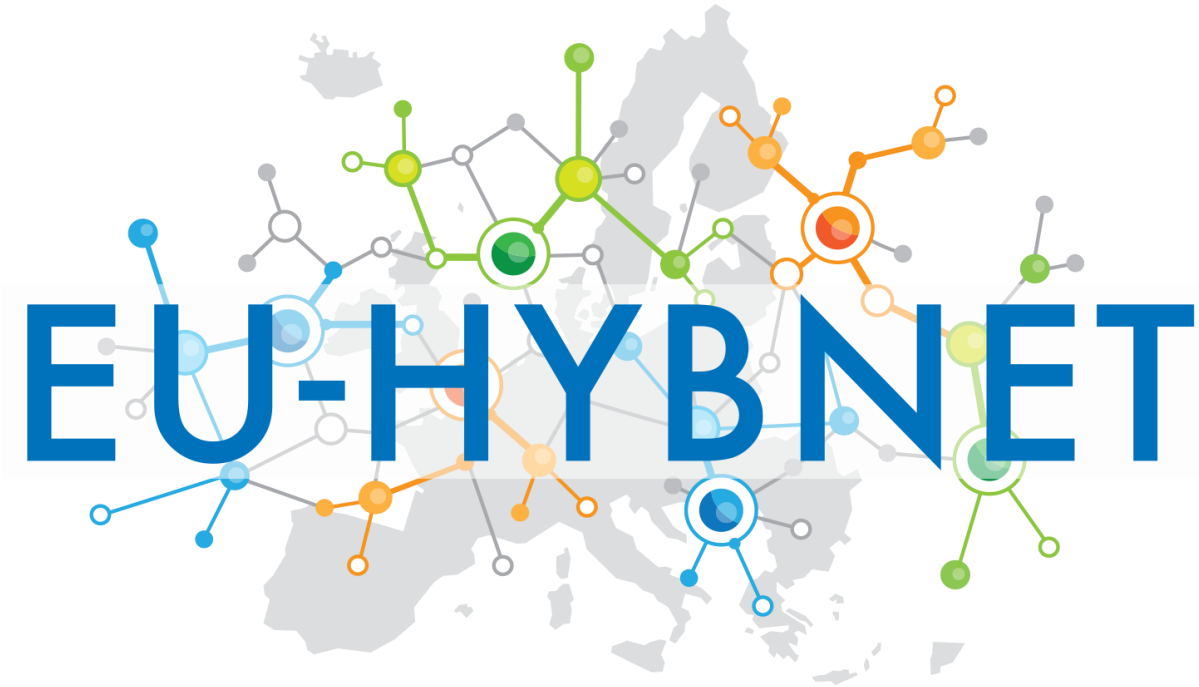

LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

DELIVERABLE 1.19

Lead Author: Hybrid CoE

Contributors: COMTESSA, 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

D1.19 LIST OF ACTORS TO THE EXTENDED EU-HYBNET NETWORK

Deliverable number	**1.19**	
Version:	**0.9**	
Delivery date:	**9.4.2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Emma Lappalainen**	**Hybrid CoE**
Contributors:	**Päivi Mattila, Julia Nevmerzhitskaya** **Son Pham**	**Laurea** **COMTESSA**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	15 March 2021	Emma Lappalainen	First draft
0.2	24 March 2021	Päivi Mattila	Review and suggestions for the content
0.3	25 March 2021	Julia Nevmerzhitskaya	Review and suggestions for the content
0.4	30 March 2021	Son Pham	Review
0.5	6 April 2021	Emma Lappalainen	Text editing
0.6	6 April 2021	Julia Nevmerzhitskaya	Review and suggestions for the content
0.7	7 April 2021	Päivi Mattila	Review and suggestions for the content
0.8	8 April 2021	Emma Lappalainen	Final text editing
0.9	9 April 2021	Päivi Mattila	Final review and submission of the D1.19

DISCLAIMER

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

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

© Copyright in this document remains vested in the Project Partners

TABLE DES MATIÈRES

1. Introduction 3
1.1 Purpose of the network extension 3
1.2 Structure of the deliverable 4
2. Network extension objectives 5
3. Selection process 6
4. New members to the extended network 8
4.1 Network 9
Network members in EU countries 11
EU organisations and projects ..... **Error! Bookmark not defined.**
Network members in EU Associated countries 12
5. Future work 13
ANNEX I. GLOSSARY AND ACRONYMS 13
ANNEX II. REFERENCES 15

TABLES AND FIGURES

Table 1: New members to the EU-HYBNET network 8
Table 2: EU-HYBNET stakeholder group in February 2021 10
Table 3: EU-HYBNET network members from EU countries 12
Table 4: EU-HYBNET network members in EU associated countries ..... **Error! Bookmark not defined.**
Table 5: Network members' organisation types ..... **Error! Bookmark not defined.**
Table 6 Glossary and Acronyms 13

Figure 1: EU-HYBNET network extension 2020-2025 ..... **Error! Bookmark not defined.**

1. INTRODUCTION

1.1 PURPOSE OF THE NETWORK EXTENSION

In EU-HYBNET project, the network is in its name: *Pan-European Network to Counter Hybrid Threats.* It 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) lays out that the development of the network responds to the objective of improving and maintaining a higher level of resilience against hybrid threats. The project will include actors in the fields 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].

The network consisted in the beginning of the project of 25 consortium partners and 16 stakeholder group organisations (table 2) and has been designed to expand annually with at least 30 new members.[2] **After the first selection of new members in March 2021, the EU-HYBNET extended network consists of 56 member organisations from 12 EU and 2 Associated Countries.** 20 members are practitioners on government and local level, or support functions to either. 19 organisations concentrate on research and higher education institutes. 9 of the organisations are from private sector. 8 organisations are non-governmental organisations and other projects.

This document / deliverable (D) 1.19, *List of new actors to the extended EU-HYBNET network*, lists the new members that have been selected to the network in March 2021. 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 March 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]

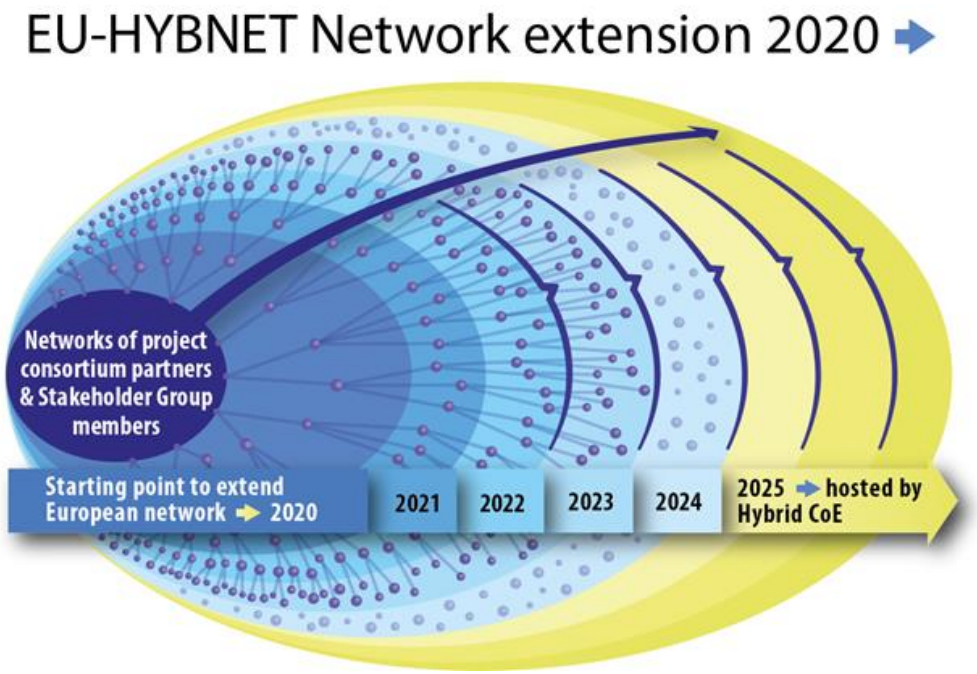

Figure 1: EU-HYBNET network extension 2020-2025

1.2 STRUCTURE OF THE DELIVERABLE

This document has three parts.

- The first part describes the **objectives** and performance indicators that have been defined for the network extension, and how they are treated in the project as per EU-HYBNET D1.7 and D1.8.
- The second part describes the **selection process** and how it was applied in the first round of applications.
- The third 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 fourth 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

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*.

The OB1. key performance indicator (KPI) target value of this Goal – of accepting at least 30 new members to join EU-HYBNET network yearly – is supported by signalling who of the relevant stakeholders have already been accepted. 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 so 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 especially 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. 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.

- The Hybrid CoE (network extension, task 1.3, leader) and the EU-HYBNET Project Management Board discusses 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.
- 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 in March 2021:

	Name	Country	Type of organisation
1.	**Bulgarian Defence Institute**	Bulgaria	Research organization
2.	**Cyber - and Information Domain Service HQ**	Germany	Practitioner
3.	**Enea**	Italy	Practitioner
4.	**Enersec Technology**	Romania	SME
5.	**European Values Centre for Security Policy**	Czech Republic	NGO
6.	**Geostrategic Intelligence Group (GIG) Ltd**	Finland	SME
7.	**GLOBSEC**	Slovakia	NGO
8.	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	France	Practitioner
9.	**National Security Authority**	Slovakia	Practitioner
10.	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Spain	Practitioner
11.	**Nord university**	Norway	Research organisation
12.	**NORSECON**	Sweden	SME
13.	**Presidium of Police Force**	Slovakia	Practitioner
14.	**Smartlink Communications**	Romania	SME
15.	**Vilnius Institute for Policy Analysis**	Lithuania	NGO

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

NETWORK MEMBERS IN EU COUNTRIES

	Country	Name of the organization	Type of the organization
1.	Belgium	**European Organisation for Security, EOS**	NGO
2.	Belgium	**European Commission Joint Research Centre, JRC**	Research organisation
3.	Bulgaria	**Bulgarian Defence Institute**	Research organization
	Croatia		
4.	Czechia	**European Values Centre for Security Policy**	NGO
5.	Estonia	**International Centre for Defence and Security, ICDS**	Research organization
6.	Estonia	**Estonian Information Authority Systems**	Practitioner
7.	Finland	**Geostrategic Intelligence Group (GIG) Ltd**	SME
8.	Finland	**Finnish Border Guard**	Practitioner
9.	Finland	**Ministry of the Interior Finland**	Practitioner
10.	Finland	**Laurea University of Applied Sciences**	Research organization
11.	Finland	**City of Espoo**	Practitioner
12.	Finland	**The European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE**	NGO
13.	France	**Institut de recherche stratégique de l'Ecole militaire IRSEM (Institute for Strategic Research)**	Practitioner
14.	France	**Ardanti! Defence**	Industry, SME
15.	France	**SafeCluster**	Research organization
16.	France	**Sopra steria**	Industry
17.	France	**Systematic**	Industry
18.	France	**Ministry for an Ecological and Solidary Transition, MTES**	Practitioner
19.	Germany	**Cyber - and Information Domain Service HQ**	Practitioner
20.	Germany	**Fraunhofer-IVI**	Research organization
21.	Germany	**Central Office for Information Technology in the Security Sphere, Zitis**	Practitioner
22.	Germany	**Bundeswehr University, COMTESSA**	Research organization
23.	Greece	**Kentro Meleton Asfaleias, KEMEA**	Research organization
24.	Greece	**SATWAYS**	SME
25.	Italy	**Enea**	Practitioner
26.	Italy	**CeSI - Centro Studi Internazionali**	Research organization

27.	Italy	**Expertsystem**	SME
28.	Italy	**Tecnoalimenti**	Research organization
29.	Italy	**Universita Cattolica del Sacro Cuore**	Practitioner
30.	Lithuania	**Vilnius Institute for Policy Analysis**	NGO
31.	Lithuania	**Lithuanian Cybercrime Centre of Excellence, L3CE**	Research organization
32.	The Netherlands	**NATO HQ JOINT FORCE COMMAND BRUNSSUM (JFCBS)**	Practitioner
33.	The Netherlands	**Ministry of Justice and Security in the Netherlands**	Practitioner
34.	The Netherlands	**Nederlandse Organisatie voor Toegepast Natuurswetenschappelijk Onderzoek TNO**	Research organization
35.	The Netherlands	**Ministry of Defence**	Practitioner
36.	Poland	**Polish Platform for Homeland Security, PPHS**	Practitioner
37.	Poland	**Polish Internal Security Agency, ABW**	Practitioner
38.	Romania	**Enersec Technology**	SME
39.	Romania	**Smartlink Communications**	SME
40.	Romania	**The "Mihai Viteazul" National Intelligence Academy, MVNIA**	Research organization
41.	Slovakia	**GLOBSEC**	NGO
42.	Slovakia	**National Security Authority**	Practitioner
43.	Slovakia	**Presidium of Police Force**	Practitioner
44.	Spain	**CSIC - Spanish National Research Council,Research group on Cryptology and Information Security (GiCSI)**	Research organization
45.	Spain	**Rey Juan Carlos University, URJC**	Research organization
46.	Spain	**Valencia Local Police**	Practitioner
47.	Spain	**Maldita (Organisation)**	NGO
48.	Sweden	**NORSECON**	SME
49.	Sweden	**Research Institutes of Sweden AB, RISE**	Research organisation

Table 3: EU-HYBNET network members from EU Countries

NETWORK MEMBERS IN EU ASSOCIATED COUNTRIES

	Country	**Name of the organization**	**Type of the organization**
50.	Norway	**Tromsø Police District**	Practitioner
51.	Norway	**Nord University**	Research organization

52.	Norway	**University of Tromsø**	Research organization
53.	Norway	**Norwegian Directorate for Civil Protection, DSB**	Practitioner
54.	Ukraine	**Ukrainian Association of Scholars and Experts in the field of Criminal Intelligence**	

5. FUTURE WORK

Before May 2021 which marks one year into the project, the EU-HYBNET PMB and Hybrid CoE will select 30 new members to the EU-HYBNET extended network.

The new network members will be 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".

Most important will be the new network members' participation in the next gaps and needs workshop, which takes place in October 2021. New network members will be invited to the workshop to provide new insights to fuel the project in the next cycle. After the new network members acceptance the project may also have closer engagement with the members in different project open events and innovation evaluations in the EU-HYBNET training event.

The next list of new members to the extended network is due April, 2022.

ANNEX I. GLOSSARY AND ACRONYMS

Table 4 Glossary and Acronyms

Term	Definition / Description
ABW	Polish Internal Security Agency
D	Deliverable
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.