ANNUAL WORKSHOP REPORT 2.

DELIVERABLE 5.11

Lead Author: UCSC

Contributors: Laurea, EOS
Deliverable classification: PUBLIC (PU)

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme, H2020-SU-SEC-2019, under grant agreement No. 883054

D5.11 ANNUAL WORKSHOP REPORT 2

Deliverable number	**5.11**	
Version:	**1.0**	
Delivery date:	**31/5/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Rachele Brancaleoni**	**UCSC**
Contributors:	**Sabina Magalini**	**UCSC**
	Päivi Mattila, Jari Räsänen, Tiina Haapanen	**Laurea**
	Vincent Perez de Leon-Huet	**EOS**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	10.05.2022	Rachele Brancaleoni, Sabina Magalini, UCSC	First draft
0.2	15.05.2022	Päivi Mattila, LAUREA	Review and text editing
0.3	16.05.2022	Vincent Perez de Leon-Huet, EOS	Review and text editing
0.4	17.05.2022	Jari Räsänen, Rachele Brancaleoni, UCSC	Review and text editing
0.5	19.05.2022	Tiina Haapanen, LAUREA	Review and text editing
0.7	20.05.2022	Pablo Hernandez, MALDITA	Review
0.8	31.05.2022	Tiina Haapanen, LAUREA	Text editing and final review
1.0	31.05.2022	Tiina Haapanen, LAUREA	Submission

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

TABLE OF CONTENTS

1. INTRODUCTION

The purpose of this report is to summarize EU-HYBNET (Pan-European Network to Counter Hybrid Threats) project's 2nd Annual Workshop's objectives and outcomes. Annual Workshops are designed to disseminate project findings for a large audience of stakeholders and to ensure vivid interaction with industry, academia and other providers of innovative solutions outside of the project consortium. Its purpose is to assess the feasibility of the project findings and possible recommendations to innovations uptake (incl. industrialisation) and standardisation.

Moreover, Annual Workshops will foster network activities, raise awareness of the project and bring together relevant practitioners and stakeholders who may join the EU-HYBNET network and its activities. Annual Workshops are part of Work Package number 5, *Communication, Dissemination and Exploitation Activities*.

The Catholic University of the Sacred Heart of Rome Italy (Università Cattolica del Sacro Cuore - UCSC) and Laurea organized the 2nd EU-HYBNET Annual Workshop on the 6th of April 2022. Due to the uncertain situation on epidemiological and political sides the event was held in a hybrid format. A total of 136 registered people from 60 organizations in 20 countries (including countries outside EU: Georgia, Kosovo, Turkey and UK). Participant organisations to the AW included 24 of the 25 project partners, and 5 NGOs, 17 SMEs, 22 Academia and research organizations and 16 practitioners. Most of the organization participated online, 23 in presence and 8 had delegates both in presence and online. Full list of organisations that were present are in Annex III.

This document is divided into five sections – they are:

Chapter 1: Provides introduction and describes the importance and content of this deliverable.

Chapter 2: Focuses on Annual Workshop objectives which explains the goals and objectives of the workshop, and how they are related to the project objectives.

Chapter 3: Describes Annual Workshop agenda and summarizes the main discussion points during the workshop. Moreover, the chapter highlights the importance of information shared and gained in the Annual Workshop.

Chapter 4: Introduces and summarizes feedback from the workshop participants collected during and after the event.

Chapter 5: Provides summary of the findings and their input and importance for future work of the project.

2. WORKSHOP OBJECTIVES

Objectives of Work Package 5, of which the Annual Workshops are part, are 1) to disseminate results and interact with other related networks; 2) to create conditions for better interaction with industry, research and academia; 3) to enrich the existing network against hybrid threats with academics, practitioners, stakeholders and industry actors across Europe. Annual Workshops work towards these Work Package objectives, which are grounded in the whole of the project's objectives. The key project objectives for the Annual Workshop are the following:

Project Objective 1: To *enrich the existing network countering hybrid threats and ensure long term sustainability*	As the event is public, the project partners could invite their networks to participate and learn about joining the EU-HYBNET network. To reach as wide audience as possible, the event was also advertised on social media channels and on platforms used by relevant stakeholders and other EU funded projects.
Project Objective 3: To *monitor developments in research and innovation activities as applied to hybrid threats*	A special effort was made to attract participants working with innovative solutions: ahead of the workshop, a call to present innovations was distributed publicly on project channels. Innovations were assessed by the innovation manager and task 3.1 lead. Moreover, the presented innovations were further assessed by the audience in the questionnaire that was sent afterwards.

The first of the project's objectives is *to enrich the existing network countering hybrid threats and ensure long term sustainability.* The Annual Workshop, in this realm, allows to identify potential new members for the network through the public event fostering interaction between participants and network members. To ensure a wide range of participants, the event was advertised on the EU-HYBNET website (www.euhybnet.eu), the project's social media channels (Twitter and LinkedIn) and via e-mail to EU-HYBNET consortium partners, stakeholder groups, network members, External Advisory Board members, innovation providers, industry, small and medium-sized enterprises, and non-governmental organizations. Partners and the project coordinator also disseminated the event through various platforms: CIRCABC, European Cluster Securing Critical Infrastuctures, CMINE, and with their contact lists of potential interested participants (e.g. Italian CBRN P3 cluster).

Moreover, a special effort was made to attract participants working with innovative solutions; ahead of the workshop, a call to present innovations was distributed publicly on project website, Twitter and LinkedIn, for any organisation or company that had an opportunity to send a suggestion for presenting their innovations to counter hybrid threats. As part of this dissemination effort, coordinators of relevant closed projects as well as known innovators were targeted and contacted through email. These innovations were assessed by the innovation manager and Task (T)3.1 "Definition of Target Areas for Improvement and Innovations" leader together with the Annual Workshop organizers. The most promising solutions were chosen for presentation. The presented innovations were further assessed by the audience through questionnaires shared during the meeting or sent afterwards. This way, the 2nd Annual Workshop also supported the project's goals to report for the European Commission in every six (6) months on the means and results *to monitor developments in research and innovation activities as applied to hybrid threats.*

Objectives to disseminate project results and to create conditions for better interaction were achieved by including in the agenda the results per work packages, and information on network membership, the networking platform and the Innovation Arena. The picture below highlights the importance of EU-HYBNET WP5 and the Annual Workshop to promote project's results and to support the project's key activities.

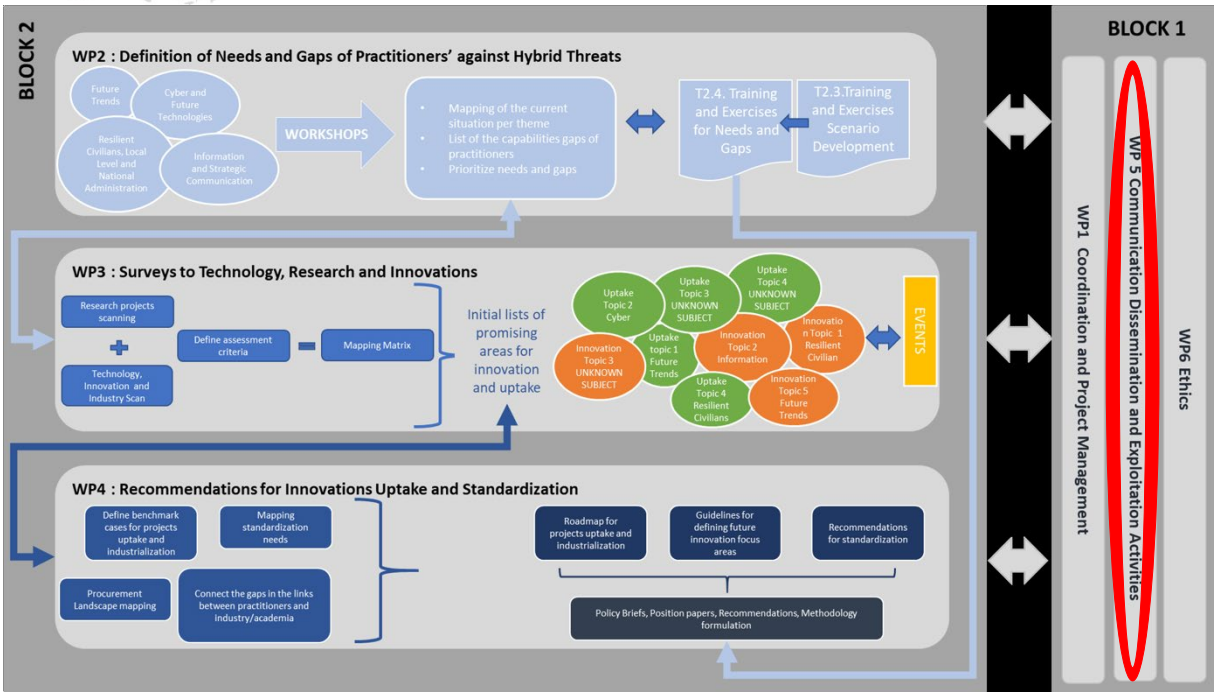


Figure 1: Structure work packages and main activities

Lastly, the importance of Annual workshop is highlighted by a fact that it stands for a yearly project milestone (MS). With the organisation of the second Annual Workshop in Rome, the following EU-HYBNET project milestone was achieved.

- MS 35 "Second Annual Workshop"

3. WORKSHOP AGENDA

The Annual Workshop (AW) consisted of four parts: the keynote speeches, work package presentations, innovation presentations, and the presentation of networking opportunities.

3.1 KEYNOTE SPEECHES

The keynote speeches were provided by high-level speakers from recognized institutions**: Mr. Giannis Skiadaresis**, *Thematic Coordinator for Infrastructure Resilience in Unit B4 – Innovation and Security Research at DG HOME in European Commission*; **Mr. Gregory Mounier**, *Head of Outreach at the European Cybercrime Centre (EC3) of Europol - the European Law Enforcement Agency*; and **Mr. Rasmus Hindrén**, *Head of International relations at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).*

Mr. Giannis Skiadaresis presented some insights on the role of innovation in responding to hybrid threats and the importance of critical infrastructure protection. Countering hybrid threats is one of the most complex challenges that EU and its member states are facing today, and it must embrace prevention as well as response and recovery. The Security Union strategy identifies the protection of critical infrastructures as one of the main priorities of the EU today and for the upcoming years. The critical entities resilience directive proposal (CER) is currently under trialog between the Parliament, Commission, and Council since January 2022; it covers natural and man-made non-cyber threats and will be complementary with NIS2 directive that covers cybersecurity aspects: these two legislations will provide a comprehensive framework for resilience against many dimensions of the hybrid threats. Mr. Skiadaresis underlined the importance of fostering the cooperation between different players in countering hybrid threats and subsequent large scale disruption and the Community of European Research and Innovation Security's (CERIS) role. Mr. Skiadaresis also highlighted the fact that the AW and the other events organized by EU-HYBNET are complementary to the activities carried out by EU to counter hybrid threats; moreover the focus that EU-HYBNET has reflects the cross-cutting priorities and the approach that the Commission suggests on future research on critical infrastructure.

Mr. Gregory Mounier presented the Innovation Lab from EUROPOL: in 2019 the Justice and Home Affairs Council defined that EUROPOL should act in the development and cooperation areas in the technological field. He shared the mission and objective of the Innovation Lab which is to provide a structure and a set of services that help LEAs avoid duplication and create synergies; the lab has 4 functions: observatory, network of innovators (including industry, researchers and practitioners), projects, and EU Innovation Hub. Activities carried out by the innovation lab include: Europol Tool Wiki, Europol Code Repository, and Europol Tool Repository (open only to LEAs). Mr. Mounier highlighted the possible way of collaboration with EU-HYBNET: sharing gaps, needs, knowledge products, collaboration in developing tools for LEAs and providing feedbacks from LEA's point of view.

Mr. Rasmus Hindrén focused his speech on two topics: the situation in Ukraine and lessons that we can initially draw, and vulnerabilities and responses specifically related to resilience of critical infrastructure. The level of hybridity of the Ukrainian situation including information, cyber, diplomatic, political, legal domains is really high, and individuals and groups especially from the Ukraine side are engaged in providing intelligence or carrying out cyber attacks. Cyber attacks against

Ukraine weren't successful, because Ukraine with the help of EU and NATO has improved the resilience of its cyber infrastructure. This represents a success story on how to build resilience against these types of attacks. Ensuring that infrastructures are resilient is a cross-cutting effort and we should start by identifying their key vulnerabilities: lack of reserves/stockpiles, longer delivery distances/global supply chain, reliability on IT systems in finance and logistics, more lean solutions, no control of public sector in critical infrastructures owned by private companies (especially in aviation or healthcare), transnational nature of hybrid threats. The combination of asymmetric techniques that adversaries have at their disposal with vulnerabilities in our critical infrastructure can easily show the real threat. Cooperation between public and private sector can be fostered by combining these three approaches in the right mix: expectation of rewards, fear of punishment, share importance of the matter. He also commented on the comprehensive framework presented by asking Mr. Skiadaresis to include defense as part of the approach.

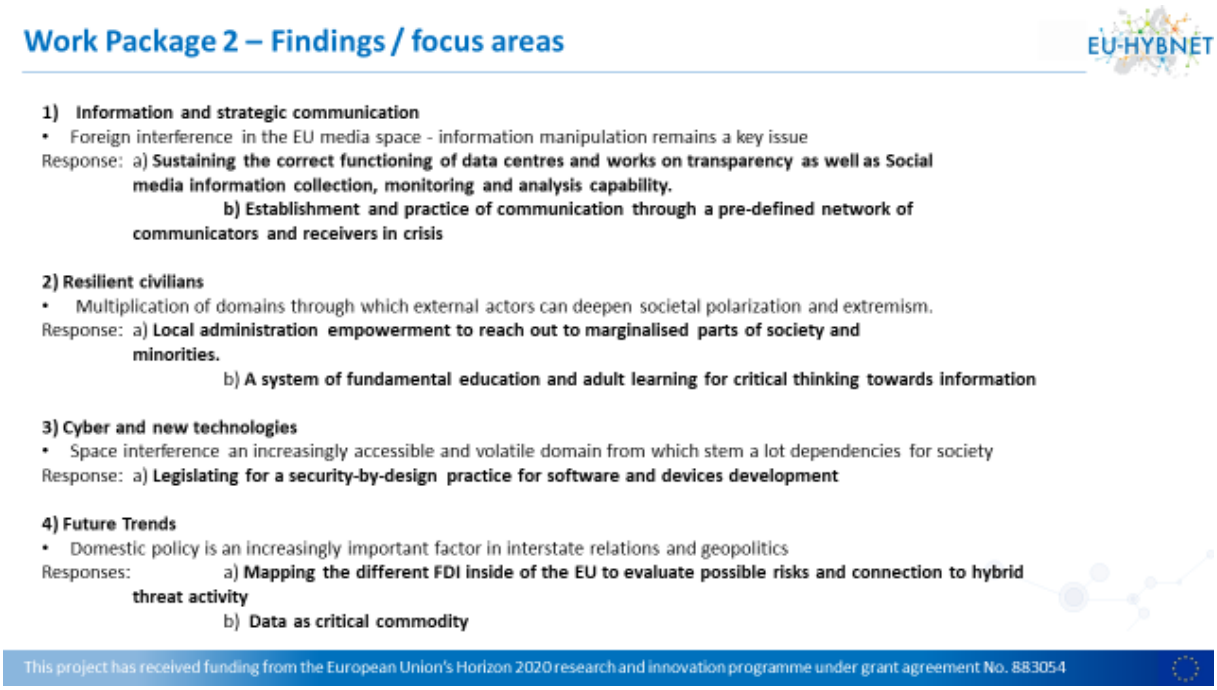
The keynote speeches provided a topical, high-level assessment on the ways to counter hybrid threats, and evoked discussion among the participants. Questions included projects and activities carried out by EUROPOL on deepfakes and manipulation of information; experiences of cooperation between LEAs and private companies on hybrid threats; applicability of the information sharing framework used in maritime activities to LEAs; building horizontal approach in EU research to support the visibility of hybrid threats; future activities to strengthen collaboration and transfer innovations between civil and defence sectors.

3.2 PROJECT RESULTS

Leaders of the EU-HYBNET Work Packages (WP) 2 "Gaps and Needs of European Actors against Hybrid Threats", WP3 "Surveys to Technology, Research and Innovations", and WP4 "Recommendations for Innovations Uptake and Standardization" provided a short overview on the most crucial project results that had been achieved in the project's second year.

Work Package 2 "Gaps and Needs of European Actors against Hybrid Threats"

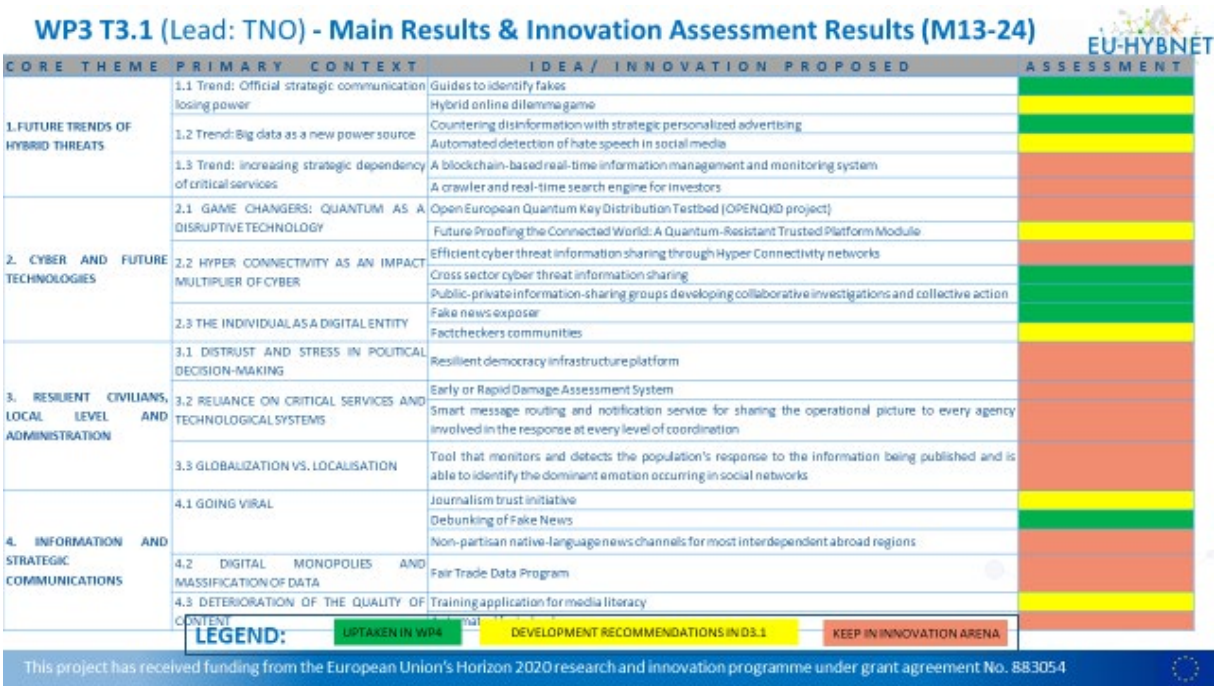
WP2 highlighted results achieved in identifying pan-European security practitioners' and other relevant actors' gaps and needs, vulnerabilities and threats to counter Hybrid Threats especially in T2.1 "Needs and Gaps Analysis in Knowledge and Performance" and in T2.2 "Research to Support Increase of Knowledge and Performance". Different threats and challenges have been identified and the threat base is very broad requiring a multidisciplinary approach. However, it was underlined that general understanding of Hybrid Threats has moved forward alike ways to recognize different activities, tools and phases as part of Hybrid Threats. An important aspect is that this recognition has defined a new way of looking at Hybrid Threats. The key focus areas and pan-European security practioners' gaps and needs, threats and vulnerabilities to counter Hybrid Threats from the second EU-HYBNET project cycle (October 2021 until March 2022) were presented as following:



In WP2, the work conducted in T2.3 "Training and Exercises Scenario Development" underlined importance of the EU-HYBNET training and exercise scenarios to provide frames for EU-HYBNET's identified promising innovations testing to EU-HYBNET's selected most critical pan-European actors' gaps and needs to counter Hybrid Threats. Morover, T2.4 "Training and Exercises for Needs and Gaps" which arranged the first EU-HYBNET training event and delivered training material for pan-European stakeholders to arrange similar trainings, described how to arrange the training and to get the access to the training material. Furthermore, importance to increase and to enhance skills to counter Hybrid Threats was well pointed out. It was also stressed that the importance of the first EU-HYBNET training event was to gain feedback from the training participants on the usability of the EU-HYBNET's identified promising innovations to counter hybrid threats.

WP3 "Surveys to Technology, Research and Innovations"

WP3 presented the results gained from T3.1 "Definition of Target Areas for Improvements and Innovations" by focusing first to a template that had been tailored for EU-HYBNET to collect and to assess innovations that are seen as possible solutions to the most critical gaps and needs to counter hybrid threats. The template played a key role in WP3 to define soundness of the solutions to the pan-European security practitioners and other relevant actors needs. Furthemore, WP3 described their results from the first project working cycle (May 2020 – September 2021) on twenty-three (23) identified promising innovations to counter Hybrid threats, and how the twenty-three (23) innovations were further analyzed in order to select nine (9) most promising innovations. The nine (9) most promising innovations are following:



WP3 T3.1 (Lead: TNO) **- Main Results & Innovation Assessment Results (M13-24)**

EU-HYBNET

CORE THEME	PRIMARY CONTEXT	IDEA / INNOVATION PROPOSED	ASSESSMENT
1. FUTURE TRENDS OF HYBRID THREATS	1.1 Trend: Official strategic communication losing power	Guides to identify fakes	
		Hybrid online dilemma game	
	1.2 Trend: Big data as a new power source	Countering disinformation with strategic personalized advertising	
		Automated detection of hate speech in social media	
	1.3 Trend: increasing strategic dependency of critical services	A blockchain-based real-time information management and monitoring system	
		A crawler and real-time search engine for investors	
2. CYBER AND FUTURE TECHNOLOGIES	2.1 GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY	Open European Quantum Key Distribution Testbed (OPENQKD project)	
		Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module	
	2.2 HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER	Efficient cyber threat information sharing through Hyper Connectivity networks	
		Cross sector cyber threat information sharing	
		Public-private information-sharing groups developing collaborative investigations and collective action	
	2.3 THE INDIVIDUAL AS A DIGITAL ENTITY	Fake news exposer	
		Factcheckers communities	
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1 DISTRUST AND STRESS IN POLITICAL DECISION-MAKING	Resilient democracy infrastructure platform	
	3.2 RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS	Early or Rapid Damage Assessment System	
		Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination	
	3.3 GLOBALIZATION VS. LOCALISATION	Tool that monitors and detects the population's response to the information being published and is able to identify the dominant emotion occurring in social networks	
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1 GOING VIRAL	Journalism trust initiative	
		Debunking of Fake News	
		Non-partisan native-language news channels for most interdependent abroad regions	
	4.2 DIGITAL MONOPOLIES AND MASSIFICATION OF DATA	Fair Trade Data Program	
	4.3 DETERIORATION OF THE QUALITY OF CONTENT	Training application for media literacy	

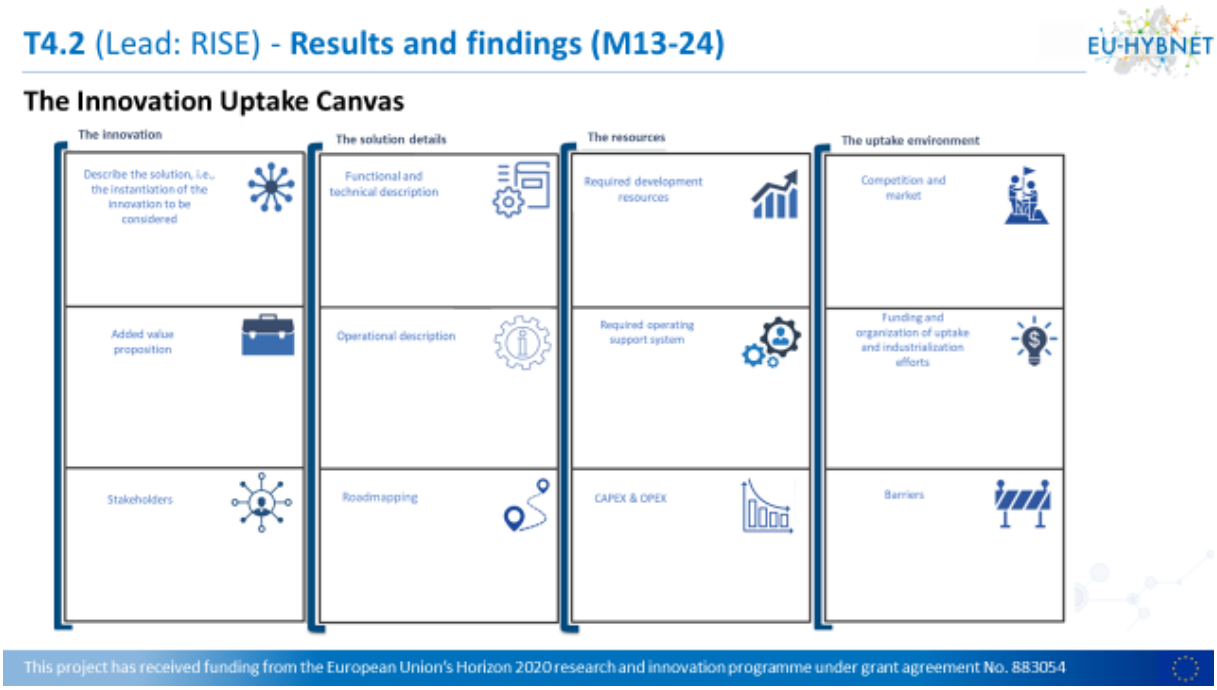
LEGEND: UPTAKEN IN WP4 | DEVELOPMENT RECOMMENDATIONS IN D3.1 | KEEP IN INNOVATION ARENA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

In addition, WP3 highlighted that the innovation mapping to the project's second working cycle's (October 2021 – March 2023) gaps and needs is now ongoing, and hence new results will be described in the next, 3rd EU-HYBNET Annual Workshop in April 2023. Lastly, it was reminded that the innovation mapping to the gaps and needs continues in the WP3 event, and hence Annual Workshop participants were warmly invited to join to the forthcoming EU-HYBNET event "The 2nd Innovation and Knowledge Exchange Workshop" that will be arranged in The Hague on June 14th 2022.

WP4 "Recommendations for Innovations Uptake and Standardization"

WP4 described first how T4.1"Mapping on the EU Procurement Landscape" had successfully identified success factors and barriers in the EU procurement landscape for innovation uptake, and in the future, the focus will be to solve the procurement landscape for non-technological innovations. In addition, T4.2 "Strategy for Innovation uptake and industrialization" explained how they had compiled an innovation uptake strategy and produced a set of recommendations for four (4) most promising innovations for an uptake. T4.2's main outcome included a creation of a detailed innovation uptake canvas to support promising innovations analysis and possible uptake process. The canvas includes 12 dedicated assessment slots to support the innovation uptake - the slots and the canvas is described in the picture below.



In WP4 T4.3 "Recommendations for Standardization" findings of standardization landscape for EU-HYBNET's most promising innovations were presented. In addition, Annual Workshop participants were invited to join the T4.3 "Innovation Standardization Workshop" on June 15th 2022 in Hague where the possibilities and challenges in the standardization landscape in the context hybrid threats wil be further investigated. Lastly, T4.4 "Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge" shortly presented its' three (3) published policy briefs and summarized their key content and focus.

3.3 INNOVATION PRESENTATIONS

As one of the EU-HYBNET Annual Workshop's (AW) goals was to focus on innovation uptake and recommendations, in the 2nd Annual workshop a session was dedicated to pitches of innovations and innovative solutions. A few months before the AW, EU-HYBNET announced the possibility for innovative solutions providers to suggest their innovation as a sound solution to counter hybrid threats. In the EU-HYBNET announcement "Call for Pitches" the areas where innovation pitches were desired were reflecting the EU-HYBNET project's 2nd cycle gaps and needs, threats to counter Hybrid Threats. This call resulted to seven (7) pitches that were presented in the 2nd Annual Workshop. The pitches were given by following organization on following innovations or innovative solutions, and some of the innovations had EC project funding background.

1. Research Driven Solution Limited: Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes, by Mr. Lorcan Connolly
2. HENSOLDT: HENSOLDT Analytics OSINT System, by Ms. Victoria Torisier
3. European Risk & Resilience Institute: Resilience Tool incl. Risk Radar, by Dr. Somik Chakravarty
4. HybridCore: Smart Navigator, by Mr. Hasan Suzen

5. Austrian Institute of Technology GMBH: Defalsif-AI Forensics Platform, by Mr. Martin Boyer
6. European External Action Service, Strategic Communication division: Disinformation Data Space, by Mr. Daniel Fritz

As already mentioned in the EU-HYBNET Deliverable 1.5 "Fourth Six Month Action Report" (April 2022) in the context of Annual Workshop, all the presented pitches on innovative solutions were providing tangible solutions to the EU-HYBNET's identified present pan-European security practitioners' and other relevant actors' gaps and needs to counter Hybrid Threats and especially in the following areas:

- critical infrastructure protection
- disinformation; information manipulation and interference
- crises management

It was also noted that even though some innovations were focusing on the same field and similar challenges, the solutions still varied and complemented each other. Partly, this also derived from their different Technical Readiness Level; this however provided more room for discussion on future development needs of the most promising innovations to counter certain Hybrid Threats challenges. Most of the discussions for this session took place during coffee breaks and social dinner due to a shortage of time. The workshop participants were also asked to assess the innovations via questionnaire during and after the Annual Workshop event. The innovation assessment results, excluding the one from EEAS that wasn't assessed, are described in ANNEX IV.

Presenting and assessing innovations is especially important to the EU-HYBNET because it's goal is to encourage the private sector to participate in the EU-HYBNET project, and involvement of the industry and SME is essential to define the most up to date tools and methods to counter hybrid threats.

3.4 NETWORKING OPPORTUNITIES

Four relevant European Commission funded security projects were invited to participate to the 2nd EU-HYBNET Annual Workshop and present innovations from their projects, because they all may deliver sound solutions to the present pan-European gaps and needs, threats to counter Hybrid Threats. Next to the four invited projects, the list below highlights which EU-HYBNET's identified critical gaps and needs and threats the project may deliver important solutions and research.

- **ALIGNER**/ Artificial Intelligence Roadmap for Policing and Law Enforcement
  - Connection to EU-HYBNET's identified Hybrid Threat area: *Digital escalation and AI-based exploitation*
  - *Grant agreement 101020574, https://aligner-h2020.eu/*

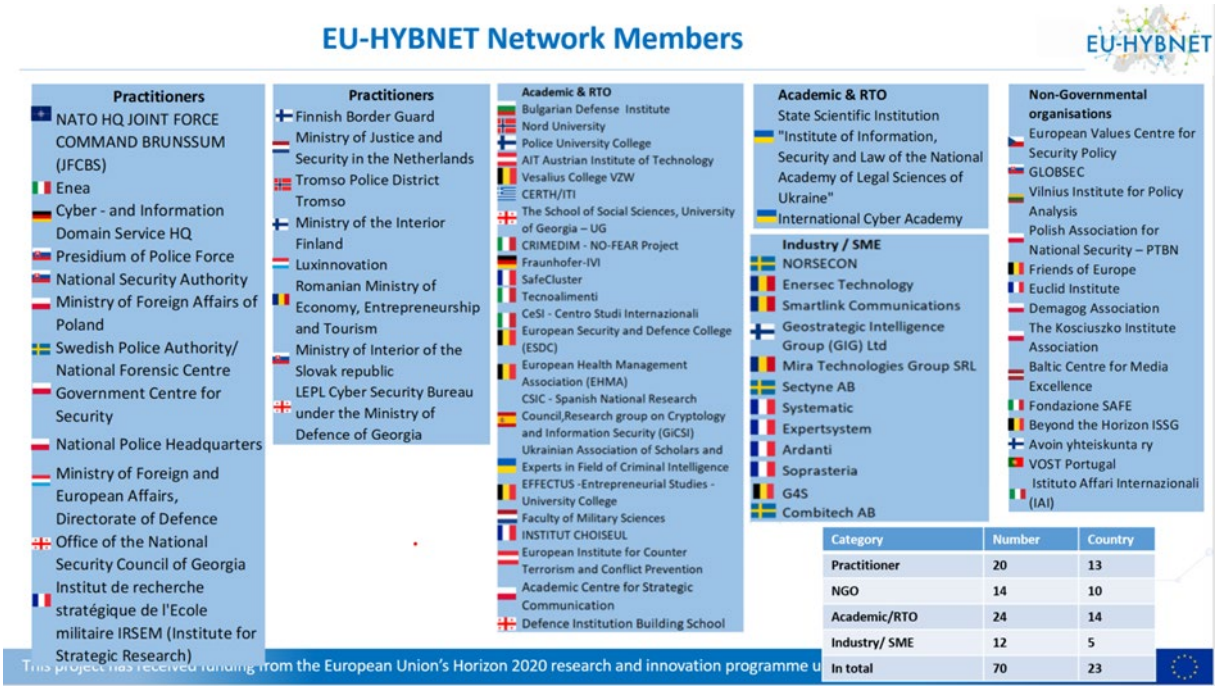
- **7SHIELD**/ Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats
  - Connection to EU-HYBNET's identified Hybrid Threat area: *Space interference and counterspace weapons*
  - *Grant agreement 883284, https://www.7shield.eu/*

- **PRECINCT**/ Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection
  - Connection to EU-HYBNET's identified Hybrid Threat area: *Exploitation of critical infrastructure weaknesses and economic dependencies*
  - *Grant agreement 101021668*, https://www.precinct.info/

- **MEDEA**/ Mediterranean practitioners' network capacity building for effective response to emerging security challenges
  - Connection to EU-HYBNET's identified Hybrid Threat area: *migration and e.g. in the context of information manipulation with the aim of destabilization*
  - *Grant agreement 787111*, https://www.medea-project.eu/

These named four project presentations and their solutions are in similar way important as the innovation pitches to the EU-HYBNET to proceed in the analysis **of research and innovation projects with a view to recommending the uptake or the industrialisation of results**. In addition, the cooperation with other Commission funded projects is highly important for the EU-HYBNET in order to increase the knowledge of EU-HYBNET results and to establish cooperation with other relevant pan-European networks and stakeholders. This activity is also supporting the EU-HYBNET's own network building initiative. Participants were asked to assess the projects too, results from ALIGNER, 7SHIELD and PRECINCT can be found in ANNEX IV, while MEDEA was not assessed.

Therefore, after the four invited projects' presentations Mr. Jari Räsänen, EU-HYBNET Network Manager at Laurea delivered a presentation on network extension, criteria for new members, and the process of applying for EU-HYBNET network membership. The networking opportunities section of the workshop provided potential new members with the basic information they would need in order to become active members. At the moment of the Annual Workshop, April 2022, EU-HYBNET Network included 70 members representing following organizations from 23 different countries.


EU-HYBNET Network Members
EU-HYBNET
Practitioners
NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)
Enea
Cyber - and Information Domain Service HQ
Presidium of Police Force
National Security Authority
Ministry of Foreign Affairs of Poland
Swedish Police Authority/ National Forensic Centre
Government Centre for Security
National Police Headquarters
Ministry of Foreign and European Affairs, Directorate of Defence
Office of the National Security Council of Georgia
Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)
Practitioners
Finnish Border Guard
Ministry of Justice and Security in the Netherlands
Tromso Police District Tromso
Ministry of the Interior Finland
Luxinnovation
Romanian Ministry of Economy, Entrepreneurship and Tourism
Ministry of Interior of the Slovak republic
LEPL Cyber Security Bureau under the Ministry of Defence of Georgia
Academic & RTO
Bulgarian Defense Institute
Nord University
Police University College
AIT Austrian Institute of Technology
Vesalius College VZW
CERTH/ITI
The School of Social Sciences, University of Georgia – UG
CRIMEDIM - NO-FEAR Project
Fraunhofer-IVI
SafeCluster
Tecnoalimenti
CeSI - Centro Studi Internazionali
European Security and Defence College (ESDC)
European Health Management Association (EHMA)
CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)
Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence
EFFECTUS -Entrepreneurial Studies - University College
Faculty of Military Sciences
INSTITUT CHOISEUL
European Institute for Counter Terrorism and Conflict Prevention
Academic Centre for Strategic Communication
Defence Institution Building School
Academic & RTO
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
International Cyber Academy
Industry / SME
NORSECON
Enersec Technology
Smartlink Communications
Geostrategic Intelligence Group (GIG) Ltd
Mira Technologies Group SRL
Sectyne AB
Systematic
Expertsystem
Ardanti
Soprasteria
G4S
Combitech AB
Non-Governmental organisations
European Values Centre for Security Policy
GLOBSEC
Vilnius Institute for Policy Analysis
Polish Association for National Security – PTBN
Friends of Europe
Euclid Institute
Demagog Association
The Kosciuszko Institute Association
Baltic Centre for Media Excellence
Fondazione SAFE
Beyond the Horizon ISSG
Avoin yhteiskunta ry
VOST Portugal
Istituto Affari Internazionali (IAI)
Category | Number | Country
Practitioner | 20 | 13
NGO | 14 | 10
Academic/RTO | 24 | 14
Industry/ SME | 12 | 5
In total | 70 | 23
from the European Union's Horizon 2020 research and innovation programme u

4. FEEDBACK

Out of 136 registered people, 12 responded to the feedback questionnaire that was shown before the closure of the event and sent via mail few days after it. Participants were satisfied with the event and with its topic (average rating 4.58/5). Participants generally considered the event worthy of their time, with no difference between those who attended in presence and online.

They assigned a very high rating to the organization of the event (average rating 4.75/5), and to the helpfulness of the staff (average rating 9.67 out of 10). This is impressing, especially considering that the event took place in an hybrid mode with attendees and speakers both online and in presence.

The selection of the speakers was considered good with an average rating of 4.33 on 5.

Examples of positive feedback:

I liked very much pitches: there was too little time to discuss them but it was good to have such a broad overview of pitches countering hybrid threats

The keynote speeches were interesting and different one from the other!

Other positive feedbacks concerned the open discussion and the thematic sessions.

Criticism was directed towards the thight agenda and the short time for discussion.

Examples of feedback:

I thik that there were too many pitches and I got a bit confused with so much information about very different projects in so little time

The presentations as they were too short and rushed, I felt we had too little time for discussion. Presentation of the speakers were too long: few sentences would be enough

We also asked to our participant the likelihood that they will participate in another event organized by EU-HYBNET.

Somewhat likely	2
Somewhat unlikely	0
Very unlikely	0
Very likely	10

5. CONCLUSION AND FUTURE WORK

Overall, the Annual Workshop achieved its goals to disseminate project findings for a large and multidisciplinary audience of stakeholders and to ensure vivid interaction with industry, academia and other providers of innovative solutions outside of the project consortium.

The Annual Workshop's organization in a Faculty of Medicine futher widened the audience encouraging the participation of students and university professors which were lead to examine the effect of hybrid threats also on the healthcare sector feeding on the ongoing COVID pandemic with all it's healthcare and non-healthcare consequences. The recent war in Ukraine was mentioned during the discussions and the some analysis of the Hybrid Threats previous to it's outburst and also ongoing were discussed. Participants proactively participated in discussions that involved also other types of input.

Based on feedback, the most valuable and inspiring content for participants were the keynote speeches and innovation presentations. The feedback of the Annual Workshop participants is highly valuable for the EU-HYBNET project in order to arrange an insightful Third EU-HYBNET Annual Worshop in 2023. The next, Third Annual Workshop, will take place on April 2023 and will be arranged by The "Mihai Viteazul" National Intelligence Academy in Romania.

ANNEX I. LIST OF ACRONYMS

ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement –project; funded by the European Commission, Grant agreement 101020574
AW	Annual Workshop
CBRN P3	Chemical Biological Radiological Nuclear Prepare Prevent Protect
CER	Proposal for a Directive on Critical Entities Resilience
CERIS	The Community of European Research and Innovation Security in DG HOME
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens.
CMINE	Crisis Management Innovation Network Europe
D	Deliverable
DG HOME	Directorate-General for Migration and Home Affairs
EOS	European Organization for Security
EU	European Union
EU-HYBNET	Empowering a pan-European Network to Counter Hybrid Threats –project; funded by the European Commission, Grant Agreement number 883054
EUROPOL	European Law Enforcement Agency
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
LAUREA	Laurea University of Applied Sciences
LEA	Law Enforcement Agency
MS	Milestone
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges –project; funded by the European Commission, Grant Agreement number 787111
NATO	North-Atlantic Treaty Organization
NGO	Non-Governmental Organization
NIS-2	Proposal for a revised Network and Information Systems Directive (NIS2)
PRECINCT	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection; funded by the Europen Commission, Grant Agreement number 101021668,
SME	Small and Medium Enterprise
T	Task
TRL	Technical Readiness Level
UCSC	Università Cattolica del Sacro Cuore
WP	Work Package

7SHIELD Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats; funded by the Europen Commission, Grant Agreement number 883284

ANNEX II. WORKSHOP AGENDA

2nd EU-HYBNET Annual Workshop:

Wednesday 06 April 2022 | 09.00 a.m. – 02.30 p.m. CEST
In presence at UCSC (Meeting room 5)
On line via Zoom call

Time CEST	Topic	Speakers
Welcome and registration		
8.30-9.00	Registration and Welcome	Senior Surgeon, Dr. Sabina Magalini/ Universita Cattolica Sacro Cuore
9.00-9.10	Keynote Speech *"The role of Research and Innovation in responding to hybrid threats"*	Policy Officer, Mr. Giannis Skiadaresis/ DG HOME
9.10-9.20	Keynote Speech "*Innovations to foster pan-European security practitioners' response to hybrid threats*"	Head of Team, Mr. Gregory Mounier/ EUROPOL, Innovation Lab
9.20-9.30	*Keynote Speech "Hybrid threats and critical infrastructure protection"*	Head of International relations, Mr. Rasmus Hindrén/ The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)
9.30-9.50	*Questions and discussion*	
EU-HYBNET's latest findings and results		
9.50-10.00	EU-HYBNET presents pan-European gaps and needs to counter hybrid threats	Senior Analyst, Mr. Maxime Lebrun/ Hybrid CoE
10.00-10.15	Innovations to counter hybrid threats	Senior Research & Innovation Manager, Dr. Souzanna Sofou/ Satways, Scientist, Mr. Okke Geurt Lucassen/ TNO
10.15-10.25	Innovation uptake and standardization activities	Research Associate, Alexios Koniaris/ KEMEA
10.25-10.40	*Questions and discussion*	
10.40-11.00	Leg stretch break	
Pitches - Innovation and ideas to counter hybrid threats by organizations and projects		
11.00-11.10	*Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes*	Mr. Lorcan Connolly/ Research Driven Solutions Limited
11.10-11.20	*HENSOLDT Analytics OSINT System*	Ms Victoria Toriser/ HENSOLDT
11.20-11.30	*Resilience Tool incl. Risk Radar*	Dr Somik Chakravarty/ European Risk & Resilience Institute
11.30-11.40	*Smart Navigator*	Mr. Hasan Suzen/HybridCore
11.40-11.50	*NORDLAB Concept*	Prof. Odd-Jarl Borch/ NORD University
11.50-12.00	*Defalsif-AI Forensics Platform*	Mr. Martin Boyer/ Austrian Institute of Technology GMBH

12.00-12.10	*Disinformation Data Space*	Mr. Daniel Fritz/ European External Action Service, Strategic Communication division
12.10-12.15	*Questions and discussion* Moderator: EU-HYBNET Innovation Manager Isto Mattila/ Laurea	
12.15-13.00	**Lunch Break**	
	EU-HYBNET Network activities and Innovations from other projects	
13.00-13.10	Artificial Intelligence Roadmap for Policing and Law Enforcement (ALIGNER) -project	Mr. Kai Pervölz/ Fraunhofer-IAIS
13.10-13.20	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats (7SHIELDS) -project	The Coordinator Gabriele Giunta/ Engineering
13.20-13.30	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection (PRECINCT) -project	Mr. Stefan Schauer/ Austrian Institute of Technology GMBH
13.30-13.40	Mediterranean practitioners' network capacity building for effective response to emerging security challenges (MEDEA) –project	The Coordinator George Kokkinis/ Centre for Security Studies KEMEA
13.40-13.50	EU-HYBNET Network today and core activities	EU-HYBNET Network Manager Jari Räsänen/ Laurea
13.50-14.10	*Questions and discussion* Moderator: Senior Surgeon, Dr. Sabina Magalini/ Universita Cattolica Sacro Cuore	
14.10-14.30	Closing remarks and wrap-up	Senior Surgeon, Dr. Sabina Magalini/ Universita Cattolica Sacro Cuore EU-HYBNET Coordinator Päivi Mattila/ Laurea

ANNEX III. LIST OF REGISTERED PARTICIPANTS AND ORGANISATIONS AND COUNTRIES

Organisation	**Country**	**Type of Actor**	**In presence/Online**
The Kosciuszko Institute Association	Poland	NGO	Online
Smartlink	Romania	SME/Industry	In presence
TNO	Netherlands	Academic/Research and Training Organization	Online
Cyber Security Bureau of the Ministry of Defence	Georgia	Practitioner (Government, local or national)	Online
Beyond the Horizon ISSG	Belgium	Academic/Research and Training Organization	Online
Academic Centre for Strategic Communication	Poland	Academic/Research and Training Organization	In presence
Research Institutes of Sweden	Sweden	Academic/Research and Training Organization	Online
Satways	Greece	SME/Industry	Online and In presence
Polish Association for National Security – PTBN	Poland	NGO	Online
Swedish Civil Contingencies Agency (MSB)	Sweden	Practitioner (Government, local or national)	Online
Laurea UAS	Finland	Academic/Research and Training Organization	In presence and Online
RINA Consulting - Centro Sviluppo Materiali SpA	Italy	SME/Industry	Online
Arescosmo SPA	EU	SME/Industry	In presence
Combitech AB	EU	SME/Industry	Online
NorseconAB	Sweden	SME/Industry	Online
DG ECHO	EU	Practitioner (Government, local or national)	Online
Erasmus Network "I Mediterranei	Italy	Academic/Research and Training Organization	Online
AIT Austrian Institute of Technology GmbH	Austria	Academic/Research and Training Organization	In presence
European Security and Defence College	EU	Academic/Research and Training Organization	In presence
Software Imagination & Vision (SIMAVI)	Romania	SME/Industry	Online
Research Driven Solutions Ltd.	Ireland	SME/Industry	Online
Quo vadis Europe	EU	Academic/Research and Training Organization	In presence

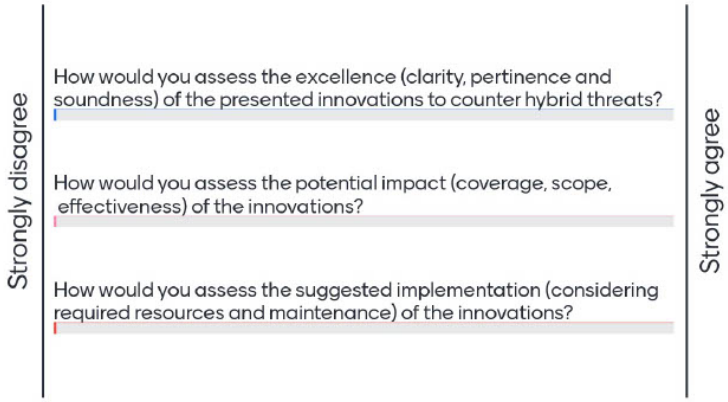
KEMEA	Greece	Academic/Research and Training Organization	Online and in presence
Europol	EU	Practitioner (Government, local or national)	In presence and online
European Commission	EU	Practitioner (Government, local or national)	In presence
Hybrid COE	Finland	Practitioner (Government, local or national)	Online
Engineering ingegneria informatica spa	Italy	SME/Industry	Online
German Council on Foreign Relations	Germany	Academic/Research and Training Organization	In presence
Fraunhofer IAIS	Germany	Academic/Research and Training Organization	Online
L3CE	Greece	Academic/Research and Training Organization	Online and In presence
HENSOLDT Analytics	Austria	SME/Industry	In presence
Hybrid Core	Belgium	SME/Industry	In presence
EEAS	EU	Practitioner (Government, local or national)	In presence
Steinbeis EU-VRi GmbH	Germany	SME/Industry	Online
DG-DEFIS	EU	Practitioner (Government, local or national)	In presence
Public University	Kosovo	Academic/Research and Training Organization	Online
VOST Portugal	Portugal	NGO	In presence
Fortinet	Belgium	SME/Industry	Online
EC-JRC	EU	Academic/Research and Training Organization	Online
Dataminr UK	UK	SME/Industry	Online
Serco	Italy	SME/Industry	Online
CS-GROUP	France	SME/Industry	Online
European Institute for Counter Terrorism and Conflict Prevention	Austria	Academic/Research and Training Organization	Online
Joint Research Centre - European Commission	EU	Academic/Research and Training Organization	In presence
The Ministry of Ecological and Solidarity Transition	France	Practitioner (Government, local or national)	In presence

Polish Platform for Homeland Security	Poland	NGO	In presence
National Intelligence Academy Mihan Viteazul	Romania	Academic/Research and Training Organization	Online
The European Organisation for Security	Belgium	SME/Industry	Online and In presence
Directorate for Civil Protection	Norway	Practitioner (Government, local or national)	In presence
Universidad Rey Juan Carlos	Spain	Academic/Research and Training Organization	Online
Bundeswehr University Munich	Germany	Academic/Research and Training Organization	Online and In presence
UCSC – Università Cattolica del Sacro Cuore	Italy	Academic/Research and Training Organization	In presence
PLV - Valencia Local Police	Spain	Practitioner (Government, local or national)	In presence
Centre for Peace Studies	Norway	Academic/Research and Training Organization	In presence
Ministry of Defence	Turkey	Practitioner (Government, local or national)	In presence
The International Centre for Defence and Security	Estonia	Practitioner (Government, local or national)	In presence
The Internal Security Agency	Poland	Practitioner (Government, local or national)	In presence
Maldita	Spain	NGO	In presence
Central Office for Information Technology in the Security Sector	Germany	Practitioner (Government, local or national)	Online
Estonian Information System Authority	Estonia	Practitioner (Government, local or national)	Online

ANNEX IV. INNOVATION ASSESSMENT RESULTS

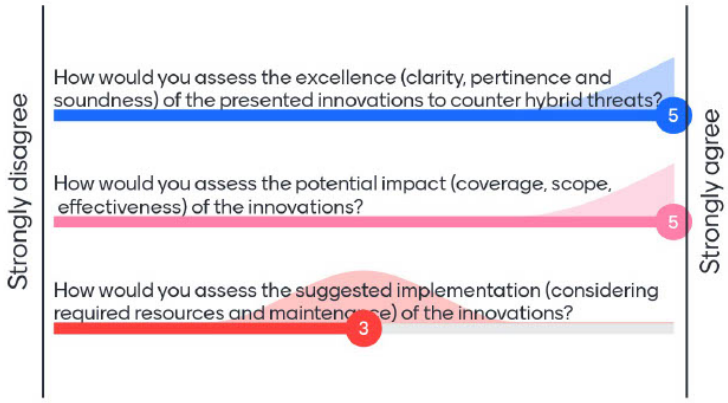
Please let us know your thoughts on the FIMI Data Space Innovation

Mentimeter



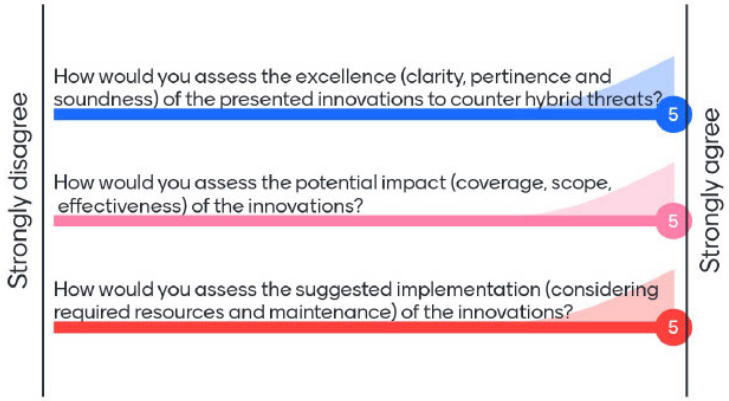
Please let us know your thoughts on the PRECINCT innovation!

Mentimeter



Please let us know your thoughts on the 7SHIELDS innovation!

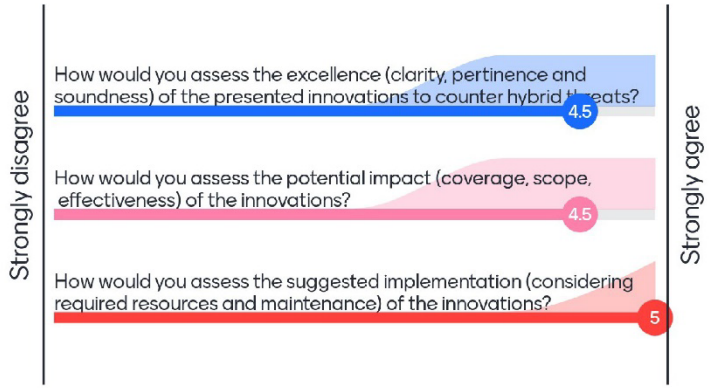
Mentimeter



1

Please let us know your thoughts on the ALIGNER innovation!

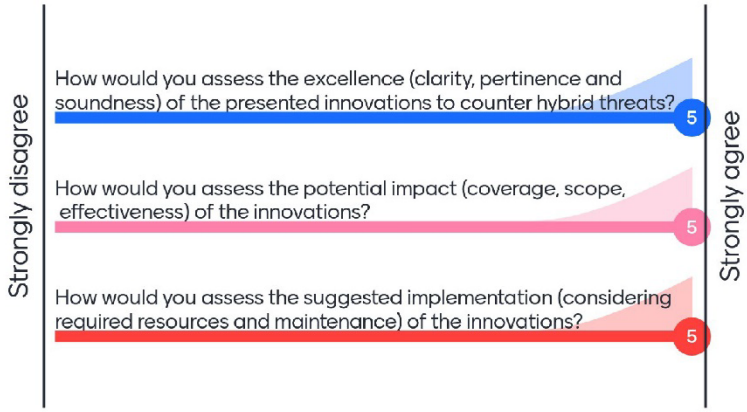
Mentimeter



2

Please let us know your thoughts on the Defalsif AI Forensics Platform innovation!

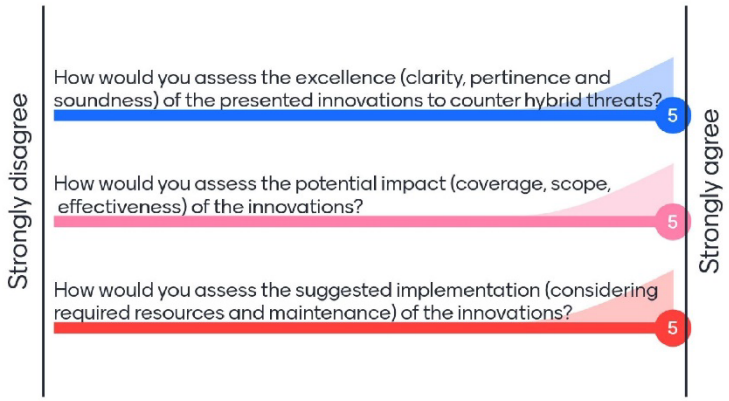
Mentimeter



2

Please let us know what you thought of the Smart Navigator innovation!

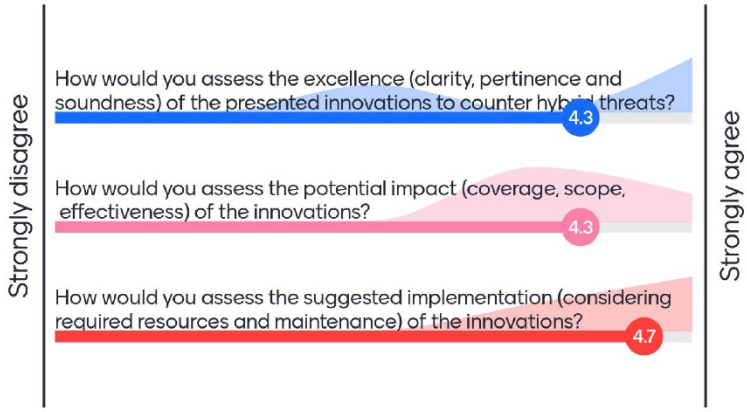
Mentimeter



2

Please let us know what you thought of the Resilience Tool incl. Risk Radar innnovation!

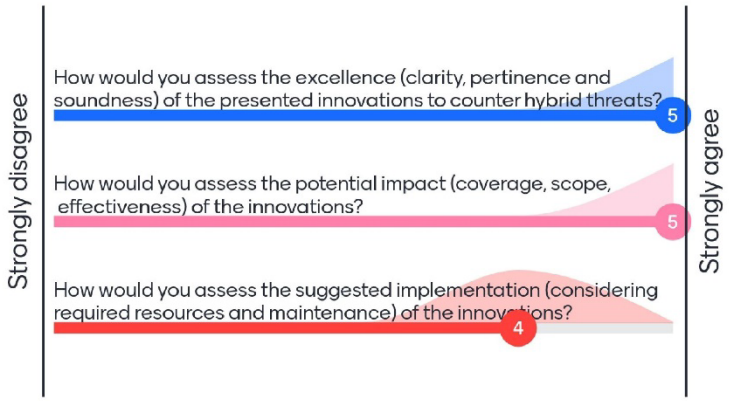
Mentimeter



3

Please let us know your thoughts on the OSINT System innovation!

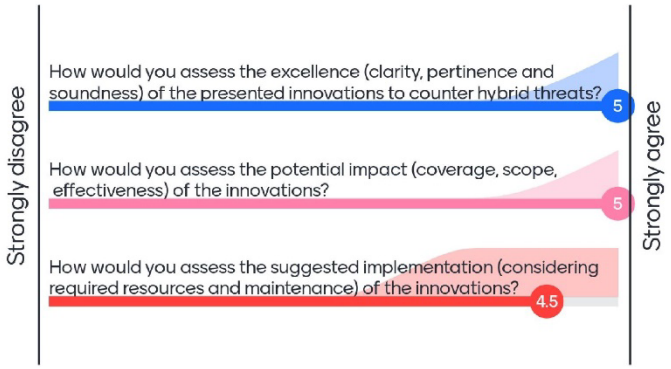
Mentimeter



1

Please let us know your thoughts on the Resilience Methodological Framework for Cascading Cyber-Physical Threats innovation!

Mentimeter



2