

ANNUAL WORKSHOP REPORT 5

DELIVERABLE 5.14

Lead Author: JRC

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

D5.14 ANNUAL WORKSHOP REPORT 3

Deliverable number	5.14	
Version:	V1.0	
Delivery date:	30/04/2025	
Dissemination level:	Public (PU)	
Classification level:	Public (PU)	
Status	Ready	
Nature:	Report	
Main authors:	Julien Theron	JRC
Contributors:	Tiina Haapanen, Isto Mattila, Petteri Partanen	LAUREA
	Kristian Reeson, Vincent Perez de Leon-Huet	EOS

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	3/03/2025	Kristian Reeson (EOS)	First draft, allocation of responsibilities
0.2	06/03/2025	Tiina Haapanen (LAU)	Text editing
0.3	18/03/2025	Tiina Haapanen (LAU)	Text editing
0.4	26/03/2025	Tiina Haapanen (LAU), Julien Theron (JRC)	Content delivery, text editing
0.5	11/04/2025	Kristian Reeson (EOS)	Content delivery
0.6	14/04/2025	Tiina Haapanen (LAU)	Content delivery, text editing
0.7	16/04/2025	Ivan Luis Martinez Villanueva (PLV)	Review
0.8	23/04/2025	Petteri Partanen (LAU)	Review
0.9	28/04/2025	Isto Mattila (LAU)	Review
0.91	29/04/2025	Tiina Haapanen (LAU)	Content and text editing based on the review comments.
1.0	30/04/2025	Tiina Haapanen (LAU)	Finalization and submission to EC

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.

© Copyright in this document remains vested in the Project Partners

CONTENTS

1. Introduction	4
1.1 Overview	4
1.2 Structure of the Deliverable	4
2. Workshop objectives	5
3. Workshop agenda	6
3.1 keynote speeches	6
3.2 EU-HYBNET's latest findings and results	7
3.3 i EU-HYBNET sessions for policy, practitioners, Industry, and Academia	9
3.4 Audience Q&A	11
4. Feedback	12
5. Conclusion	12
Annex I. Glossary and acronyms	13
Annex II. Workshop agenda	14
Annex III. Participant Organisations and Countries	20
Annex IV. Evaluation forms and answers	22
Annex V. dissemination materials	28

TABLES

Table 1 the key project objectives for the Annual Workshop	5
Table 2 Glossary and Acronyms	13
Table 3 AW agenda	15
Table 4 Distribution of number of participant organizations per type of organization and country	21

FIGURES

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities	6
Figure 2 Distribution per countries	20
Figure 3 Distribution of number of participant organizations per type of organization	20
Figure 4 EU-HYBNET 4th AW Feedback Form	23
Figure 5 Evaluation form: event overall satisfaction	23
Figure 6 Evaluation form: general contents' assessment	24
Figure 7 Evaluation form: event arrangements' assessment	24
Figure 8 Evaluation form: keynote speeches' assessment	24
Figure 9 Evaluation form: presentation of EU-HYBNET results' assessment	25
Figure 10 Evaluation form: question 7	25

Figure 11 Evaluation form: question 8..... 26

Figure 12 Evaluation form: Inveted time’s assessment 26

Figure 13 Evaluation form: organisers’ assessment..... 26

Figure 14 Evaluation form: comments..... 27

Figure 15 AW Invitation 28

1. INTRODUCTION

1.1 OVERVIEW

The purpose of this report is to summarize EU-HYBNET (Pan-European Network to Counter Hybrid Threats) project's third 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, policy makers, security practitioners, SMEs, NGOs, 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.

Annual Workshops are part of Work Package number 5, *Communication, Dissemination and Exploitation Activities*. The 5th Annual Workshop presented the project's 5th year findings and highlighted the relevance of the results and networking activities. The event was addressed to the EU-HYBNET network members and pan-European stakeholders; it hosted lectures from policy makers, security practitioners, industry, SMEs, academia, and NGOs.

The JRC, EOS and LAUREA organized the fifth and final EU-HYBNET Annual Workshop that took place on February 12th 2025, in Brussels (Belgium). The event was attended by 53 participants from 33 organizations in 13 countries, out of a total of 84 registered people. The event was live-streamed, and 24 registered representatives attended online. The week of the events, it was announced that a strike would occur on the day after Annual Workshop, disrupting travel plans¹ as many participants were planning to travel back to their country of origin the night of February the 13th. This caused a number of participants to drop down, compared to other events, as well as a few speakers change their in-person attendance to online. Despite this setback, the organising team continued to move forward with the event, and assisted the participants with their travel plans as best as possible.

Participant organisations in the AW included 15 of the 25 project partners, 3 European institutions or EU agencies (European Research Executive Agency, DG HOME and EEAS), 0 stakeholders of the 17 stakeholder group organizations, 1 External Advisory Board (EAB) member of the 5 EU HYBNET EAB member organizations, and 7 members out of 132 network member organizations (at that time). 7 participating organisations came from outside EU-HYBNET networks. Full list of organisations that were present and participant statistics can be found in Annex III.

1.2 STRUCTURE OF THE DELIVERABLE

The Annual Workshops report is divided into five sections:

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 the Annual Workshop's agenda and summarizes the main discussion points. The chapter also highlights the key take-aways 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 importance of findings for the future work of the project.

2. WORKSHOP OBJECTIVES

Objectives of Work Package 5, of which the Annual Workshops are part of, 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:

Table 1 the key project objectives for the Annual Workshop

Project Objective 1: <i>To enrich the existing network countering hybrid threats and ensure long term sustainability</i>	Aiming to further extend the existing EU-HYBNET network, the project partners disseminated among their networks the opportunity to participate and to learn about joining the EU-HYBNET network. The event was also advertised on social media channels and on platforms used by relevant stakeholders and other EU funded projects. Event itself provided an arena for enhancing networking and collaboration within the experts working in the field of countering hybrid threats, and in addition the sustainability of Network after project closure was presented.
Project Objective 3: <i>To monitor developments in research and innovation activities as applied to hybrid threats</i>	In the event EU-HYBNET results in monitoring developments in research and innovation activities we presented (WP3, WP4). Event also included a specific session for industry to present innovation activities in EU-HYBNET network.

The first of the project's objectives – ***to enrich the existing network countering hybrid threats and ensure long term sustainability***. The annual Workshop does this by identifying potential new members to the network, as the events are public and enable all participants to interact with the network members. To ensure a wide range of participants, the event was advertised on EU-HYBNET website (www.euhybnet.eu), project's social media channels (Twitter and LinkedIn) and via e-mail to EU-HYBNET consortium partners, stakeholders group, network members, External Advisory Board members, innovation providers, industry, small and medium-sized enterprises, and non-governmental organizations. Also, the project partners disseminated the event among their networks. EU-HYBNET network will be hosted by Hybrid CoE after project closure and future activities were presented in the 5th Annual Workshop.

The 3rd project's objective – ***to monitor developments in research and innovation activities as applied to hybrid threats***. The Annual workshop presented EU-HYBNET results in innovation and research monitoring (WP3, WP4). The Session for industry included presentations and discussions from EU-HYBNET industry network members Maltego and Logically-AI and H2020 project PREATORIAN

With the organisation of the fifth Annual Workshop in Brussels, the following EU-HYBNET project milestone was achieved: MS 38 “Fifth Annual Workshop”.

Figure 1 highlights the role of EU-HYBNET WP5 and of the Annual Workshop to promote the project’s results and to support the project’s key activities:

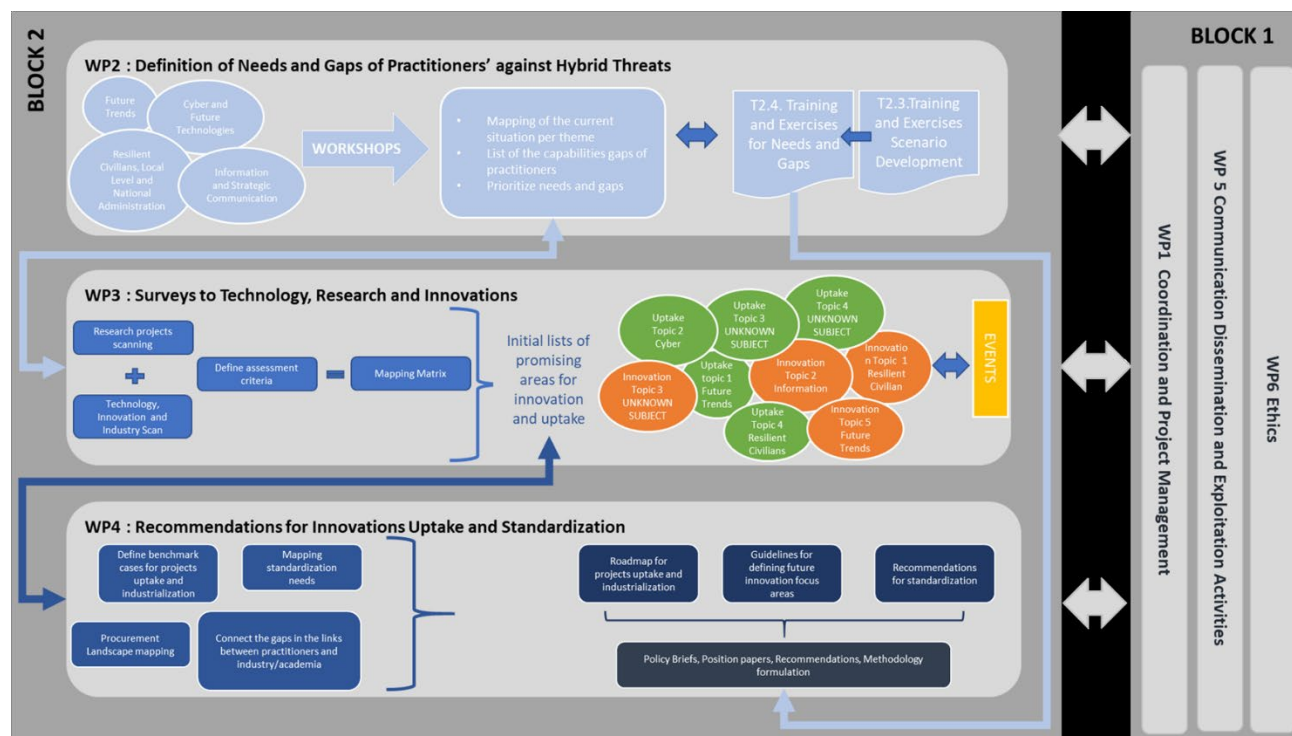


Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

3. WORKSHOP AGENDA

The workshop consisted of three parts:

1. Welcome and registration, opening the event and providing introductory and practical information;
2. Key notes speeches on EU-HYBNET and the Big Picture, discussing the greater context of hybrid threats;
3. EU-HYBNET’s latest findings and results, outlining the project’s final results;

3.1 KEYNOTE SPEECHES

The three keynote speeches were provided by high-level speakers from recognized institutions: **Mr Antonios Platias**, *Executive Director; Brig. General (ret.) Foreign Affairs Institute*, **Mr. Todor Tagarev**, *Institute of ICT, Bulgarian Academy of Sciences*, and a Q&A session guided by **Mr Isto Mattila**, *EU-HYBNET Coordinator, Laurea University of Applied Sciences*.

The presentation **"Linking Hybrid Threats Needs and Gaps with the Defense and Security Domain"** by Antonios Platias highlights the complexity of hybrid threats, which exploit vulnerabilities across political, economic, and cyber domains, making them difficult to detect and counter. It identifies key challenges in the EU’s response, including a lack of structured frameworks, early detection

mechanisms, inter-sectoral coordination, societal resilience measures, and the underutilization of the defense and security sector. The absence of a unified political alignment and an outdated *Strategic Compass* exacerbate these issues, while weak intelligence-sharing and insufficient societal defenses allow disinformation and foreign interference to undermine democratic institutions. To address these gaps, the presentation advocates for enhanced defense-sector involvement, AI-driven threat detection, cross-domain task forces, cyber defense teams, and improved civil-military cooperation. It calls for a *Pan-European Hybrid Resilience Strategy* to integrate hybrid threats into EU security planning, establish legal frameworks for collective responses, and create a *Hybrid Threat Intelligence Fusion Center* to improve crisis response. The urgency of action is emphasized, particularly given hybrid threats to the EU's southern flank—such as weaponized migration, energy security manipulation, and cyber-attacks—while the EU must assert leadership in hybrid defense to strengthen its strategic autonomy and resilience.

"Network-based Approach to Counter Disinformation: Political and Research Perspectives", delivered by Prof. Todor Tagarev at the EU-HYBNET 5th Annual Workshop, examines the rising threat of disinformation and foreign influence, particularly from Russia, which exploits divisive issues such as COVID-19, Ukraine support, and major events to fragment public opinion and undermine trust in information sources. Highlighting the fragmented and ineffective counter-disinformation efforts across Europe, the presentation introduces the *Countering Disinformation Ecosystem (CoDE)*, a *whole-of-society* initiative engaging journalists, students, academia, IT companies, and public authorities to enhance resilience beyond traditional fact-checking. CoDE's initiatives include developing IT tools, training modules, and hackathons to identify and counter disinformation, while also creating an intelligence-driven decision-support environment using structured taxonomies, ontologies, and knowledge graphs. Hackathon-based exercises, such as *RESIST 2*, focus on recognizing misinformation, strategic communication, and early warning systems. The presentation also highlights collaboration opportunities, including research contributions to *Connections: The Quarterly Journal*, which will feature a special issue on malign influence in 2025. Ultimately, the discussion underscores the need for a comprehensive, structured, and technology-driven approach to countering disinformation through multi-disciplinary expertise and cross-sectoral cooperation.

3.2 EU-HYBNET'S LATEST FINDINGS AND RESULTS

After the lunch break, EU-HYBNET partners presented their latest findings and results from the past 5 years through panel discussions. The **topics** discussed in the round table were:

- Gaps and Needs
- Technology and Innovation Mapping
- Recommendations for Innovation Uptake and Standardization
- Insights from Network Building

The *Gaps and Needs* section presented by Maxime Lebrun, *Deputy Director R&A, Hybrid CoE*, focused on analyzing the space between current responses and best practices in addressing hybrid threats, as well as the resources required to bridge these gaps. Key priority areas identified included enhancing the safety of migration processes and strengthening regulations on social media to mitigate the risks of disinformation. Over the past five years, research has highlighted four critical areas where gaps persist and improvements are needed. As such, the methodology evolved to refine insights, focusing

on four core themes: Cyber and Future Technologies, Information and Strategic Communications, Resilient Civilians and Local Administration, and Future Trends of Hybrid Threats. Guided by conceptual models like *The Landscape of Hybrid Threats* and the *CORE Resilience Model*, the final evaluation prioritized key areas for improvement by analyzing past findings. The results highlight the need for a multi-dimensional, strategic approach to hybrid threats, emphasizing enhanced resilience through structured methodologies, collaboration, and adaptability.

The presentation "*Final Gaps and Needs Evaluation*", delivered by Maxime Lebrun at the **EU-HYBNET 5th Annual Workshop**, assesses the gaps between current and best practices in countering hybrid threats and the resources required to bridge them. Over the course of the project, the methodology evolved to refine insights, focusing on four core themes: **Cyber and Future Technologies, Information and Strategic Communications, Resilient Civilians and Local Administration, and Future Trends of Hybrid Threats**. Guided by conceptual models like *The Landscape of Hybrid Threats* and the *CORE Resilience Model*, the final evaluation prioritized key areas for improvement by analyzing past findings. The results highlight the need for a **multi-dimensional, strategic approach** to hybrid threats, emphasizing enhanced resilience through **structured methodologies, collaboration, and adaptability**. The study concludes that **better coordination, resource allocation, and policy development** are essential to strengthening Europe's response to evolving hybrid threats.

The presentation "*Technology and Innovation Mapping*", delivered by Dr. Souzanna Sofou and participants of T3.2 at the EU-HYBNET 5th Annual Workshop, summarizes a five-year study on hybrid threats and technological solutions to counter them, focusing on cybersecurity, civil resilience, and strategic communication. It highlights key concerns such as doxxing, which exposes individuals to cyber harassment, and SLAPPs (Strategic Lawsuits Against Public Participation), which threaten media freedom. Solutions like *Breach Guard* for online data protection and legal support networks such as *CASE* help mitigate these risks. The presentation also emphasizes countering disinformation through proactive strategies like *prebunking*, exemplified by the *BAD NEWS* game, and promoting journalistic integrity via the *Journalism Trust Initiative (JTI)*. Future hybrid threat trends include weaponized migration, gaps in intelligence foresight, and cross-border security challenges, with the *CONNECTOR CE-CISE* framework proposed to enhance real-time intelligence sharing among European security agencies. While artificial intelligence and quantum technologies could improve hybrid threat detection, challenges in ethics, legality, and public acceptance remain obstacles to implementation. The presentation concludes that hybrid threats require a holistic, technology-driven, and cooperative approach, urging enhanced interdepartmental and international collaboration alongside continuous innovation in cybersecurity, media resilience, and strategic intelligence to effectively counter evolving threats.

The presentation "Recommendations for Innovations Uptake and Standardization" from the EU-HYBNET 5th Annual Workshop, led Afroditi Gagara Kozonaki, Research associate, KEMEA, outlines key findings from a multi-year effort to improve hybrid threat resilience through innovation adoption and standardization. It maps the EU procurement landscape, focusing on innovation procurement and joint procurement procedures, identifying both success factors and barriers, and analyzing national funding schemes that support these efforts. The study highlights the importance of cyber and quantum security, disinformation regulation through the Digital Services Act (DSA) and Digital Markets Act (DMA), and media literacy training as critical areas for improvement. Four promising innovations were identified for further development and uptake: a mobile application to report harassment and violence, AI-enhanced disaster emergency communications, the Media Pluralism Monitor, and the Starlight Disinformation-Misinformation toolset. The presentation also emphasizes the need for real-time information sharing between critical entities to enhance early detection and mitigation of hybrid threats, recommending policy briefs, reports, and strategic roadmaps for innovation integration. Key takeaways include the necessity of AI for hybrid threat detection, improving public-private collaboration, and addressing procurement and funding barriers that hinder

innovation adoption. Standardization remains a priority, with recommendations focused on critical infrastructure protection, strategic communication, cybersecurity, and media resilience. The workshop underscores that tackling hybrid threats requires interdepartmental coordination, better situational awareness, and a structured approach to innovation adoption, ensuring that new technologies are effectively implemented to strengthen societal and institutional resilience against evolving security challenges.

The presentation *Building a Network: Insights*, delivered by Maxime Lebrun from *Hybrid CoE*, highlights the development of a pan-European network focused on countering hybrid threats. The network comprises over 150 organizations with a vested interest, mandate, or expertise in addressing hybrid challenges, fostering collaboration, information sharing, and strategic alignment across various sectors. The initiative emphasizes openness, networking, and events to strengthen cooperation among stakeholders while facilitating publications and joint research efforts. The network aligns with Horizon Europe's objective of connecting and integrating market actors, policymakers, and security practitioners, ensuring that knowledge and resources are effectively mobilized to counter emerging threats. Key principles guiding the network's development include diversity, cohesion, and sustainability, reinforcing the need for a resilient and adaptive framework that supports long-term cooperation and innovation in addressing hybrid security risks. The presentation underscores that building an inclusive, well-connected, and responsive network is critical to enhancing Europe's capacity to detect, deter, and respond to hybrid threats.

3.3 | EU-HYBNET SESSIONS FOR POLICY, PRACTITIONERS, INDUSTRY, AND ACADEMIA

The final part of the Annual Workshop dealt with panels examining:

- **Session for Policy – Julien Theron** (*Researcher in Hybrid Threats, JRC*), **Giannis Skiadaresis** (DG HOME)
- **Session for Practitioners - Sabina Magalini** (*UCSC*), **Hans van Leeuwe** (*NL Ministry of Defence*)
- **Session for Industry - Beth Lambert** (*Logically AI*), **Frédéric Guyomard** (*EDF*), and **Jean Backhus** (*Maltego*)
- **Session for Academia – Articles written during the course of the project; avenues for further research - Souzanna Sofou** (*Senior Research and Innovation Manager at Satways*) and **Gunhild Hoogensen Gjörv** (*UIT*)

Session for Policy – Julien Theron (*Researcher in Hybrid Threats, JRC*), **Giannis Skiadaresis** (DG HOME)

In the policy session of the EUHYBNET Annual Workshop, speakers Julien Theron and Giannis Skiadaresis emphasized the critical need for strategic coherence and citizen engagement in the face of hybrid threats. The discussion underscored that hybrid threats aim not only to disrupt infrastructure but also to sow division between citizens and governments. As such, the panel highlighted that strategy must precede ideology, with a focus on combating disinformation and societal “contamination.” Citizens were recognized as the first line of defense, underscoring the strong connection between democratic resilience and security. Giannis Skiadaresis noted that increasingly sophisticated threats demand equally advanced tools and strategies. Addressing these challenges at the EU level requires

both increased investment in defense and a shared strategic vision. Importantly, the speakers called for raising public awareness to ensure citizens are informed and resilient in a shifting geopolitical landscape.

Session for Practitioners - Sabina Magalini (UCSC), Hans van Leeuwe (NL Ministry of Defence)

The presentation "*Hybrid Threats and the Role of the Military*", delivered by Hans van Leeuwe from the Counter Hybrid Unit of the Netherlands Ministry of Defense (NL MOD) at the EU-HYBNET 5th Annual Workshop, examines the evolving nature of hybrid threats and the need for a whole-of-government and whole-of-society approach to counter them. Operating in the grey zone between war and peace, hybrid threats exploit societal vulnerabilities through military intimidation, espionage, cyberattacks, disinformation, foreign interference, and economic coercion, making attribution and response difficult. The DIMEFIL framework (Diplomacy, Information, Military, Economic, Financial, Intelligence, and Lawfare) and PMESII model (Political, Military, Economic, Social, Information, and Infrastructure) illustrate the broad scope of hybrid strategies and their security impacts. The "Connecting the Dots" initiative highlights interagency cooperation, with the Dutch Justice & Security, Foreign Affairs, and Defense ministries leading a national response framework in collaboration with international partners. Since 2023, a whole-of-government approach has strengthened efforts to protect critical infrastructure, democracy, and economic security, while a whole-of-society strategy emphasizes civil-military cooperation, particularly in areas like medical logistics for NATO operations. The EU-HYBNET network supports these initiatives by fostering international cooperation and resilience-building. The presentation concludes that effective hybrid threat mitigation demands cross-sector collaboration, adaptive strategies, and strengthened national and European resilience against increasingly complex security challenges. Sabina Magalini shed light on the increasing vulnerability of healthcare systems to hybrid threats. These threats operate on multiple levels, with the first targeting public perception through disinformation and the manipulation of trust—sometimes even involving corruption within the health workforce. Such tactics are designed to erode confidence in the healthcare system and, by extension, the government. Magalini stressed the importance of the scientific and medical communities actively denouncing individuals who spread falsehoods or stir public fear. The second layer of hybrid attacks involves direct operational disruptions, such as sabotaging hospital infrastructure through cyberattacks that affect electricity or internet access. These actions aim to weaken essential services, foster public dissatisfaction, and ultimately create societal fractures. Given that hospitals often lack the capacity to manage such complex threats, Magalini advocated for the creation of dedicated commissions that meet regularly to address these challenges. She emphasized that hybrid attacks can take many forms—economic, legal, informational—and require coordinated, proactive defense strategies.

Session for Industry - Beth Lambert (Logically AI), Frédéric Guyomard (EDF), and Jean Backhus (Maltego)

The presentation "Protection of Critical Infrastructures from Advanced Combined Cyber and Physical Threats", delivered by Frédéric Guyomard (Electricité de France) at the EU-HYBNET Final Workshop (February 2025), examines the evolving cybersecurity threat landscape and strategies for enhancing critical infrastructure (CI) resilience. It highlights new cyber threats, including industrial espionage, destabilization operations, targeted mobile attacks, and enhanced offensive capabilities, emphasizing the increasing complexity of cybersecurity. The PRAETORIAN project, funded by EU Horizon 2020,

seeks to strengthen European CI security by coordinating protection against combined cyber and physical threats. Key objectives include hazard evaluation, vulnerability assessments, and security measure implementation to minimize risks. The Critical Entities Resilience Directive (EU 2557/2024) is presented as a framework for ensuring resilience, operational continuity, and recovery capabilities. The RESIST-SURVIVE-RECOVER model promotes proactive risk management and crisis response, while the EU-CIP Knowledge Hub serves as a collaborative digital platform for knowledge sharing, innovation, and training among CI stakeholders. The presentation concludes that protecting critical infrastructure requires a comprehensive approach, integrating technological advancements, regulatory frameworks, and international cooperation to safeguard vital services against evolving hybrid threats. Beth Lambert then emphasized the vital role industry leaders play in countering hybrid threats by leveraging their sector-specific expertise and fostering cross-sector collaboration. Drawing on her work addressing foreign interference campaigns and information operations, Lambert highlighted that hybrid threats often exploit gaps between industries—targeting vulnerabilities in areas such as media, technology, and critical infrastructure. To build resilience, she advocated for a more integrated approach where private sector actors share threat intelligence, align risk mitigation strategies, and engage in joint preparedness initiatives. Lambert stressed that no single sector can address these threats alone; instead, collective action, informed by deep knowledge of individual sectors and enhanced by cross-disciplinary cooperation, is essential to disrupt the complex and evolving tactics of hybrid actors.

Session for Academia – Articles written during the course of the project; avenues for further research
 - **Souzanna Sofou** (*Senior Research and Innovation Manager at Satways*) and **Gunhild Hoogensen Gjørsv** (*UIT*)

The presentation "*Session for Academia*", delivered by Dr. Souzanna Sofou (SATWAYS) and Prof. Gunhild Hoogesen-Gjørsv (UIT) at the EU-HYBNET 5th Annual Workshop, highlights five years of academic research on hybrid threats across four key areas: Resilient Civilians, Cyber and Future Technologies, Information and Strategic Communication, and Future Trends of Hybrid Threats. Studies have examined disinformation, identity-based hybrid threats, critical infrastructure protection, and foreign investments in sensitive sectors, as well as mis- and disinformation during COVID-19. Research on cybersecurity explores quantum technology, 5G vulnerabilities, and hybrid cyber threats, while strategic communication focuses on disinformation responses, historical narrative manipulation, and climate change-related propaganda. Additionally, studies on future hybrid threats analyze uncrewed systems targeting critical infrastructure, conspiracy theories on social media, and migration as a geopolitical tool. The session also presents EU-HYBNET's efforts to strengthen critical infrastructure resilience, emphasizing data governance, digital security, and risk assessment tools such as CIRP, the ResilienceTool, and RiskRadar for identifying emerging threats. Blockchain-based monitoring systems are proposed to protect European industries from foreign influence. The presentation concludes that academic research is essential for shaping hybrid threat responses, stressing the importance of interdisciplinary collaboration, technological innovation, and robust data governance to enhance Europe's resilience against evolving security challenges.

3.4 AUDIENCE Q&A

In the final part of the workshop, after the presentations on the various sessions were finished, a Q&A session was held to answer any of the questions the participants might have had for the speakers.

The most relevant questions addressed related to how synergies can be established between different practitioner networks, the way the index of vulnerability to FIMI was constructed, and if it can be expanded to other countries, for example in the Western Balkans.

4. FEEDBACK

As with each EU-HYBNET event, participants were given a feedback form (see Annex) to be filled out at the end of the event or after its conclusion.

The format used was a Microsoft Form, and the link was shared via QR code towards the end of the event and sent to registered participants after the conclusion of the event. The event conductor encouraged participants to fill in the evaluation forms.

The results will be the average of the answers given by participants, with graphs showing the distribution available in the annex IV. The 5th and final Annual Workshop received very positive feedback from the participants. Overall satisfaction of the event was 4,67 out of 5. General content, event arrangement and keynote speeches all received 4.83 average rating out of 5. Presentations on EU-HYBNET results were rated 4.50 on average. The participant found event organisers very helpful (5/5) and assessed the time invested to the event valuable (4.83/5).

In terms of general comments and feedback, there were a few comments applauding the event and the organisation. Participants have picked different parts of event most interesting, which can be considered as a sign of a successful event agenda. One of the final comments stated “Thank you - overall this was a very good final meeting » and this echoes the atmosphere at the event.

5. CONCLUSION

5th Annual workshop achieved its goals to disseminate EU-HYBNET’s 5th year project findings and to discuss innovations and challenges when countering hybrid threats together with an audience of pan-European stakeholders, academia, SMEs, NGOs, policy makers and industry representatives. Although the Brussels strike seemed to affect participants joining the event, the discussions and interaction with the audience was vivid. It can be stated that EU-HYBNET has been able to connect these different actors in the field and co-operation will surely continue also post-project.

The 5th and final Annual workshop has been successful also based on the feedback that was gathered after the event. Overall event was rated with an average 4.67 out of 5. This has been the trend also in all 4 prior Annual Workshops, which shows that the project has been successful with the events and hybrid threats is more topical than ever.

ANNEX I. GLOSSARY AND ACRONYMS

Table 2 Glossary and Acronyms

Term	Definition / Description
AW	Annual Workshop
EOS	European Organization for Security
EU-HYBNET	Pan-European Network to Counter Hybrid Threats
LAUREA	LAUREA University of Applied Sciences
JRC	Joint Research Centre
NGO	Non-governmental organization
H2020	Horizon 2020
EEAS	European Union External Action
CTI	Open Cyber Threat Intelligence Platform
EAB	External Advisory Board
SME	Small and medium-sized enterprise
PLV	Valencia Local Police
WP	Work Package
OB	Objective
D	Deliverable
PU	Public
KPI	Key performance indicators
DG HOME	The Directorate-General for Migration and Home Affairs
PRAETORIAN	Protection of Critical Infrastructures from advanced combined cyber and physical threats
Q&A	Questions and answers
CoDE	Countering Disinformation Ecosystem
RESIST 2	Counter-disinformation toolkit
DSA	Digital Services Act
UCSC	Catholic University of the Sacred Heart of Rome
NL MoD	Netherlands Ministry of Defence
EDF	Électricité de France
UiT	The Arctic University of Norway
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threat

ANNEX II. WORKSHOP AGENDA

Time CET	Topic	Speakers
Welcome and registration		
11:00-11:30	Registration	
11:30-11:45	Welcome & Practical information	Julien Theron , <i>Researcher in Hybrid Threats, European Commission Joint Research Council</i> Isto Mattila , <i>EU-HYBNET Coordinator, Laurea University of Applied Sciences</i>
EU-HYBNET and the Big Picture		
11:45-12:30	Linking Hybrid Threats Needs and Gaps with the Defense and Security Domain	Antonios Platias , <i>Executive Director; Brig. General (ret.) Foreign Affairs Institute</i>
	Network-based Approach to Counter Disinformation: Political and Research Perspectives	Todor Tagarev , <i>Institute of ICT, Bulgarian Academy of Sciences.</i>
12:30-13:00	Audience Q&A	Host: Isto Mattila , <i>EU-HYBNET Coordinator, Laurea University of Applied Sciences</i>
13:00-14:00	LUNCH	
EU-HYBNET’s latest findings and results		
14:00-14:30	Gaps & Needs	Maxime Lebrun , <i>Deputy Director R&A, Hybrid CoE</i>
14:30-15:00	Technology and Innovation Mapping	Souzanna Sofou , <i>Senior Research Engineer & Innovation Manager, SATWAYS</i>
15:00-15:30	Recommendations for Innovation Uptake and Standardization	Afroditi Gagara Kozonaki , <i>Research associate, KEMEA</i>

15:30-15:45	Insights from Network Building	Maxime Lebrun , <i>Deputy Director R&A, Hybrid CoE</i>
15:45-16:00	Q&A	Host: Isto Mattila , <i>Laurea University of Applied Sciences</i>
16:00-16:15	Coffee break	
16:15-16:45	Session for Policy	Julien Theron , <i>Researcher in Hybrid Threats, JRC</i> Giannis Skiadaresis , <i>DG HOME</i> Rolf Blom , <i>RISE</i>
16:45-17:15	Session for Practitioners	Sabina Magalini , <i>UCSC</i> Hans van Leeuwe , <i>NLD Ministry of Defence</i>
17:15-17:45	Session for Industry	Beth Lambert , <i>Logically AI</i> Frédéric Guyomard , <i>EDF</i> Jean Backhus , <i>Maltego</i>
17:45-18:15	Session for Academia – Articles written during the course of the project; avenues for further research.	Souzanna Sofou , <i>SATWAYS</i> Gunhild Hoogensen Gjørsv , <i>UIT</i>
	Q/A	Host: Julien Theron, JRC
18:15-18:30	Closing remarks Mr. Isto Mattila, EU-HYBNET Coordinator Dr. Julien Theron, JRC	
18:30 – 21:00	<i>Buffet and Social Dinner at the M.A.I. directly following the event</i>	

Table 3 AW agenda

Biography**Antonios Platias**

Antonios Platias (MBA) is a retired Brigadier General and former National Defense Policy Director of the Hellenic Ministry of Defense, with extensive staff and field experience in NATO and EU positions and operations. He currently serves as Executive Director of the Foreign Affairs Institute (FAINST)—an Athens-based think tank that hosts an annual Forum on Hybrid Threats, Cyber Security, and Artificial Intelligence—and as a Member of the Advisory Council of OPEWI (Europe's War Institute), a Brussels-based think tank. Deeply involved in raising awareness of hybrid threats since his active service, he continues to leverage his expertise as Managing Director of the European Defense Venture Studio and Chief Strategy & Innovation Officer at Seeders, a private Athens-

based company that, along with his other affiliations, is a member of EU-HYBNET. Antonios regularly writes and speaks on geopolitics, hybrid threats, defense innovation and European integration.

Afroditi Gagara Kozonaki

Afroditi Gagara Kozonaki (MSc) is a research associate at the Hellenic Centre for Security Studies (KEMEA) of the Hellenic Ministry of Citizen Protection since 2020. She has obtained MSc in “Geopolitical Analysis, Geo-Strategic Synthesis and Defence and International Security Studies” from the National and Kapodistrian University of Athens (2021) and holds a BSc in Political Science from the University of Crete (2013). Her main research fields of interest include countering terrorism, political violence, and Grand Strategy issues. Her professional experience includes research work and involvement in EU and Nationally Funded R&D projects related to research & prevention policy regarding Organized Crime, Radicalization, Terrorism, Cybercrime and Combatting Trafficking in Human Beings.

Beth Lambert

Beth Lambert is Account Director at Logically, a tech company that works with democratic governments to tackle hybrid threats and foreign interference at scale using AI and expert OSINT investigators.

She is the former Head of Counter Disinformation for the UK Government's Department for Digital where she oversaw the department's policy response to disinformation issues covering public health, public safety and national security. In 2021 Beth was elected Chair of the Council of Europe's expert advisory committee on the integrity of the information environment.

In 2020 she was awarded a Churchill Fellowship for her research on international best practice in combating state-backed disinformation campaigns, including foreign interference and manipulation in elections. Her research showcased successful interventions in combating disinformation operations and FIMI campaigns.

Frédéric Guyomard

Frédéric Guyomard is an expert research engineer at Electricité De France (EDF-R&D-Lab ParisSaclay) and I have been working for 20 years in the field of computer and digital security. He graduated in Electronics and Telecommunication systems and with a Master degree in IT security and cybercrime (Troyes University of Technology). He has been specialised for 15 years in Digital Security and the assessment of industrial environments by participating in large-scale projects, both for the renovation of installations and in the concerns of new projects for the EDF group (AMI, Nuclear, Transport, monitoring, renewable energy, smart-grids and smart-charging).

In 2019 he was involved in the Important Project of Common European Interest – Cybersecurity items: two of my proposals selected to be recommended among the 6 workstreams to be prioritised. He is currently the Coordinator of the H2020 project "PRAETORIAN", a consortium of 23 partners in 7 EU countries, dealing with the combined cyber and physical threat to Critical Infrastructures in Europe. This grant-funded project aims to develop risk reduction and incident management tools on the cascading effects resulting from the realisation of these threats. He leads the EXERA Cybersecurity Technical Committee, and is a member of ECSO and ENCS. Furthermore, he is the author of the Cybersecurity research roadmap for EDF Lab.

Giannis Skiadaresis

Mr. Giannis Skiadaresis is the Area Coordinator for Strengthened Security research and Innovation (SSRI) in the Unit on Security Research and Innovation of Directorate General for Migration and Home Affairs (DG HOME) in European Commission. Mr. Skiadaresis holds an MA in EU International Relations and Diplomacy, from the College of Europe in Bruges where he was a laureate of ENP-EU scholarship awarded by the European Commission. He has also graduated from the Leadership programme of Harvard Kennedy School and from the Strategic Innovation Programme of University of Oxford. He has worked in the Cabinet of Commissioner Avramopoulos on Migration, Home affairs and Citizenship and in other posts at DG HOME in the European Commission. His experience also includes Industrial Policy, New Technologies and Innovation, International relations, security and defence policy, business development and coordination of EU-funded Projects.

Gunhild Hoogensen Gjørsv

Gunhild Hoogensen Gjørsv is Professor in Critical Peace and Conflict Studies (Security and Geopolitics) at the UiT-The Arctic University of Norway, and Arctic 5 Chair in Security Studies (arcticfive.org). Hoogensen Gjørsv's research examines comprehensive security dynamics in the context of hybrid threats and warfare, civil-military interaction (out of area operations, and Norwegian total defence), and Arctic perceptions of security focusing on "bottom-up" and intersectional approaches. She leads a variety of projects regarding hybrid threats and civilians.

UiT profile page: <https://uit.no/ansatte/gunhild.hoogensen.gjorv>

Hans van Leeuwe

Hans van Leeuwe is head of the Counter Hybrid Unit of the Netherlands Ministry of Defence (MOD) since 2018. This Unit participates in HYBNET as practitioner since the start of HYBNET in 2020. On behalf of the MOD he also is Steering Board member of the European Hybrid CoE and of the NATO StratCom CoE. Before joining the Counter Hybrid Unit Van Leeuwe drafted the NLD Defence White Paper-2018. He represented the MOD at the UN-discussions on Lethal Autonomous Weapon Systems (LAWS) in Geneva in 2015-2018. Before that amongst other things he was the executive secretary of the Peace and Security Committee of the independent Advisory Council on International Affairs of the Netherlands during four years. Hans van Leeuwe started working for the MOD in 1996. He studied management and organizational science in 1988-1995.

Isto Mattila

Professor Isto Mattila works for international security research in the University of Turku, Finland in the Department of Information Technology. Prof. Mattila has wide working experience covering diverse assignments in different organisations national and international level. He is a Captain Navy, Finnish Border Guard. As from 2008 to 2014 he has worked for the European Commission, DG MARE. He was a second penholder for Maritime Security Strategy and designed new information sharing mechanism (CISE) between maritime authorities in EU, which is now hosted by EMSA. He has held the position of R&D Director at Laurea UAS and he was the project coordinator of the AI-ARC Horizon 2020 project, which aims to build information sharing and anomaly detection to Arctic stakeholders.

Julien Theron

Dr Julien Theron taught at the universities of Budapest (BME), Beirut (USJ, USEK), Paris (Nanterre, Panthéon-Assas). He also collaborated with the French Institute of International Relations (IFRI) and the International Institute for Strategic Studies (IISS). He is a former Senior Fellow in European Security of the Norwegian Institute for Defence Studies (IFS). In policy, he worked for the French government (MFA, MoD, INSP) as well as for the

European Union (EU) and the United Nations (UN). He is a lecturer in War Studies at Sciences Po's Paris School of International Affairs and a researcher in Hybrid Threats for the European Commission Joint Research Centre (JRC).

Maxime Lebrun

Prior to taking up his post as Deputy Director R&A at The European Centre of Excellence for Countering Hybrid Threats, Maxime worked at the Baltic Defence College in Tartu as a Lecturer in War and Conflict Studies and as Acting Department Director. During that time, he was also a Non-Resident Research Fellow at the International Centre for Defence and Security. Maxime holds a master's degree in International Relations from Sciences Po Lyon with a specialization in strategic, military and security studies from Sciences Po Aix-en-Provence.

Rolf Blom

Dr. Blom has since 2011 worked as a project leader and senior researcher in the Cybersecurity unit at RISE. Before that he held an Expert position in Mobile Communications Security at Ericsson Research. He has been active in OMA and 3GPP security standardization and has contributed to security standardization in the IETF. He has also been involved in different EU projects, e.g. SHAMAN on 3G security, SEGRID on smart grid security and 5G-ENSURE on security for 5G. Dr. Blom holds a M.Sc. (1972) in Electrical Engineering from the Royal Institute of Technology in Stockholm and a Ph.D. (1979) in Information Theory from Linköping University.

Sabina Magalini

Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli (FPG) and Assistant Professor of Surgery at the Rome Catholic University School of Medicine (UCSC). She is also an Associate Researcher of the Italian National Council of Research (CNR-IASI); Fellow of the American College of Surgeon, of the American Association for the Surgery of Trauma and of the European Society for Trauma and Emergency Surgery (ESTES).

Souzanna Sofou

Dr. Souzanna Sofou, Senior Research and Innovation Manager at Satways Ltd, serves as the EU-Hybnets WP3 Leader: Surveys to Technology, Research and Innovations. She is a Dipl. Mining and Metallurgical Engineer and a holder of an MBA in Engineering –Economic Systems. With respect to basic research, her Doctoral Thesis and most of her published research work fall in the fields of computational rheology, rheometry and polymer processing. In the area of applied research, she has worked in FP7 & Horizon 2020 projects in various fields, including security, new product development, metallurgy, polymer processing, RET modelling, software development and value management. She also has background and experience in Intellectual Property, as she has received relevant training and has worked in this field as a Product Design Engineer for a multinational company. Dr. Sofou has served as the innovation, exploitation and dissemination manager in several H2020, EDF and PCP projects and is an experienced research proposals writer and project manager. She is responsible for the Innovation Management of Satways products.

Todor Tagarev

Prof. Tagarev is Head of the Centre for Security and Defence Management, Institute of ICT, Bulgarian Academy of Sciences. He has held several senior positions in Bulgaria's Ministry of Defence, including two terms as Defence Minister – March–May 2013 and June 2023–April 2024.

Prof. Tagarev combines governmental experience with theoretical knowledge and background in cybernetics, complexity, and security studies. Cognitive warfare is becoming an area of his research interest. He currently leads one of the work packages of a project aiming to strengthen the national ecosystem for countering disinformation.

He is author and co-author of over 150 books, articles and conference papers, with significant experience in leading national and international interdisciplinary research teams.

UiT profile page: <https://uit.no/ansatte/gunhild.hoogensen.gjorv>

ANNEX III. PARTICIPANT ORGANISATIONS AND COUNTRIES

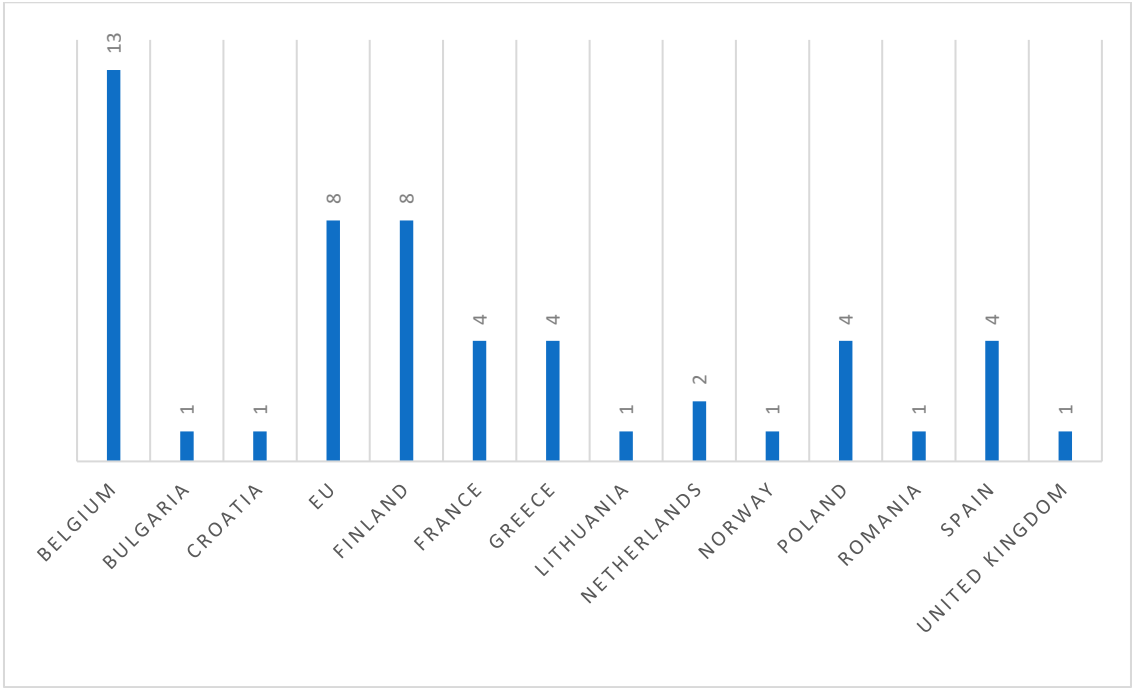


Figure 2 Distribution per countries

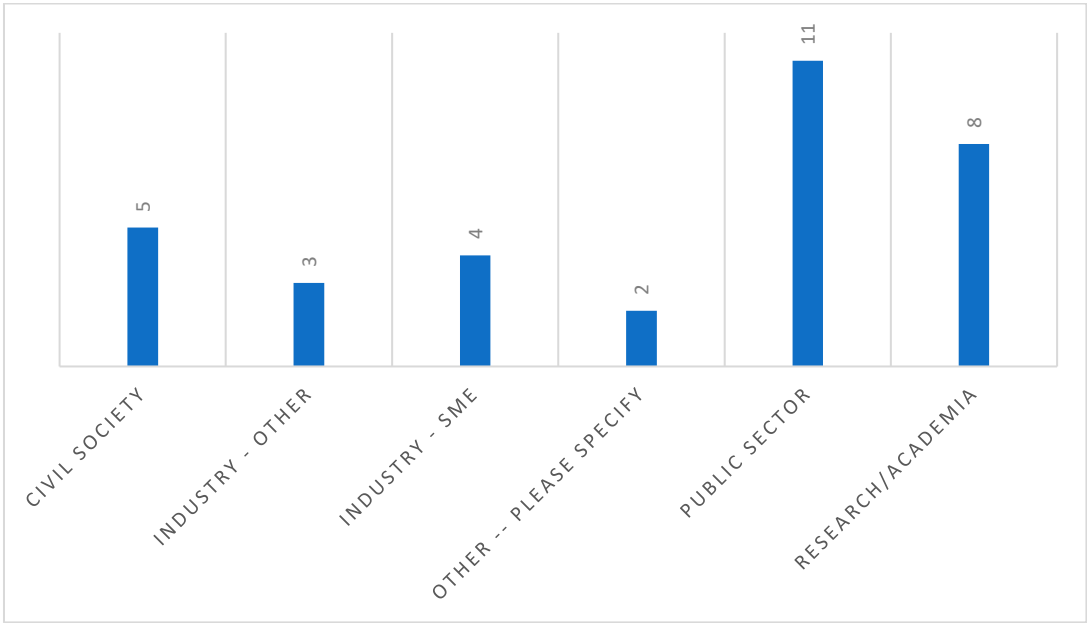


Figure 3 Distribution of number of participant organizations per type of organization


	Civil Society / NGO	Industry Other	Industry - SME	Other -- Please Specify	Public Sector	Research/ Academia	Grand total
Belgium	2	2	1	1	0	1	7
Bulgaria						1	1
EU					2	1	3
Croatia	1						1
Finland				1	1	1	3
France		1	1		2		4
Greece	1		1		1		3
Lithuania						1	1
Netherlands					1	1	2
Norway						1	1
Poland					3		3
Romania						1	1
Spain	1				1		2
United Kindom			1				1
Total	5	3	4	2	11	8	33






Table 4 Distribution of number of participant organizations per type of organization and country


ANNEX IV. EVALUATION FORMS AND ANSWERS






EU-HYBNET 5th Final Annual Workshop Feedback Form


* Required






1. Overall, how satisfied were you with the event? * 


    






2. How would you assess the general content, topics of the event? * 


    






3. How would you assess the event arrangements? * 


    

4. How relevant did you find the keynote speeches? * 


    

5. How would you evaluate the presentations of EU-HYBNET results? * 


    

6. What was your favorite part of the event? * 


Enter your answer






7. What was your favorite topic of the event ? * 


Enter your answer






8. What was your least favorite part of the event? 


Enter your answer

9. How would you assess the time invested to the event participation? * 

10. How helpful were the event organisers? * 

11. Any other comments? 

Enter your answer

Submit

Figure 4 EU-HYBNET 4th AW Feedback Form

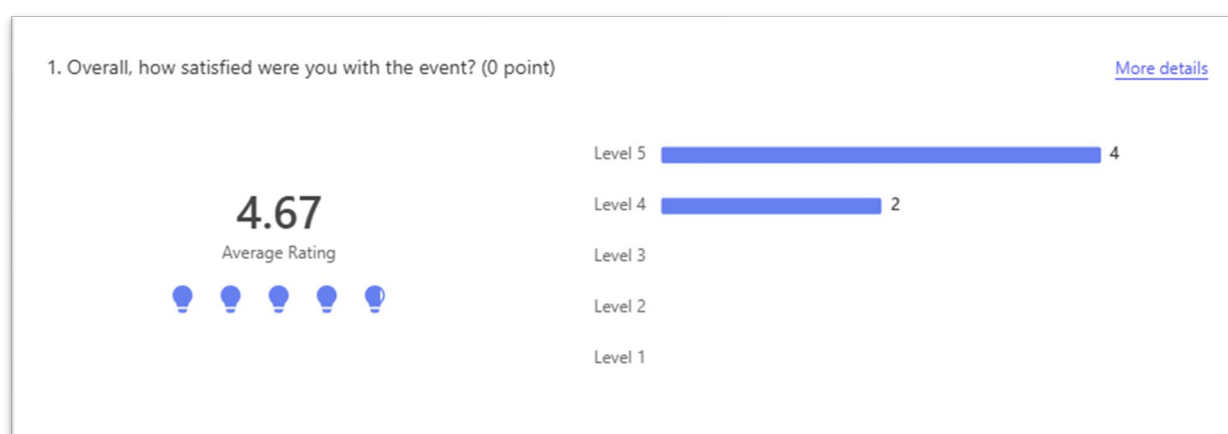


Figure 5 Evaluation form: event overall satisfaction

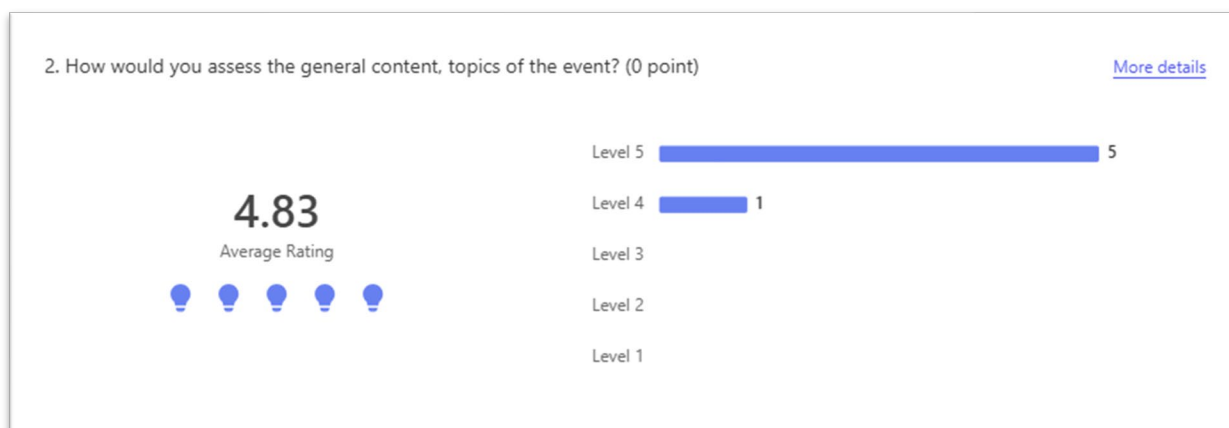


Figure 6 Evaluation form: general contents' assessment

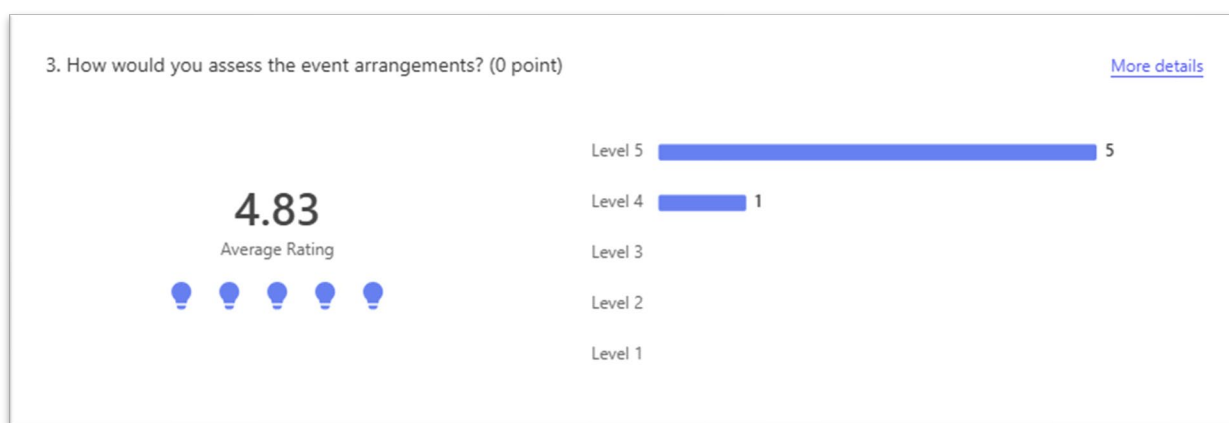


Figure 7 Evaluation form: event arrangements' assessment

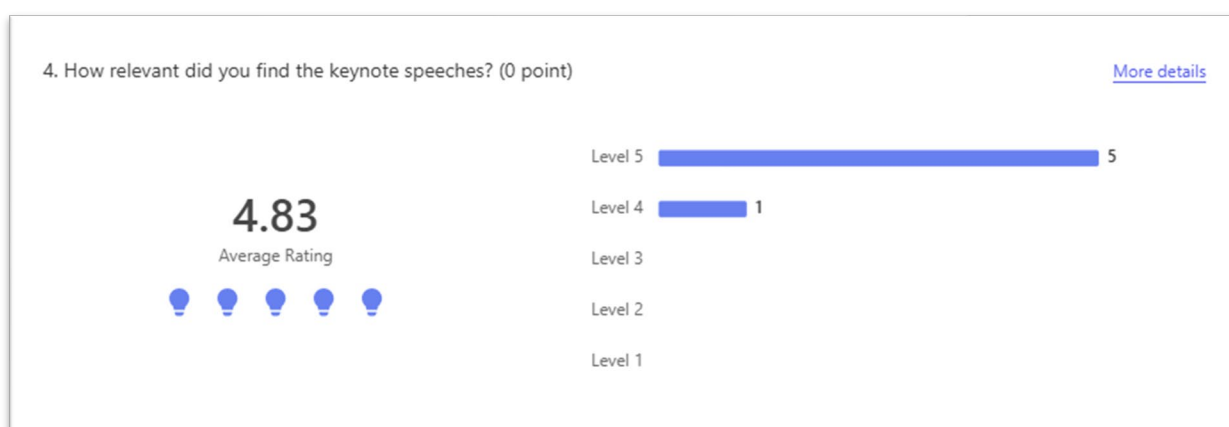


Figure 8 Evaluation form: keynote speeches' assessment

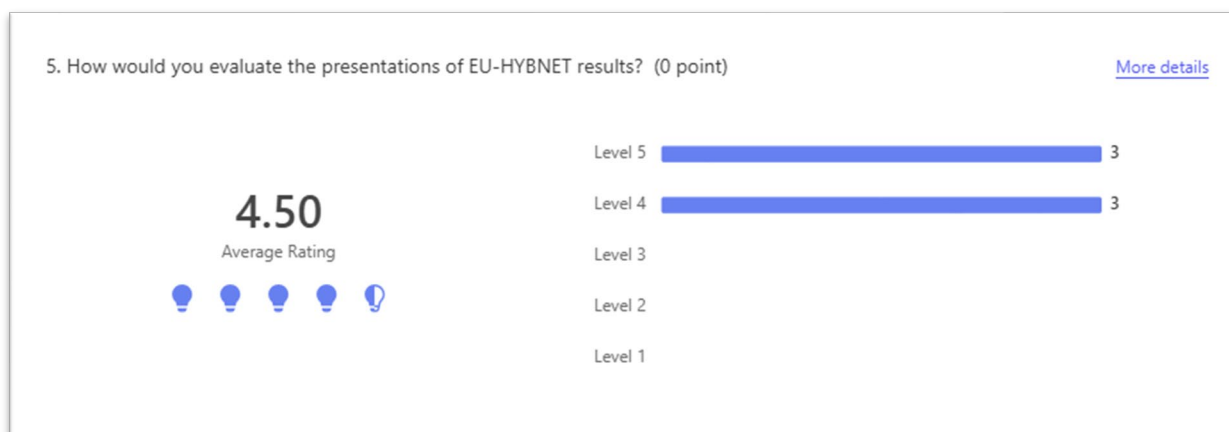


Figure 9 Evaluation form: presentation of EU-HYBNET results' assessment

7. What was your favorite topic of the event ?

6 Responses

ID ↑	Name	Responses
1	anonymous	Session for academia
2	anonymous	Findings and results of the project
3	anonymous	Network-based Approach to Counter Disinformation: Political and Research Perspectives
4	anonymous	all the part were excellent
5	anonymous	Reflections on the use of disinformation as a hybrid threat in initial discourses
6	anonymous	influence and FIMIs

Figure 10 Evaluation form: question 7

8. What was your least favorite part of the event?

5 Responses

ID ↑	Name	Responses
1	anonymous	Recommendation for innovation uptake
2	anonymous	Session for academia, but only because I'm not academia
3	anonymous	Technology and Innovation Mapping
4	anonymous	Some of the interventions with the latest discoveries and achievements became a bit long.
5	anonymous	the keynote speech (not enough practical)

Figure 11 Evaluation form: question 8

9. How would you assess the time invested to the event participation? (0 point)

[More details](#)

Figure 12 Evaluation form: Inveted time's assessment

10. How helpful were the event organisers? (0 point)

[More details](#)

Figure 13 Evaluation form: organisers' assessment

11. Any other comments?

3 Responses

ID ↑	Name	Responses
1	anonymous	Thank you for everything!
2	anonymous	Excellent
3	anonymous	Thank you - overall this was a very good final meeting

Figure 14 Evaluation form: comments

ANNEX V. DISSEMINATION MATERIALS



Figure 15 AW Invitation