LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

DELIVERABLE 1.23

Lead Author: Hybrid CoE

Contributors: LAUREA,

Deliverable classification: Public

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

D1.21 LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

Deliverable number	**1.23**	
Version:	**V1.0**	
Delivery date:	**29.04.2025**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Sophie Bujold**	**Hybrid CoE**
Contributors:	**Jari Räsänen**	**LAUREA**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	25.03.2025	Sophie Bujold / Hybrid CoE	First draft
0.2	04.04.2025	Hanne Dumur-Laanila / Hybrid CoE	Review
0.3	08.04.2025	Sophie Bujold / Hybrid CoE	Second draft
0.4	14.04.2025	Sophie Bujold / Hybrid CoE	Editing
0.5	23.04.2025	Jari Räsänen / Laurea	Editing
0.6	23.4.2025	Margriet Drent / NL MoD	Review
0.6	25.04.2025	Sophie Bujold / Hybrid CoE	Final draft
0.7	28.4.2025	Isto Mattila / Laurea	Final review
1.0	29.4.2025	Tiina Haapanen / Laurea	Final structural editing and submission to EC

DISCLAIMER

CONTENTS

TABLES AND FIGURES

1. INTRODUCTION

1.1. PURPOSE OF THE NETWORK EXTENSION

The *Pan-European Network to Counter Hybrid Threats* is a network of practitioners (NoP) project, which means that extending and managing the network of stakeholders has been one of its core tenets. The EU-HYBNET Description of Action (DoA) states that the development of the network responds to the objective of improving and maintaining a higher level of resilience against hybrid threats. The project network includes actors in the field of comprehensive security at local, regional, national and international levels across the European Union (EU) and beyond: practitioners, members from industry, small and medium-sized enterprises, academia, NGOs, and other actors relevant to countering hybrid threats in the EU and the EU Associated Countries (AC)[1].

When the project started in 2020, the network consisted of 25 consortium partners and 16 stakeholder organisations (see Table 2). The goal has been that the network would expand by adding at least 30 new members annually.[2] Although the network has grown steadily over the past five years, the final years have seen some difficulties in finding new network applicants and lower application numbers, likely due to the project coming to an end. In particular, this was especially seen after the project events concluded, as these events themselves were greatly appealing to new network members. During the final reporting period, and once the events concluded, potential applicants could have perceived that the benefit of joining the project had lessened slightly. However, concrete network extension activities were undertaken by consortium members to address this and to meet the Key Performance Indicator (KPI) of 30 new network members annually. These actions are explained in Section 3 of this report, entitled "The European Commission's requested improvements to the network and actions taken by the consortium". Particular emphasis was placed on finding more security practitioners, Small to Medium Enterprises (SMEs), industry organizations, and Non-Governmental Organizations (NGOs) to invite to join the network, as well as organizations from EU countries entirely lacking EU-HYBNET network members.

In the final month of the EU-HYBNET project (M60), together with the consortium partners and network member organizations, the network consists of 40 practitioners, 35 industry/SME organizations, 26 NGOs and 60 organizations representing academia and research organizations. In total, the final EU-HYBNET network encompasses an impressive 161 organizations.

This deliverable (D) 1.23, *List of new actors to the extended EU-HYBNET network*, lists the new members to the network between M37 (April 2024) and M60 (April 2025). At the time of writing, the application and selection process to the EU-HYBNET network has closed. The last applications to the network were submitted on 28 February, in order to allow for the review and selection processes to occur. Throughout the duration of the EU-HYBNET project, this deliverable has been published annually. As this is the final deliverable of this series, D1.23 will cover the new network members accepted during the last year of the project and depict the network members at the time of the project's completion.

[1] The following countries are associated to Horizon 2020: Iceland, Norway, Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, Serbia, Turkey, Israel, Moldova, Switzerland, Faroe Islands, Ukraine, Tunisia, Georgia, Armenia.
[2] The current plans to sustain the network are described in detail in Deliverable 1.24, *EU-HYBNET network Sustainability Initial Report.*

The growth of the network has been a significant driver of the content and results of the project. The extended EU-HYBNET network is a group of stakeholders who are invited to contribute to the project's tasks on a voluntary basis. The input from these network members in the annual Gaps and Needs Workshop[3] has formed the starting point for proceedings within each project cycle. The gaps and needs stemming from the workshops were those identified by network members, and the project outcomes – research, exercises, innovation mapping, and recommendations for policy and procurement – reflect those specific gaps and needs. Network members have also been the main contributors on the project's online platforms, Innovation Arena and TUOVI, where challenges have been proposed, alongside possible ideas to surmount them. In each of the project's four cycles, network members were invited to EU-HYBNET events, such as the Annual Workshop and Future Trends Workshop, where the identified gaps and needs were addressed by the demonstrations and testing of promising innovations and other measures to counter hybrid threats. Network members were also given opportunities to cooperate through research and the writing of articles for the project.

The main objective of this document is to list and describe the new members to the EU-HYBNET network. The document also briefly describes the selection process and objectives as per the project documents.[4] In addition, the document acknowledges the EC's requested improvements for the network extension given by the European Commission during the three periodical reviews and addresses the actions taken by the consortium to address them. Finally, this document addresses the network status at the project's completion.

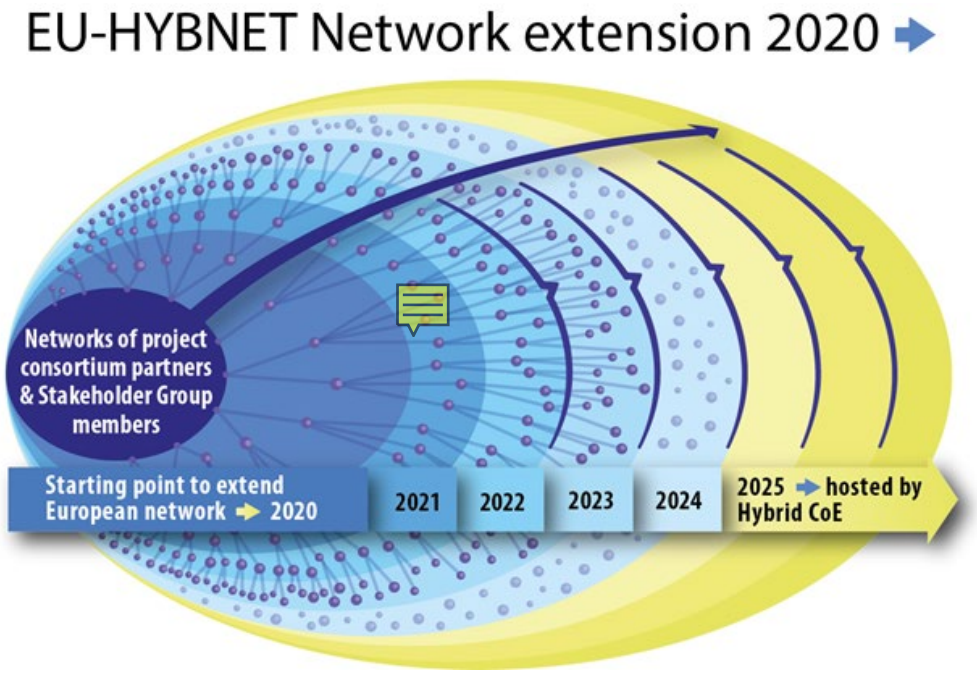

Figure 1: EU-HYBNET network extension 2020-2025

[3] The workshop objectives are described in detail in Deliverable 2.3, *Gaps and Needs Workshop.*
[4] The network extension process is covered in more detail in Deliverable 1.7, *Definition of the eligibility criteria for new actors.*

1.2. STRUCTURE OF THE DELIVERABLE

This document has six sections:

- The first section provides an introduction to D1.23 and outlines its content.
- The second section describes the objectives and Key Performance Indicators (KPI) that were defined for the network extension, and how they were addressed in the project as per EU-HYBNET D1.7 "Definition of the eligibility criteria for new actors" and D1.24 "EU-HYBNET Network Sustainability Initial Report".
- The third section describes the European Commission's requested improvements to the network and actions taken by the consortium.
- The fourth section describes the **selection process** and how it has been applied since the first round of applications.
- The fifth section is the **list of new members** to the network, their type and focus areas, including a complete list of all network members.
- The sixth section briefly describes the European Centre of Excellence for Countering Hybrid Threats' (Hybrid CoE) plan to host the network after the project ends.

2. NETWORK EXTENSION OBJECTIVES

2.1. PROJECT OBJECTIVES AND KEY PERFORMANCE INDICATORS

Throughout the project's duration, the EU-HYBNET network extension contributed to all seven project objectives (OB) to varying degrees. This section explains how the network extension activities supported each objective and contributed to the tasks as described in the project proposal.

OB1: **To enrich the existing network countering hybrid threats and ensure long term sustainability.** The network extension supported this objective, especially regarding Goal 1.1: *To identify potential members of the network that have demonstrated concerns/appreciation for dangers associated with proliferation of hybrid threats and encourage them to join the network and engage in its activities*.

In order to reach the KPI target value of accepting at least 30 new members to the network each year, and for the purpose of finding suitable new network members, the project frequently consulted its relevant stakeholders and analysed the network on a monthly basis to verify how capable the current network was at responding to the project's four core themes and the 13 hybrid threat domains under focus. This enabled an understanding of what type of organisations and stakeholders the project would seek to integrate into the network.

OB2: **To define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats.** The network extension supported this objective by ensuring that the new members represented a distinct field of European comprehensive security, and that their expertise was relevant to the work already ongoing or planned in the project. This ensured that the insights gathered in the project represented the views of current, relevant actors, contributing to Goal 2.3, which is *to gather and define insights from European practitioners, industry, SME and academic actors on future trends.*

OB3: **To monitor developments in research and innovation activities as applied to hybrid threats**. This objective was supported by the network extension, as new members to the network represented relevant actors with demonstrated work on hybrid threat topics. All members were encouraged to participate in research in order to ensure that the outputs of the project covered the most significant developments and contemporary issues deemed relevant to European practitioners, industry, SME and academic actors, as per Goals 3.1 and 3.2 (*to monitor significant developments in research areas and activities in order to define and recommend solutions for European actors; to monitor significant developments in technology that will lead to recommending solutions for European actors' gaps and needs*). The inclusion of new members in the project's research activities and structured work within the core themes supported the KPIs of producing at least 8 reports every 18 months that addressed research findings and technological innovations.

OB4: **To indicate priorities for innovation uptake and industrialization and to determine priorities for standardization for empowering the Pan-European network to effectively counter hybrid threats**. In a similar fashion to OB3, the network extension supported the indication of priorities in innovation uptake and industrialization by ensuring that the new network members represented relevant areas, including the private sector. This supported reaching Goal 4.1, which was *to compile recommendations*

for uptake and industrialisation of innovation outputs (incl. social/non-technical). A variety of actors were included in the network to enable the output of both technical and social innovations. New members were invited to join the discussion and contribute to the work towards policy recommendations at the end of each of the four project cycles. The KPI was to write at least seven policy briefs over five years for both wider audiences and policy makers, and this was achieved.

OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network.

The extension of the network and its sustainable existence is grounded in the fact that after the project's completion, the Hybrid CoE (The European Centre of Excellence for Countering Hybrid Threats) will host the network and prior the project completion, will create a detailed roadmap for the activities necessary to increase membership and to ensure its sustainability. The continuous application process throughout the project worked towards Goal 5.1 (*to establish platforms for innovation exchange*) and supported the work to reach the KPI of at least 30 new stakeholder group members joining the network each year, and specifically, joining the Innovation Arena platform.

OB6: To foster capacity building and knowledge exchange on countering hybrid threats.

The network extension served the purpose of fulfilling the Goal 6.4 under this project objective: *to empower European practitioners, industry, SME and academic actors' capacity to counter hybrid threats by offering relevant trainings and materials*. Being an EU-HYBNET network member provided these actors with a chance to increase their own capacities to counter hybrid threats. This was achieved through the Gaps and Needs events, other project events, through trainings and exercises and by collaborating with consortium members in writing articles. Network members also have had access to background materials, as well as the opportunity to participate in knowledge exchange using the Innovation Arena and working area TUOVI.

OB7: To create basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats.

The EU-HYBNET network extension supported all goals under this specific project objective. It worked towards identifying relevant stakeholders, who were invited to share information in the training event and to benefit from online training material (Goal 7.1). It also empowered European actors to recognize innovations and trends by supporting the focus of new potential members, that they be relevant, motivated, and able to attract other new network members (Goal 7.2). The project supported the establishment of links with other European networks and missions in related fields of interest by defining the ability to attract new members as one of the criteria for the new members (Goal 7.3). It supported informing EU Member States' (MS) national policymaking bodies (Goal 7.4) by ensuring that different actors and relevant policy practitioners were invited and accepted into the network. Finally, the network extension facilitated the creation of a wide network of European stakeholders (Goal 7.5) by focusing on the four core project themes, under which network members were offered opportunities to contribute to project work.

3. THE EUROPEAN COMMISSION'S REQUESTED IMPROVEMENTS TO THE NETWORK EXTENSION AND ACTIONS TAKEN BY THE CONSORTIUM

3.1. RESULTS BASED ON REQUESTED IMPROVEMENTS AFTER THE EUROPEAN COMMISSION'S FIRST AND SECOND REVIEWS

The first EU-HYBNET project review by the European Commission (EC) took place in September 2021, where it was suggested that the number of participants in project events should be higher, the network should be enhanced and broadened, and the project should work to build a common understanding of hybrid threats and how they could be countered. It was further suggested that analysis be conducted on where membership was lacking. Concrete actions were undertaken to address these suggestions, as outlined in previous reports at length. Of note was the encouragement for consortium partners to support the network extension and to arrange tailored events aimed at certain types of network member groups, as this continued throughout the rest of the project's duration.

The second project review occurred in November 2022. The EC noted that although attendance at events had been good, there should be greater awareness as to the difference between registered participants and actual participants to the events. Further, it was also suggested that the project evaluate the activity of network members and remove inactive members. To address the suggested improvements from the second review, as well as to continue to address those from the first review, consortium partners reached out to relevant entities in EU Member States who could be interested in the project. The consortium also organized a social media campaign to increase the visibility of the project and to further support the network extension. Finally, the consortium worked to increase the involvement of network members in project work, such as by the co-authoring of research articles under T2.2.

Despite the actions taken, the KPI to reach 30 new network members yearly has been difficult to achieve. Especially since 2023, there has been a lower number of applications to the network. However, the growth of the network was still significant each year, attendance to the events was satisfactory, and collaboration strengthened between consortium partners and network members, which strengthened the EU-HYBNET network as a whole.

3.2. THE EUROPEAN COMMISSION'S REQUESTED IMPROVEMENTS IN THE THIRD PROJECT REVIEW

After the third EC review of the EU-HYBNET project on 27 February 2024, the EC suggested two improvements pertaining to network extension:

- The project should continue to widen and deepen the network, focusing especially on getting new network members from Denmark, Malta, and Estonia.
- The project could focus not only on interactions between network members, but the internal happenings of network members.

3.2.1. ACTIONS TAKEN ON REQUESTED IMPROVEMENTS AFTER THE THIRD REVIEW

The consortium has continued to pursue the improvements suggested by the EC after all three project reviews. Regarding the third review in particular, the consortium took the following measures under T1.3:

1. Actions to increase the number of participants in the project events, such as increased communication about events and personal outreach to potential participants.
2. Outreach to relevant entities in Member States and additional participants from industry to SMEs, as well as outreach through existing network members.
3. Continual analysis of where network membership is lacking alongside targeted efforts to reach out to identified organisations that could be interested in network membership.
4. Hosted a dedicated workshop with two EU-HYBNET network members as a side-event to the project's 3rd Innovation Standardization Workshop in autumn 2024.
5. Hosted a webinar to showcase the work of an EU-HYBNET network member in April 2025.

EU-HYBNET network members have remained engaged in project activities and were invited to all EU-HYBNET project events, as well as occasionally to other events organised by consortium partners. Outreach continued to potential network members in Denmark, Malta and Estonia, as well as to other relevant organisations in other countries. Collaboration between existing network members continued and resulted in tangible outcomes, such as research articles, for instance. The project successfully hosted a thought-provoking workshop with EU-HYBNET network members Traversals and Maltego in October and Brussels, which demonstrated the benefits of collaboration within the network, and which was well-received by event participants. In April 2025, the project facilitated a webinar where network member Logically, an AI-company based in the United Kingdom, presented its work on information threats posed by foreign actors, namely Russia and China. These kinds of events helped to strengthen network bonds and increase knowledge exchange amongst project participants. They also support the EC's request to pay more attention to the internal happenings of network members.

3.2.2. RESULTS BASED ON THE ACTIONS TAKEN

During this final reporting period, the number of applications to the EU-HYBNET network decreased, likely due to the project's impending conclusion, and the KPI target to reach 30 new network members yearly was not reached. Further, no new network members joined the project from the countries lacking them – Denmark, Estonia, and Malta. As in previous years, the consortium also rejected those applicants who do not meet the eligibility criteria set at the beginning of the project.

Between April 2024 and April 2025, the EU-HYBNET network grew by 23 new network members. T1.3 has ensured the network represents a wide variety of stakeholders: new members include 2 national or local level practitioners, 10 research and/or education institutions, 3 NGOs, and 8 SMEs from 9 countries. With the new members, the network consists of 25 consortium partners and 136 Network Members from 27 countries, out of which 30 are practitioners, 49 research and/or education institutions, 24 NGOs, and 33 SMEs. At the end of April 2025, the final EU-HYBNET network includes a total of 161 members (consortium partners, stakeholder group members, and new network members).

As the project approached its conclusion, the EC acknowledged in their third review that the project itself and the network it has built have worked to contribute to awareness about hybrid threats in

Europe, which did not exist when the project began. During this final reporting period, network members remained engaged and active in the project and expressed interest in maintaining synergies with each other beyond the project's conclusion and even independently of any formally arranged mechanisms.

4. SELECTION PROCESS

The selection process is described in detail in D1.7, *The eligibility criteria of the new network members*. The basic principles were as follows:

- All of the applicants had to apply using the application form which was accessible via the official EU-HYBNET website, where the accession criteria are also shared: https://euhybnet.eu/join-the-network/. All applicants had to submit this form, even if they had been in contact with project partners via other means, or if they were EU organisations and thus eligible for membership automatically.
- Entities from otherwise eligible non-EU countries with which the EU has not entered into an agreement on the security procedures for the exchange of classified information were not considered eligible to join the EU-HYBNET network. This condition was added to the eligibility criteria of new network members in January 2022 at the project's Executive Board meeting.
- The Hybrid CoE (network extension, task 1.3, leader) and the EU-HYBNET Project Management Board discussed all applications and together made the decisions over silent approval procedure during the week after the talks.
- Consortium Partners were informed about the outcome of the talks, and pursuant to the EU-HYBNET Description of Action, the Consortium Partners could take part in the silent approval procedure over the selected applicants. They could break silence if they did not agree with the application results.
- Successful applicants were notified by the Network Manager upon their acceptance of the relevant minutes of the accession talks or upon further actions. As a sign of acceptance and membership, the new members were then given access to the Innovation Arena and TUOVI platform and were informed on proceedings of EU-HYBNET. T1.3. leader and the Laurea Network Manager held regular welcome briefs for new network members.

5. NEW MEMBERS TO THE EXTENDED NETWORK

As the result of the accession talks between Hybrid CoE and the Project Management Board, the following organisations were accepted to the EU-HYBNET network during the D1.23 reporting period, that is, project months M48-M60/April 2024-April 2025:

	Name	Country	Type of organisation
	Prosegur Research	Spain	SME/Industry
	OPEWI	Belgium	Academia
	EFE Verifica – Agencia EFE	Spain	SME
	Universidad Cardenal Herrera CEU	Spain	Academia
	Universidad Internacional de Valencia (VIU)	Spain	Academia
	Fraunhofer FOKUS	Germany	Academia
	Seeders	Greece	SME
	Center for East European Policy Studies (CEEPS)	Latvia	NGO
	GraphAware	UK	SME
	Foreign Affairs Institute (FAINST)	Greece	NGO
	University of Turku	Finland	Academia
	Vilnius City Municipality Administration	Lithuania	Practitioner
	Home Office	UK	Practitioner
	International Republican Institute (IRI) Europe ASBL	Belgium	NGO
	Logically	UK	SME
	Ghent University BIGDATPOL	Belgium	Academia
	The Elcano Royal Institute for International and Strategic Studies	Spain	Academia
	Center of Excellence for Police and Security Research (CEPOLIS) at the Bavarian Police Academy	Germany	Academia
	Turku Ammattikorkeakoulu	Finland	Academia
	Kyiv Institute of the National Guard of Ukraine	Ukraine	Academia
	EU DisinfoLab	Belgium	NGO
	European Foundation for Democracy	Belgium	NGO

Table 1: New members to the EU-HYBNET network

Please note that the above-listed organisations gave their consent to be listed as a public member of the EU-HYBNET network.

5.1. NETWORK

The new members have been added to the already existing network that consists of consortium partners and EU-HYBNET Stakeholder Group members.

The following organisations formed the initial EU-HYBNET network in 2020:

	Name	Country	Type of organisation
	Ardanti! Defence	France	Industry, SME
	CeSI - Centro Studi Internazionali	Italy	Research organisation
	CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)	Spain	Research organisation
	Expertsystem	Italy	SME
	European Security and Defence College	EU	Research organisation
	European Health Management Association (EHMA)	EU	NGO
	Finnish Border Guard	Finland	Practitioner
	Fraunhofer-IVI	Germany	Research organisation
	Ministry of Justice and Security in the Netherlands	The Netherlands	Practitioner
	Ministry of the Interior Finland	Finland	Practitioner
	SafeCluster	France	Research organisation
	Sopra steria	France	Industry
	Systematic	France	Industry
	Tecnoalimenti	Italy	Research organisation
	Tromsø Police District, Norway	Norway	Practitioner
	Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence	Ukraine	Research association
	Laurea University of Applied Sciences	Finland	Research organisation
	Polish Platform for Homeland Security, PPHS	Poland	Practitioner
	University of Tromsø, UiT	Norway	Research organisation
	Research Institutes of Sweden AB, RISE	Sweden	Research organisation
	Kentro Meleton Asfaleias, KEMEA	Greece	Research organisation
	Lithuanian Cybercrime Centre of Excellence, L3CE	Lithuania	Research organisation
	Rey Juan Carlos University, URJC	Spain	Research organisation

	Ministry for an Ecological and Solidary Transition, MTES	France	Practitioner
	European Organisation for Security, EOS	Belgium	NGO
	Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO (RTO)	The Netherlands	Research organisation
	SATWAYS	Greece	SME
	City of Espoo	Finland	Practitioner
	Universita Cattolica del Sacro Cuore	Italy	Practitioner
	European Commission Joint Research Centre, JRC	Belgium	Research organisation
	The "Mihai Viteazul" National Intelligence Academy, MVNIA	Romania	Research organisation
	The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE	Finland	NGO
	Ministry of Defence	The Netherlands	Practitioner
	International Centre for Defence and Security, ICDS	Estonia	Research organisation
	Valencia Local Police	Spain	Practitioner
	Polish Internal Security Agency, ABW	Poland	Practitioner
	Norwegian Directorate for Civil Protection, DSB	Norway	Practitioner
	Estonian Information Authority Systems	Estonia	Practitioner
	Maldita (Organisation)	Spain	NGO
	Central Office for Information Technology in the Security Sphere, Zitis	Germany	Practitioner
	Bundeswehr University, COMTESSA	Germany	Research organisation

Table 2: EU-HYBNET initial network members

5.1.1. NETWORK MEMBERS IN EU COUNTRIES

	Country	**Name of the organization**	**Type of the organisation**
1.	Austria	**European Institute for Counter Terrorism and Conflict Prevention**	Research organisation
2.	Austria	**HENSOLDT Analytics**	SME
3.	Austria	**CIN Consult GmbH**	Practitioner
4.	Belgium	**European Organisation for Security, EOS**	NGO
5.	Belgium	**European Commission Joint Research Centre, JRC**	Research organisation

6.	Belgium	**European Security and Defence College (ESDC)**	Research organisation
7.	Belgium	**European Health Management Association (EHMA)**	Research organisation
8.	Belgium	**G4S**	Industry
9.	Belgium	**Beyond the Horizon ISSG**	NGO
10.	Belgium	**Friends of Europe**	NGO
11.	Belgium	**Vesalius College VZW, part of the Brussels School of Governance and Vrije Universiteit Brussel (VUB)**	Research organisation
12.	Belgium	**Hybrid Core BV**	SME
13.	Belgium	**Stad Geel**	Practitioner
14.	Belgium	**OPEWI**	Academia
15.	Belgium	**Ghent University BIGDATPOL**	Academia
16.	Belgium	**International Republican Institute (IRI) Europe ASBL**	NGO
17.	Belgium	**EU DisinfoLab**	NGO
18.	Belgium	**European Foundation for Democracy**	NGO
19.	Bulgaria	**Bulgarian Defence Institute**	Research organisation
20.	Croatia	**EFFECTUS - Entrepreneurial Studies - University College**	Research organisation
21.	Croatia	**Hybrid Warfare Research Institute**	NGO
22.	Croatia	**University of Dubrovnik**	Research organisation
23.	Czechia	**European Values Centre for Security Policy**	NGO
24.	Czechia	**National Counterterrorism, Extremism and Cybercrime Agency**	Practitioner
25.	Cyprus	**CyberEcoCul Global Services**	SME
26.	Estonia	**International Centre for Defence and Security, ICDS**	Research organisation
27.	Estonia	**Estonian Information Authority Systems**	Practitioner
28.	Finland	**Geostrategic Intelligence Group (GIG) Ltd**	SME
29.	Finland	**Finnish Border Guard**	Practitioner
30.	Finland	**Ministry of the Interior Finland**	Practitioner
31.	Finland	**Laurea University of Applied Sciences**	Research organisation
32.	Finland	**City of Espoo**	Practitioner
33.	Finland	**The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE**	NGO
34.	Finland	**Avoin yhteiskunta ry**	NGO

35.	Finland	**Police University College (fin: Poliisiammattikorkeakoulu)**	Research organisation
36.	Finland	**University of Turku**	Academia
37.	Finland	**Turku Ammattikorkeakoulu**	Academia
38.	France	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	Practitioner
39.	France	**Ardanti! Defence**	Industry, SME
40.	France	**SafeCluster**	Research organisation
41.	France	**Sopra steria**	Industry
42.	France	**Expertsystem**	
43.	France	**Systematic**	Industry
44.	France	**Ministry for an Ecological and Solidary Transition, MTES**	Practitioner
45.	France	**Euclid Institute**	NGO
46.	France	**INSTITUT CHOISEUL**	Research organisation
47.	France	**SIGNALERT SARL**	SME
48.	Greece	**S**ATWAYS	
49.	Greece	**Kentro Meleton Asfaleias (KEMEA)**	Research organisation
50.	Greece	**Information Technologies Institute / Centre for Research and Technology Hellas (CERTH/ITI)**	Research organisation
51.	Greece	**FORTH - Foundation for Research and Technology - Hellas - Institute of Computer Science**	Research organisation
52.	Greece	**Seeders**	SME
53.	Greece	**Foreign Affairs Institute (FAINST)**	NGO
54.	Germany	**Cyber - and Information Domain Service HQ**	Practitioner
55.	Germany	**Fraunhofer-IVI**	Research organisation
56.	Germany	**Central Office for Information Technology in the Security Sphere, Zitis**	Practitioner
57.	Germany	**Bundeswehr University, COMTESSA**	Research organisation
58.	Germany	**Maltego Technologies GmbH**	SME
59.	Germany	**Marshall Center**	Research organisation
60.	Germany	**Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg**	Research organisation
61.	Germany	**Traversals Analytics and Intelli-gence GmbH**	SME
62.	Germany	**Fraunhofer FOKUS**	Academia

63.	Germany	**Center of Excellence for Police and Security Research (CEPOLIS) at the Bavarian Police Academy**	Academia
64.	Hungary	**DataSenseLabs Ltd.**	SME
65.	Ireland	**UCD Centre for Cybersecurity and Cybercrime Investigation**	Academia
66.	Italy	**Enea**	Practitioner
67.	Italy	**CeSI - Centro Studi Internazionali**	Research organisation
68.	Italy	**Tecnoalimenti**	Research organisation
69.	Italy	**Universita Cattolica del Sacro Cuore**	Practitioner
70.	Italy	**Fondazione SAFE - Security and Freedom for Europe**	NGO
71.	Italy	**CRIMEDIM - NO-FEAR Project**	Research organisation
72.	Italy	**SAPIENZA University of Rome - Department of Human Neuroscience - Interpersonal Violence Research Lab (InterViRe)**	Research organisation
73.	Latvia	**Baltic Centre for Media Excellence**	NGO
74.	Latvia	**Center for East European Policy Studies (CEEPS)**	NGO
75.	Lithuania	**Vilnius Institute for Policy Analysis**	NGO
76.	Lithuania	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Research organisation
77.	Lithuania	**Vilnius City Municipality Administration**	Practitioner
78.	Luxembourg	**Ministry of Foreign and European Affairs, Directorate of Defence**	Practitioner
79.	Luxembourg	**DG SAFE/European Parliament**	NGO
80.	The Netherlands	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Practitioner
81.	The Netherlands	**Ministry of Justice and Security in the Netherlands**	Practitioner
82.	The Netherlands	**Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO**	Research organisation
83.	The Netherlands	**Ministry of Defence**	Practitioner
84.	The Netherlands	**Faculty of Military Sciences**	Research organisation
85.	The Netherlands	**The Hague Centre for Strategic Studies**	SME
86.	The Netherlands	**Ministry of Foreign Affairs**	Practitioner
87.	The Netherlands	**Ridgeway Information EU B.V**	SME
88.	The Netherlands	**Tilt**	Practitioner
89.	The Netherlands	**ISR Nederland BV**	SME

90.	Poland	**Polish Platform for Homeland Security, PPHS**	Practitioner
91.	Poland	**Polish Internal Security Agency, ABW**	Practitioner
92.	Poland	**Academic Centre for Strategic Communication**	Research organisation
93.	Poland	**National Police Headquarters**	Practitioner
94.	Poland	**Government Centre for Security**	Practitioner
95.	Poland	**The Kosciuszko Institute Association**	NGO
96.	Poland	**Demagog Association**	NGO
97.	Poland	**Ministry of Foreign Affairs of Poland**	Practitioner
98.	Poland	**Polish Association for National Security – PTBN**	NGO
99.	Poland	**The Polish Financial Supervision Authority**	Practitioner
100.	Portugal	**VOST Portugal**	NGO
101.	Portugal	**Polytechnic Institute of Setubal - School of Technology**	Academia
102.	Romania	**Enersec Technology**	SME
103.	Romania	**Smartlink Communications**	SME
104.	Romania	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Research organisation
105.	Romania	**Romanian Ministry of Economy, Entrepreneurship and Tourism**	Practitioner
106.	Romania	**Mira Technologies Group SRL**	SME
107.	Romania	**New Strategy Center**	NGO
108.	Romania	**Center for the study of democracy**	Academia
109.	Romania	**Safetech INNOVATIONS SA**	SME
110.	Romania	**Zetta Cloud**	SME
111.	Romania	**Carol I National Defence University**	Academia
112.	Romania	**Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering "Traian Lalescu"**	Academia
113.	Romania	**National Cybersecurity Directorate**	Academia
114.	Romania	**GREENSOFT SRL**	SME
115.	Slovakia	**GLOBSEC**	NGO
116.	Slovakia	**National Security Authority**	Practitioner
117.	Slovakia	**Presidium of Police Force**	Practitioner
118.	Slovakia	**Ministry of Interior of the Slovak republic**	Practitioner
119.	Slovakia	**National Security Analytical Centre (NBAC)**	Practitioner
120.	Slovakia	**Strategic Analysis**	NGO

121.	Spain	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Research organisation
122.	Spain	**Rey Juan Carlos University, URJC**	Research organisation
123.	Spain	**Valencia Local Police**	Practitioner
124.	Spain	**Maldita (Organisation)**	NGO
125.	Spain	**Universidad Isabel I de Castilla**	Research organisation
126.	Spain	**DLT Code**	SME
127.	Spain	**SECURE IDENTITY TECHNOLOGIES SL (IDBOTIC)**	NGO
128.	Spain	**Correcta**	SME
129.	Spain	**Prosegur Research**	SME
130.	Spain	**EFE Verifica – Agencia EFE**	SME
131.	Spain	**Universidad Cardenal Herrera CEU**	Academia
132.	Spain	**The Elcano Royal Institute for International and Strategic Studies**	Academia
133.	Sweden	**NORSECON**	SME
134.	Sweden	**Research Institutes of Sweden AB, RISE**	Research organisation
135.	Sweden	**Sectyne AB**	SME
136.	Sweden	**Swedish Police Authority/ National Forensic Centre**	Practitioner
137.	Sweden	**Combitech AB**	Industry
138.	Sweden	**Risk and Crisis Centre Mid-Sweden University**	Academia

Table 3: EU-HYBNET network members from EU Countries

Please note that the above-listed organisations provided their consent to be listed as a public member of the EU-HYBNET network. Other network member organisations that did not do so are therefore not listed here or in the following section.

5.1.2. NETWORK MEMBERS IN EU ASSOCIATED THIRD COUNTRIES

	Country	**Name of the organization**	**Type of the organization**
139.	Georgia	**LEPL Cyber Security Bureau under the Ministry of Defence of Georgia**	Practitioner
140.	Georgia	**Defence Institution Building School**	Research organisation
141.	Georgia	**Office of the National Security Council of Georgia**	Practitioner
142.	Georgia	**The School of Social Sciences (of the University of Georgia - UG)**	Research organisation

143.	Norway	**University of Tromsø**	Research organisation
144.	Norway	**Norwegian Directorate for Civil Protection, DSB**	Practitioner
145.	Norway	**Tromso Police District Tromso**	Practitioner
146.	Norway	**Nord University**	Research organisation
147.	Norway	**SINTEF Digital, Dept. of Software Engineering, Safety and Security**	Research organisation
148.	Ukraine	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	Research organisation
149.	Ukraine	**State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"**	Research organisation
150.	Ukraine	**Institute of Legal Personnel Training for the Security Service of Ukraine Yaroslav Mudryi National Law University**	Academia
151.	Ukraine	**Kyiv Institute of the National Guard of Ukraine**	Academia
152.	United Kingdom	**GraphAware**	SME
153.	United Kingdom	**Home Office**	Practitioner
154.	United Kingdom	**Logically**	SME

Table 4: EU-HYBNET network members from EU Associated Countries

6. PROJECT COMPLETION

The EU-HYBNET project officially comes to an end in April 2025, after five years of events, activities and network-building. Applications to the extended EU-HYBNET network were open until the end of February 2025 (M58), to allow for the Project Management Board and Hybrid CoE to process and screen all applications before the end of the project.

Hybrid CoE is to host the network after the project ends. The plan remains largely as described in D1.24 *EU-HYBNET Network Sustainability Initial Report (M30)*, but the newest version is the one to be relied upon: D1.25 *EU-HYBNET Network Sustainability Final Report (M60)*. At the time of writing, D1.25 is forthcoming. As stated previously, during the transition process, Hybrid CoE reserves the right to re-review and re-screen the network members as well as to deny accession in cases where the given network member has been inactive or demonstrated a lack of competence during the project. This initiative also responds to the recommendation given by the EC after the second periodical review.

At the time of the project's completion in April 2025, the EU-HYBNET network encompasses a strong, vibrant community of organisations dedicated to countering hybrid threats and increasing the EU's abilities in doing so. Over the past five years, the project has seen numerous innovative ideas, important research on a wide range of hybrid threat topics, fundamental network-building, and thought-provoking events and trainings that were all crucial to the project's success. The insights, ideas, and bonds created in the project will last long beyond the project's completion in 2025.

ANNEX I. GLOSSARY AND ACRONYMS

Table 4: Glossary and acronyms

Term	Definition / Description
ABW	Polish Internal Security Agency
AC	Associated Countries
AIT	Austrian Institute of Technology
B.V	Besloten vennootchap (Private limited company)
KPI	Key performance indicator
OB	Objectives
WP	Work Package
CA	Consortium Agreement
CeSI	Centro Studi Internazionali
CSIC	Spanish National Research Council
T	Task
D	Deliverable
DG SAFE	Directorate-General for Security and Safety
DoA	Description of Action
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
EC	European Commission
EOS	European Organisation for Security Scrl
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
EU-HYBNET	Pan-European Network to Counter Hybrid Threats
EHMA	European Health Management Association
FTW	Future Trends Workshop
FORTH	Foundation for Research and Technology Hellas – Institute of Computer Science
GIG	Geostrategic Intelligence Group Ltd
GmbH	Gesellschaft mit beschränkter Haftung (Limited Liability company)
Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Centre of Excellence for Countering Hybrid Threats
Hybrid Core BV	Hybrid Core is a decision tech firm that develops a hybrid AI decision support system for smarter digital decisions by organizations
HQ	Headquarters
IA	Innovation Arena
IAI	Istituto Affari Internazionali
ICDS	International Centre for Defence and Security, Estonia
IRSEM	Institut de recherche stratégique de l'Ecole militaire (Institute for Strategic Research)

JFCBS	NATO HQ JOINT FORCE COMMAND BRUNSSUM
JRC	JRC - Joint Research Centre - European Commission
KEMEA	Kentro Meleton Asfaleias
KPI	Key Performance Indicator
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
LAUREA	Laurea-ammattikorkeakoulu Oy
LEPL	Cyber Security Bureau under the Ministry of Defence Georgia
LTD	Limited
M	Month
MALDITA	MALDITA
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
NGO	Non-Governmental Organization
NBAC	National Security Analytical Centre
NLD MoD	Ministry of Defence/NL
OB	Project Objective
PLV	Ayuntamiento de Valencia / Valencia Local Police
PMB	EU-HYBNET Project Management Board
PPHS	Polish Platform for Homeland Security
PTBN	Polish Association for National Security
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
RISE	RISE Research Institutes of Sweden Ab
RTO	University of Turku, Department of Future Technologies, Finland - third linked party to Laurea
SATWAYS	SATWAYS
SME	Small- and Medium-sized Enterprise
SRL	Società a responsabilità limitata (Limited Liability Company)
T	Task
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
UCSC	Universita Cattolica del Sacro Cuore
UiT	Universitetet i Tromsoe
UniBW	Universitaet der Bundeswehr München
URJC	Universidad Rey Juan Carlos
WP	Work Package
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
PU	Public

NoP	Network of Practitioners

ANNEX II. REFERENCES

[1] European Commission Decision C (2014)4995 of 22 July 2014.

[2] Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.