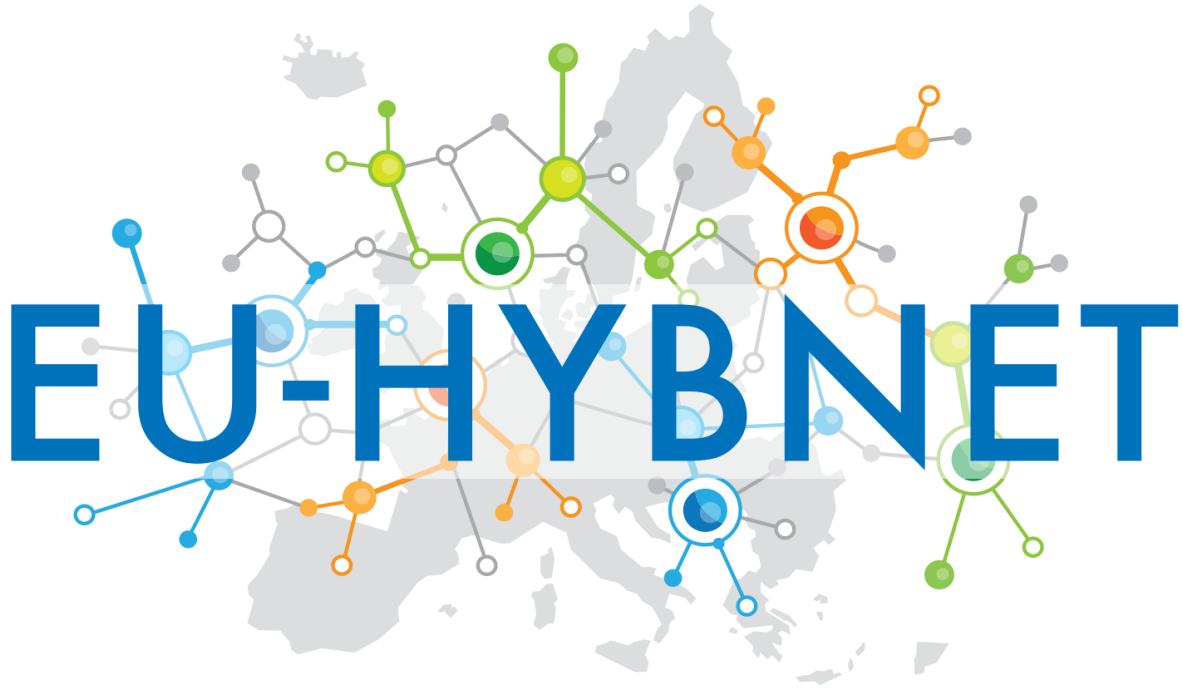

LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

DELIVERABLE 1.22

Lead Author: Hybrid CoE

Contributors: LAUREA, PLV
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	**1.22**	
Version:	**V1.0**	
Delivery date:	**28/3/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Hanne Dumur-Laanila**	**Hybrid CoE**
Contributors:	**Päivi Mattila, Jari Räsänen**	**LAUREA**
	Valencia Local Police (PLV) team	**PLV**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	06/03/2024	Hanne Dumur-Laanila/ Hybrid CoE	First draft
0.2	07/03/2024	Hanne Dumur-Laanila/ Hybrid CoE	Editing
0.3	12/03/2024	Hanne Dumur-Laanila/ Hybrid CoE	Section 5. updated; editing section 3.
0.4	17/03/2024	Jari Räsänen/ Laurea	Review and comments
0.5	18/03/2024	Hanne Dumur-Laanila/ Hybrid CoE	Editing
0.6	25/03/2024	Päivi Mattila/ Laurea	Review
0.7	26/03/2024	PLV team/ PLV	Review
0.8	27/03/2024	Hanne Dumur-Laanila/ Hybrid CoE	Final Editing, ready D1.22
1.0	28/03/2024	Päivi Mattila/ Laurea	Final review and submission of D1.22

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 is one of its core values. 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 and beyond the European Union: practitioners, members from industry, small and medium-sized enterprises, academia, NGOs, and other actors relevant to counter hybrid threats in the EU and the EU Associated Countries (AC)[1].

When the project started, the network consisted of 25 consortium partners and 16 stakeholder group organisations (table 2). The network has been designed to expand annually with at least 30 new members.[2] Although the network has continued to grow steadily over the past years, the fourth round of selection has faced some difficulties finding new applicants to the network. In order to reach out the gap to meet the KPI with at least 30 new network members annually, the consortium took new actions to increase the number of applicants. These actions are further explained in section 3. "The European Commission's requested improvements to the network and actions taken by the consortium." The consortium will continue to identify ways how to increase the number of applications. Special focus is to reach out new members from the following fields: security practitioners, SMEs, industry and NGOs. The project will also look for new potential members from the missing EU countries. The work on analysing where membership is lacking is conducted on a monthly basis by Laurea Network Manager.

At current stage (M 46), together with consortium partner and stakeholders, the network consist of 37 practiotioners; 27 industry/SME organizations; 21 NGO's and 50 organizations are representing academia/research organisations. In total, network has 138 organisations, including consortium partners and stakeholders.

In addition to listing new members to the network between M36 (April 2023) – M46 (March 2024), this deliverable (D) 1.22, *List of new actors to the extended EU-HYBNET network*, also considers the suggested improvements by EC after the first and second reviews, actions taken, and future work. The application and selection are both ongoing processes. The deliverable is published yearly and will cover the members that are accepted by the end of April in years 2021, 2022, 2023, 2024, and April in 2025.

The growth of the network is a significant driver of the project content. The extended EU-HYBNET network is a group of stakeholders, who are invited to contribute to the project tasks on voluntary basis. The input from extended network members in Gaps and Needs Workshop[3] forms the starting point for project proceedings in each project cycle. The mapped gaps and needs are specifically those

[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.*
[3] The workshop objectives are described in detail in Deliverable 2.3, *Gaps and Needs Workshop.*

of the extended network members, and the project outcomes – research, exercises, innovation mapping and finally recommendations for policy and procurement – reflect the workshop results. The network members are the main contributors of the project platforms Innovation Arena and TUOVI, where ideas and challenges are also mapped. In each cycle, network members are invited to EU-HYBNET events, such as Annual Workshop, Future Trends Workshop and other relevant events, where identified gaps and needs will be addressed by testing the promising innovations and other measures to counter hybrid threats. Furthermore, network members are invited to all EU-HYBNET open events and to cooperate in research and writing of articles.

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

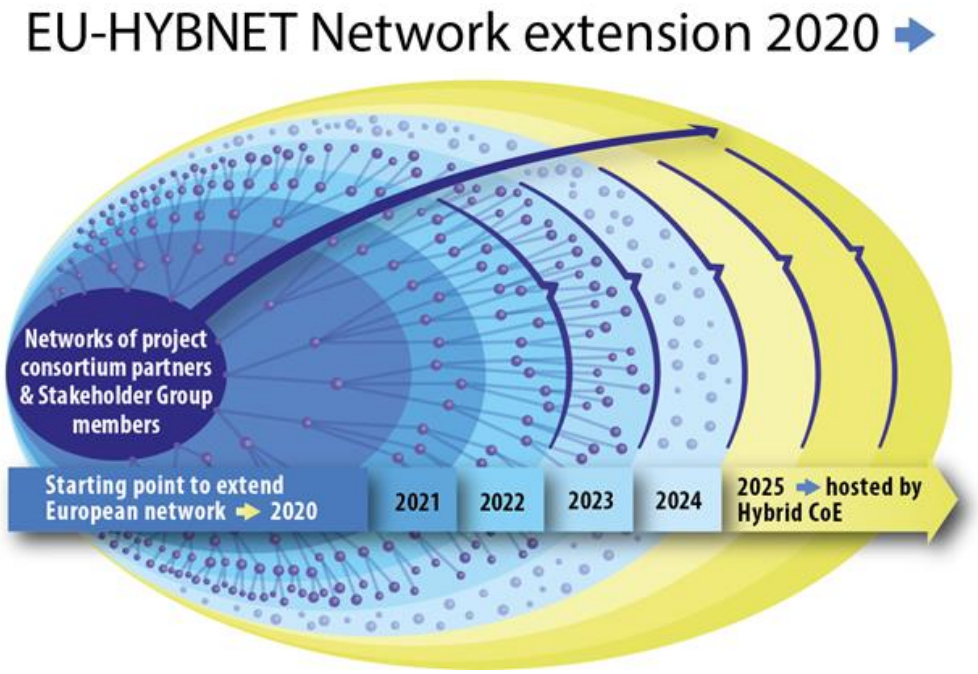

Figure 1: EU-HYBNET network extension 2020-2025

1.2. STRUCTURE OF THE DELIVERABLE

This document has six sections:

- The first section provides an introduction to the D1.22 and highlights its core content.
- The second section describes the **objectives** and key performance indicators (KPI) that have been defined for the network extension, and how they are treated in the project as per EU-HYBNET

[4] The network extension process is covered in more detail in Deliverable 1.7, *Definition of the eligibility criteria for new actors.*

Deliverable (D)1.7 “Definition of the eligibility criteria for new actors” and D1.24 “EU-HYBNET Network Sustainability Plan”.

- 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 list of network members as a whole.
- The sixth part provides description of future work.

2. NETWORK EXTENSION OBJECTIVES

2.1. PROJECT OBJECTIVES AND KEY PERFORMANCE INDICATORS

The network extension **contributes to all seven project objectives (OB)** with varying emphasis. This chapter explains how it supports each objective and performs 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 supports this objective aiming especially towards 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 key performance indicator (KPI) target value of accepting at least 30 new members to join EU-HYBNET network yearly, and for the purpose of finding suitable new network members, the project continuously consults all its relevant stakeholders as well as analyses the network monthly for being aware how the network responses to the project's four core themes and 13 domains under discussions. This supports the understanding of what is the type of the stakeholders that the project welcomes to the network. Listing the new members is important as the desired scope of stakeholders is very wide.

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 supports this project objective by ensuring that the new members represent a distinct field of the European comprehensive security, and they must be relevant for work that is already done or planned for countering hybrid threats. This ensures, that the insights that the project gathers represent the views of current and relevant actors from a wide range of security and industry, 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**. The network extension supports also this objective, as new members represent relevant actors and have done work in the framework of hybrid threats. The new members will be encouraged to participate in research, in order to ensure that the reports cover the most significant developments and contemporary issues relevant to the 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 to the research activities and structured work in the core themes support the KPIs of producing at least 8 reports every 18 months that address 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 the similar fashion to the project objective 3, the network extension supports indication of priorities in innovation uptake and industrialization by ensuring that the new members represent relevant areas, including private sector. This supports reaching the Goal 4.1, which is to compile recommendations for uptake/industrialisation of innovation outputs (incl. social/non-technical). Variety of actors are included the network to enable the output of both technical and social innovations. The new members are invited to join the discussion and contribute to the work towards policy recommendations in the end of each of the four project cycles (KPI: at least 7 policy briefs over 5 years for wider audiences and policy makers).

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 continue to host the network and make use of its platforms, which will ensure that network activities will be able to sustain a long-lasting impact. The continuous application process works towards Goal 5.1 (*to establish platforms for innovation exchange*) by ensuring that the KPI of at least 30 new Stakeholder Group members joining to the Innovation Arena yearly.

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

The network extension serves 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 member will mean that these actors will have a chance to build their own capacity to counter hybrid threats, as they are invited to gaps and needs events and exercises. The new network members will be invited to the events, and they will have access to the background materials, as well as the opportunity to participate in developing both via 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 network extension supports all goals under this project objective. It works towards identifying the relevant stakeholders, who are invited to share information in the training event and to benefit from the online training material (Goal 7.1). It also empowers European actors to recognise innovations and trends by supporting the focus of new potential members – they are relevant, motivated, and able to attract again new relevant network members (Goal 7.2). It supports the work towards establishing links with other European Networks and missions in related fields of interest by defining ability to attract new members as one of the criteria for the new members (Goal 7.3). It supports informing EU MS national policymaking bodies (Goal 7.4) by ensuring that different actors and also policy relevant practitioners will be invited and accepted in the network. Finally, it supports creating the wide network of European stakeholders (Goal 7.5) by paying attention to the four core themes, under which the new members will be organised and offered opportunities to lead and work in sub-themes in the growing network.

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 REVIEW

After the first European Commission (EC) EU-HYBNET project review in September 2021, the EC suggested a number of improvements to EU-HYBNET's community extension. The review stated that the number of participants in project events should be higher, the network should be further enhanced and broadened - including relevant entities in Member States and additional participants from industry and SMEs - and the project should buttress the cohesion of the network by building a common understanding of the aim in countering hybrid threats. Furthermore, the European Commission proposed the project to analyse where the membership is lacking and to identify missing organisations.

The proposed improvements have been implemented by taking actions to increase the number of participants in the project events, broadening the network and inviting relevant entities from Member States and especially focusing on finding new members from industry to SME to strengthen the cohesion of the network through a common understanding of « countering hybrid threats » concept and analysing on a continuous basis where the membership was lacking.

The project's information sharing platform TUOVI was used regularly for advertising projects events and sharing information and material about hybrid threats. Further, the D1.24 « Network Sustainability Initial Report, submitted in M30/Oct 2022 under T1.3 describes the roadmap how to increase the network, concrete engagement measures during the project and how the eligibility criteria supports the membership and sustainability of the network.

To foster the network extension and support to reach the KPI of 30 new network members yearly several actions were taken. All consortium partners were encouraged and supported to arrange tailored events to certain type of network member group, e.g. practitioners, SMEs etc, in their EU MS and to support partners in their network extension work. In addition, Laurea Network Manager analysed on a continuous basis the network and where the membership is lacking.

3.2. THE EUROPEAN COMMISSION'S REQUESTED IMPROVEMENTS IN THE SECOND PROJECT REVIEW TO THE NETWORK EXTENSION

After the second European Commission (EC) EU-HYBNET project review in November 2022, the EC suggested a number of improvements to EU-HYBNET's community extension:

- Although the attendance to events has been good, the project should have greater awareness to distuingish between registered and actual attendees;
- The project should evaluate the activity of the network members and warn inactive organisations about the removal of the network;
- The project partners should discuss together the future of the network.

3.2.1. ACTIONS TAKEN ON REQUESTED IMPROVEMENTS AFTER THE SECOND REVIEW

The consortium has continued to improve the actions suggested by EC after both reviews. The attendance between the registered participants versus actual attendees has been monitored. The eligibility criteria has supported the acceptation and/or rejection of potential network members. The consortium has reserved the right to review and screen the network members and to deny accession, in cases where the given network member would have been inactive, demonstrated a lack of competence during the project life cycle, or raised security concerns during the application process. The plan and proceeding on the network sustainability is seen valid at the moment. Hybrid CoE will host the network after the project ends in 2025.

In addition, the consortium took the following measures under T1.3:

1. Actions to increase the number of participants in the project events
2. Enhance and broaden the network, including reaching out to relevant entities in Member States and additional participants from industry to SMEs
3. Strengthening the cohesion of the network through a common understanding of the "countering hybrid threats" concept
4. Continue to analyse where the membership is lacking with targeted efforts to reach out the identified missing organisations

The consortium has tried to attract especially SMEs and security practitioners via social media and newsletter. Further, as part of the improvements listed above, T1.3. contributed to organising a social media campaign that took place in autumn 2023 with a goal to increase project visibility and extension of the network. The social media campaign was co-planned between consortium partners with the lead of WP5.

Under T1.3, many efforts have been done to engage the network members to join the project work. In autumn 2023, an email to consortium members was sent by T1.3. leader and Laurea Network manager to encourage consortium partners to collaborate with network members. An excel list of network organizations, that describes the area of expertise with contact details was created to support this initiative. List is updated when new network members are approved to the network.

The EU-HYBNET network members have been engaged and invited to all EU-HYBNET project events or other events organised by consortium partners. Further, consortium have taken measures to increase collaboration between consortium partners and network members also in other forms, such as co-authoring research articles under T2.2. task.

3.2.2. RESULTS BASED ON THE ACTIONS TAKEN

The number of applications decreased and the annual KPI target to reach 30 new network members yearly was not achieved. Since then new network members have been gained and the current goal is to reach the gap.

Between April 2023-March 2024, 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 5 national or local level practitioners, 7 research and/or education institutions, 3 NGOs, and 8 SMEs from 14 countries. With the new members, the network consists of 25 consortium partners and 113 Network

Members from 27 countries, out of which 28 are practitioners, 39 research and/or education institutions, 19 NGOs, and 27 SMEs. At the end of January 2024, EU-HYBNET Network includes altogether 138 members (consortium partners, stakeholder group members, new network members).

During the reporting period, Ireland and Cyprus joined the EU-HYBNET network for the first time. The consortium will continue to identify ways how to increase the number of applications, especially from the missing EU countries. The work on analysing where membership is lacking is conducted on a monthly basis by Laurea Network Manager. At the same time T1.3. will continue to evaluate the activity of the network while continue embracing the cooperation opportunities in the project.

The abovementioned actions have resulted in new applications to the network, and new cooperative projects between consortium partners and network members are underway. The participation of the network practitioners in the EU-HYBNET events has been wide. Network members have actively joined the project events and expressed interest in arranging webinars or workshops for other network members. Further, under T2.2. new cooperation efforts have develop by co-authoring articles. All these actions have strengthened the collaboration between consortium partners and network members, resulting in increased activity in the network.

4. SELECTION PROCESS

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

- All of the applicants must apply using the application form which is accessible via official EU-HYBNET website, where the accession criteria is also shared: https://euhybnet.eu/join-the-network/ . All applicants must submit this form, even if they have 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 shall not be considered eligible to join the EU-HYBNET network. This condition was added to the eligibility criteria of new network members in January 2022 in the project's Executive Board meeting.
- The Hybrid CoE (network extension, task 1.3, leader) and the EU-HYBNET Project Management Board discuss the applications, and together make the decision over silent procedure during the week after the talks.
- Consortium Partners are informed about the outcome of the talks and pursuant to the EU-HYBNET Description of Action, the Consortium Partners can take part in the silent approval procedure over the selected applicants and break silence.
- Successful applicants are notified by the Network Manager upon acceptance of the relevant minutes of the accession talks or upon further actions. As a sign of acceptance and membership, the new members are given access to the Innovation Arena and Tuovi platform and are informed on proceedings of EU-HYBNET. T1.3. leader and Laurea Network Manager hold 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 D1.22 reporting period that is project months (M) 36-M47/ April 2023-March 2024:

	Name	Country	Type of organisation
1.	**Traversals Analytics and Intelligence GmbH**	Germany	SME
2.	**DLTCode**	Spain	SME
3.	**Stad Geel**	Belgium	Practitioner
4.	**Zetta Cloud**	Romania	SME
5.	**Carol I National Defence University**	Romania	Academia
6.	**Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering "Traian Lalescu"**	Romania	Academia
7.	**Tilt**	Netherlands	Practitioner
8.	**National Security Analytical Centre (NBAC)**	Slovakia	Practitioner
9.	**SECURE IDENTITY TECHNOLOGIES SL (IDBOTIC)**	Spain	NGO
10.	**Institute of Legal Personnel Training for the Security Service of Ukraine Yaroslav Mudryi National Law University**	Ukraine	Academia
11.	**Polytechnic Institute of Setubal School of Technology**	Portugal	Academia
12.	**DG SAFE/European Parliament**	Luxemburg	NGO
13.	**UCD Centre for Cybersecurity and Cybercrime Investigation**	Ireland	Academia
14.	**DataSenseLabs Ltd.**	Hungary	SME
15.	**Correcta**	Spain	SME
16.	**ISR Nederland BV**	Netherlands	SME
17.	**CIN Consult GmbH**	Austria	Practitioner
18.	**Risk and Crisis Centre Mid-Sweden University**	Sweden	Academia
19.	**National Cybersecurity Directorate**	Romania	Academia
20.	**City of Imatra**	Finland	Practitioner
21.	**Strategic Analysis**	Slovakia	NGO
22.	**CyberEcoCul Global Services**	Cyprus	SME
23.	**GREENSOFT SRL**	Romania	SME

Table 1: New members to the EU-HYBNET network

5.1. NETWORK

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

The following organisations have formed the initial EU-HYBNET network:

	Name	Country	Type of organisation
1.	**Ardanti! Defence**	France	Industry, SME
2.	**CeSI - Centro Studi Internazionali**	Italy	Research organization
3.	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Spain	Research organization
4.	**Expertsystem**	Italy	SME
5.	**European Security and Defence College**	EU	Research organization
6.	**European Health Management Association (EHMA)**	EU	NGO
7.	**Finnish Border Guard**	Finland	Practitioner
8.	**Fraunhofer-IVI**	Germany	Research organization
9.	**Ministry of Justice and Security in the Netherlands**	The Netherlands	Practitioner
10	**Ministry of the Interior Finland**	Finland	Practitioner
11	**SafeCluster**	France	Research organization
12	**Sopra steria**	France	Industry
13	**Systematic**	France	Industry
14	**Tecnoalimenti**	Italy	Research organization
15	**Tromsø Police District, Norway**	Norway	Practitioner
16	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	Ukraine	Research association
17	**Laurea University of Applied Sciences**	Finland	Research organization
18	**Polish Platform for Homeland Security, PPHS**	Poland	Practitioner
19	**University of Tromsø, UiT**	Norway	Research organization
20	**Research Institutes of Sweden AB, RISE**	Sweden	Research organisation
21	**Kentro Meleton Asfaleias, KEMEA**	Greece	Research organization
22	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Lithuania	Research organization

23	**Rey Juan Carlos University, URJC**	Spain	Research organization
24	**Ministry for an Ecological and Solidary Transition, MTES**	France	Practitioner
25	**European Organisation for Security, EOS**	Belgium	NGO
26	**Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO (RTO)**	The Netherlands	Research organization
27	**SATWAYS**	Greece	SME
28	**City of Espoo**	Finland	Practitioner
29	**Universita Cattolica del Sacro Cuore**	Italy	Practitioner
30	**European Commission Joint Research Centre, JRC**	Belgium	Research organisation
31	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Romania	Research organization
32	**The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE**	Finland	NGO
33	**Ministry of Defence**	The Netherlands	Practitioner
34	**International Centre for Defence and Security, ICDS**	Estonia	Research organization
35	**Valencia Local Police**	Spain	Practitioner
36	**Polish Internal Security Agency, ABW**	Poland	Practitioner
37	**Norwegian Directorate for Civil Protection, DSB**	Norway	Practitioner
38	**Estonian Information Authority Systems**	Estonia	Practitioner
39	**Maldita (Organisation)**	Spain	NGO
40	**Central Office for Information Technology in the Security Sphere, Zitis**	Germany	Practitioner
41	**Bundeswehr University, COMTESSA**	Germany	Research organization

Table 2: EU-HYBNET initial network members

5.1.1. NETWORK MEMBERS IN EU COUNTRIES

	Country	Name of the organization	Type of the organization
1.	Austria	**AIT Austrian Institute of Technology GmbH**	Research organisation
2.	Austria	**European Institute for Counter Terrorism and Conflict Prevention**	Research organisation
3.	Austria	**HENSOLDT Analytics**	SME
4.	Austria	**CIN Consult GmbH**	Practitioner

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

33.	France	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	Practitioner
34.	France	**Ardanti! Defence**	Industry, SME
35.	France	**SafeCluster**	Research organisation
36.	France	**Sopra steria**	Industry
37.	France	**Expertsystem**	
38.	France	**Systematic**	Industry
39.	France	**Ministry for an Ecological and Solidary Transition, MTES**	Practitioner
40.	France	**Euclid Institute**	NGO
41.	France	**INSTITUT CHOISEUL**	Research organisation
42.	France	**SIGNALERT SARL**	SME
43.	Greece	**S**ATWAYS	
44.	Greece	**Kentro Meleton Asfaleias (KEMEA)**	Research organisation
45.	Greece	**Information Technologies Institute / Centre for Research and Technology Hellas (CERTH/ITI)**	Research organisation
46.	Greece	**FORTH - Foundation for Research and Technology - Hellas - Institute of Computer Science**	Research organisation
47.	Germany	**Cyber - and Information Domain Service HQ**	Practitioner
48.	Germany	**Fraunhofer-IVI**	Research organisation
49.	Germany	**Central Office for Information Technology in the Security Sphere, Zitis**	Practitioner
50.	Germany	**Bundeswehr University, COMTESSA**	Research organisation
51.	Germany	**Maltego Technologies GmbH**	SME
52.	Germany	**Marshall Center**	Research organisation
53.	Germany	**Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg**	Research organisation
54.	Germany	**Traversals Analytics and Intelli-gence GmbH**	SME
55.	Hungary	**DataSenseLabs Ltd.**	SME
56.	Ireland	**UCD Centre for Cybersecurity and Cybercrime Investigation**	Academia
57.	Italy	**Enea**	Practitioner
58.	Italy	**CeSI - Centro Studi Internazionali**	Research organisation
59.	Italy	**Tecnoalimenti**	Research organisation
60.	Italy	**Universita Cattolica del Sacro Cuore**	Practitioner
61.	Italy	**Istituto Affari Internazionali (IAI)**	NGO

62.	Italy	**Fondazione SAFE - Security and Freedom for Europe**	NGO
63.	Italy	**CRIMEDIM - NO-FEAR Project**	Research organisation
64.	Italy	**SAPIENZA University of Rome - Department of Human Neuroscience - Interpersonal Violence Research Lab (InterViRe)**	Research organisation
65.	Latvia	**Baltic Centre for Media Excellence**	NGO
66.	Lithuania	**Vilnius Institute for Policy Analysis**	NGO
67.	Lithuania	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Research organisation
68.	Luxembourg	**Luxinnovation**	Practitioner
69.	Luxembourg	**Ministry of Foreign and European Affairs, Directorate of Defence**	Practitioner
70.	Luxembourg	**DG SAFE/European Parliament**	NGO
71.	The Netherlands	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Practitioner
72.	The Netherlands	**Ministry of Justice and Security in the Netherlands**	Practitioner
73.	The Netherlands	**Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO**	Research organisation
74.	The Netherlands	**Ministry of Defence**	Practitioner
75.	The Netherlands	**Faculty of Military Sciences**	Research organisation
76.	The Netherlands	**The Hague Centre for Strategic Studies**	SME
77.	The Netherlands	**Ministry of Foreign Affairs**	Practitioner
78.	The Netherlands	**Ridgeway Information EU B.V**	SME
79.	The Netherlands	**Tilt**	Practitioner
80.	The Netherlands	**ISR Nederland BV**	SME
81.	Poland	**Polish Platform for Homeland Security, PPHS**	Practitioner
82.	Poland	**Polish Internal Security Agency, ABW**	Practitioner
83.	Poland	**Academic Centre for Strategic Communication**	Research organisation
84.	Poland	**National Police Headquarters**	Practitioner
85.	Poland	**Government Centre for Security**	Practitioner
86.	Poland	**The Kosciuszko Institute Association**	NGO
87.	Poland	**Demagog Association**	NGO
88.	Poland	**Ministry of Foreign Affairs of Poland**	Practitioner

89.	Poland	**Polish Association for National Security – PTBN**	NGO
90.	Poland	**The Polish Financial Supervision Authority**	Practitioner
91.	Portugal	**VOST Portugal**	NGO
92.	Portugal	**Polytechnic Institute of Setubal - School of Technology**	Academia
93.	Romania	**Enersec Technology**	SME
94.	Romania	**Smartlink Communications**	SME
95.	Romania	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Research organisation
96.	Romania	**Romanian Ministry of Economy, Entrepreneurship and Tourism**	Practitioner
97.	Romania	**Mira Technologies Group SRL**	SME
98.	Romania	**New Strategy Center**	NGO
99.	Romania	**Center for the study of democracy**	Academia
100.	Romania	**Safetech INNOVATIONS SA**	SME
101.	Romania	**Zetta Cloud**	SME
102.	Romania	**Carol I National Defence University**	Academia
103.	Romania	**Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering "Traian Lalescu"**	Academia
104.	Romania	**National Cybersecurity Directorate**	Academia
105.	Romania	**GREENSOFT SRL**	SME
106.	Slovakia	**GLOBSEC**	NGO
107.	Slovakia	**National Security Authority**	Practitioner
108.	Slovakia	**Presidium of Police Force**	Practitioner
109.	Slovakia	**Ministry of Interior of the Slovak republic**	Practitioner
110.	Slovakia	**National Security Analytical Centre (NBAC)**	Practitioner
111.	Slovakia	**Strategic Analysis**	NGO
112.	Spain	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Research organisation
113.	Spain	**Rey Juan Carlos University, URJC**	Research organisation
114.	Spain	**Valencia Local Police**	Practitioner
115.	Spain	**Maldita (Organisation)**	NGO
116.	Spain	**Universidad Isabel I de Castilla**	Research organisation
117.	Spain	**DLT Code**	SME
118.	Spain	**SECURE IDENTITY TECHNOLOGIES SL (IDBOTIC)**	NGO
119.	Spain	**Correcta**	SME

120.	Sweden	**NORSECON**	SME
121.	Sweden	**Research Institutes of Sweden AB, RISE**	Research organisation
122.	Sweden	**Sectyne AB**	SME
123.	Sweden	**Swedish Police Authority/ National Forensic Centre**	Practitioner
124.	Sweden	**Combitech AB**	Industry
125.	Sweden	**Risk and Crisis Centre Mid-Sweden University**	Academia

Table 3: EU-HYBNET network members from EU Countries

5.1.2. NETWORK MEMBERS IN EU ASSOCIATED COUNTRIES

	Country	**Name of the organization**	**Type of the organization**
126.	Georgia	**LEPL Cyber Security Bureau under the Ministry of Defence of Georgia**	Practitioner
127.	Georgia	**Defence Institution Building School**	Research organisation
128.	Georgia	**Office of the National Security Council of Georgia**	Practitioner
129.	Georgia	**The School of Social Sciences (of the University of Georgia - UG)**	Research organisation
130.	Norway	**University of Tromsø**	Research organisation
131.	Norway	**Norwegian Directorate for Civil Protection, DSB**	Practitioner
132.	Norway	**Tromso Police District Tromso**	Practitioner
133.	Norway	**Nord University**	Research organisation
134.	Norway	**SINTEF Digital, Dept. of Software Engineering, Safety and Security**	Research organisation
135.	Ukraine	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	Research organisation
136.	Ukraine	**International Cyber Academy**	Research organisation
137.	Ukraine	**State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"**	Research organisation
138.	Ukraine	**Institute of Legal Personnel Training for the Security Service of Ukraine Yaroslav Mudryi National Law University**	Academia

6. FUTURE WORK

The EU-HYBNET Project Management Board (PMB) and Hybrid CoE will continue to select new members to the EU-HYBNET extended network until April 2025 (M60). In addition, the project continue to map the current needs of the network in order to see where it lacks in expertise. A special effort will be dedicated to find suitable candidates that would bring added value to the network. In this purpose, a new social media campaign was planned early 2024 to promote up-coming project events in Valencia, Spain and on the other hand, to attract new members to the network. To ensure that the network is balanced between Member States, the project will continue to analyse the network on a regular basis, collaborate collectively between consortium partners and to identify and contact organisations directly. T1.3. leader will continue to send reminders to consortium partners to suggest new potential network members. In addition, the project will seek to find potential candidates from those countries where it is still lacking membership.

New collaborative efforts are underway between consortium partners and network organizations. Few network member organizations are willing to arrange webinars or workshops targeted for other network member organizations. T1.3. is keen to support these initiatives. Another initiative is to co-author 4th year research article between consortium partners and network members under T2.2.

Furthermore, throughout the project cycles, the consortium partners have taken several actions in order to raise understanding of hybrid threats in the network. In 2021, T1.3. leader, Hybrid CoE produced a video recording of one of its webinars “Hybrid Threat Concept and its applications” and published it at the TUOVI platform so that it is accessible to all network members. Another video “Hybrid Threats – What are they and why do they matter?”, also published by Hybrid CoE was shared to consortium partners and network member organizations early 2024. The video have been circulated by the project partners in social media in order to attract new members to the network while raising general awareness on hybrid threats and how malign actors operate. The video have also been used to promote EU-HYBNET events, such as the 4th Future Trends workshop and the 4th Annual Workshop, that will take place in Valencia, Spain in April 2024. On this occasion, a video version with Spanish subtitles will be circulating on social media.

The project will continue to invite new network members to the project platforms Innovation Arena and Tuovi, and to join the public events by EU-HYBNET. The importance and functions of TUOVI and Innovation Arena has been described in EU-HYBNET deliverables D5.9 “Innovation Arena” and D1.15 “Established EU-HYBNET Network Platforms”.

Hybrid CoE is to host the network after the project ends in 2025. The plan, as described in the D1.24 EU-HYBNET network Sustainability Initial Report (M30), is to invite network members to join Hybrid CoE expert networks. During the transition process, Hybrid CoE will reserve the right to review and screen the network members and also to deny accession, in particular in cases where the given network member would have been inactive or demonstrated a lack of competence during the project life cycle. This initiative will respond also to the recommendation given by the EC after the second periodical review.

Prior the project ends, T1.3. have two main reports to compile, due April 2025 (M60). D1.23 List of Actors to the Extended Network and D1.25. EU-HYBNET network Sustainability Final Report. This latter deliverable will describe the final plan for Hybrid CoE to host network after the project ends.

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	Cnsortium 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 Center 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

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.