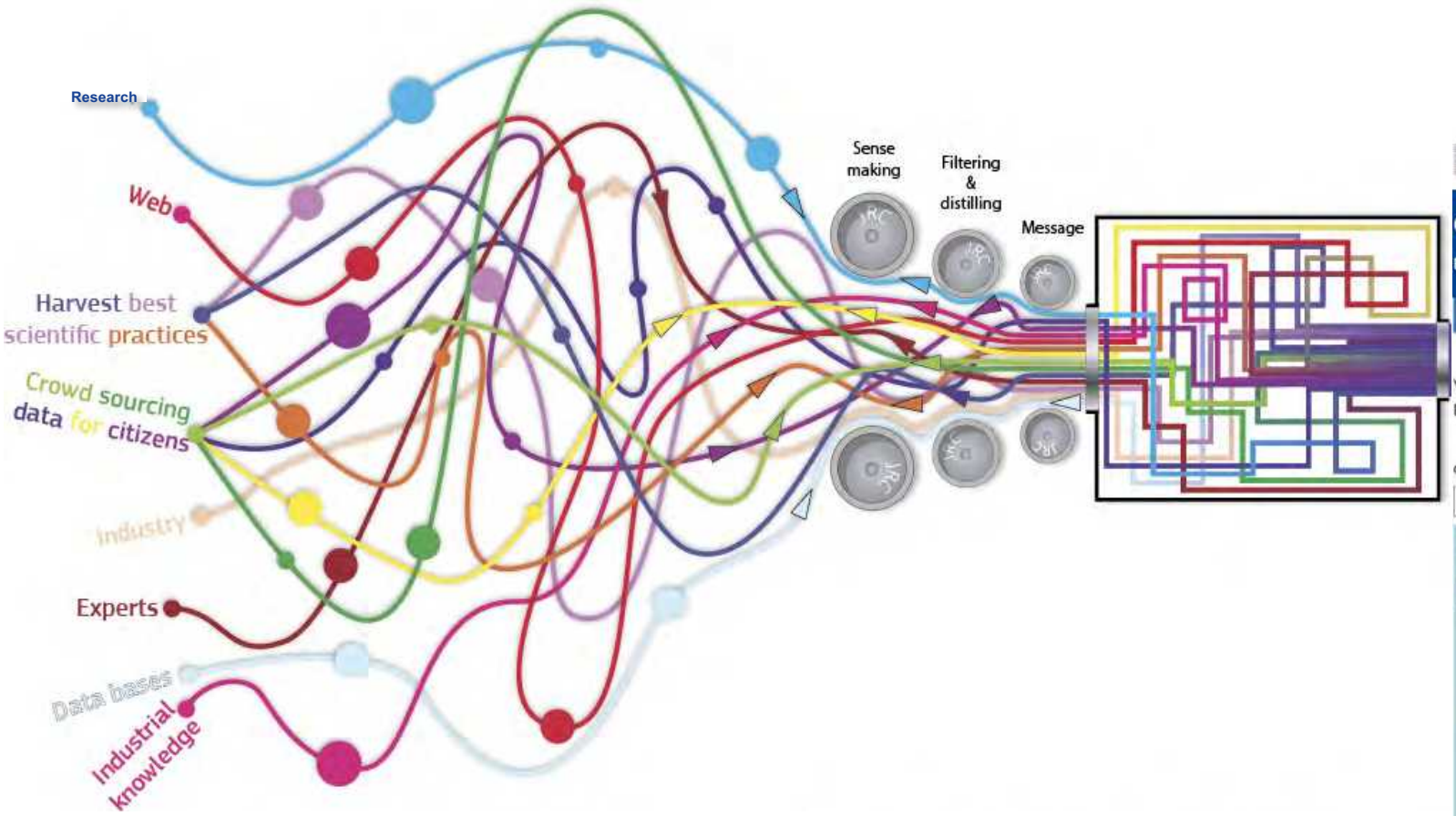
Cybersecurity Atlas

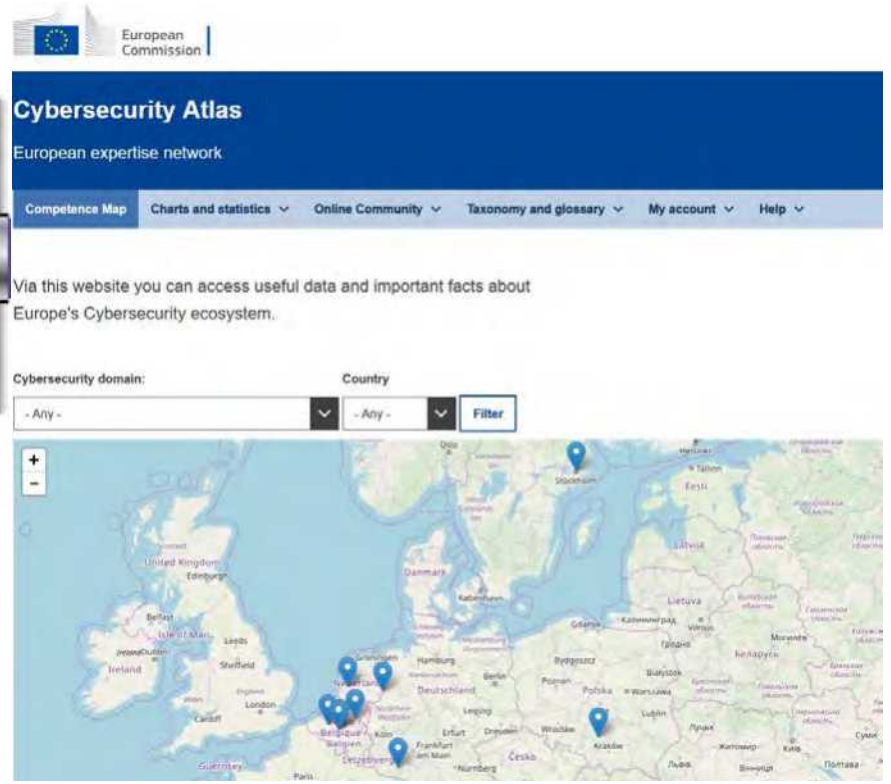
CONVERGENCE NEXT 2022

Francesco BARBATO
Programme Officer
EC – DG CNECT H1 - Cybersecurity Technology & Capacity Building

2 June 2022

European Cybersecurity Atlas





European Commission

Why a Cybersecurity Atlas

- Facilitate the establishment of a community of practice
- Help identifying collaboration opportunities
- Map the different Cybersecurity competencies in Europe
- A knowledge management tool for the ECCC
- Raise the visibility of participants within the Community
- Support European Cybersecurity R&I coordination
- Contribute to the development of EU funding programmes
- Provide input to cybersecurity policymakers

Today: The members of the 4 H2020 Pilots

In the near future: the ECCC, the NCCs and the Community

European Commission

European Cybersecurity Technology and Innovation Ecosystem

European Competence Centre:

- It will manage the funds foreseen for cybersecurity under Digital Europe Programme and Horizon Europe 2021-2027
- It will facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- It will support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- National capacity building and link with existing initiatives

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors

European Commission

Cybersecurity Competence Community

Academic and research organisations

Industry (demand and supply)

Public Authorities

Other stakeholders

Union bodies with relevant experience

Relevant Associations

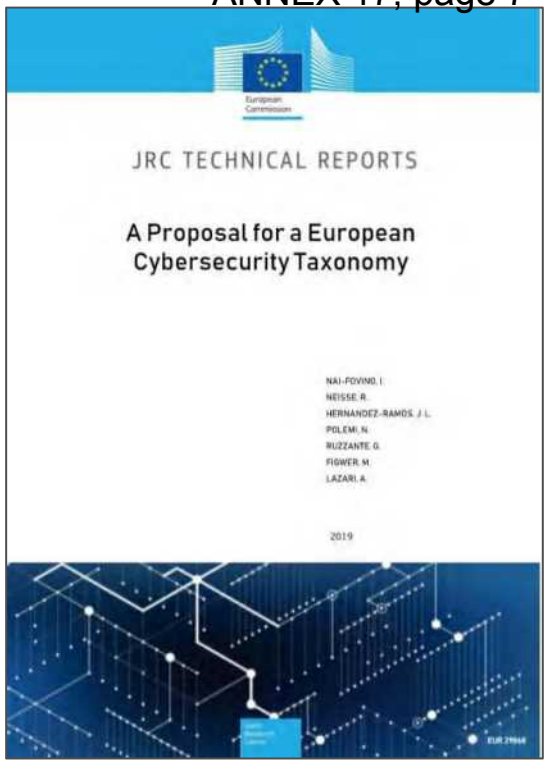
- Support the Centre and the Network in achieving the mission and objectives
- Enhance and disseminate cybersecurity expertise across the Union
- Participate in activities promoted by the Network and the Centre
- Participate in the working groups on specific activities
- Promote the outcomes of specific projects

European Commission

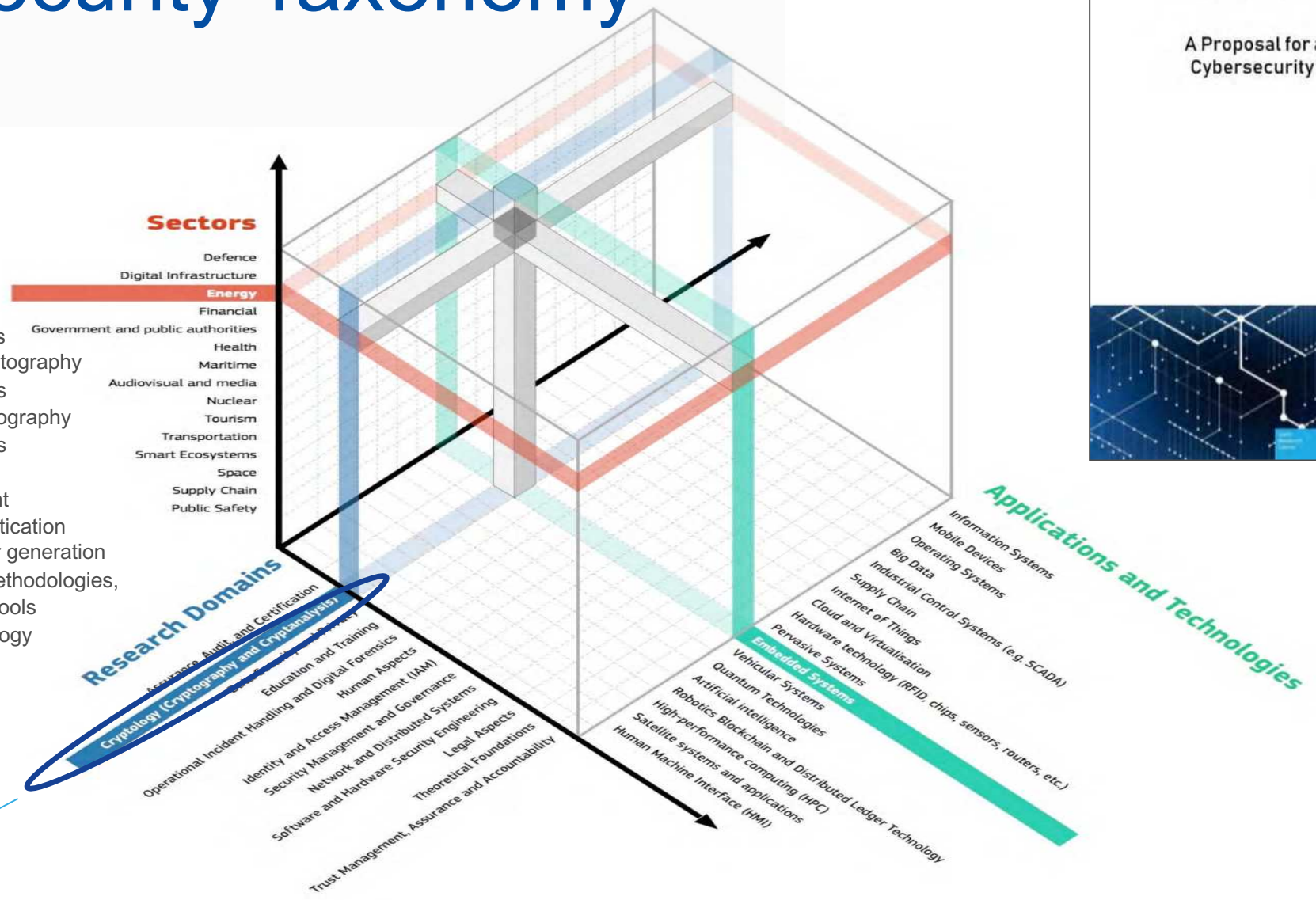
Atlas Foundations

- European Cybersecurity Taxonomy
- Cybersecurity Patent and Research Analysis
- Pan-European Survey 2018

Cybersecurity Taxonomy



- Digital signatures
- Asymmetric cryptography and cryptanalysis
- Symmetric cryptography and cryptanalysis
- Hash functions
- Key management
- Message authentication
- Random number generation
- Cryptanalysis methodologies, techniques and tools
- Quantum cryptology
- Post-quantum cryptology
- Mathematical foundations of cryptography

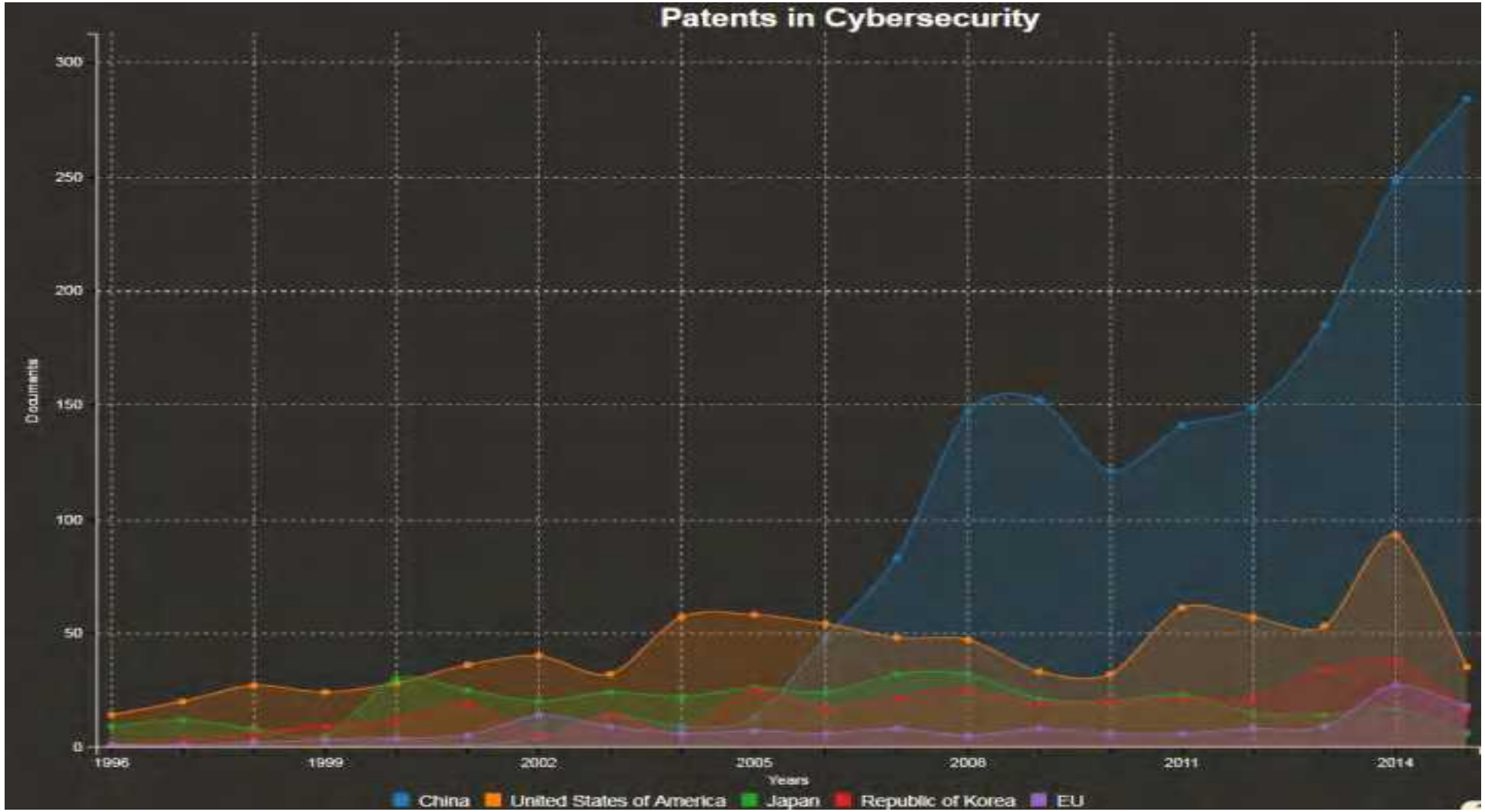


Survey

More than 700 expertise centres registered in the mapping of cybersecurity centres of expertise conducted in 2018

European Commission

Patents



European Commission

Stakeholders

- Research institutions
- Industry
- Startups
- Students
- Researchers
- Job-seekers
- Market analysts
- Policy Analysts
- National authorities
- EU Institutions
- ECSO and its network

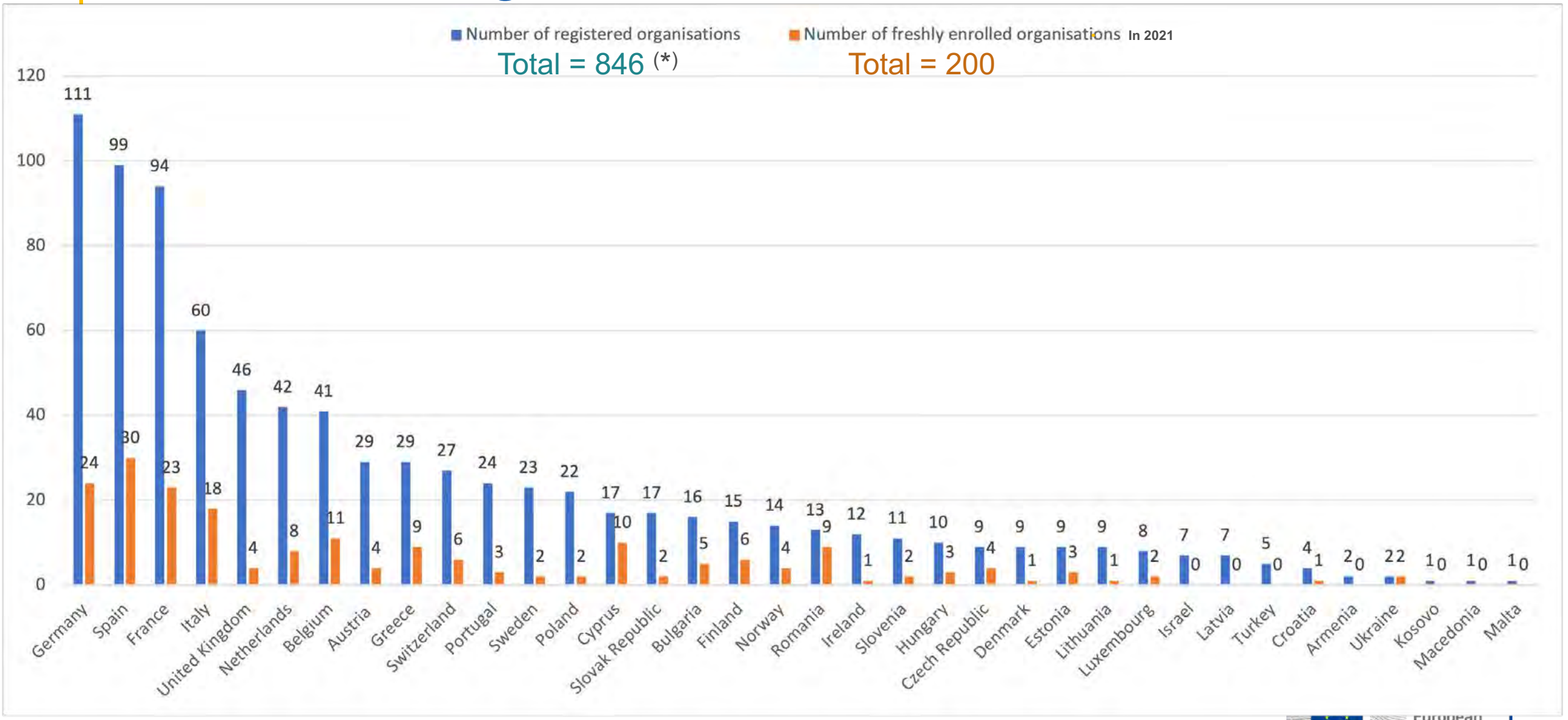
The Atlas as a resource

- Who in Europe is working on which domains, subdomains, sectors, technologies and use cases of the cybersecurity taxonomy?
- Who are the key researchers?
- What are networks?
- What are the time dynamics? (trends/disappearing fields)
- What kind of topic combinations are popular?
- Are there local/regional specialties or hotspots?
- What is the funding allocated for each knowledge domain and research area?
- How does the funding allocated translate to publications and patents?
- Provide awareness of cybersecurity community and support the EC on managing work programmes and funding priorities

Benefits

- Networking: the Atlas provides tools giving opportunities to enlarge the research network
- Visibility: the Atlas wants to become the preferred source of information on cybersecurity activities in the EU
- Contribution to EU policies, programmes and events (e.g. "*when the Commission plans something on AI for cybersecurity, it will consulted entities flagged AI in the Atlas*")
- Link with ENISA sectorial activities
- Access to relevant information from / and on EU projects
- Get students for your course
- Get applicants for your job listing
- Better market studies / insights
- Key Researchers visibility

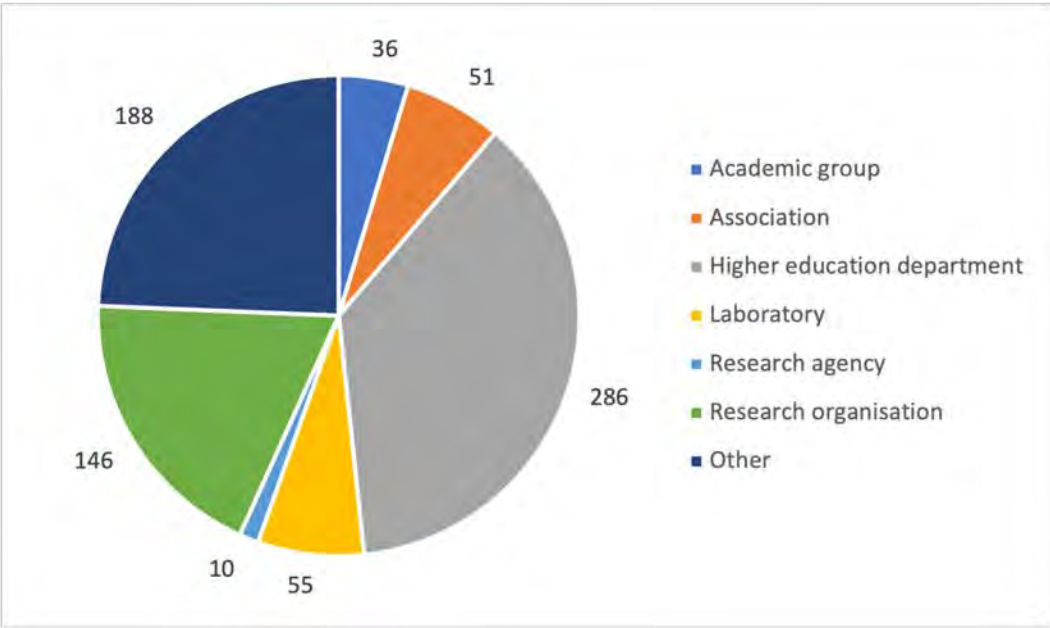
Number of organisations / countries



(*) Total = number of organisations registered during the survey of 2018 + freshly enrolled

European Commission

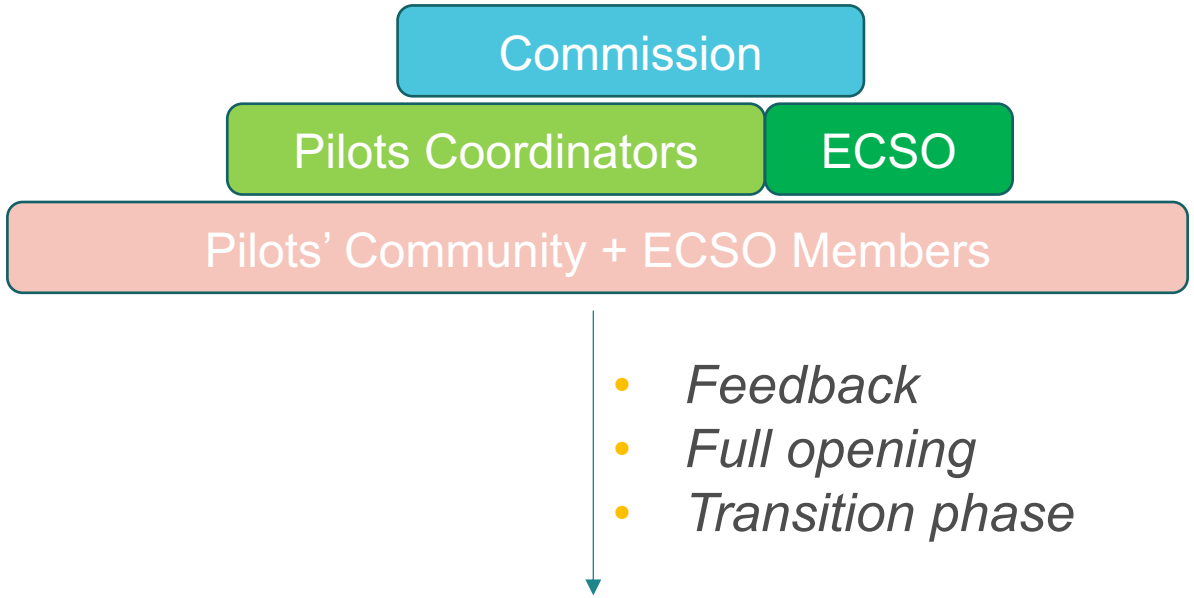
Number of organisations / types



European Commission

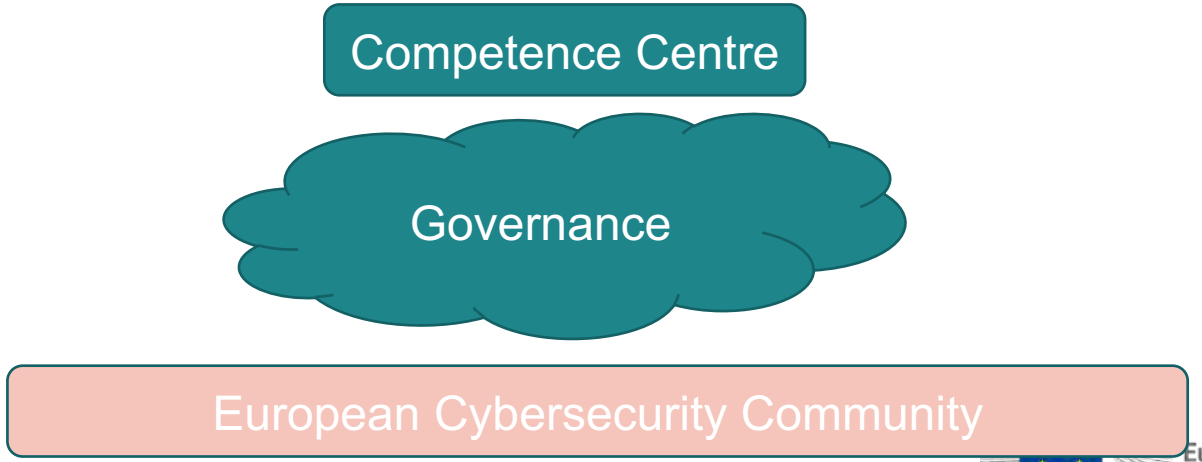
Governance

Phase 1
Piloting Phase



Phase 2

Full Production
Phase



The ATLAS evolution

- Federation of NCCs national digital portals
- European Level Communication strategy
- Cross-Country Visibility
- Cross-Country Collaborations

- Under the hood: adoption of semantic technologies and transition of the taxonomy to an ontology currently being explored

Thank you!

Francesco BARBATO

francesco.barbato@ec.europa.eu

European Commission

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

WE NEED A STRONGER EUROPEAN CYBERSECURITY RESEARCH AND INNOVATION COMMUNITY

Marco Barros Lourenco
Research and Innovation Team

02 | 06 | 2022

ABOUT ENISA

WHAT WE DO


Foresight
Capacity Building
Empowering Communities
Knowledge
Operational Cooperation
Cybersecurity Policy
Trusted Solutions

ENISA STRATEGIC OBJECTIVES

SO1 - "Empowered and engaged communities across the cybersecurity ecosystem"

SO2 - "Cybersecurity as an integral part of EU policy

SO3 - "Effective cooperation amongst operational actors within the Union in case of massive cyber incidents"

SO4 - "Cutting-edge competences and capabilities in cybersecurity across the Union"

SO5 - "High level of trust in secure digital solutions"

SO6 - "Foresight on emerging and future cybersecurity challenges"

SO7 - "Efficient and effective cybersecurity information and knowledge management for Europe"

ENISA is expected to contribute to the EU Strategic Research Agenda in the field of cybersecurity (Art. 11 of the Cybersecurity Act)

ENISA is not a research body or organisation.

Our role is to advise EU Institutions, Bodies, Agencies and Member States on Research and Innovation Priorities in the field of cybersecurity.

“ENISA should strive for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.” CSA (4)

We advise the European Cybersecurity Competence Centre (ECCC) defining a strategic agenda and a work program.

Based in Bucharest, the ECCC will be the Union's main strategic instrument to pool investment in cybersecurity research and technology deployment, thus contributing to industrial development.

CYBER SECURITY IS A TEAM SPORT


Cybersecurity relies on a multi- and inter-disciplinarity of topics and specialties to achieve success. Research is at the forefront of learning more about threats and how to protect from them.


A stronger research community will generate the drive and perspective to create long lasting change and face the challenges through collaboration and cooperation.

WHAT'S NEXT?

- Establish the ECCC Competence Community.
- Atlas as the main reference to identify members from the Community
- Interlink other sources of information with Atlas (Cordis, etc.)
- Call for action to build a stronger Community
- Mobilize the community to continue discussing the needs and priorities

THANK YOU FOR YOUR ATTENTION

+30 281 4409536

info@enisa.europa.eu

www.enisa.europa.eu

Roadmapping for the future

4Pilots + ECSO Roadmap focus group

CONVERGENCE NEXT

Brussels, 2 June 2022

The roadmap focus group

- Early 2019: lauch of four pilot cybersecurity competence networks.
- End 2020: establishing a cross-pilot focus group on roadmaps.
- Spring-summer 2021:
  - exchanges on roadmap content and processes between pilots,
  - prioritisation of cybersecurity challenges.
- Autumn 2021 – Winter 2022:
  - delivering the document “Cybersecurity Research Focus Areas Priorities”,
  - to be integrated into the EU Cybersecurity Atlas.

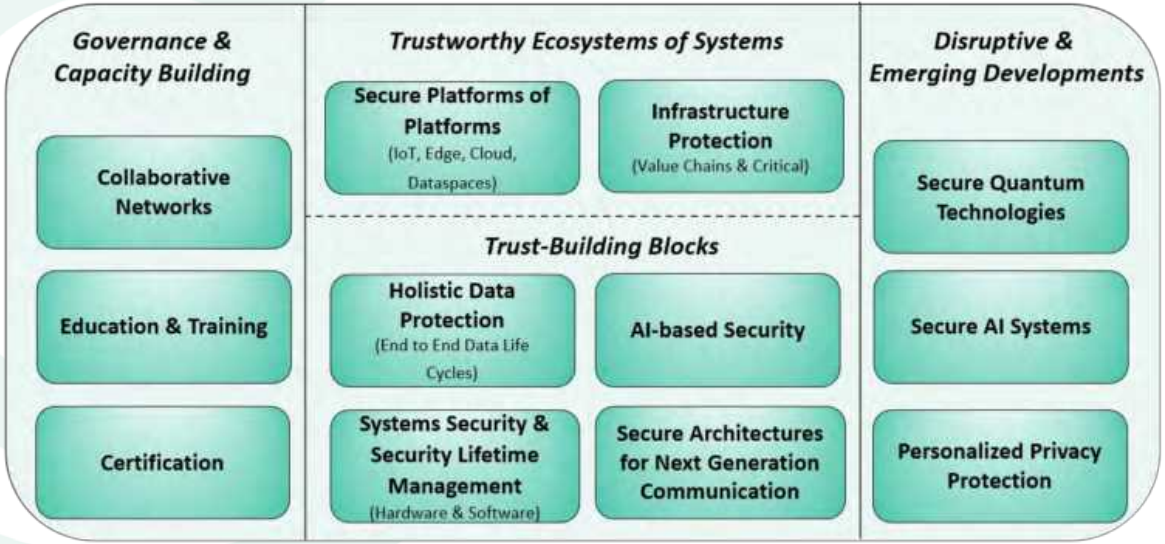
How did we do it?

- Brainstorming
- Monthly Meetings
- We started simple and built on it:
  - **Define a small number of priorities**
    - One line for each
    - Deliver them
  - For each priority **write a short paragraph**
    - Explaining what it is
  - For each priority **give supporting evidence**
    - Deliverables, papers, etc.

Cybersecurity challenges document

Cybersecurity Research Focus Areas Priorities: The 4 Pilots & ECSO Perspective

As per August 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

Trustworthy eco-system of systems

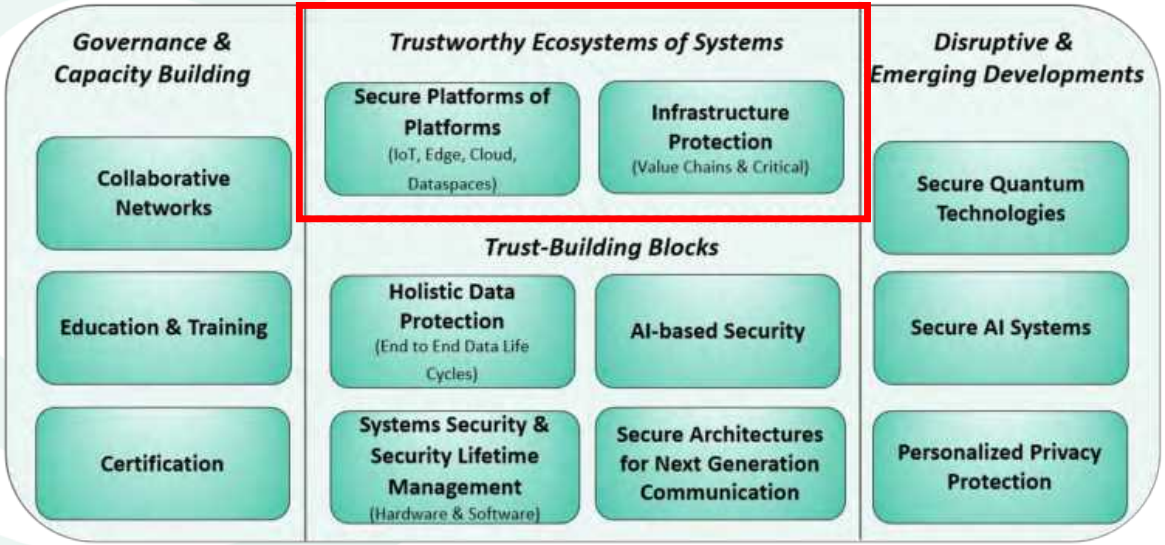
Evangelos Markatos

Cybersecurity challenges document

ANNEX 19, page 6

Cybersecurity Research Focus Areas Priorities: The 4 Pilots & ECSO Perspective

As per August 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

Ecosystems of Systems
What is it? What are they?

- A trip down memory lane:
- Back in the **80's computing was simple**:
  - No hard drive
  - No network
  - No Internet
  - Software arrived in floppy disks
- Things were **self-contained**
- Very **few interactions among computers**
- Or
- Any interaction happened was at the speed
  - Of floppy disks…

Image from:
https://commons.wikimedia.org/wiki/File:IBM_PC_5150.jpg

Ecosystems of Systems
What is it?

- A trip down memory lane:
- In the **90's** people started to use the **Internet**:
  - Email, ftp, the web
  - Computers started to interact via the network
    - Browse the Web
    - Download documents, images, songs
- The Network services were nice
  - But they were not essential

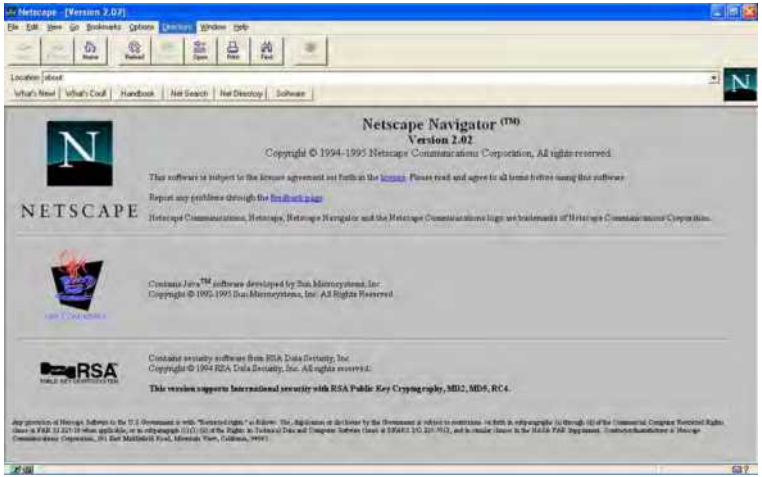


Image from:
https://commons.wikimedia.org/wiki/File:Netscape_Navigator_2_Screenshot.png

Ecosystems of Systems
What is it?

- A trip down memory lane:
- In the 00's people started to **depend** on the **Internet**:
  - Lots of new services:
    - Google, Gmail, Facebook, Twitter, YouTube
  - Computers started to need the network
- The **Network services became essential**
  - Functioning without them was difficult
  - Not impossible – but difficult

Image from:
https://commons.wikimedia.org/wiki/File:Netscape_Navigator_2_Screenshot.png

Ecosystems of Systems What is it?

- A trip down memory lane:
- In the 10's people started to put all services on-line:
  - **Online Banking**:
    - Physical banks (buildings) were slowly closing down
  - **Online trading**: stockmarket was online
  - **e-government**: taxes, official documents, were online
  - **Cloud**: all data (and computation) were in the cloud
  - **Software** was distributed on-line
    - frequently "as-a-service"
- The **Network became the computer**
  - Functioning without a network
    - was next almost impossible

The trend

ANNEX 19, page 11

- 80’s: Computing was self-contained
- 90’s: Internet was a nice “add-on”
- 00’s: Internet became essential
- 10’s: Internet became absolutely necessary
- 20’s: COVID made on-line the only option
  - physical/offline was impossible or even illegal!

Ecosystems of Systems What is it?

- Now that everything is on the network we wonder:
- What is a computer?
- What is my computer?
- How many computers do I use every day?
- How can I protect them?
- Who is responsible for protecting them?
- How can I be protected from them?

Trustworthy ecosystems of systems: Cloud, Edge, Fog: Systems of Systems

Main topics:

- Secure **Platforms of Platforms**
  - **IoT, Edge, Cloud, Dataspaces**
- **Infrastructure Protection**
  - **Value Chains**
  - **Critical Infrastructures**

Secure Platforms of Platforms

- Cloud Infrastructures **Vulnerabilities Mitigation**
  - Mitigate the vulnerabilities that exist in the cloud
- Secure Integration of **Untrusted IoT** in Trusted Environments
  - Not all components will be trusted
- **EU** Multi-Cloud, Edge & IoT
- Trust & Security **for Massive connected IoT Ecosystems** & Lifecycle Management
  - How do you make sure that they are secure for life?

Infrastructure Protection

- Security **across Value Chains**: From Industry 5.0 to Supply Chains
  - Supply chains involve several actors…
- **Critical Infrastructures** Protection & Resilience
- Trusted **Information Sharing** & Collaborative Threat Intelligence Management
  - Sharing brings knowledge

Why are these important?

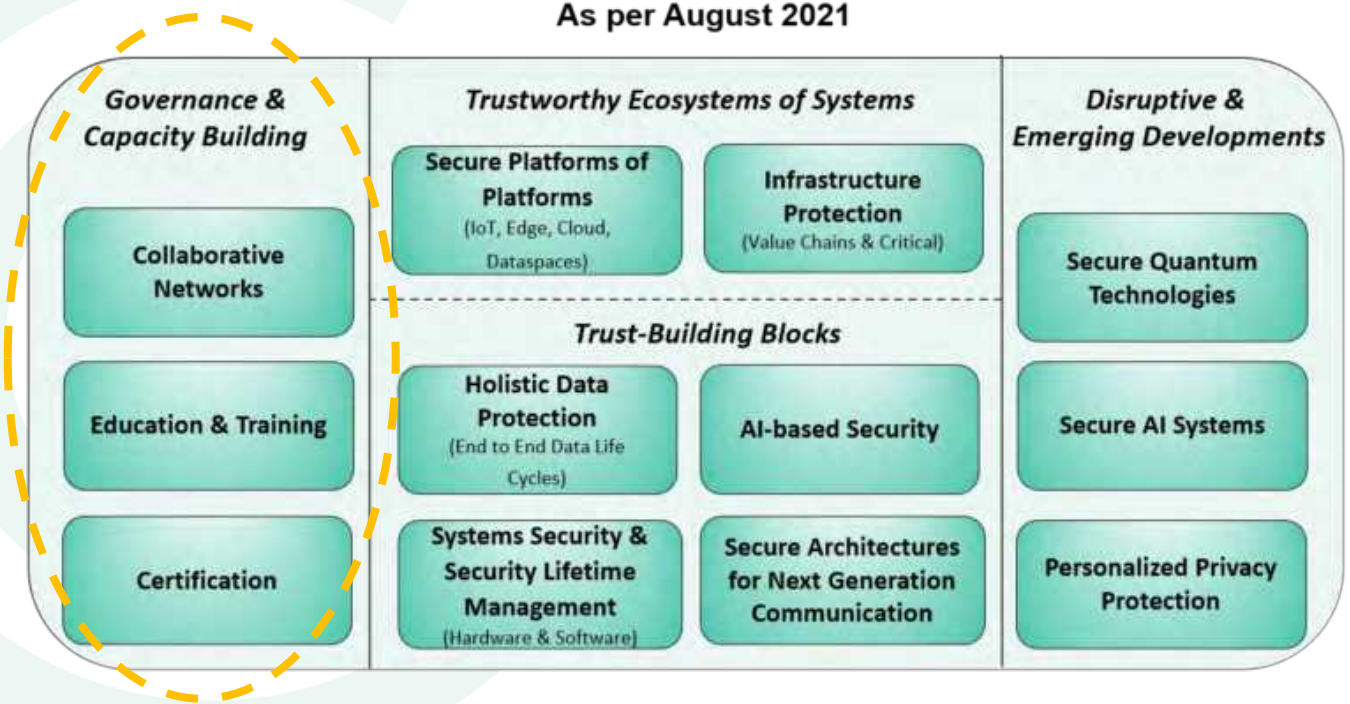
- We have to use ecosystems of systems
  - There is no easy way “back”
  - COVID has shown that on-line might be the only option
- Each app uses several computers and software modules
  - Lots of them are being developed outside Europe
- Securing Ecosystems of Systems is necessary for
  - **European Digital Sovereignty**

Governance and Capacity building

Theodora Tsikrika

Cybersecurity Research Focus Areas Priorities: The 4 Pilots & ECSO Perspective

As per August 2021



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

Governance & Capacity Building

Support to EU ambition for maintaining sovereignty and becoming a global leader in the digital economy, guided by democratic values and resilient to cybersecurity threats

- Research into Governance structures:
  - Available cybersecurity competencies and capacity: overview, organise, enhance
  - Certify competencies, products, services
  - Ultimately, respond effectively to current and future cybersecurity challenges

Collaborative Networks

- **Landscape**
  - Growing diversity and sophistication of cyber threats
  - Need for integration of broad spectrum of competencies & resources
    - human, technological, financial
  - Beyond the powers of a single organisation or even a single country

- **Research Focus**
  - Establish efficient & sustainable collaborations among variety of organisations
  - Varying legal, legal, organisational and cultural contexts
  - Understand requirements, design and implement effective norms and models, and the supporting infrastructure

Education & Training

The Human Factor

key for both cybersecurity and competitiveness of Europe's digital economy

- **Landscape**
  - Growing demand for cybersecurity professionals
  - New levels of awareness for policy-makers, non-technical personnel, and citizens
- **Research Focus**
  - Shared understanding of the evolving requirements to the competences of professionals
  - Developing more comprehensive frameworks and infrastructures
  - Supporting the enhancement of cybersecurity skills and competencies
  - Cyber ranges, federations, re-use of training scenarios, monitoring and evaluating trainees' knowledge and performance, …

Governance & Capacity Building

Collaborative Networks

Education & Training

Certification

Certification

- **Landscape**
  - Need for high levels of confidence that a particular device, product, system, process, or service are designed, delivered, and operate according to defined security policies
  - Increased interconnectedness among systems and organisations
  - Cybersecurity certification is expected to facilitate these guarantees and formally attest or confirm certain security characteristics

- **Research Focus**
  - Further investigation and development of the (currently complex) evaluation process (risk assessment, requirements analysis, verification and testing procedures, …)
  - Existing standardised approaches cover only partially the needs of cybersecurity certification
  - Ensure security throughout the lifetime of the design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation

Governance & Capacity Building

Collaborative Networks

Education & Training

Certification

Roadmap processes

Arthur van der Mees, Thomas Jensen

The SPARTA Roadmap Process

Mission-oriented

- Mission: strengthen European Strategic Digital Autonomy with respect to cyber security

Technology focus: horizontal technologies, generic, not sector-specific

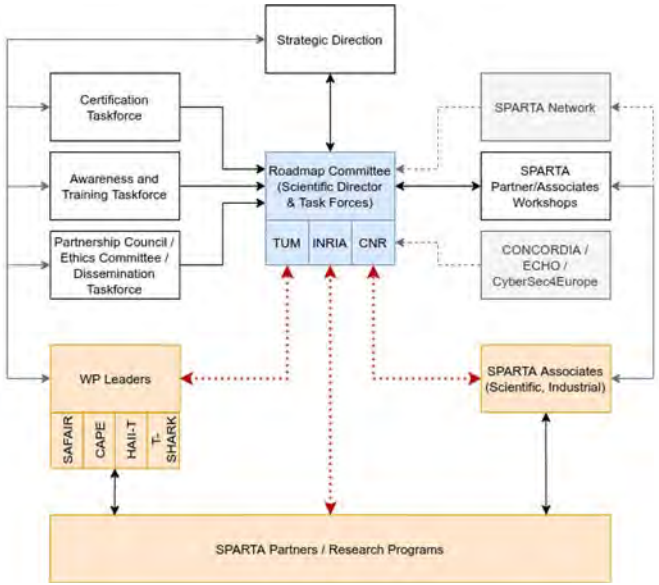
- Identify Technological white spots to be filled to address the mission

Design Process

- Iterative, agile: review, discuss, adjust,
- Open: early discussions with all stake holder within the community
- Guided by a governance process: defining criteria and rules

Results:

- Guidelines for policy makers to develop strategies that:
  - strengthen the EU's cybersecurity capacity,
  - close cyber skill gaps and,
  - address current and emerging challenges appropriately short, midterm and long term activities



ROADMAP V0

Identification of White Spots

- Analysis of strategic research Agendas (national, EU): identification of interesting white spots
- Identification of 5 initial Challenges (SPARTA Research Programme)
- Identification of additional > 60 Challenges: clustering and prioritization was necessary

Research Domains

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	
Assurance, Audit, and Certification	■			■	■		■			■		■	7
Cryptology				■	■		■				■		4
Data Security and Privacy		■		■	■		■		■		■		6
Education and Training	■	■	■		■	■	■	■	■	■	■		10
Operational Incident Handling and Digital Forensics	■			■		■	■	■	■	■	■	■	9
Human Aspects				■	■						■		3
Identity and Access Management											■		1
Security Management and Governance	■	■	■		■	■	■	■	■	■	■	■	11
Network and distributed Systems				■	■	■							3
Software and Hardware Security engineering	■	■				■	■		■				5
Security Measurements	■								■	■			3
Legal Aspects		■	■					■		■	■		5
Theoretical Foundations													0
Trust Management, Assurance, and Accountability				■							■		2

Technologies

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	
Artificial Intelligence;							■			■	■	■	4
Big Data;				■	■					■			4
Blockchain and Distributed Ledger Technology (DLT);							■					■	2
Cloud and Virtualisation;					■		■			■		■	4
Embedded Systems;					■					■			3
Hardware technology (RFID, chips, sensors, routers, etc.)													0
Industrial Control Systems (e.g. SCADA);				■	■		■			■		■	6
Information Systems;												■	1
Internet of Things;				■			■					■	4
Mobile Devices;					■								1
Operating Systems													0
Pervasive systems													0
Quantum Technologies;				■			■						2
Robotics;												■	2
Satellite systems and applications;					■								1
Supply Chain;						■						■	2
Vehicular systems													0

Sectors

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	
Audiovisual and media													0
Defence									■				1
Digital Infrastructure													0
Energy					■		■		■	■			4
Financial					■		■		■				3
Government and public authorities							■						1
Health				■	■				■	■	■		5
Maritime													0
Nuclear													0
Public safety													0
Tourism							■						1
Transportation				■	■		■		■				4
Smart ecosystems					■								1
Space									■				1
Supply Chain													0

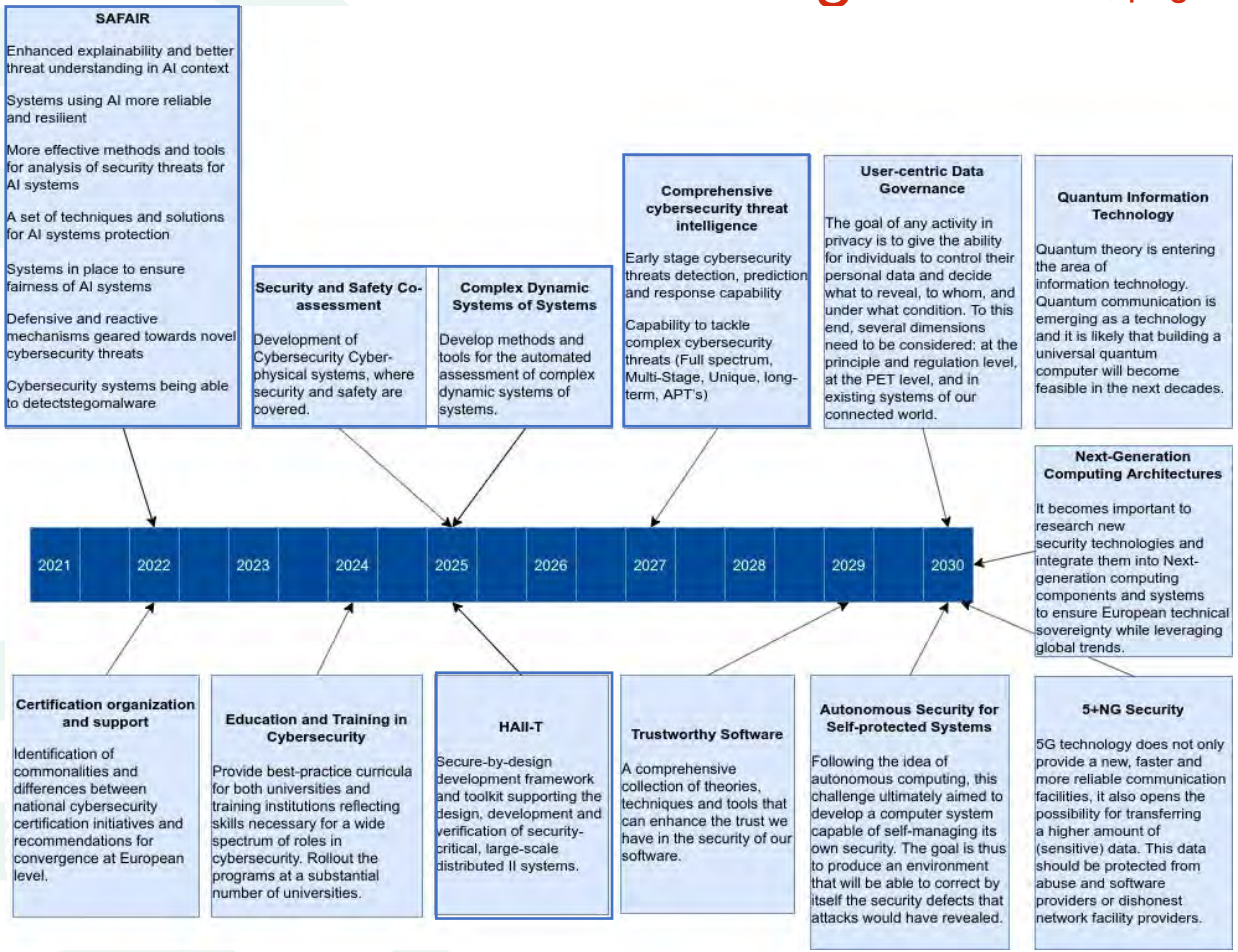
ROADMAP V1: Extension and Clustering

13 Mission Programmes

Clustering

- 3 Dimensions: closely connected:
  - Technology, Education,
  - Certification
- Benefits for EU and the single market
- SWOT (EU view)

Original SPARTA research programs marked with blue frames



Roadmap V2: Prioritisation

Discussion with the Community: due to Covid 19: digital formats

► SPARTA network, associates and interested parties

Lessons Learned

► Using only digital formats for feedback is insufficient

Development of online Tooling:

► Interactive online survey to collect roadmap feedback

Result based on feedback and discussion:

Priority	Roadmap Challenge
1	Secure Certifiable AI Systems
2	Trustworthy Software
3	User-Centric Data Governance
4	Collaborative Threat Intelligence Management
5	Secure Next Generation Communication Systems
6	Continuous Security Assessment
7	Trustworthy Certifiable Hardware
8	Secure Integration of Untrusted IoT in Trusted Environments
9	Complex Dynamic Systems of Systems
10	Autonomous Security for Self-Protected Systems
11	Quantum Information Technology

SPARTA Roadmapping – Some lessons learned

- **No one-size-fits-all solution!**
  - To cover different points of view, e.g. technology, economy, sector requirements, human centering it is valuable to establish a multi-view Roadmap with **a technology kernel and different views**

- **SPARTA process: Decisions that have been proven effective**
  - Mission-oriented approach: very useful (guidance!).
  - Open: continuous feedback from the expert community
  - Agility: Roadmapping should be seen as a process
  - Joining forces, using the established cyber security networks was of utmost importance.
  - Interactive, guided online surveys have proven to be effective.
  - Using a governance structure to coordinate the process has been shown effective.

- **Lessons learned to improve the process**
  - Face-2-Face reviews and discussion have proven to be more effective than only digital formats.
  - A transfer roadmap should be integrated to foster the transfer of research results into concrete capabilities.

Root Source,
Segment,
Structure,
Systemise,
Visualise

How to Build, Achieve & Sustain European Digital Sovereignty?

Contextual, Impact-based, Symbiosis of Four Intertwined Main Domains

as mentioned in the ECCC & NCC Network Regulation

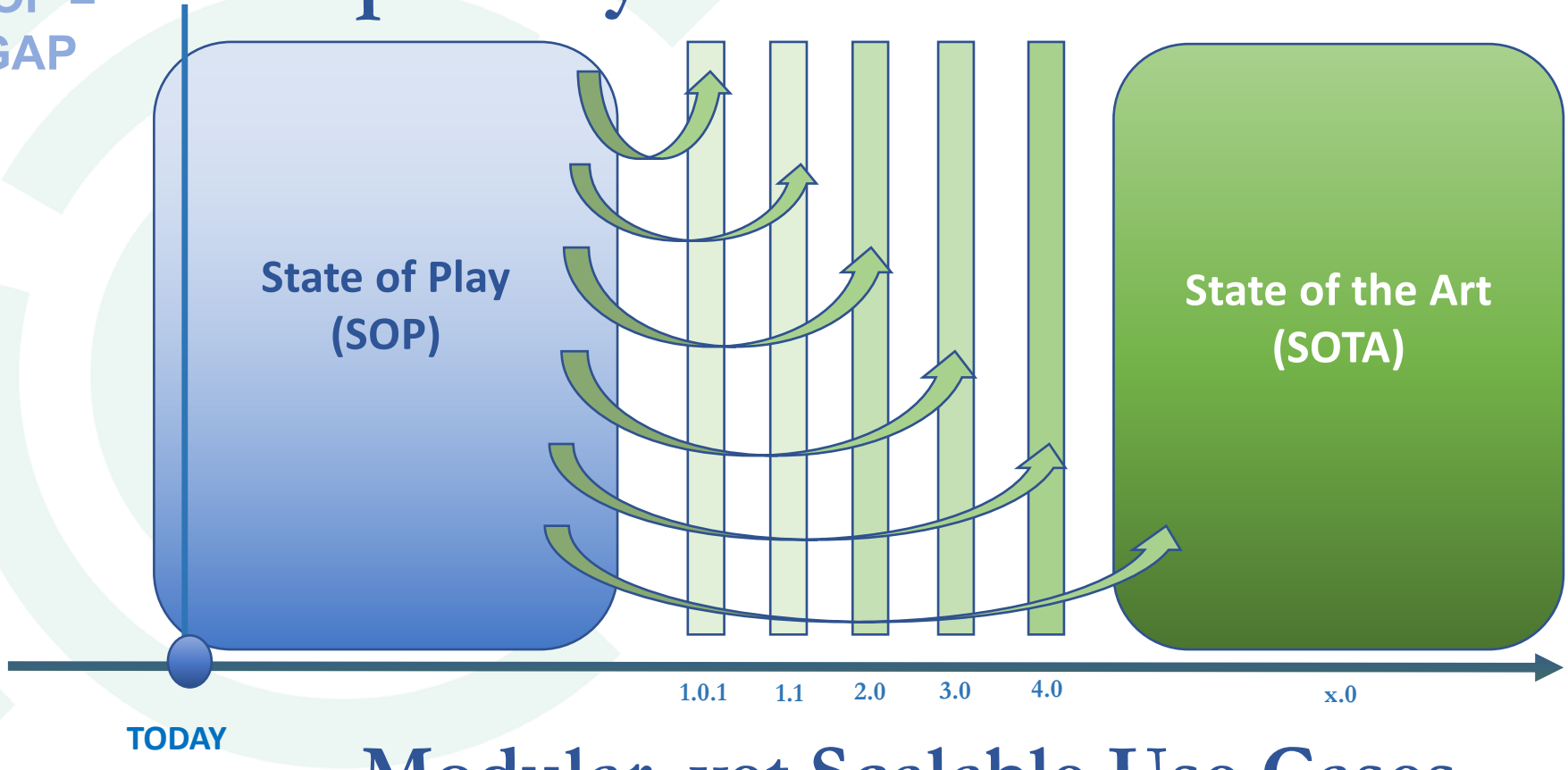
CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

From Technology-centric to Stakeholders-centric

Human-, Persona- & Societal-Centric, Use Case-driven, Data-Centric & Technology Agnostic

SOTA -/- SOP = GAP

Gap Analysis leads to Use Cases



Modular, yet Scalable Use Cases

CONCORDIA Cybersecurity Roadmap for European Digital Sovereignty

A. Research & Innovation
B. Education & Skills
C. Economic Perspectives
D. Legal & Policy Perspectives
E. Certification & Standardisation
F. Investment Strategies
G. Community Building
H. Other Objectives, Challenges & Scenarios

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

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Human-Centric Digital Ecosystems & Multi-Angled Omni-Stakeholders & Influencers

1. **The User** (Convenience-Focused, Cheap, Curious, Creative, Opportunistic)
2. **Customers** Who Are Willing To Pay (B2x, x2x)
3. **Suppliers & Value Ecosystem** (Secure In, Secure Inside, Secure Out, Secure After)
4. **Physical, Cyber-Physical & Cyber Ecosystems and Society** (including Non-Users)
5. **Malicious Actors** (They Are Patient. And They Collaborate! We Do Not, Enough)
6. **Act First Seek Forgiveness Later Technology & Data Titans**
7. **Investors & Financers** (they invest, and want a Return on Investment)
8. **Policy Makers**, Standardisation Development Organisations & Markets
9. **Authorities** (Who is responsible for what, and are they capable?)
10. **Data Access**: Law Enforcement, Intelligence Services & Defence

Roadmapping for the future

4Pilots + ECSO Roadmap focus group

CONVERGENCE NEXT

Brussels, 2 June 2022

1–3 June 2022
Brussels

CONVERGENCE NEXT

Cyber Competence Network

CCN Education focus group

Boning FENG, OsloMet

Led by

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

The CCN Education group

the creation of a European education ecosystem for cybersecurity

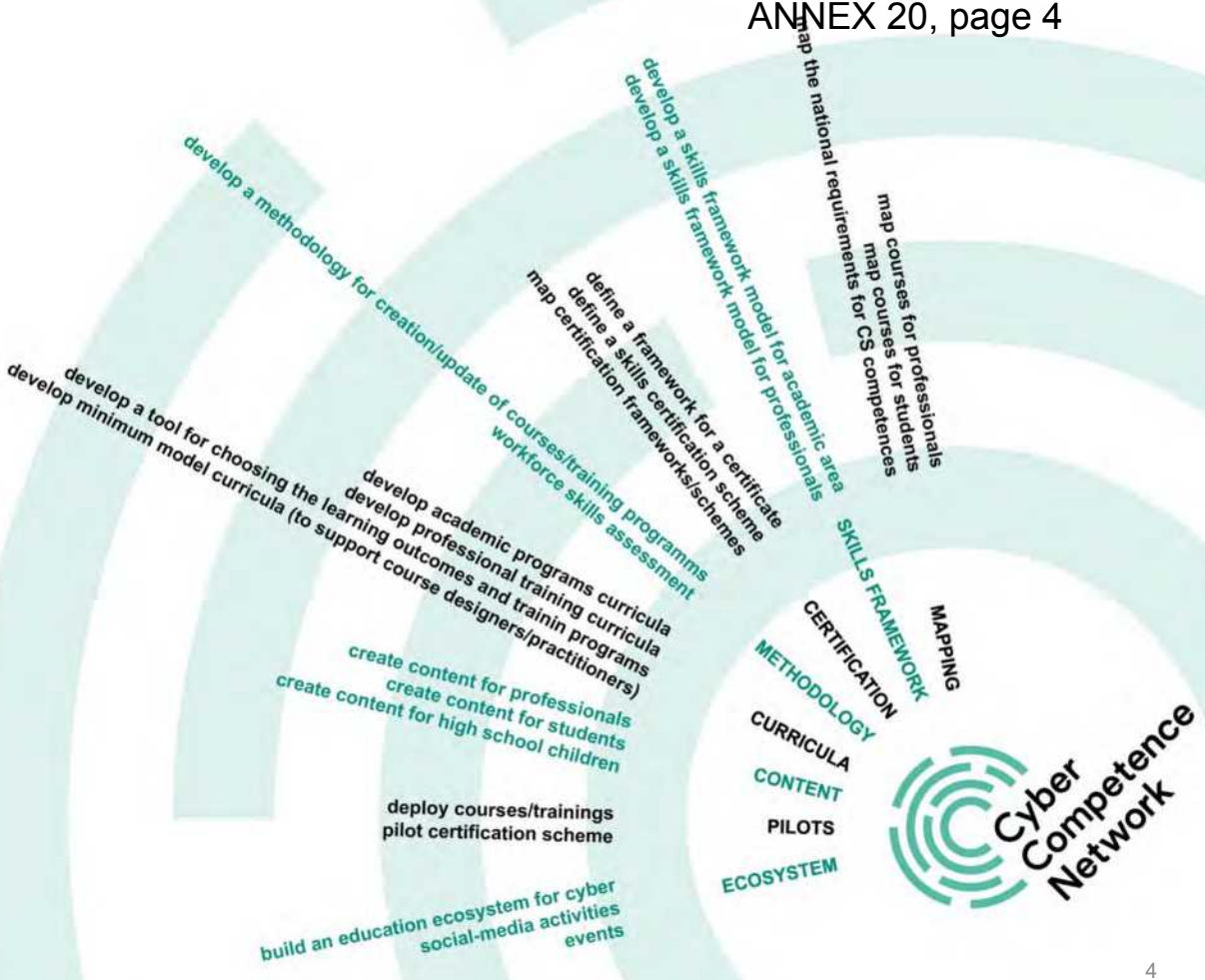
- Objective: share, support, collaborate

The CCN Education group is looking into the creation of a European education ecosystem for cybersecurity to support the work of the future network of cyber competence centres and contribute to the EU efforts in closing the cybersecurity skills gap.

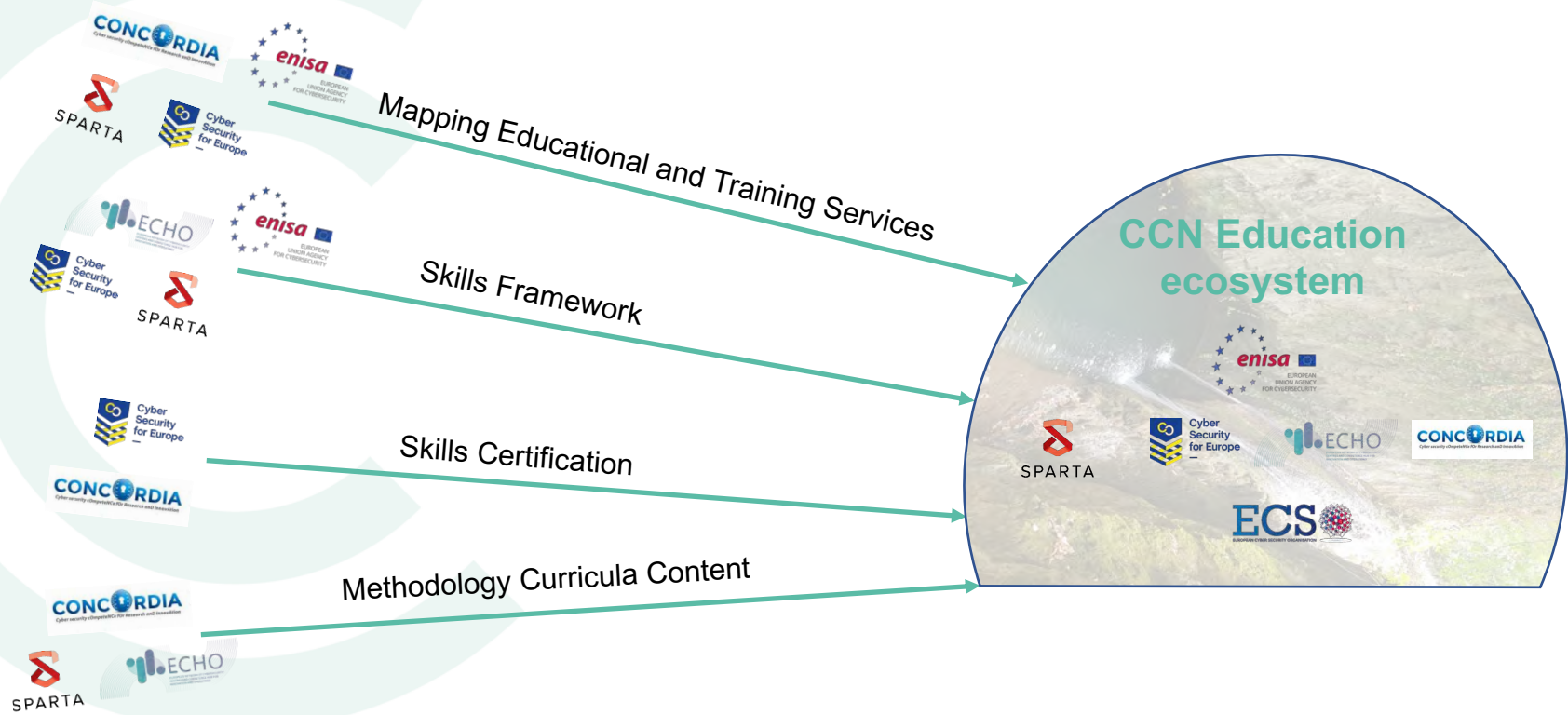
- Outcome: building the European Cybersecurity Education Ecosystem

Overview of the different activities covered by the pilots

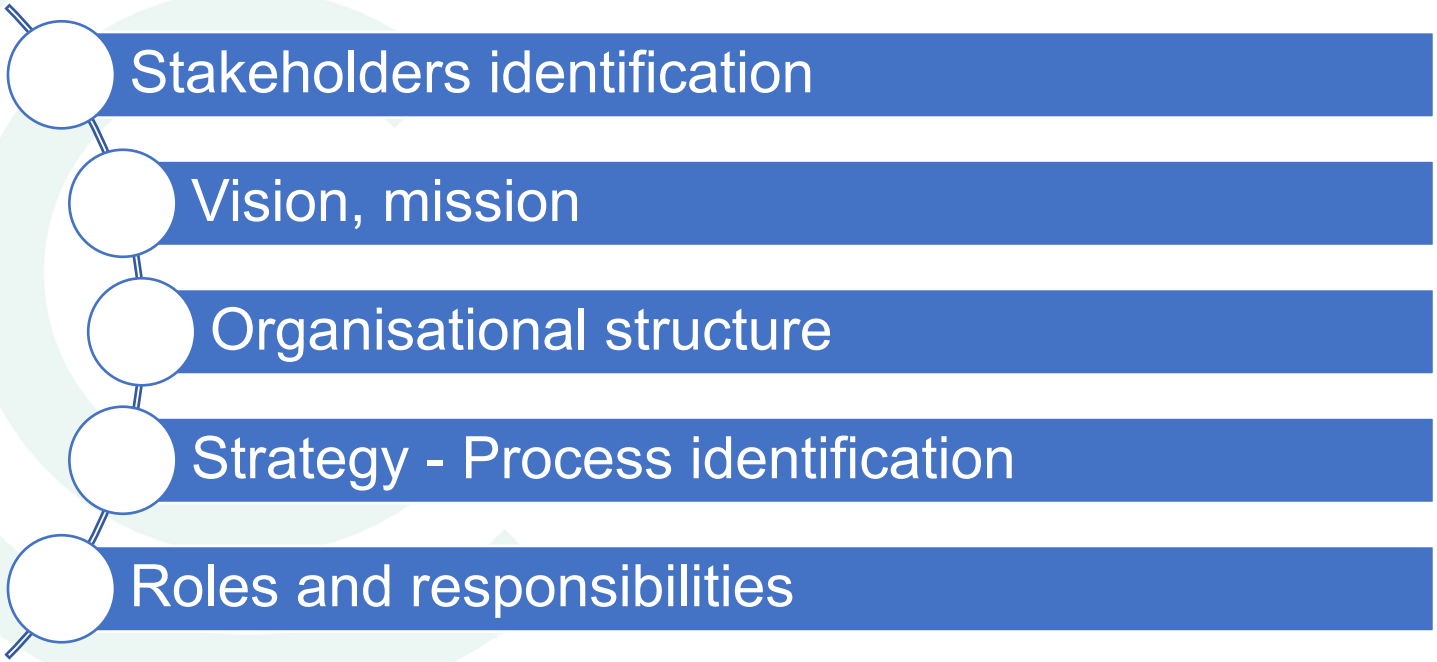
[link to CCN Edu page]



One Direction – Different Approaches



The European Education Ecosystem Governance model



The European Education Ecosystem Governance model

Your feedback is needed

contact@cybercompetencenetwork.eu


1–3 June 2022
Brussels
CONVERGENCE NEXT
Cyber Competence Network

CCN focus group on education

Carlos E. Budde
Ass. Prof. @ Università di Trento
CS4E: Cybersecurity Skills and Capability Building (WP6)

01

Some results by SPARTA

Jan Hajný

CURRENT STATUS & ACHIEVEMENTS

SPARTA

Achievements

- **Deliverables**:
  - All deliverables (D9.1, D9.2, D9.3, D9.4, D9.5) submitted on time
  - Available: https://www.sparta.eu/deliverables/
- **Results**:
  - Education Map published
    - https://www.sparta.eu/study-programs/
  - Curricula Designer published
    - https://www.sparta.eu/curricula-designer/
  - Papers published
    - https://www.sparta.eu/papers/
- **Events**:
  - Go Cyber with SPARTA at ULPGC
  - Go Cyber with SPARTA at La Reunion
  - ARES ETACS Workshop 2021 and 2022
    - https://www.ares-conference.eu/workshops-eu-symposium/etacs-2022/

On-going

- **ENISA AHWG**
  - Feedback on EU CSF
- **Education Focus Group**
  - Transfer to REWIRE

Coming up

- **WP9 finished in January 2022**
- **SPARTA finishes in June 2022**
- **REWIRE to follow up**

02

Some results by ECHO

Pavel Varbanov

ECHO-Educational Outcomes

Sector-specific Skills Framework

- Energy, healthcare, maritime;
- Assets;
- Risks (vulnerabilities and threats)
- Impact;
- Competences to avoid risks and respond adequately.

Sector-specific training program

- LOs
- Methodology
- Content
- Tools
- Evaluation

Pilot trainings for ICT professionals
on CTI,
Incident Response,
Incident Recovery

ECHO EUROPEAN NETWORK OF CYBERSECURITY CENTRES AND COMPETENCE HUB FOR INNOVATION AND OPERATIONS

ECHO project has received funding from the European Union's
Horizon H2020 research and innovation programme under the grant agreement no 830943

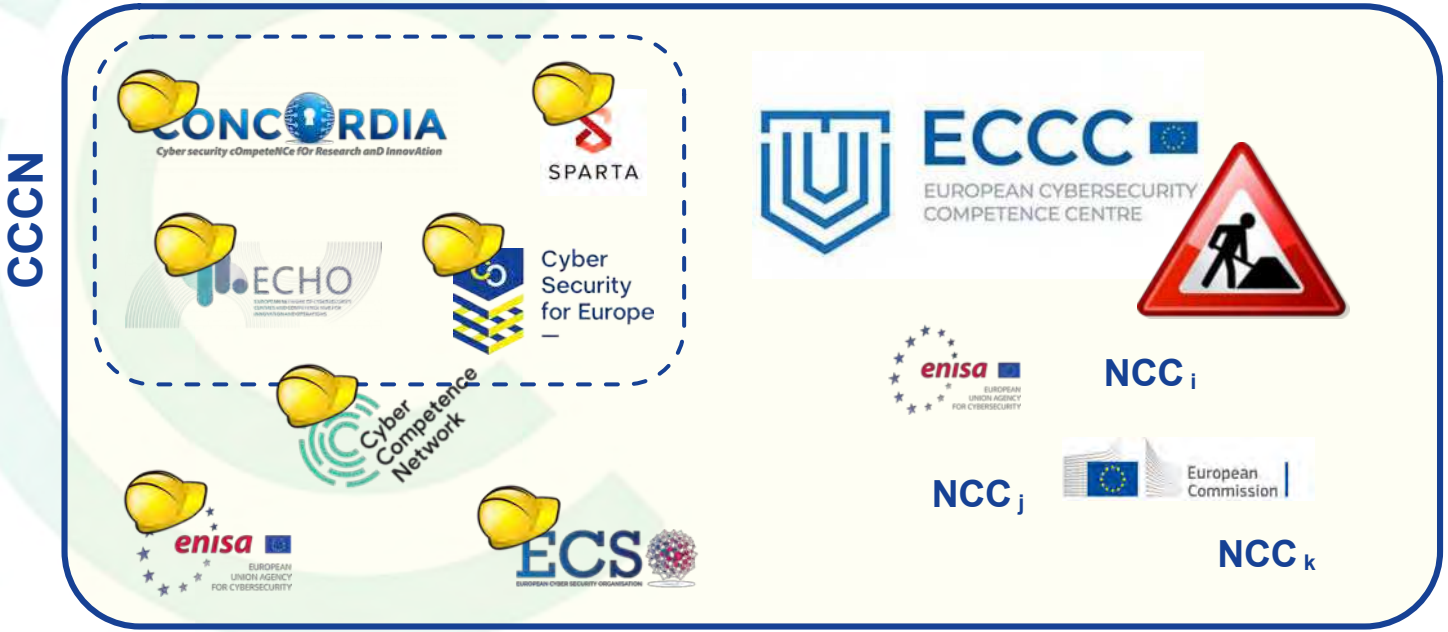
03

Some results by CS4E

Carlos E. Budde

Baustelle panorama

European Cybersecurity Industrial, Technology and Research Competence Centre (CCCN)



Educational curricula: university++

Massive
Open
Online
Courses

Serious Games:

- Cryptoclub
- Cyberciege
- Interland
- Dropit!
- …

BSc courses

MSc courses

PhD curricula

Cyber Ranges

Utility? Validity?

… out of 3

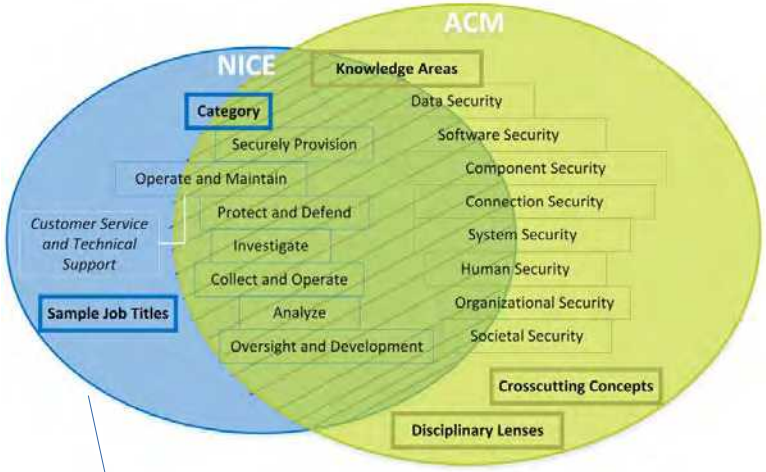
Data protection lawyer	2	0	3
Software engineer	1	3	0
IoT security manager	3	2	1
Risk management			
Network architecture			
Privacy of personal data			

Skills assessment framework

		Scenario											
	Skill	DP	SC	ST	NA	IS	IA	UI	UE	CL	SI	CB	CS
Data Security	Cryptography	1.0	2.0	1.0	2.0	1.0	1.3	1.3	1.3	2.4	0	0	1.3
	Digital Forensics	0	1.0	0	0	0	1.6	1.6	1.6	1.6	1.0	0	1.1
	Data Integrity and Authentication	0	2.0	2.0	2.0	2.0	2.6	2.6	2.6	2.5	1.0	2.7	1.1
	Access Control	0	2.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	2.0	0	1.1
	Secure Communication Protocols	1.0	3.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	1.0	2.8	1.3
	Cryptanalysis	0	0	0	0	0	1.0	1.0	1.0	1.0	0	0	1.3

Knowledge Units / Specialties

Knowledge Area / Category



Education and training review

Design of education and professional framework

Assessment study (ongoing)

Preliminary study covered **29 participants**
(industry and academia) across **11 EU countries**

Budde[1] Karinsalo[2] Vidor[1] Salonen[2] Massacci[1,3]
[1] *VTT Technical Research Centre, Finland*
[2] *University of Trento, Italy*
[3] *Vrije Universiteit, The Netherlands*

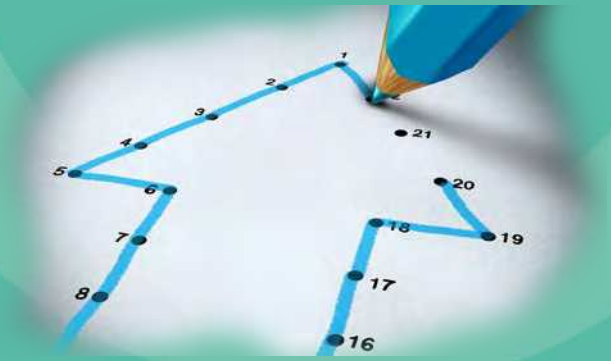
Key takeaways:

- **Priorities of academia and industry are not well aligned**
  - Academia's top-3 education areas: 1. Organisational security 2. System security 3. Data security
  - Industry's top-3 training areas: 1. Societal security 2. Software security 3.Organisational security

- **Human Security is not considered fundamental**
  - The area includes *Social Engineering* which is a key skill in most successful attacks.
    Yet Data Security is ranked higher according to both the academic and industrial respondents.

Full report to come, contacts: carlosesteban.budde@unitn.it Anni.Karinsalo@vtt.fi

Some connecting lines



Ongoing *study*, but survey done

Preliminary study covered **29 participants**
(industry and academia) across **11 EU countries**

		Scenario											
	Skill	DP	SC	ST	NA	IS	IA	UI	UE	CL	SI	CB	CS
Data Security	Cryptography	1.0	2.0	1.0	2.0	1.0	1.3	1.3	1.3	2.4	0	0	1.3
	Digital Forensics	0	1.0	0	0	0	1.6	1.6	1.6	1.6	1.0	0	1.1
	Data Integrity and Authentication	0	2.0	2.0	2.0	2.0	2.6	2.6	2.6	2.5	1.0	2.7	1.1
	Access Control	0	2.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	2.0	0	1.1
	Secure Communication Protocols	1.0	3.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	1.0	2.8	1.3
	Cryptanalysis	0	0	0	0	0	1.0	1.0	1.0	1.0	0	0	1.3

ECHO

Cyber Security for Europe

CONCORDIA

SPARTA

ECS
EUROPEAN CYBER SECURITY ORGANISATION

WG5 PAPER

European Cybersecurity Education and Professional Training: Minimum Reference Curriculum

SWG 5.2 I Education & Professional Training

November 2021 (version 1.0)

EUCS06 - Enterprise Cybersecurity Practitioner

Competence Level: Advanced
The subject is proposed to be 5 ECTS. The subject can be extended to 10 ECTS with comprehensive coverage of Enterprise Cyber Security body of knowledge with practice learning activities.

Alternative names:

- **Enterprise Network Security**
- **Advanced Enterprise Security**

Subject contents and topics	Learning outcomes (competences)
> Organisational Security and Privacy Policies > Enterprise Risk Management	The student is able to demonstrate the knowledge and skills of - enterprise security and advanced risk manage-

EUCS06 - Cybersecurity Analyst

Competence Level: Advanced
The subject is proposed to be 5 ECTS.

Alternative names:

- **Systems Security**
- **Enterprise Systems Security**
- **Information and Data Security**
- **Data Systems Security**

Subject contents and topics	Learning outcomes (competences)
> Threat Management > Vulnerability Management > Cyber Incident Response > Security and Architecture Tool Sets > Attack cycle > The role of the analyst in cyber threat intelligence > Attribution	The student is able to demonstrate the knowledge, skills and abilities of - network architecture and reconnaissance principles - select appropriate tools for network reconnaissance and vulnerability analysis - threat identification and threat mitigation principles - analyse network vulnerabilities with network reconnaissance and analysing tools - security incidents investigation and monitoring principles - present the results of network reconnaissance and vulnerability analysis in professional format

Suitable job roles:

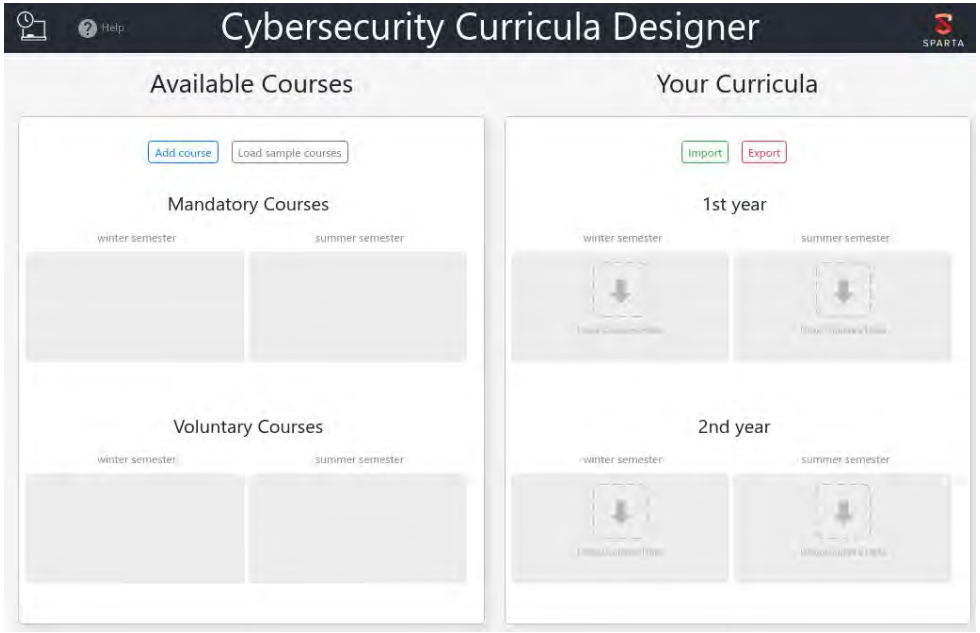
- Cybersecurity Analyst
- Threat Intelligence Analyst

Frameworks and wheels

Frameworks and wheels

https://www.sparta.eu/curricula-designer/

SPARTA



Frameworks and wheels

https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf

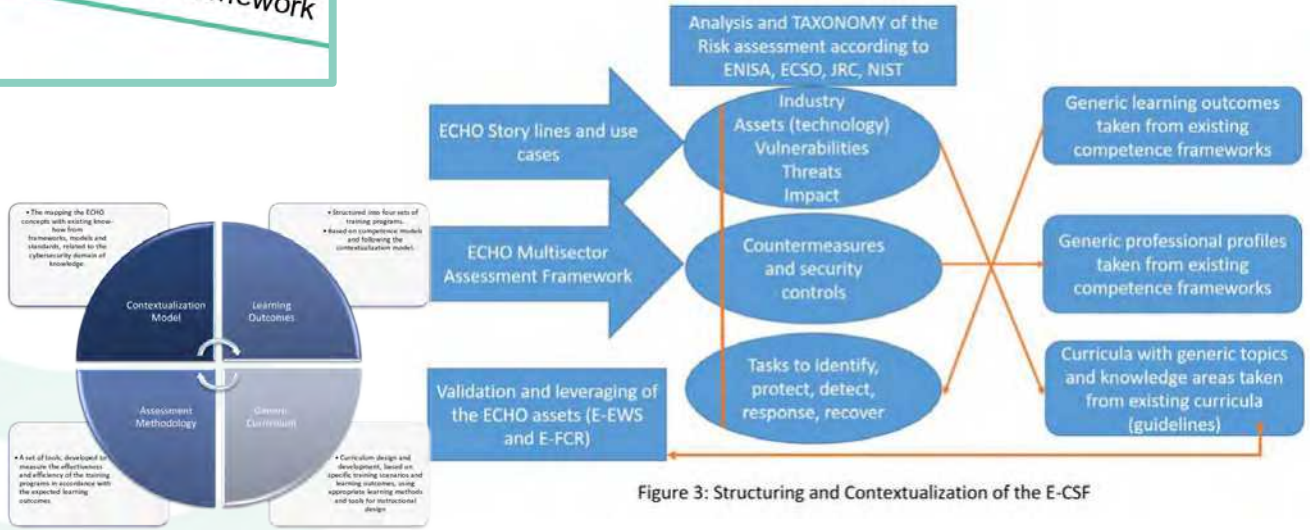
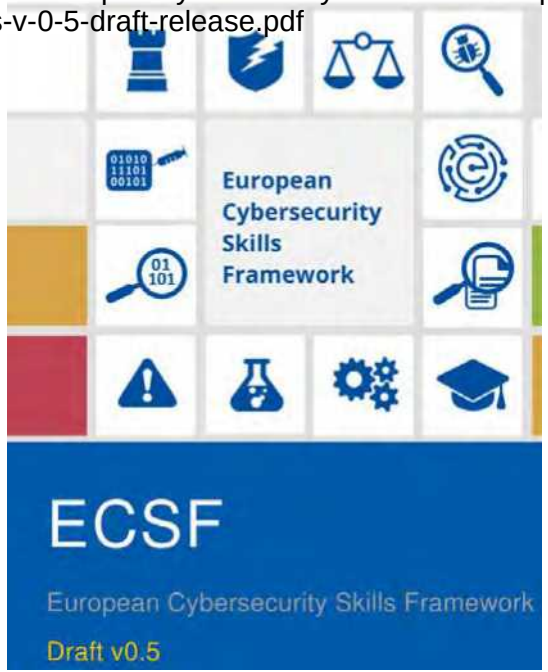


Figure 3: Structuring and Contextualization of the E-CSF

Frameworks and wheels

enisa

https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-framework/ecsf-profiles-v-0-5-draft-release.pdf



Frameworks and wheels

https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf

		Scenario											
	Skill	DP	SC	ST	NA	IS	IA	UI	UE	CL	SI	CB	CS
Data Security	Cryptography	1.0	2.0	1.0	2.0	1.0	1.3	1.3	1.3	2.4	0	0	1.3
	Digital Forensics	0	1.0	0	0	0	1.6	1.6	1.6	1.6	1.0	0	1.1
	Data Integrity and Authentication	0	2.0	2.0	2.0	2.0	2.6	2.6	2.6	2.5	1.0	2.7	1.1
	Access Control	0	2.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	2.0	0	1.1
	Secure Communication Protocols	1.0	3.0	2.0	3.0	3.0	2.0	2.0	2.0	2.5	1.0	2.8	1.3
	Cryptanalysis	0	0	0	0	0	1.0	1.0	1.0	1.0	0	0	1.3

CCN focus group on education

Carlos E. Budde
Ass. Prof. @ Università di Trento
CS4E: Cybersecurity Skills and Capability Building (WP6)

Establishing a European Education Ecosystem for Cybersecurity

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

Establishing an European Education Ecosystem for Cybersecurity

PROMOTING

Courses and trainings for professionals

- 80+ courses and trainings
- online/F2F/blended
- Industry specific or horizontal

CREATING

CONCORDIA workshop on Education for Cybersecurity professionals

Powered by

eit Digital

- methodology for course creation
- courses for Cybersecurity Consultant profile
- skills certification scheme

COLLABORATING

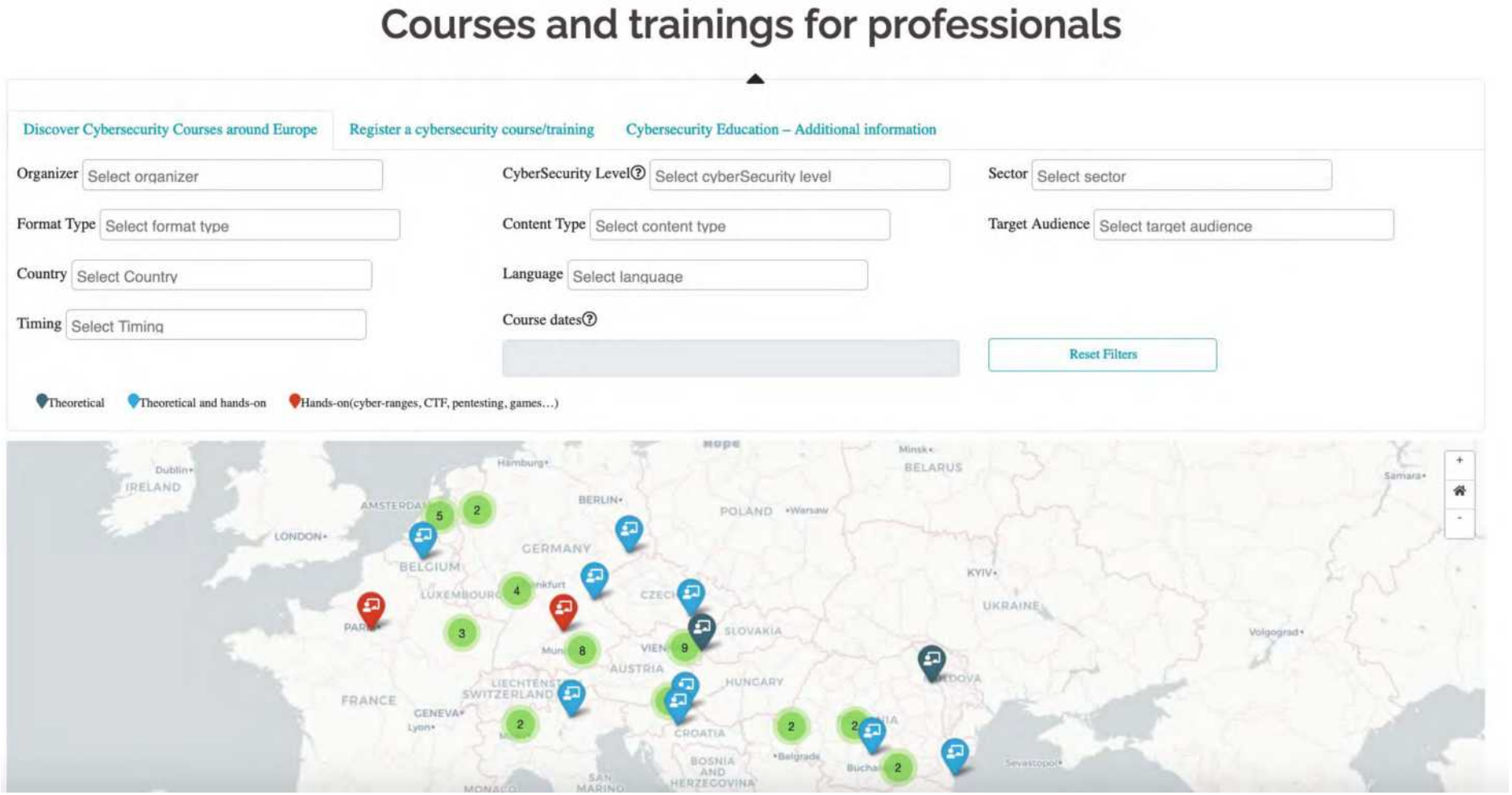
Cyber Competence Network

- 4 pilot projects
- 1 group on Education
- several topics
- regular events

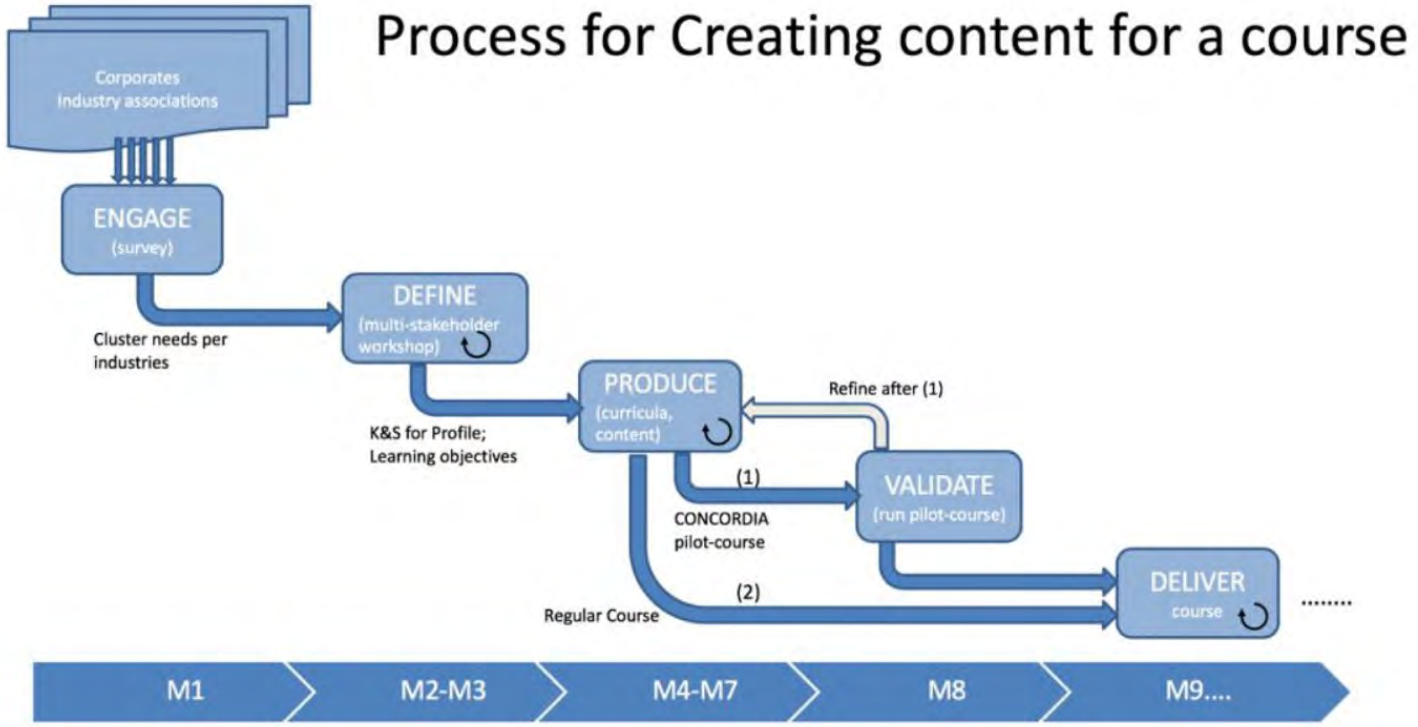
SHARING

- Engaging with the ecosystem (events)
- Sharing the findings (reports, news, blogposts)

Mapping courses for professionals

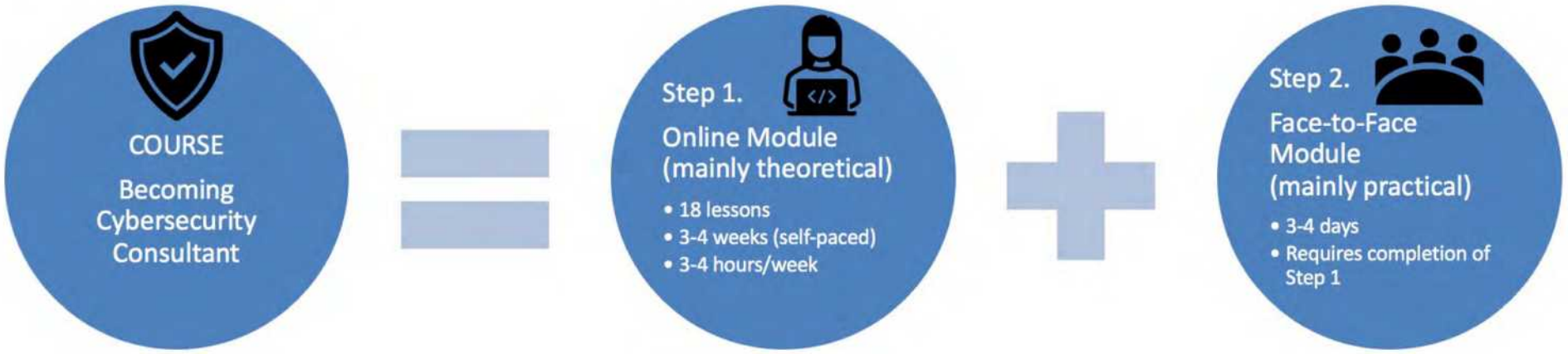


Methodology for creation & deployment of courses for cybersecurity professionals



- Understand your target audience
- Look into their needs
- The course content
- Choosing the lecturers
- Lesson design
- The delivery strategy
- Consider the evaluation strategy
- The importance of certification
- Looking into partnering

Organise Courses for cybersecurity professionals



Run Certification exams

Build a Cybersecurity Roadmap

Challenges (C) / Recommendations (R)	C1. The Skills gap is persisting	C2. Difficult to understand the trainings big picture	C3. Difficult to see the trainings offer big picture	C4. No EU Cybersecurity Skills Framework	C5. Heterogeneity of competencies related terminology	C6. Cyber-attacks threaten all industries	C7. Cybersecurity is not only about technology	C8. Different level of cybersecurity preparedness	C9. Lack of cybersecurity culture	C10. COVID-19 impacting the digital world
R1. Mapping: one single EU map for all offers of programs, courses, trainings										
R2. Terminology: setup and adopt a standard cyber Education related lexicon										
R3. Culture: improving the cyber-aware attitude at all levels										
R4. Target: expand the target audience of courses to non traditional categories										
R5. Course Content: industry specific, soft skills included, hands-on approach										
R6. Course Language: English as main language										
R7. Knowledge validation: from EU self assessment tool to Certification										
R8. European label for courses: endorsing courses based on specific criteria										
R9. Cybersecurity Insurance: considering the human factor										
R10. Cybersecurity Skills preparedness Radar										
R11. Increase Opportunities for Women in Cyber										

Recommendations	Initiating actors						Direct relevance level					Implementation time		
	EU insitutions	Member states	Companies	Course providers	Certification bodies	Insurance companies	EU level	Member states	Companies	Course providers	individuals	Short term	Medium term	Long term
R1 - Mapping: one single EU map for all offers of programs, courses, trainings														
R2 - Terminology: setup and adopt a standard cyber Education related lexicon														
R3 – Culture: improving the cyber-aware attitude at all levels														
R4 – Target: expand the target audience of courses to non traditional categories														
R5 – Course Content: industry specific, soft skills included, hands-on approach														
R6 – Course Language: English as main language														
R7 – Knowledge validation: from EU self assessment tool to Certification														
R8 - European label for courses: endorsing courses based on specific criteria														
R9 – Cybersecurity Insurance: considering the human factor														
R10 - Cybersecurity Skills preparedness Radar														
R11 - Increase Opportunities for Women in Cyber														

Contribute to building the ecosystem

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Home ▼ Downloads ▼ Workshops ▼ Events ▼ Publicity News Blog
Assets ▼

Observer Stakeholders Group (OSG)

Login

Register

Description

Organizations, such as standardization and certification bodies, have dedicated membership and schedule guidelines. However, their functionality is critical to the actual penetration of technology, regulations, and policies into the operational Cybersecurity ecosystems for industry and governments. Cognizant of the limits of external engagement with such bodies, the OSG is specially designed to interface (as a bi-directional "observe & coordinate") with the CONCORDIA ecosystem certification and standardization groups that are especially important for the EU Cybersecurity Act.

The envisaged "observe & coordinate" interaction of OSG and CONCORDIA will also form the basis for establishing the European Cybersecurity Certification Framework.

Get in touch!

https://www.concordia-h2020.eu/

contact@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.youtube.com/concordiah2020

ECS
EUROPEAN CYBER SECURITY ORGANISATION

WG5 Activities

Nina Olesen, Head of Sector

Convergence event
Brussels, 3 June 2022

About ECSO

ECSO was created in 2016 as the contractual counterpart to the European Commission for implementing Europe's unique Public-Private Partnership in Cybersecurity. Today, ECSO builds upon the many success of the Partnership and remain the privileged partner of the European Commission in supporting the establishment of the European Cybersecurity Competence Centre. It also positions itself as the obvious partner to the Competence Centre in driving the European Cybersecurity Community.

OUR GOAL: coordinate the development of the European Cybersecurity Ecosystem supporting the protection of European Digital Single Market, ultimately to contribute to the advancement of European digital sovereignty and strategic autonomy.

ECSO federates the European Cybersecurity public and private stakeholders including:

Large companies (user and provider)

SMEs & start-ups

Research centres, Universities

European, National and Regional clusters & association

Local, regional and national public administrations

Investors

End-users and operators of critical infrastructures and essential services

Our membership has grown from 132 members in June 2016 to more than 275 members across 29 countries in 2022, connecting more than 2000 organisations in Europe

Working Groups

WC1: STANDARDISATION, CERTIFICATION AND SUPPLY CHAIN MANAGEMENT

WC2: MARKET DEPLOYMENT, INVESTMENTS AND INTERNATIONAL COLLABORATION

WC3: CYBER RESILIENCE OF ECONOMY, INFRASTRUCTURE & SERVICES

WC4: SUPPORT TO SMES, COORDINATION WITH COUNTRIES AND REGIONS

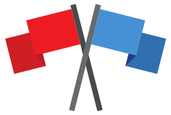
WC5: EDUCATION, TRAINING, AWARENESS, CYBER RANGES

WC6: SRIA AND CYBER SECURITY TECHNOLOGIES

WG5 - Education, training, awareness, cyber ranges, human factors

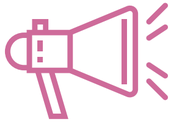
About

ESCO WG5 aims to contribute towards a cybersecurity capability and capacity-building effort for a cyber resilient next generation (NextGen) digital Europe, through increased education, professional training, skills development, as well as actions on awareness-raising, expertise-building and gender inclusiveness.



Cyber Ranges

Support education/training/HR



Raise awareness

Promote gender inclusion and attract more experts to the field

Educate the youth

Collaboration with the ECC Pilots

In 2019, ECSO collaborated with the Pilots on a survey to assess how organisations in Europe address competence development through simulations, exercises etc.
The aim was to understand how to deliver solutions better fitting the needs of European organisations in raising cyber resilience. The data for the 'Simulation-based Competence Development Study' was gathered through an online survey which took place from September to November 2019 and a report is available on the ECSO and CCN websites.

ECSO released a report on 'Understanding European Cybersecurity HR Recruitment Processes' in December 2021 based on a survey conducted from March to May 2021. The survey and report was also a collaboration between ECSO and the Pilots and aimed at highlighting the main issues facing the cybersecurity recruitment sector and gave recommendations as to how to better support the sector (i.e. through the development of a dedicated HR Cyber Toolkit and regular exchange with the HR community).

HR survey results

The overall purpose of the survey was to assess how organisations in Europe currently address the recruitment of cybersecurity specialists, given the well-known shortage of cybersecurity specialists in the EU and worldwide.

The data for the report was gathered through an online survey which took place from April until the end of May 2021.
The number of respondents amounted to forty-four (n=44), and their positions varied from employee to director from forty (40) different European organisations. The number of respondents was limited which naturally affects the representativeness and validity of results. Nevertheless, the responses provide an initial overview of the situation.

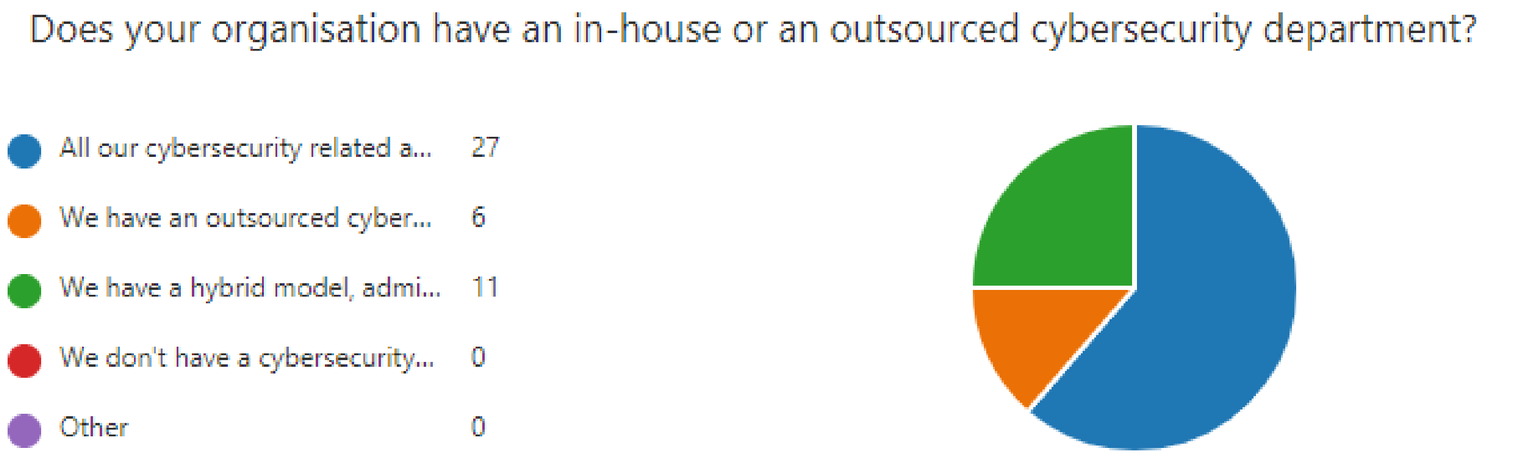
The organisations that the respondents represented were mainly medium to large size organisations (over 50 employees). 13 organisations with between 5 and 50 employees, 7 organisations between 50 to 250, and 24 organisations with more than 250 employees. No organisations with less than five employees who responded to the survey

HR survey: on recruitment processes

All respondents indicated that they have some type of dedicated cybersecurity team. 27 use an internal cybersecurity department, while others handle cybersecurity matters with an outsourced or hybrid model.

When it comes to recruitment, IT organisations tend to have inhouse cybersecurity recruitment teams more often than non-IT organisations

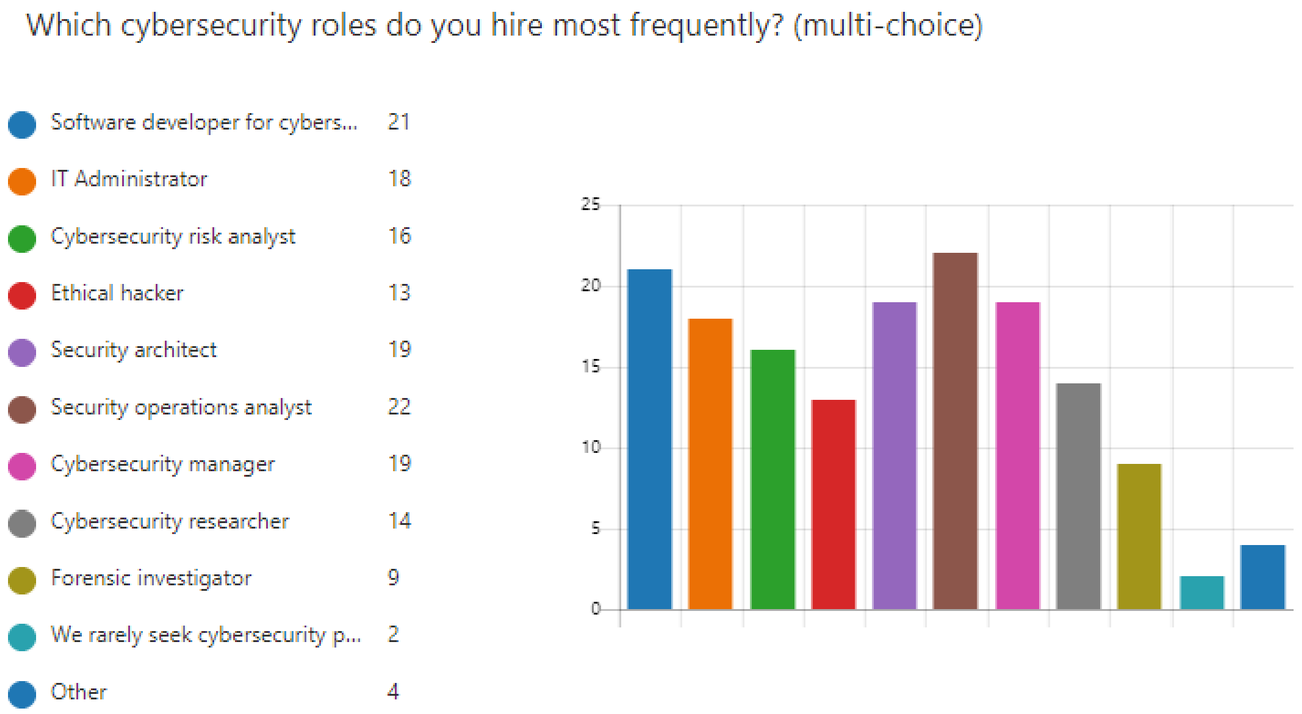
38 organisations have a dedicated recruitment department. Of the 6 respondents who indicated that they don't have a dedicated recruitment department, 3 of them manage recruitment matters directly in-house (by management), while 2 of them use a combination of recruitment agency plus some in-house research.



HR survey: on roles

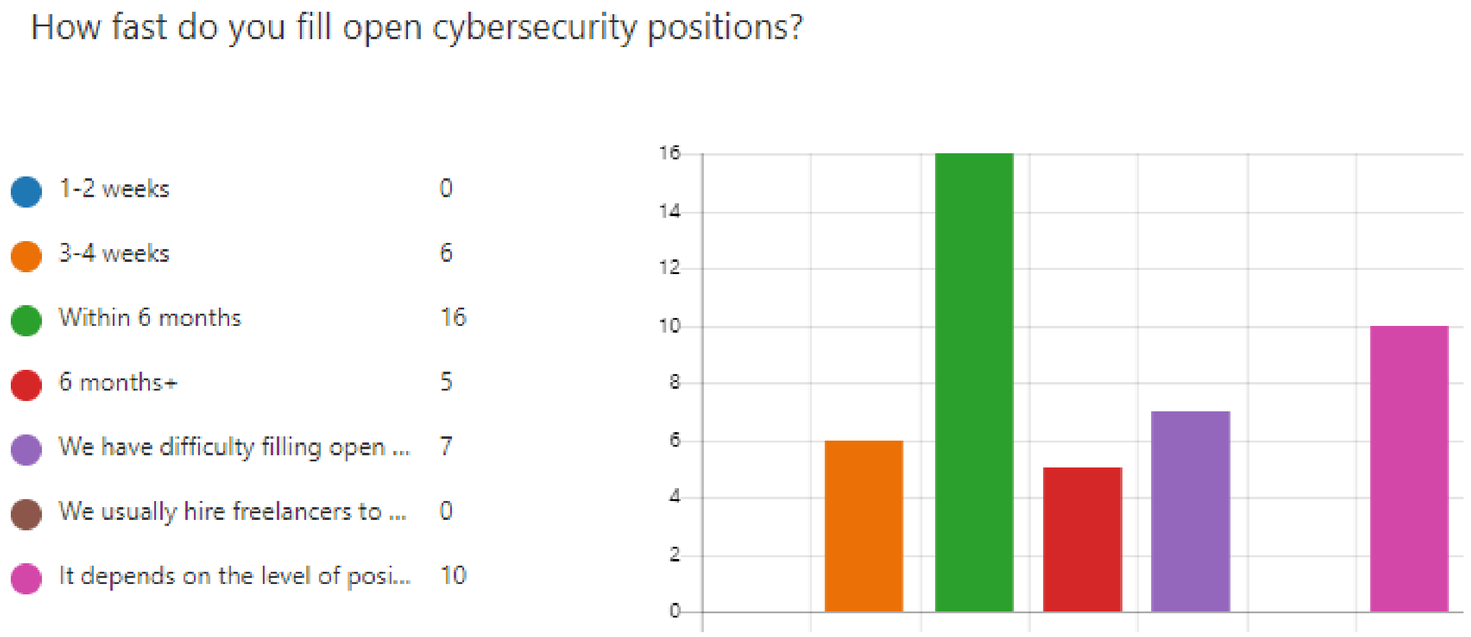
The most frequently hired role, as per the responses, is the Security operations analysts (22), immediately followed by Software developers for cybersecurity products/solutions (21). The survey also clearly lists a serious interest in Security architects (19) and Cybersecurity managers (19).

Lesser sought-after roles are Cybersecurity researcher (14) and Forensic investigator (9) while two organisations even responded that they rarely seek cybersecurity professionals.



HR survey: on filling cybersecurity positions

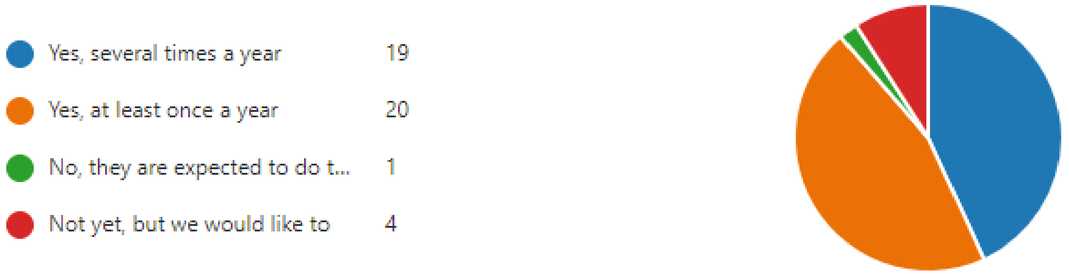
It is interesting to understand how much time, on average, these organisations need to fill their cybersecurity positions. While no one states that they are able to fill the positions in 1-2 weeks, the majority indicates up to 6 months for the recruitment process, which is considerably slower than in other knowledge domains. 7 respondents stated that they have difficulties with filling their cybersecurity positions.



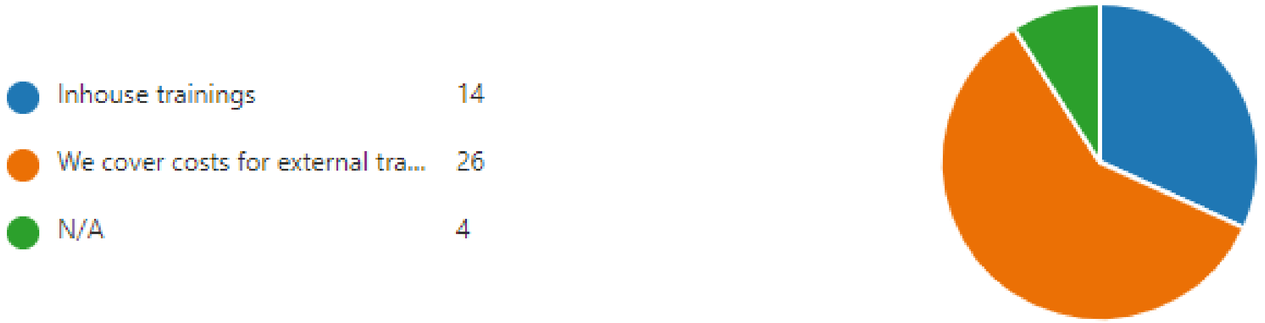
HR survey: on trainings

Organisations seem to be investing in the education of their cybersecurity professionals: 39 offer at least one (paid) training per year. Trainings are mainly provided via external organisations but 14 respondents indicated that they're delivered inhouse.

Do you offer trainings for your cybersecurity professionals? (business conference attendance doesn't count)



How do you offer trainings opportunities to your personnel?



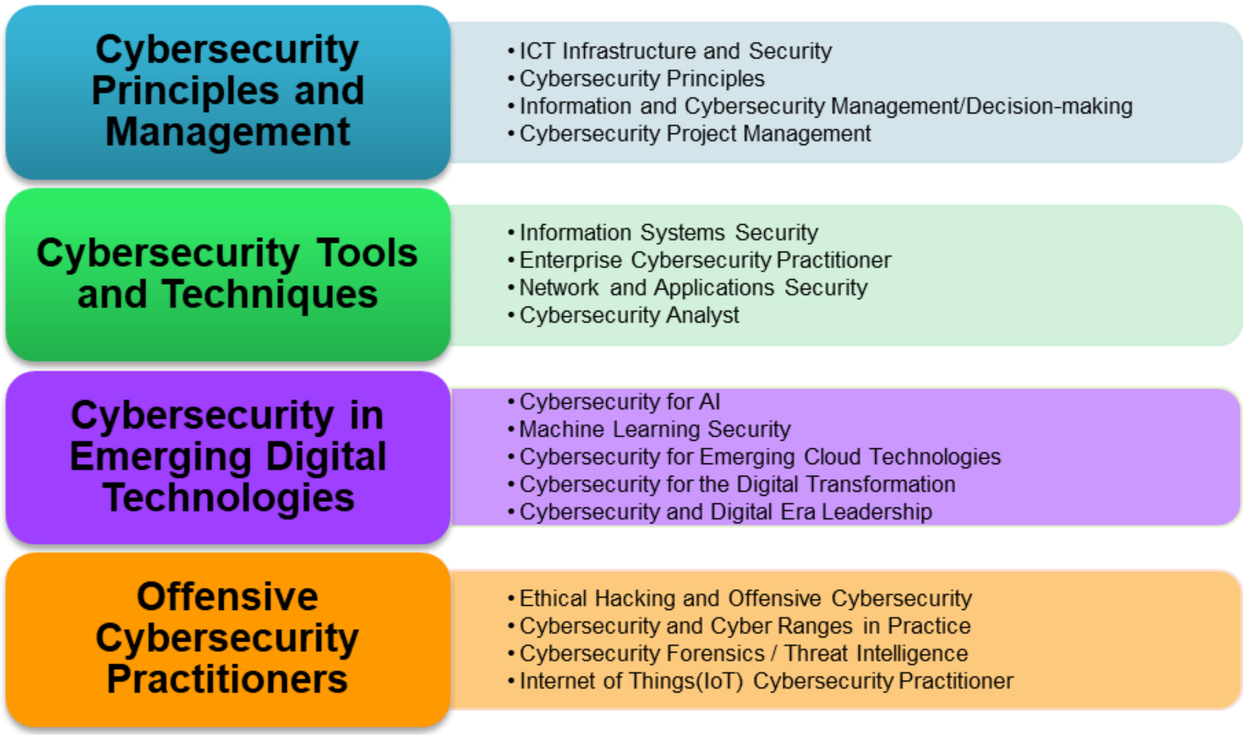
Minimum Reference Curriculum

ECSO released the first version of its Minimum Reference Curriculum (MRC) in November 2021.

The MRC is aimed at supporting practitioners and course designers with guidelines relative to the competence & skills development framework along with pedagogical methodologies for the higher education programme requirements (compatible with EQF and ECTS). The curriculum is organised in four main clusters and mapped to relevant certifications and career paths.

The MRC will be a living document, to be updated every 6 months according to feedback from ECSO members and the community, as well as the latest developments in the field.
It will also be mapped to the ENISA Cybersecurity Skills Framework once that is finalised.

Version 2 of the MRC was released in May 2022.



ENISA Ad Hoc WG – Developing a European Cybersecurity Skills Framework

ECSO is part of the ENISA Ad Hoc WG on Developing a European Cybersecurity Skills Framework (ECSF), helping to shape an overarching European-wide framework and provide a common taxonomy for cybersecurity job roles. ECSO is playing a strong role in the definition and integration of 'soft skills' across the framework.

The ECSF and its User Manual will be released in September 2022 and ENISA will organise the conference "Cybersecurity Skills - Building a Cybersecurity Workforce" in Athens on 20-21 September to culminate with the release. An open call for speakers has been launched by ENISA.

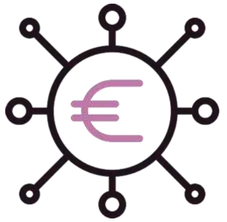
The ECSF complements existing activities of ECSO and the ECC Pilots, and ECSO intends to map its work, i.e. Minimum Reference Curriculum, to the framework and overall taxonomy.

Building the European Cybersecurity Education Ecosystem

Harmonise policies, approaches and taxonomies

Link existing communities & initiatives

Implement concrete actions for the benefit of the sector, in close collaborations with key stakeholders



Increase public and private funding on education & training

Collaborate closely with Member States/national public administrations

ECSO concrete actions on education / skills (for 2022 and beyond) include:

"Cybersecurity Education Made in Europe" label

European Cybersecurity Job Platform

WOMEN 4CYBER

Women4Cyber Academy

YOUTH 4CYBER

Education for youth

ECS
EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Organisation (ECSO)
29, Rue Ducale
1000 - Brussels
BELGIUM

nina.olesen@ecs-org.eu www.ecs-org.eu

@ecso

ECS
EUROPEAN CYBER SECURITY ORGANISATION

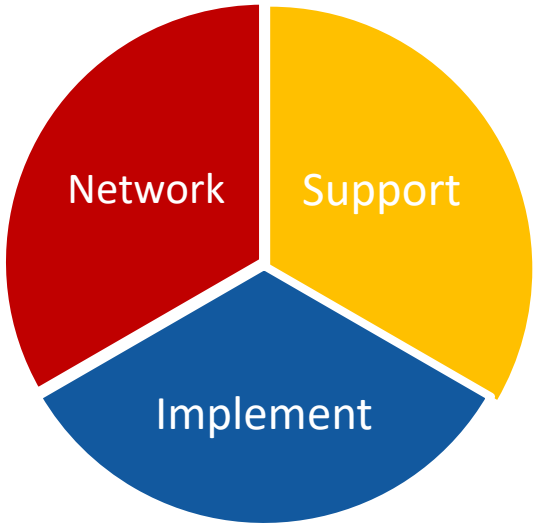
Building Europe's cybersecurity community

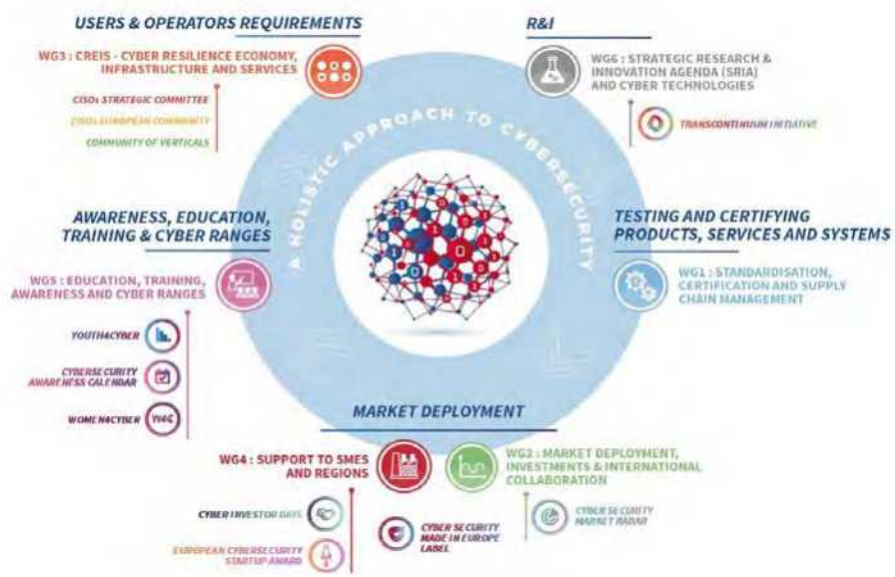
Roberto Cascella

03 June 2022
Convergence Next

ECSO's Vision

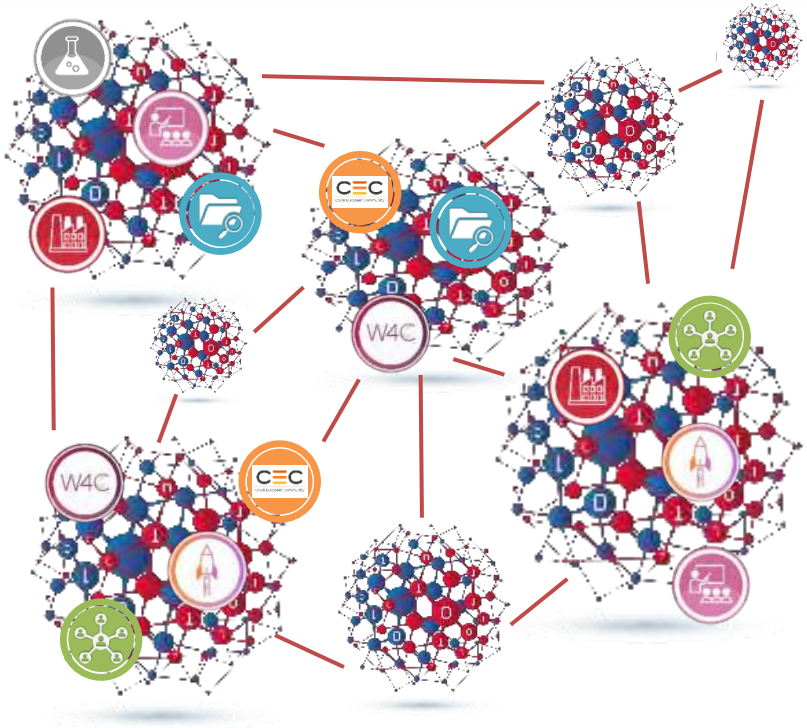
To achieve a Cyber resilient digital Europe and increase European Digital Sovereignty & Strategic Autonomy through the establishment of trusted & resilient supply chains for cybersecurity solutions and services.





EU cybersecurity ecosystems & communities – a partial view

Users of cybersecurity:
IT & operational focus



Communities → **Ecosystems**

European Cyber Security Organisation (ECSO)
29, Rue Ducale
1000 - Brussels
BELGIUM

secretariat@ecs-org.eu www.ecs-org.eu

@ecso

The future of the Cybersecurity Community in Europe

According to CyberSec4Europe

Cyber Security for Europe

- Our case-study: CHECK in Toulouse, France
  - [*CHECK = Community Hub of Expertise in Cybersecurity Knowledge = Grassroots / Bottom-up*]
  - Barriers aplenty
  - Opportunities abound
- Institute of Cybersecurity in Occitanie – ICO
  - It's a spill-over effect
  - 5-year project funded by the Occitanie Region
  - Hosted by the CNRS
- Revision of Regulation (ECCC & NNCC) – Recommendations:
  - Definition of "Community", or, better, of its perimeter, based on its required contributions
  - Framework / Structure for the "Community"
  - Dedicated funding channels

Afonso Ferreira – CNRS, France