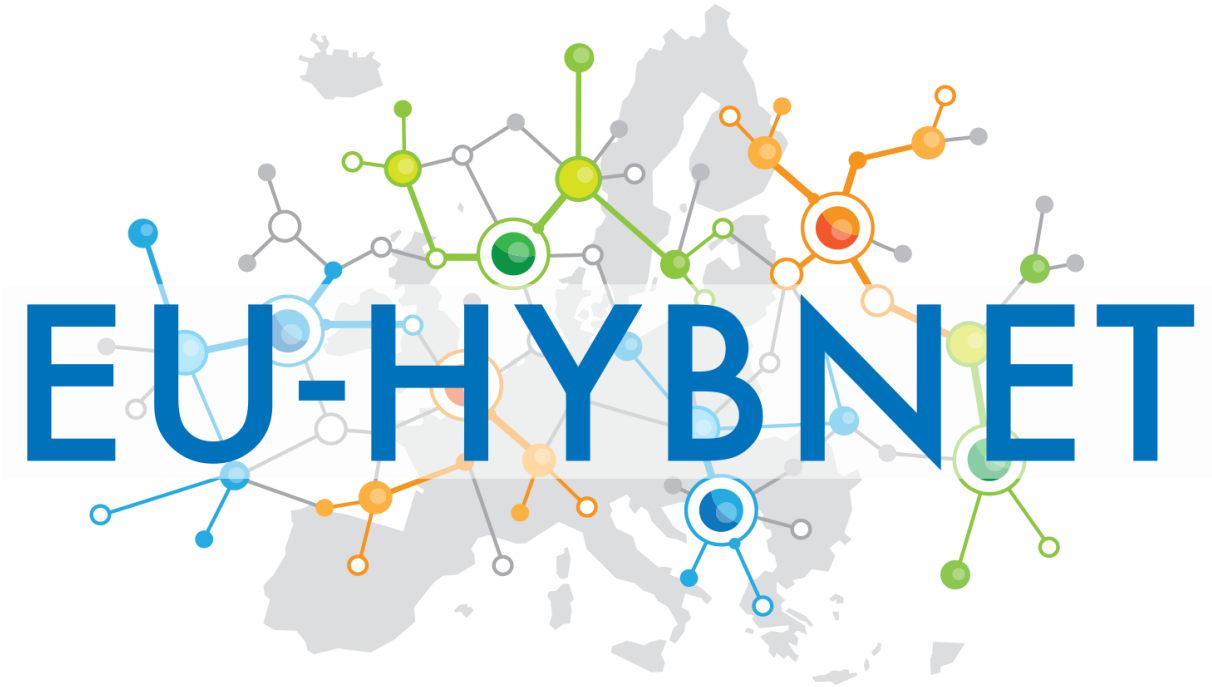

LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

DELIVERABLE 1.20

Lead Author: Hybrid CoE

Contributors: JRC, 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

D1.20 LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

Deliverable number	**1.20**	
Version:	**1.0**	
Delivery date:	**29.3.2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Maria Soukkio**	**Hybrid CoE**
Contributors:	**Päivi Mattila, Jari Räsänen**	**Laurea**
	Monica Cardarilli, Rainer Jungwirth	**JRC**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	23 March 2022	Maria Soukkio/ Hybrid CoE	First draft
0.2	23 March 2022	Jari Räsänen/ Laurea	Review and comments for text editing
0.3	25 March 2022	Päivi Mattila/ Laurea	Review and text editing. Comments for text editing.
0.4	28 March 2022	Maria Soukkio/ Hybrid CoE	Text editing
0.5	29 March 2022	Monica Cardarilli, Rainer Jungwirth/ JRC	Review
0.6	29 March 2022	Maria Soukkio/ Hybrid CoE	Final text editing and review
1.0	29 March 2022	Päivi Mattila/ Laurea	Final review and submission

DISCLAIMER

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

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

TABLE OF CONTENTS

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].

In the beginning of the project the network consisted of 25 consortium partners and 16 stakeholder group organisations (table 2) and it 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 consists 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.

This document / deliverable (D) 1.20, *List of new actors to the extended EU-HYBNET network*, lists the new members that have been selected to the network in March 2022. It is important to remember, that the application and selection are both ongoing processes. The deliverable is published yearly and will cover the members that have been 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 training event 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.

[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 1.8, *EU-HYBNET network Sustainability Plan.*
[3] The workshop objectives are described in detail in Deliverable 2.2, *Gaps and Needs Workshop*

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 first project periodic review in September 2021.

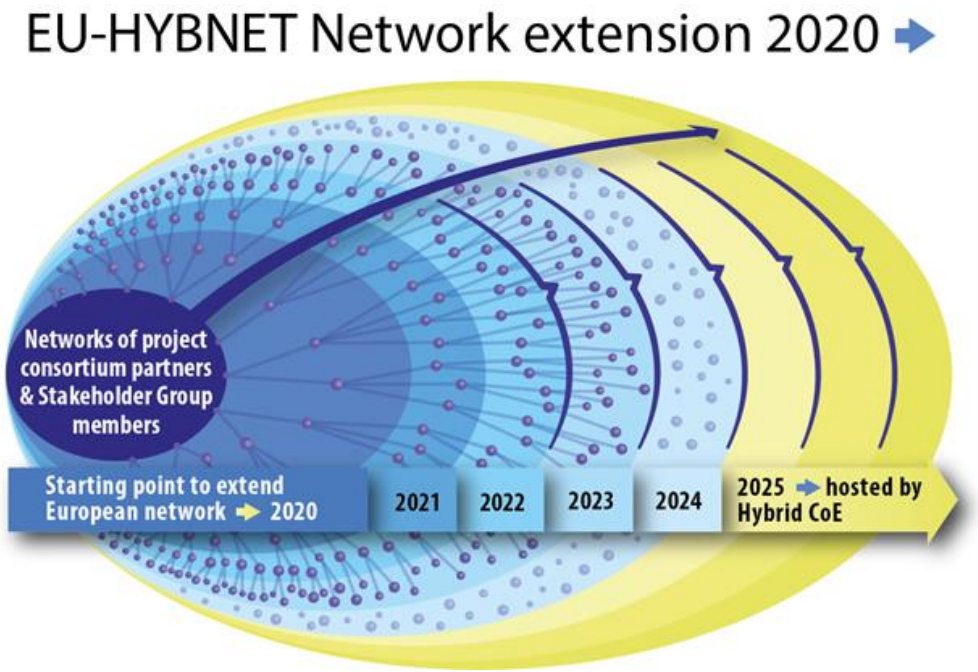

Figure 1: EU-HYBNET network extension 2020-2025

1.2 STRUCTURE OF THE DELIVERABLE

This document has five parts.

- The first part provides an introduction to the D1.20 and highlights its core content.
- The second part 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 D1.8 "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 part describes the **selection process** and how it has been applied since the first round of applications.
- The fourth part 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.
- The fifth part provides a summary and description of future work.

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

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

In the first Europen Comission (EC) EU-HYBNET project review in September 2021, the European Commission 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 -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 taken into account in the project followed by well planned measures so as to deliver the requested results in the network extension. The results from the D1.20 reporting period highlight that the planned project measures to the EC improvements have been fruitfully conducted. However, the project will continue its work in the network extension in a manner that the requested improvements are well achieved in the future as well.

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 D1.20 reporting period that is project months (M) 12-M23/ May 2021-March 2022:

	Name	Country	Type of organisation
1.	**VOST Portugal**	Portugal	NGO
2.	**AIT Austrian Institute of Technology GmbH**	Austria	Research organisation
3.	**State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"**	Ukraine	Research organisation
4.	**LEPL Cyber Security Bureau under the Ministry of Defence of Georgia**	Georgia	Practitioner
5.	**International Cyber Academy**	Ukraine	Research organisation
6.	**Istituto Affari Internazionali (IAI)**	Italy	NGO
7.	**Defence Institution Building School**	Georgia	Research organisation
8.	**Combitech AB**	Sweden	Industry
9.	**Academic Centre for Strategic Communication**	Poland	Research organisation
10.	**Ministry of Interior of the Slovak republic**	Slovakia	Practitioner
11.	**G4S**	Belgium	Industry
12.	**European Institute for Counter Terrorism and Conflict Prevention**	Austria	Research organisation
13.	**Faculty of Military Sciences**	The Netherlands	Research organisation
14.	**EFFECTUS - Entrepreneurial Studies - University College**	Croatia	Research organisation
15.	**Beyond the Horizon ISSG**	Belgium	NGO
16.	**Avoin yhteiskunta ry**	Finland	NGO
17.	**Romanian Ministry of Economy, Entrepreneurship and Tourism**	Romania	Practitioner
18.	**Luxinnovation**	Luxembourg	Practitioner
19.	**Fondazione SAFE - Security and Freedom for Europe**	Italy	NGO
20.	**Baltic Centre for Media Excellence**	Latvia	NGO
21.	**Ministry of Foreign and European Affairs, Directorate of Defence**	Luxembourg	Practitioner

22.	**National Police Headquarters**	Poland	Practitioner
23.	**Office of the National Security Council of Georgia**	Georgia	Practitioner
24.	**Government Centre for Security**	Poland	Practitioner
25.	**The Kosciuszko Institute Association**	Poland	NGO
26.	**Swedish Police Authority/ National Forensic Centre**	Sweden	Practitioner
27.	**Demagog Association**	Poland	NGO
28.	**The School of Social Sciences (of the University of Georgia - UG)**	Georgia	Research organisation
29.	**Euclid Institute**	France	NGO
30.	**Friends of Europe**	Belgium	NGO
31.	**Sectyne AB**	Sweden	SME
32.	**Information Technologies Institute / Centre for Research and Technology Hellas (CERTH/ITI)**	Greece	Research organisation
33.	**Mira Technologies Group SRL**	Romania	SME
34.	**Vesalius College VZW, part of the Brussels School of Governance and Vrije Universiteit Brussel (VUB)**	Belgium	Research organisation
35.	**Ministry of Foreign Affairs of Poland**	Poland	Practitioner
36.	**INSTITUT CHOISEUL**	France	Research organisation
37.	**CRIMEDIM - NO-FEAR Project**	Italy	Research organisation
38.	**Polish Association for National Security - PTBN**	Poland	NGO
39.	**Police University College (fin: Poliisiammattikorkeakoulu)**	Finland	Research organisation

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 February 2021

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.	Belgium	**European Organisation for Security, EOS**	NGO
4.	Belgium	**European Commission Joint Research Centre, JRC**	Research organisation
5.	Belgium	**G4S**	Industry
6.	Belgium	**Beyond the Horizon ISSG**	NGO
7.	Belgium	**Friends of Europe**	NGO
8.	Belgium	**Vesalius College VZW, part of the Brussels School of Governance and Vrije Universiteit Brussel (VUB)**	Research organisation
9.	Bulgaria	**Bulgarian Defence Institute**	Research organisation
10.	Croatia	**EFFECTUS - Entrepreneurial Studies - University College**	Research organization
11.	Czechia	**European Values Centre for Security Policy**	NGO
12.	Estonia	**International Centre for Defence and Security, ICDS**	Research organisation
13.	Estonia	**Estonian Information Authority Systems**	Practitioner
14.	Finland	**Geostrategic Intelligence Group (GIG) Ltd**	SME
15.	Finland	**Finnish Border Guard**	Practitioner
16.	Finland	**Ministry of the Interior Finland**	Practitioner
17.	Finland	**Laurea University of Applied Sciences**	Research organisation
18.	Finland	**City of Espoo**	Practitioner
19.	Finland	**The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE**	NGO
20.	Finland	**Avoin yhteiskunta ry**	NGO
21.	Finland	**Police University College (fin: Poliisiammattikorkeakoulu)**	Research organisation
22.	France	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	Practitioner
23.	France	**Ardanti! Defence**	Industry, SME
24.	France	**SafeCluster**	Research organisation

25.	France	**Sopra steria**	Industry
26.	France	**Systematic**	Industry
27.	France	**Ministry for an Ecological and Solidary Transition, MTES**	Practitioner
28.	France	**Euclid Institute**	NGO
29.	France	**INSTITUT CHOISEUL**	Research organisation
30.	Greece	**Information Technologies Institute / Centre for Research and Technology Hellas (CERTH/ITI)**	Research organisation
31.	Germany	**Cyber - and Information Domain Service HQ**	Practitioner
32.	Germany	**Fraunhofer-IVI**	Research organisation
33.	Germany	**Central Office for Information Technology in the Security Sphere, Zitis**	Practitioner
34.	Germany	**Bundeswehr University, COMTESSA**	Research organisation
35.	Greece	**Kentro Meleton Asfaleias, KEMEA**	Research organisation
36.	Greece	**SATWAYS**	SME
37.	Italy	**Enea**	Practitioner
38.	Italy	**CeSI - Centro Studi Internazionali**	Research organisation
39.	Italy	**Expertsystem**	SME
40.	Italy	**Tecnoalimenti**	Research organisation
41.	Italy	**Universita Cattolica del Sacro Cuore**	Practitioner
42.	Italy	**Istituto Affari Internazionali (IAI)**	NGO
43.	Italy	**Fondazione SAFE - Security and Freedom for Europe**	NGO
44.	Italy		
45.	Italy	**CRIMEDIM - NO-FEAR Project**	Research organisation
46.	Latvia	**Baltic Centre for Media Excellence**	NGO
47.	Lithuania	**Vilnius Institute for Policy Analysis**	NGO
48.	Lithuania	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Research organisation
49.	Luxembourg	**Luxinnovation**	Practitioner
50.	Luxembourg	**Ministry of Foreign and European Affairs, Directorate of Defence**	Practitioner
51.	The Netherlands	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Practitioner
52.	The Netherlands	**Ministry of Justice and Security in the Netherlands**	Practitioner
53.	The Netherlands	**Nederlandse Organisatie voor Toegepast**	Research organisation

		Natuurswetenschappelijk Onderzoek TNO	
54.	The Netherlands	**Ministry of Defence**	Practitioner
55.	The Netherlands	**Faculty of Military Sciences**	Research organisation
56.	Poland	**Polish Platform for Homeland Security, PPHS**	Practitioner
57.	Poland	**Polish Internal Security Agency, ABW**	Practitioner
58.	Poland	**Academic Centre for Strategic Communication**	Research organisation
59.	Poland	**National Police Headquarters**	Practitioner
60.	Poland	**Government Centre for Security**	Practitioner
61.	Poland	**The Kosciuszko Institute Association**	NGO
62.	Poland	**Demagog Association**	NGO
63.	Poland	**Ministry of Foreign Affairs of Poland**	Practitioner
64.	Poland	**Polish Association for National Security - PTBN**	NGO
65.	Portugal	**VOST Portugal**	NGO
66.	Romania	**Enersec Technology**	SME
67.	Romania	**Smartlink Communications**	SME
68.	Romania	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Research organisation
69.	Romania	**Romanian Ministry of Economy, Entrepreneurship and Tourism**	Practitioner
70.	Romania	**Mira Technologies Group SRL**	SME
71.	Slovakia	**GLOBSEC**	NGO
72.	Slovakia	**National Security Authority**	Practitioner
73.	Slovakia	**Presidium of Police Force**	Practitioner
74.	Slovakia	**Ministry of Interior of the Slovak republic**	Practitioner
75.	Spain	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Research organisation
76.	Spain	**Rey Juan Carlos University, URJC**	Research organisation
77.	Spain	**Valencia Local Police**	Practitioner
78.	Spain	**Maldita (Organisation)**	NGO
79.	Sweden	**NORSECON**	SME
80.	Sweden	**Research Institutes of Sweden AB, RISE**	Research organisation
81.	Sweden	**Sectyne AB**	SME
82.	Sweden	**Swedish Police Authority/ National Forensic Centre**	Practitioner
83.	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
84.	Georgia	**LEPL Cyber Security Bureau under the Ministry of Defence of Georgia**	Practitioner
85.	Georgia	**Defence Institution Building School**	Research organisation
86.	Georgia	**Office of the National Security Council of Georgia**	Practitioner
87.	Georgia	**The School of Social Sciences (of the University of Georgia - UG)**	Research organisation
88.	Norway	**University of Tromsø**	Research organisation
89.	Norway	**Norwegian Directorate for Civil Protection, DSB**	Practitioner
90.	Ukraine	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	
91.	Ukraine	**International Cyber Academy**	Research organisation
92.	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 Baord (PMB) and Hybrid CoE will continue to annually select 30 new members to the EU-HYBNET extended network. In addition, the project will start to map the current needs of the network in order to see where it lacks in expertise and special effort will be dedicated to finding suitable candidates that would bring added value to the network.

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 EU-HYBNET project will organize two roadshows, one in Rome during the EU-HYBNET Annual Workshop (6th of April) and EU-HYBNET Future Trends Workshop (5th of April) and another one in the EU-HYBNET Innovation and Knowledge Exchnage Workshop in Netherlands (14th of June) to attract more SME's to the network. Invitations have already been sent to 11 Italian SME's to attend the Annual Workshop and the Future Trends Workshopin Rome on the 5th of April 2022 and to Annual Workshop on the 6th of April 2022.

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".

An important event for the new network members' participation was the EU-HYBNET Gaps and Needs workshop on Septmeber 2021 alike the follow-up event to it that is the EU-HYBNET training and exercises event which takes place in September 2022. In the Gaps and Needs event the new network members were invited to provide new insights for the 2nd project cycle (September 2021 – April 2023) on the most important pan-European vulnerabilities, gaps and needs to counter Hybrid Threats. In September 2022 the Gaps and Needs event participant will be able not only to learn about but also to test the most promising innovations to gaps and needs. This will further support the EU-HYBNET to deliver solutions for the pan-European practitioners and other relavant actors (industry, sMEs, academia, NGOS) to counter hybrid threats, and also to highlight for the EU-HYBNET network members the relevance to belong to the EU-HYBNET network. In short, the named events next to other project events supports closer engagement with the network members and this will ensure a better cohesion within the network alike increase of knowledge and skills of hybrid threats and measures to counter hybrid threats.

The next list of new members to the extended network is due March, 2023.

ANNEX I. GLOSSARY AND ACRONYMS

Table 4 Glossary and Acronyms

Term	Definition / Description
EC	European Commission
AC	Associated Countries
DoA	Description of Action
KPI	Key performance indicator
OB	Objectives
WP	Work Package
CA	Cnsortium Agreement
T	Task
D	Deliverable
ABW	Polish Internal Security Agency
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
GIG	Geostrategic Intelligence Group Ltd
Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
IA	Innovation Arena
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
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
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 (UNICAT)	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.