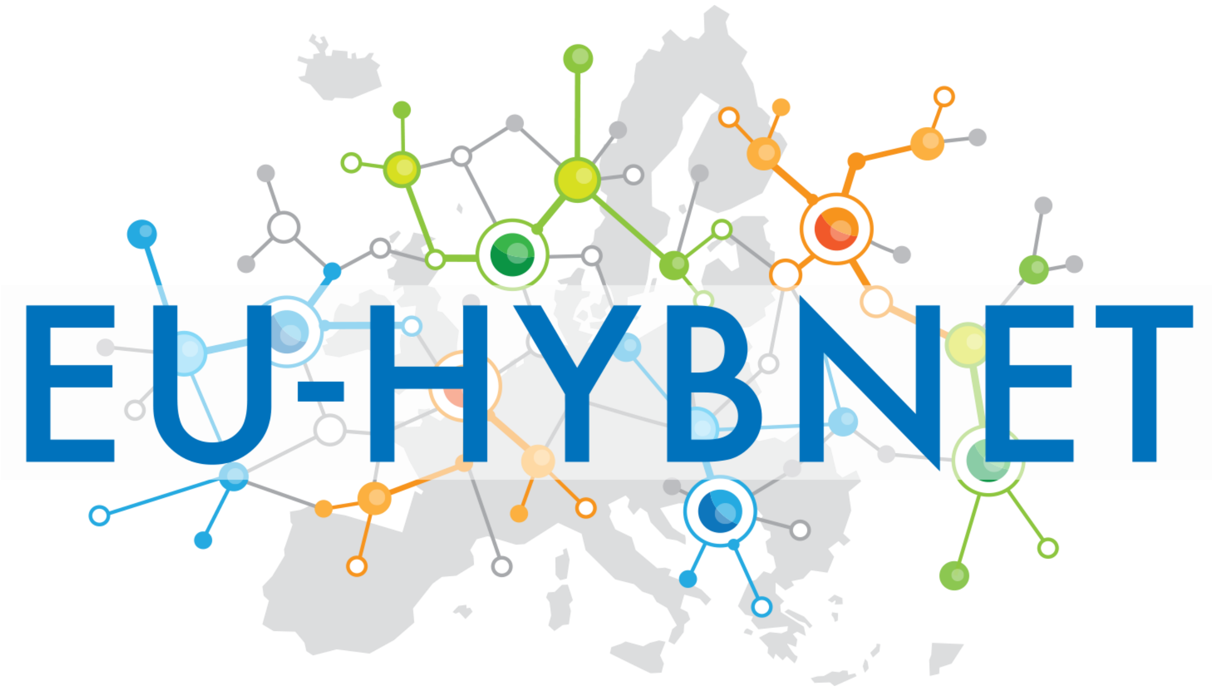

LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

DELIVERABLE 1.21

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	**1.21**	
Version:	**1.0**	
Delivery date:	**03.4.2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Hanne Dumur-Laanila**	**Hybrid CoE**
Contributors:	**Jari Räsänen, Päivi Mattila**	**Laurea**
	Jakub Rodzen	**ABW**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	1.3.2023	Hanne Dumur-Laanila	First draft
0.2	6.3.2023	Hanne Dumur-Laanila	Text editing
0.3	13.3.2023	Hanne Dumur-Laanila	Suggestions from the second review added
0.4	20.3.2023	Jari Räsänen	Updated list of network members added and review
0.5	27.3.2023	Päivi Mattila	Review and text editing
0.6	3.4.2023	Jakub Rodzen	Review
0.7	3.4.2023	Hanne Dumur-Laanila	Final editing
1.0	3.4.2023	Päivi Mattila	Final review and submission of the D1.21 to the 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.

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] After the second selection of new members in March 2022, the EU-HYBNET extended network consisted of 70 member organisations from 19 EU and 3 Associated Countries. 20 members are practitioners on government and local level, or support functions to either. 24 organisations concentrate on research and higher education institutes. 12 of the organisations are from private sector. 14 organisations are non-governmental organisations and other projects. The third round of selection has been successful and the network has continued to grow steadily. At current stage (M 35), the network consists of 33 practiotioners; 21 industry/practitioner organizations; 18 NGO's and 43 organizations are representing academia/research organization. In total network has 115 members.

In addition of listing new members to the network between M24 (April 2022) – M35 (March 2023), this deliverable (D) 1.21, *List of new actors to the extended EU-HYBNET network*, considers also the future work and suggested improvements by EC after the first and second review. 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 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. The new members are also invited to cooperate in research and writing of articles. In addition, network members are invited in each cycle to EU-HYBNET events, such as Annual Workshop, Future Trends Workshop and other relevant events, where

[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 2.2, *Gaps and Needs Workshop*

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.

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 project documents.[4] In addition the document acknowledges the EC's requested improvements for the network extension given in the EC's second project periodic review in November 2022.

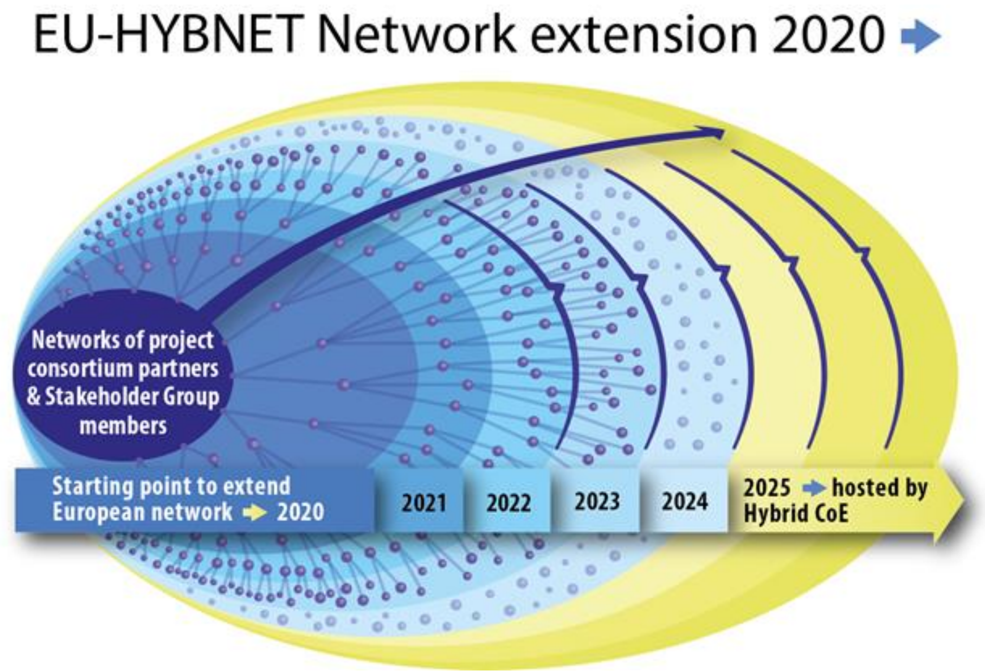
EU-HYBNET Network extension 2020 ➔
Networks of project consortium partners & Stakeholder Group members
Starting point to extend European network ➔ 2020
2021
2022
2023
2024
2025 ➔ hosted by Hybrid CoE

Figure 1: EU-HYBNET network extension 2020-2025

1.2 STRUCTURE OF THE DELIVERABLE

This document has five sections:

- The first section provides an introduction to the D1.21 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 Deliverable (D)1.7 "Definition of the eligibility criteria for new actors" and D1.24 "EU-HYBNET Network Sustainability Plan". In addition, the EC's **requests for improvements** in the network extension are highlighted, and measures to conduct the improvements shortly described.
- The third section describes the **selection process** and how it has been applied since the first round of applications.
- The fourth section is the **list of new members** to the network, their type and focus areas. In the third part, is also an update of the network as a whole.

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

- The fifth part provides a summary and 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.

2.2 RESULTS BASED ON REQUESTED IMPROVEMENTS TO THE NETWORK EXTENSION AFTER THE 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 have been lacking.

The project's information sharing platform TUOVI has been 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 have been taken. All consortium partners are 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 analyses on a continuous basis the network and where the membership is lacking.

The project will continue to carry these above mentioned activities also in the future.

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

In November 2022, the EC suggested new improvements to consider within the EU-HYBNET community extension. The review suggested the following improvements for future work:

- 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;

The project will continue to improve the actions suggested by EC. The attendance between the registered participants versus actual attendees will be monitored. The eligibility criteria supports 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 or demonstrated a lack of competence during the project life cycle. The plan and proceeding is seen valid at the moment.

3. 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.

4. 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 D1.21 reporting period that is project months (M) 24-M35/ April 2022-March 2023:

	Name	Country	Type of organisation
1.	**HENSOLDT Analytics**	Austria	SME
2.	**Hybrid Core BV**	Belgium	SME
3.	**New Strategy Center**	Romaina	NGO
4.	**Center for the Study of Democracy**	Romania	Academia
5.	**Hybrid Warfare Research Institute**	Croatia	NGO
6.	**The Hague Centre for Strategic Studies**	Netherlands	SME
7.	**Ministry of Foreign Affairs**	Netherlands	Practitioner
8.	**SIGNALERT SARL**	France	SME
9.	**Maltego Technologies GmbH**	Germany	SME
10.	**Universidad Isabel I de Castilla**	Italy	Academia
11.	**Safetech INNOVATIONS SA**	Romania	SME
12.	**SAPIENZA University of Rome - Department of Human Neuroscience - Interpersonal Violence Research Lab (InterViRe)**	Italy	Academia
13.	**FORTH - Foundation for Research and Technology - Hellas - Institute of Computer Science**	Greece	Academia
14.	**Ridgeway Information EU B.V**	Netherlands	SME
15.	**SINTEF Digital, Dept. of Software Engineering, Safety and Security**	Norway	Academia
16.	**The Polish Financial Supervision Authority**	Poland	Practitioner
17.	**University of Dubrovnik**	Croatia	Academia
18.	**Marshall Center**	Germany	Academia
19.	**Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg**	Germany	Academia
20.	**National Counterterrorism, Extremism and Cybercrime Agency**	Czechia	Practitioner

Table 1: New members to the EU-HYBNET network

4.1 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 as of March 2023.

4.1.1 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.	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.	Bulgaria	**Bulgarian Defence Institute**	Research organisation
14.	Croatia	**EFFECTUS - Entrepreneurial Studies - University College**	Research organization
15.	Croatia	**Hybrid Warfare Research Institute**	NGO
16.	Croatia	**University of Dubrovnik**	Research organisation
17.	Czechia	**European Values Centre for Security Policy**	NGO
18.	Czechia	**National Counterterrorism, Extremism and Cybercrime Agency**	Practitioner
19.	Estonia	**International Centre for Defence and Security, ICDS**	Research organisation
20.	Estonia	**Estonian Information Authority Systems**	Practitioner
21.	Finland	**Geostrategic Intelligence Group (GIG) Ltd**	SME
22.	Finland	**Finnish Border Guard**	Practitioner
23.	Finland	**Ministry of the Interior Finland**	Practitioner

24.	Finland	**Laurea University of Applied Sciences**	Research organisation
25.	Finland	**City of Espoo**	Practitioner
26.	Finland	**The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE**	NGO
27.	Finland	**Avoin yhteiskunta ry**	NGO
28.	Finland	**Police University College (fin: Poliisiammattikorkeakoulu)**	Research organisation
29.	France	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	Practitioner
30.	France	**Ardanti! Defence**	Industry, SME
31.	France	**SafeCluster**	Research organisation
32.	France	**Sopra steria**	Industry
33.	France	**Expertsystem**	
34.	France	**Systematic**	Industry
35.	France	**Ministry for an Ecological and Solidary Transition, MTES**	Practitioner
36.	France	**Euclid Institute**	NGO
37.	France	**INSTITUT CHOISEUL**	Research organisation
38.	France	**SIGNALERT SARL**	SME
39.	Greece	SATWAYS	
40.	Greece	**Kentro Meleton Asfaleias (KEMEA)**	Research organisation
41.	Greece	**Information Technologies Institute / Centre for Research and Technology Hellas (CERTH/ITI)**	Research organisation
42.	Greece	**FORTH - Foundation for Research and Technology - Hellas - Institute of Computer Science**	Research organisation
43.	Germany	**Cyber - and Information Domain Service HQ**	Practitioner
44.	Germany	**Fraunhofer-IVI**	Research organisation
45.	Germany	**Central Office for Information Technology in the Security Sphere, Zitis**	Practitioner
46.	Germany	**Bundeswehr University, COMTESSA**	Research organisation
47.	Germany	**Maltego Technologies GmbH**	SME
48.	Germany	**Marshall Center**	Research organisation
49.	Germany	**Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg**	Research organisation
50.	Italy	**Enea**	Practitioner
51.	Italy	**CeSI - Centro Studi Internazionali**	Research organisation

52.	Italy	**Tecnoalimenti**	Research organisation
53.	Italy	**Universita Cattolica del Sacro Cuore**	Practitioner
54.	Italy	**Istituto Affari Internazionali (IAI)**	NGO
55.	Italy	**Fondazione SAFE - Security and Freedom for Europe**	NGO
56.	Italy	**CRIMEDIM - NO-FEAR Project**	Research organisation
57.	Italy	**SAPIENZA University of Rome - Department of Human Neuroscience - Interpersonal Violence Research Lab (InterViRe)**	Research organisation
58.	Latvia	**Baltic Centre for Media Excellence**	NGO
59.	Lithuania	**Vilnius Institute for Policy Analysis**	NGO
60.	Lithuania	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Research organisation
61.	Luxembourg	**Luxinnovation**	Practitioner
62.	Luxembourg	**Ministry of Foreign and European Affairs, Directorate of Defence**	Practitioner
63.	The Netherlands	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Practitioner
64.	The Netherlands	**Ministry of Justice and Security in the Netherlands**	Practitioner
65.	The Netherlands	**Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO**	Research organisation
66.	The Netherlands	**Ministry of Defence**	Practitioner
67.	The Netherlands	**Faculty of Military Sciences**	Research organisation
68.	The Netherlands	**The Hague Centre for Strategic Studies**	SME
69.	The Netherlands	**Ministry of Foreign Affairs**	Practitioner
70.	The Netherlands	**Ridgeway Information EU B.V**	SME
71.	Poland	**Polish Platform for Homeland Security, PPHS**	Practitioner
72.	Poland	**Polish Internal Security Agency, ABW**	Practitioner
73.	Poland	**Academic Centre for Strategic Communication**	Research organisation
74.	Poland	**National Police Headquarters**	Practitioner
75.	Poland	**Government Centre for Security**	Practitioner
76.	Poland	**The Kosciuszko Institute Association**	NGO
77.	Poland	**Demagog Association**	NGO
78.	Poland	**Ministry of Foreign Affairs of Poland**	Practitioner

79.	Poland	**Polish Association for National Security - PTBN**	NGO
80.	Poland	**The Polish Financial Supervision Authority**	Practitioner
81.	Portugal	**VOST Portugal**	NGO
82.	Romania	**Enersec Technology**	SME
83.	Romania	**Smartlink Communications**	SME
84.	Romania	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Research organisation
85.	Romania	**Romanian Ministry of Economy, Entrepreneurship and Tourism**	Practitioner
86.	Romania	**Mira Technologies Group SRL**	SME
87.	Romania	**New Strategy Center**	NGO
88.	Romania	**Center for the study of democracy**	Academia
89.	Romania	**Safetech INNOVATIONS SA**	SME
90.	Slovakia	**GLOBSEC**	NGO
91.	Slovakia	**National Security Authority**	Practitioner
92.	Slovakia	**Presidium of Police Force**	Practitioner
93.	Slovakia	**Ministry of Interior of the Slovak republic**	Practitioner
94.	Spain	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Research organisation
95.	Spain	**Rey Juan Carlos University, URJC**	Research organisation
96.	Spain	**Valencia Local Police**	Practitioner
97.	Spain	**Maldita (Organisation)**	NGO
98.	Spain	**Universidad Isabel I de Castilla**	Research organisation
99.	Sweden	**NORSECON**	SME
100.	Sweden	**Research Institutes of Sweden AB, RISE**	Research organisation
101.	Sweden	**Sectyne AB**	SME
102.	Sweden	**Swedish Police Authority/ National Forensic Centre**	Practitioner
103.	Sweden	**Combitech AB**	Industry

Table 3: EU-HYBNET network members from EU Countries

4.1.2 NETWORK MEMBERS IN EU ASSOCIATED COUNTRIES

	Country	**Name of the organization**	**Type of the organization**
104.	Georgia	**LEPL Cyber Security Bureau under the Ministry of Defence of Georgia**	Practitioner

105.	Georgia	**Defence Institution Building School**	Research organisation	
106.	Georgia	**Office of the National Security Council of Georgia**	Practitioner	
107.	Georgia	**The School of Social Sciences (of the University of Georgia - UG)**	Research organisation	
108.	Norway	**University of Tromsø**	Research organisation	
109.	Norway	**Norwegian Directorate for Civil Protection, DSB**	Practitioner	
110.	Norway	**Tromso Police District Tromso**	Practitioner	
111.	Norway	**Nord University**	Research organisation	
112.	Norway	**SINTEF Digital, Dept. of Software Engineering, Safety and Security**	Research organisation	
113.	Ukraine	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	Research organisation	
114.	Ukraine	**International Cyber Academy**	Research organisation	
115.	Ukraine	**State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"**	Research organisation	

5. FUTURE WORK

The EU-HYBNET Project Management Board (PMB) and Hybrid CoE will continue to annually select 30 new members to the EU-HYBNET extended network. In addition, and according to suggestions given by EC, 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. 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.

The 3rd cycle of the project will start with the Gaps & Needs event, organized in Rome, Italy on 28th of March. The event is followed by Future Trends Workshop (FTW) and Annual Workshop, both held in Bucharest, Romania 19.-20.4.2023. Gaps and Needs event will pave the way to gather further insights of the pan-European vulnerabilities, gaps and needs to counter hybrid threats while FTW and Annual Workshop will continue to build up on the project results and provide a fruitful platform to interact with EU-HYBNET network members and other relevant stakeholders to the project.

In order to raise understanding of hybrid threats in the network, the Hybrid CoE has 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.

The new network members are invited 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”.

The next list of new members to the extended network is due March, 2024.

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
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
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
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
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
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
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.