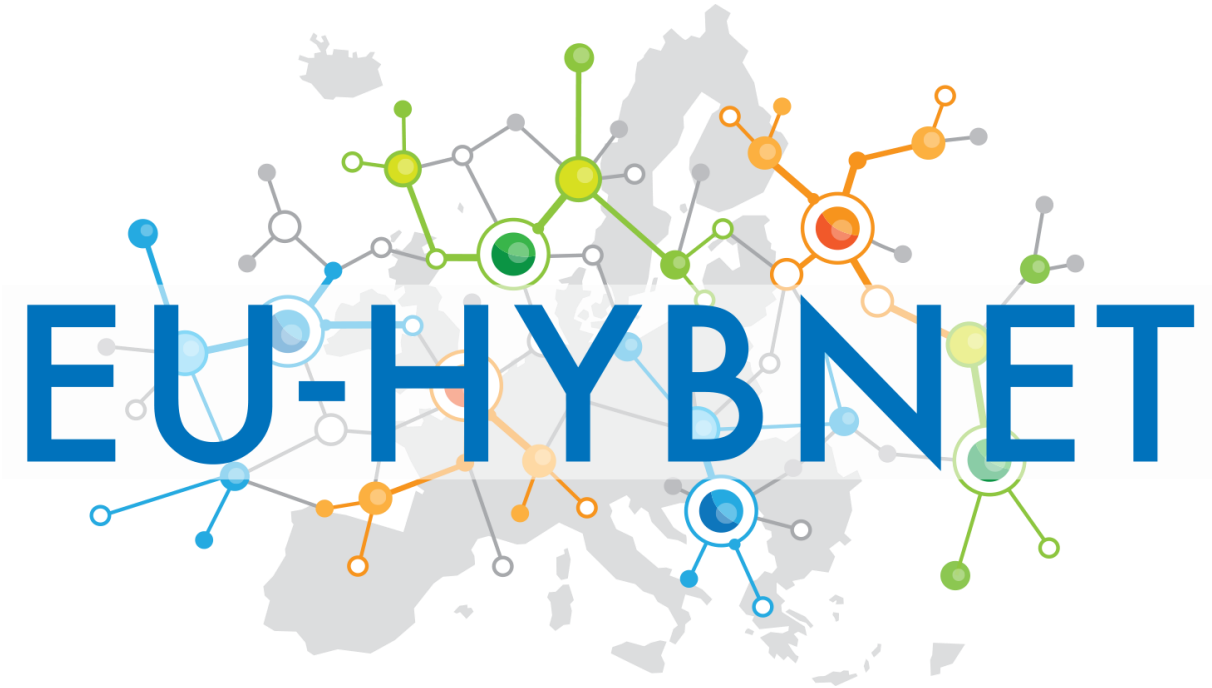

EU-HYBNET NETWORK SUSTAINABILITY INITIAL REPORT

DELIVERABLE 1.24

Lead Author: Hybrid CoE

Contributors: MoD NL, Laurea
Deliverable classification: PU

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

D1.24 EU-HYBNET NETWORK SUSTAINABILITY INITIAL REPORT

Deliverable number	**1.24**	
Version:	**1.0**	
Delivery date:	**31/10/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	**Maria Soukkio, Maxime Lebrun, Teija Tiilikainen**	**Hybrid CoE**
Contributors:	**Jari Räsänen, Päivi Mattila**	**Laurea**
	Margriet Drent	**MoD NL**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	3.10.2022	Maria Soukkio	First draft
0.2	6.10.2022	Maxime Lebrun	Review and editing
0.3	10.10.2022	Teija Tiilikainen	Review and editing
0.4	18.10.2022	Jari Räsänen, Päivi Mattila	Review and comments
0.6	20.10.2022	Margriet Drent	Review and comments
0.7	28.10.2022	Maxime Lebrun	Text Editing
0.8	31.10.2022	Päivi Mattila	Final document version delivery
0.9	31.10.2022	Maxime Lebrun	Final Review
1.0	31.10.2022	Päivi Mattila	Final version for 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

FIGURES

1. INTRODUCTION

The landscape of hybrid threats refers to domains and tools through which state and non-state actors aim to weaken social cohesion, decrease citizens' trust to democracy, and obfuscate democratic states decision-making processes. Hybrid threats challenge the resilience of European Union Member States, as they tend to target cohesion, trust, and unity of action within the European Union. This challenge is underlined in the EU Security Union Strategy.[1] The Security Union Strategy's goals are shared by the EU-HYBNET project and the EU-HYBNET Network aims to deliver measures to the Strategy's goals.

The EU-HYBNET project (Empowering a Pan-European Network to Counter Hybrid Threats) aims to monitor strategic research and innovation relevant to hybrid threats; express common requirements to fill capability and other gaps; designate priorities for areas requiring more standardization; and empower a pan-European network of practitioners. The project relies significantly on two leading partners, the Joint Research Center of the European Commission and on the Hybrid CoE's conceptual model to characterize hybrid threats. The project is creating a state-of-the-art network which will be able to support synergies among European, subnational and national networks, in particular with security practitioners, academia and the industry. The project aims to connect existing resources to connect gaps and dots coherently in the innovation solutions and research landscape. This will contribute to increasing EU awareness and capabilities established to detect hybrid threats. **The long-term sustainability of the network is paramount in ensuring the objectives mentioned above.**

The EU-HYBNET network is currently formed by 25 project consortium partners and 16 Stakeholder Group (SG) members. The EU-HYBNET project has, by 15 October 2022, accepted 65 additional members to its network and will continue accepting at least 30 new members to EU-HYBNET network on a yearly basis. EU-HYBNET creates conditions for enhanced interaction with practitioners, industry, and academia for a meaningful dialogue and for increasing membership in the network. The project consortium partners and EU-HYBNET SG form the basis of the network. Project activities, such as Innovation and Knowledge Exchange workshops, supports the process of attracting and engaging new members. The network has also explored and created synergies with already established national and European networks of practitioners, and other projects and networks, thereby having contributed to a comprehensive Pan-European network in the field of hybrid threats.

The sustainability of the EU-HYBNET network is based upon extensive participation of practitioners and other relevant pan-European actors in the key network activities created around, but not exclusively, the EU-HYBNET four core themes: "Future Trends of Hybrid Threats", "Cyber and Future Technologies", "Resilient Civilians, Local Level and National Administration", "Information and Strategic Communication". These practitioners and other actors come from different fields enabling a wide outreach to other networks. Furthermore, sustainability is ensured by the continued involvement of key EU-HYBNET project partner, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), who will host the network after the conclusion of the project.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

1.1 OVERVIEW

The main objective of this document is to deliver an initial sustainability plan for the EU-HYBNET Network to ensure the vitality of the EU-HYBNET Network during and after the project. The extension of the EU-HYBNET Network and its sustainable existence is grounded in the fact that after the project's completion, Hybrid CoE will continue to host the EU-HYBNET network. The sustainability of the network is based on the three key elements:

1) Initial composition of the network – project partners and Stakeholder Group,
2) Network extension and engagement during the project duration – new active members,
3) Network sustainability after the project's end – hand-over of the network to Hybrid CoE.

This document describes the strategic actions to be taken by the EU-HYBNET project in order to ensure, on the one hand, network expansion during the project and on the other, sustainability of the network after the end of the project. The goal is to provide a clear plan of what should be done to secure the long-lasting impacts of the network. The deliverable corresponds to EU-HYBNET project Task (T) 1.3 "EU-HYBNET Community Extension".

The EU-HYBNET sustainability initial report is based on the D1.8 EU-HYBNET Network Sustainability Plan and it serves as the basis for D1.25 "EU-HYBNET Network Sustainability Final Report", which will be submitted during M60. The network sustainability reports describe how the project has been able to deliver network sustainability and what could be improved.

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 2 describes the **aims of the EU-HYBNET network** and the network's role in support of countering hybrid threats. It presents the basis of the network sustainability, including the network Key Performance Indicators (KPIs) and their relationship to the project objectives.
- Section 3 provides an overview of the **network structure** and describes the roles of different types of the network members in the project. Special attention is given to practitioners as network members because EU-HYBNET is, according to its funding instrument, a "Network of Practitioners" (NoP) project.
- Section 4 introduces the **network engagement and sustainability plan during the project**, and underlines connections to other EU-HYBET tasks, activities and events, as well as key tools to engage and expand the network. Cooperation with other relevant European Commission funded projects is highlighted in this chapter.
- Section 5 presents the **sustainability plan beyond the project lifecycle**, including the ownership and maintenance of the network and the platforms.
- Section 6 assesses **critical risks to the sustainability of the network** and provides mitigation measures.
- Section 7 provides summary of the D1.24 and explains project's way forward in the network sustainability activities.

2. EU-HYBNET NETWORK AIMS

2.1 AIMS OF THE EU-HYBNET NETWORK

EU-HYBNET enables knowledge sharing and facilitates cooperation between industry, practitioners, academics, NGOs – the goal is to connect resources, innovations and solutions to the European practitioners' most critical gaps and needs in countering hybrid threats. EU-HYBNET seeks to connect resources, innovations and solutions through a series of "project cycles". Ripping the benefits from its diverse Consortium members and while expanding and engaging its network, EU-HYBNET defines a threat landscape associating it with a series of gaps and needs relevant to European practitioners. In parallel and taking into account the results from the threat landscape definition, Consortium partners monitor strategic research and innovation relevant to hybrid threats, in order to better connect resources and solutions to identified gaps and needs. The combination of both feeds into the definition of target areas for improvement. Based on this output, the Consortium subsequently defines needs for standardization where appropriate.

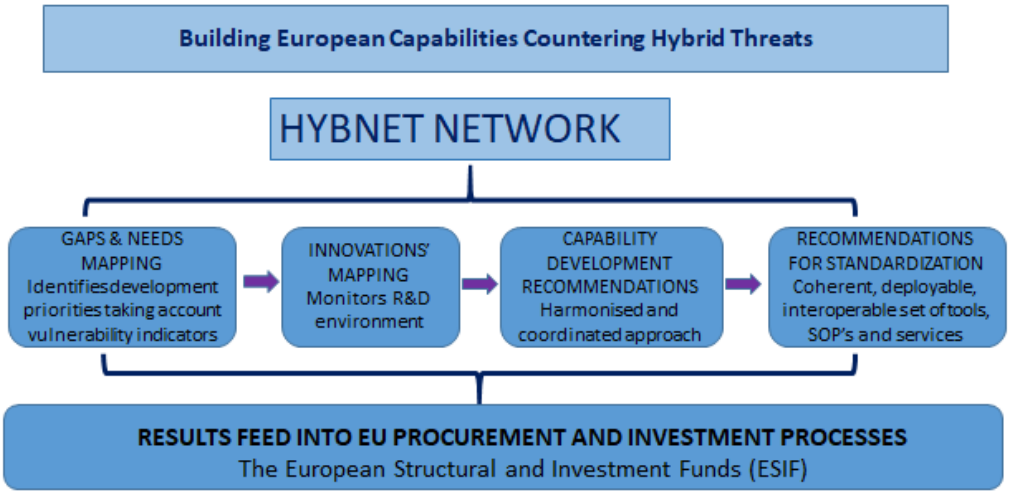

Figure 1 EU-HYBNET Network key activities and process

2.2 PROJECT ACTIVITIES, OBJECTIVES AND KEY PERFORMANCE INDICATORS

The key feature and added value of EU-HYBNET is the network extension. The extension provides the means for empowering the EU-HYBNET network and for facilitating the activities of project partners and stakeholder group members, by continuously identifying potentially new, key actors to join the network. New network members will be accepted into the network throughout the years of the project duration. This process is illustrated in the figure below.

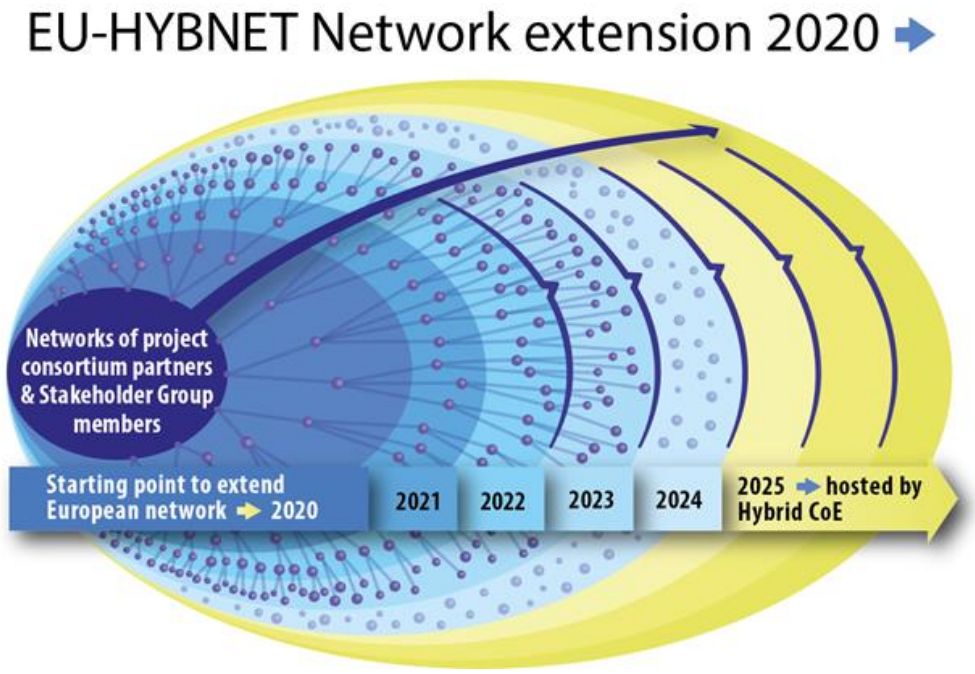

Figure 2 EU-HYBNET extension plan

The strength of the EU-HYBNET network is the key long-term impact that the project foresees. EU-HYBNET builds a network eco-system starting from the grassroots level and to include the practical experience of practitioners at local levels across the EU. This enables paying strict attention to signals below the threshold of crisis. All project activities are planned and conducted in a manner that supports ways of finding and attracting new and potentially valuable European actors (especially practitioners, industry, SMEs and academic actors, NGOs) to the EU-HYBNET Network.

The importance of the network is reflected in the project management board's structure which includes a dedicated Network Manager role. The activities of Network Manager are described in detail in chapter 3.1. The importance of network building and extension to the EU-HYBNET project is highlighted in the project Objectives (OB), key performance indicators (KPI) and project milestones (MS).

The EU-HYBNET network extension activities are part of the EU-HYBNET Work Package (WP) 1 "Coordination and Project Management" and Task 1.3 "EU-HYBNET Community Extension". However, as mentioned above, the project activities related to engaging the EU-HYBNET network members are part of each WP. The figure below describes the EU-HYBNET project workflow and activities.

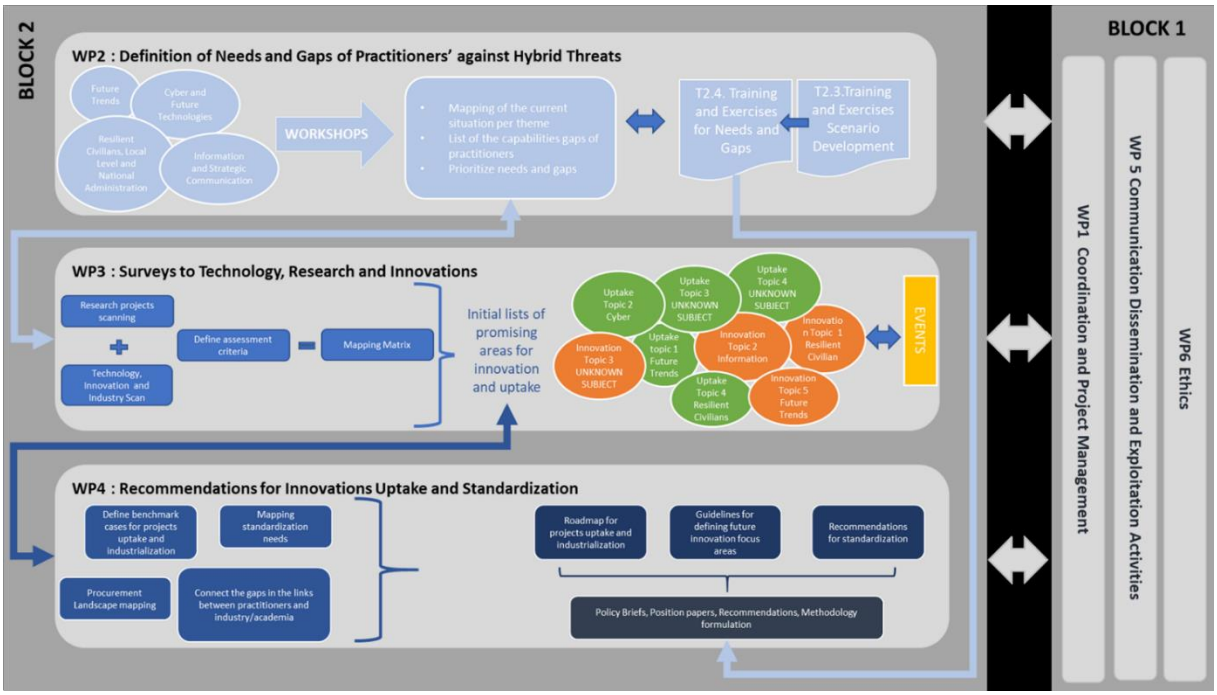

Figure 3 EU-HYBNET project content and work flow between work packages

The EU-HYBNET network extension is primarily linked to project **Objective 1:** *To enrich the existing network for countering hybrid threats and ensure long term sustainability*, and supports project Objectives (OB) 5, 6 and 7. The OB key performance indicators (KPI) for the network extension is the amount of new members accepted annually, which is set to a minimum 30 new actors. For the purpose of the sustainability plan, the network-specific KPIs were set-up to support the project-level OB KPIs described in the EU-HYBNET Description of Action (DoA). The detailed connection between the project objectives and the network sustainability KPIs are described in the table below.

Table 1 EU-HYBNET objectives and KPIs

EU-HYBNET objective: To enrich the existing network countering hybrid threats and ensure long term sustainability			
Goals related to the network sustainability		**Project-specific KPI**	**Network-specific KPI**
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	- -At least 30 new members to join the EU-HYBNET network yearly	- At least 2 new expressions of interest from external actors monthly - At least 5 new members applied to the network bimonthly
1.4	To achieve sustainability, Hybrid CoE will lead the post-project activities for EU-HYBNET with established EU, national /sub-national networks of practitioners. Note: Hybrid CoE does not need to use the name EU-HYBNET any more after the project has ended	- Sustainability plan as to how the Network will continue to be active after project completion is finalized and ready for execution	- Sustainability plan is published - Hybrid CoE takes over the network maintenance and ownership after April 2025.

OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network			
Goal		**Project-specific KPI**	**Network-specific KPI**
5.1	To establish a platform for information exchange through an Innovation Arena, along with an associated web site	- At least 30 new users of the Innovation arena (IA) yearly	- Level activity by users in the IA (at least 1 new activity per month)
5.2	To set up community forums that will empower the European network to engage in productive exchanges on research and innovation, needs/gaps, uptake, policy issues, standardisation	- At least 3 events per year; at minimum100 participants - Innovation arena (IA) and Web site are in use by at least 4 forums (see KPI for Goal 5.1)	- At least 30% of the network members participating in each event
5.3	To create a roadmap for the activities necessary to increase membership in the European network assigned to deal with hybrid threats, including the steps necessary to ensure its sustainability	- The roadmap is put in place to be adhered to by EU-HYBNET members, all new members, and especially Hybrid CoE upon project completion	- The roadmap presented in D5.1 Section 6 is further enhanced in this document in Sections 4 and 5
OB6: To foster capacity building and knowledge exchange on countering hybrid threats			
Goal		**Project-specific KPI**	**Network-specific KPI**
6.1	To arrange dialogue sessions for EU and EU MS practitioners, industry, SME and academic actors to strengthen capacity and hybrid threat knowledge exchange	- At least three yearly project events are executed with a minimum of 100 participants each time	- At least 1/3 of the network members participating in each event
6.3	To enhance knowledge exchange, increase knowledge/capacity of actor-actor interactions, esp. with industry	- At least 4 published research papers yearly – 1 in each of the four project core themes	- At least 1 article annually co-authored with EU-HYBNET network member(s) - At least 1 new joint project proposal by the network members
6.4	To empower European practitioners, industry, SME and academic actors' capacity to counter hybrid threats by offering relevant trainings and materials	- At least 1 training event every 20 months; at min. 60 participants on site and via webinar for others	- At least 50 participants are network active members. Note: active means that member joins the project events and/or contributes to the project proceeding in any other way
OB7. To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats			
Goal		**Project-specific KPI**	**Network-specific KPI**
7.1	To share information on EU-HYBNET activities and training possibilities among European stakeholders	- At least one training event every 20 months; min. 3 over 5 years	- At least 50 network members taking part in every training event
7.3	To establish links with other European Networks and missions in related fields of interest (e.g. Community of Users)	- Annual EU-HYBNET workshop for stakeholders and other related networks/actors to build links	- Minimum 30 network members participating in the first annual workshop, minimum 80 members participating in the final EU-

			HYBNET stakeholder workshop
7.5	To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically	- At least 2 events yearly where over 100 actors will meet	- Systematic engagement of the network members in the online (TUOVI, IA) and offline (events) activities, at least 1 coordinated activity per month and hosted by Laurea/ Project Management Board (PMB) members (coordinator, project manager, innovation manager, network manager)

2.3 BASIS FOR THE NETWORK SUSTAINABILITY

EU-HYBNET project follows an engagement process based on the Spectrum of Public Participation by the International Association of Public Participation (IAP2) and moves beyond the empowering stage to address the sustainability aspect of the network (see Fig. 3). In line with the overall goal of empowering European actors to collaboratively counter hybrid threats, the 'Spectrum' addresses the process of developing trust and transparency among the network members. As the EU-HYBNET network has grown, the focus of engagement activities has shifted from the early levels of engagement by informing and consulting, towards more collaborative activities.

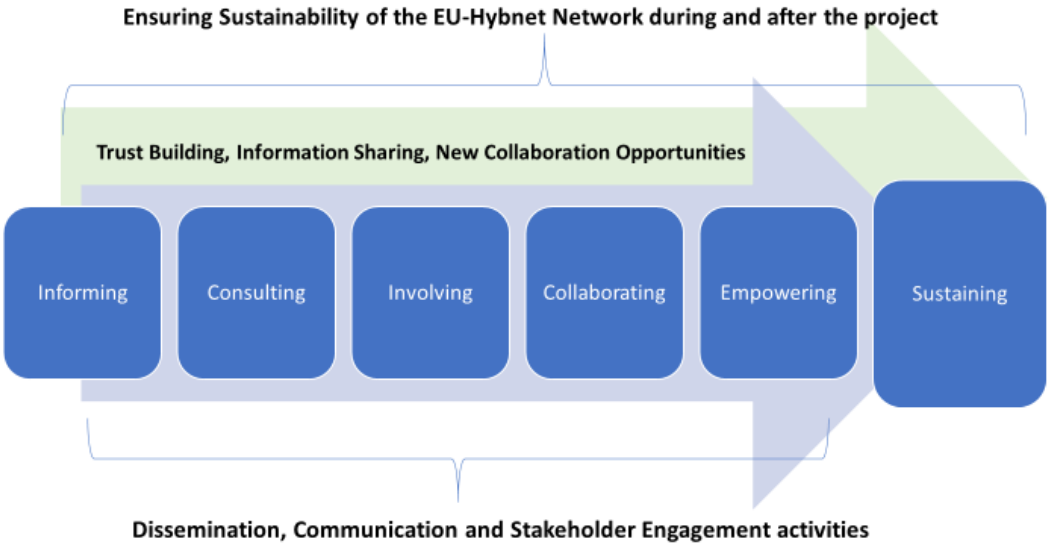

Figure 4 Basis for EU-HYBNET Sustainability

One of the key aspects in ensuring network sustainability is the trust building process. We are using the Collaborative Maturity Model as the basis for the trust building process of the network – this is described in Figure 4 below. The idea is that during the network formation stage, (years 1-3) the core activities will concentrate on the information sharing and creating a secure enabling environment for cooperation and information exchange. As the project progresses and the network grows, the

emphasis shifts from networking towards identification of new cooperation opportunities and joint contributions towards the development of innovations and recommendations. The chief objective of EU-HYBNET is to create and sustain a working dynamic among the network members in order to constantly increase the quality of the project's outputs and contribute relevant and timely input to EU policy.

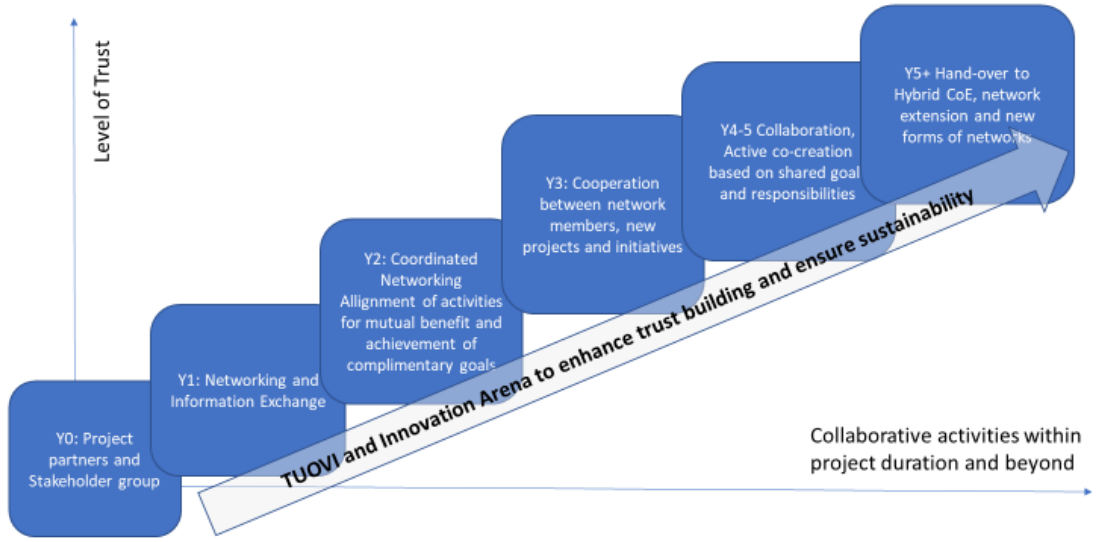

Figure 5 Trust building process for EU-HYBNET network

2.4 BENEFITS OF JOINING THE NETWORK

EU-HYBNET's core network element is that it needs to benefit its members. First, the EU-HYBNET network is a means and an opportunity to identify common challenges and exchange experience and best practices to counter hybrid threats. New members will have an incentive to join one of the most cutting-edge and high visibility research projects on hybrid threats in Europe. The network activities are planned so that the time that members spend on networking activities will provide benefit for both the members and the project. These two core approaches and promises are explained in more detail below. The general benefit of network membership is that the network members will get to know each other and create synergies from their networking and probable cooperation. There is an inherent added value in learning who the pan-European practioners and other relevant actors are, who take measures against hybrid threats in various different fields and domains within Europe.

During the project life-span, another benefit of network membership is to receive the general **information sharing** that is taking place in the network. Laurea as project coordinator shares information on upcoming relevant events, research findings, and policy documents to benefit the network members, by gaining access to timely and relevant information on measures to counter hybrid threats and fill knowledge gaps. The information is shared in the EU-HYBNET networking platform called TUOVI, via emails and during project events. All network releasable documents and event

invitations can be found on the TUOVI platform, and hence, it functions as a **library or archive** for network members at any time. Network members are also encouraged to share their own information on TUOVI and so the platform also has a bigger role in **information sharing** for European practitioners and other relevant actors to counter hybrid threats. The network provides an arena for practitioners and other key actors (industry, SME, academia, NGOs) to have important **discussions about necessary tools, innovations and security solutions** that enhance European capabilities to counter hybrid threats. Network members may expect to be **engaged in prominent European initiatives** relevant to countering hybrid threats. Initiatives, for example, may include European Commission (EC) open consultations.

The table below lists the EU-HYBNET network benefits for its network members and stakeholders.

Table 2 EU-HYBNET Network Membership benefits

Services	EU-HYBNET external stakeholder, wider audience	EU-HYBNET network member
Access to project resources		
Newsletter	x	x
Access to public deliverables and project results (via project web-page, twitter and linked-in)	x	x
Access to Innovation Arena and Information sharing among key European actors		x
Access to latest research and innovation materials on hybrid threats (via TUOVI portal)		x
Access to network members' contacts for new collaborative initiatives		x
Access to defined needs, gaps and innovations	x/ innovations	x/ gaps & needs and innovations
Participation in EU-HYBNET events		
Participation to EU-HYBNET Gaps and Needs events		x
Participation in Innovation and Knowledge Exchange events	x	x
Participation to EU-HYBNET Future Trends Workshop	x	x
Participation in EU-HYBNET training events		x
Participation to EU-HYBNET Annual Workshop	x	x
Participation to Task 4.3 workshops on innovation standardization	x/ invitation	x/ according to T4.3 need
EU-HYBNET project events with other projects	x/ invitation	x/ invitation

2.5 NETWORK CODE OF CONDUCT

EU-HYBNET is a diverse community of different actors. It is expected to include over a hundred practitioners and other key actors during the five years of the project's duration. At its best, diversity can increase creativity and innovation performance, however, it can also lead to difficult processes due

to lack of shared vision or understanding of the network goals. To avoid possible conflicts and to prevent misconduct, EU-HYBNET network members are expected to adhere to a Code of Conduct which was jointly developed by Laurea/ EU-HYBNET coordinator and Hybrid CoE by project in 2021.

3.NETWORK GOVERNANCE AND MEMBER PROFILES

The EU-HYBNET Network is a Pan-European network of practitioners and other key actors (industry, SMEs, academia, NGOs) in countering hybrid threats. The network is open to EU and Associated Countries based on the eligibility criteria described in EU-HYBNET Deliverable 1.7.

3.1 NETWORK GOVERNANCE STRUCTURE

The composition of the EU-HYBNET network includes the consortium partners and the EU-HYBNET Stakeholder Group (SG) which consists of a variety of practitioners, European Union (EU) Agencies and Offices, and actors from industry, SMEs, academia, NGOs, cities, and regions who are dealing with European measures against hybrid threats. The EU-HYBNET Network will grow with ca. 30 annually accepted network members during the project's five years. In 2022 the EU-HYBNET SG consisted of the following 16 members:

Practitioners

- Ministry of Justice and Security – **Law and justice** (NL)
- Finnish Border Guard - **Border and maritime security, internal and external security** (FI)
- Ministry of the Interior Finland, Dep. for Rescue Services - **Internal security, CBRN, Civil Protection and emergency response** (FI)
- Tromso Police District – **Law enforcement** (NO)

EU Agencies and Offices

- European Security and Defence College - **Crises management** (EU, BE)

Industry, SME

- Soprasteria - **Information technology, digital services** (FR)
- Systematic - **Critical infrastructure** (FR)
- Expertsystem - **Critical infrastructure** (FR)
- Ardanti!Defence- **Information technology, digital services** (FR)

RTO, research association, organisations

- European Health Management Association - **Health care** (EU, BE)
- Fraunhofer-IVI - **Critical infrastructure, electricity grids** (DE)
- Institute for Public Goods and Policies; Spanish National Research Council - **Fake news and strategic communication** (ES)
- Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence - **Law enforcement** (UA)
- CE.S.I. Istituto di Analisi di Politica Internazionale - **International Politics** (IT)
- Tecnoaliamenti - **Food security** (IT)
- SafeCluster - **Security technology** (FR)

The EU-HYBNET consortium partners also represent the following practitioners, industry and academia/ research organizations:

Practitioners

- France Ministry for an Ecological and Solidary Transition (MTES) (FR)
- Espoo City and Region (Espoo) (FI)
- Universita Cattolica Sacro Cuore (UCSC) (IT)
- The European Centre of Excellence for countering Hybrid Threats (Hybrid CoE) (FI)
- Netherlands Ministry of Defence (MoD) (NL)
- Valencia Local Police (PLV) (ES)

- Polish Internal Security Agency (ABW) (PO)
- Norwegian Directorate for Civil Protection (DSB) (NO)
- Estonian Information Systems Authority (RIA) (EE)
- Central Office for Information Technology in the Security Sphere (ZITiS) (DE)
- Bundeswehr University (COMTESSA) (DE)

Industry, SME

- Satways (GR)

RTO, Research associations, Organisations

- Polish Platform for Homeland Security (PPHS) (PO)
- Arctic University of Norway (UiT) (NO)
- Research Institutes of Sweden (RISE) (SE)
- Center for Security Studies (KEMEA) (GR)
- Lithuanian Cybercrime Centre of Excellence for Training, Research and Education (L3CE) (LT)
- University of Rey Juan Carlos (URJC) (ES)
- European Organization for Security (EOS) (BE)
- Netherlands Organisation for Applied Scientific Research (TNO) (NL)
- Joint Research Centre EC (JRC) (EU)
- The Mihai Viteazul National Intelligence Academy (MVNIA) (RO)
- International Centre for Defence and Security (ICDS) (EE)
- Maldita (ES)

Selection of new EU-HYBNET Network members is carried out in project Task 1.3 "EU-HYBNET Community Extension". Both EU-HYBNET consortium partners and Stakeholder Group members will identify potential new actors to join the EU-HYBNET Network. Organizations and actors who wish to join the EU-HYBNET network may also contact the project independently (without the invitation) and apply for an EU-HYBNET network membership. The selection criteria of new network members are described in detail in the EU-HYBNET deliverable 1.7 "Definition of the eligibility criteria for new actors".

Operational network management is the responsibility of the EU-HYBNET Network Manager at Laurea UAS, the EU-HYBNET coordinator organization. The Hybrid CoE, who is the leader of T1.3 "EU-HYBNET Community Extension", will also have an important role with the network. The responsibilities of the EU-HYBNET Network Manager include the following activities:

- Serve as the Point of Contact (PoC) for EU-HYBNET consortium partners, network members, and potential network members;
- Represent the EU-HYBNET Network during events and in cooperation with other EU projects;
- Participate in discussions regarding possibilities to join the network;
- Take part in the selection of new network members as a member of the EU-HYBNET Project Management Board (PMB)
- Contribute to Action reporting by providing recommendations regarding network management, engagement and extension
- Focus on dissemination and communication activities from a network management, extension and hosting point of view.

3.2 NETWORK MEMBER PROFILES

Because EU-HYBNET is an EC Network of Practitioners (NoP) project, the focus of network extension activities lies heavily on European practitioners. The EU-HYBNET follows the European Commission definition of practitioners, which states that *a practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection*.[2] In addition, practitioners in the hybrid threat context are expected to have a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats. The EU-HYBNET practitioners are categorised as follows:

I) *ministry level* (administration),
II) *local level* (cities and regions),
III) *support functions to ministry and local levels* (incl. Europe's third sector).

This definition of practitioner is mentioned in EU-HYBNET Description of Action (DoA) Part B document.

Other key EU-HYBNET network members are representatives from European industry, SMEs, academia and NGOs. These actors are central to delivering innovative solutions for practitioners' needs and provide research and development activities for practitioners and other stakeholders in the field.

3.3 ASSOCIATED PARTNERS

EU-HYBNET network members are not limited to the above-mentioned actors. EU institutions are by default considered associated partners and can follow and take part to activities per their interests without any vetting process.

[2] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156

4. NETWORK SUSTAINABILITY PLAN DURING THE PROJECT

This section introduces the network engagement, sustainability plan and concrete engagement measures during the project, and underlines connections to other EU-HYBNET tasks, activities and events, as well as key tools to engage and expand the network.

The sustainability plan is based on the EU-HYBNET D5.1 "Dissemination, Communication and Exploitation Strategy" and the stakeholders engagement strategy defined in this document. For the sake of articulation, we make a distinction between e*ngagement* as initial awareness-raising activity and attraction of new network members, and *sustainability* as maintenance of engaged stakeholders within the EU-HYBNET network. For this reason, the following key objectives of the network engagement and sustainability plan are defined respectively as:

1. To raise awareness and **create interest** to attract new members to the network (corresponding to Informing, Consulting and Involving stages of the EU-HYBNET sustainability process presented in Chapter 2.4)
2. To **maintain interest** and encourage communication and joint activities among network members (corresponding to Collaborating, Empowering and Sustaining stages)

The engagement of new network members will happen throughout the 5 years of the project. The 2 objectives above will be implemented through the project cycles, starting from raising awareness among potential new members (via dissemination activities and via open invitation to join the network) and proceeding with the network engagement activities (via facilitating interactions between the network members).

4.1 CONNECTIONS TO EU-HYBNET TASKS AND ACTIVITIES

The EU-HYBNET network members are not passive actors learning and benefiting from the project's results and findings but also active contributors to the project. The network aspires to ensure close interaction between the project consortium and network members and thereby to provide sustainability for the network activities.

The network members are expected and encouraged to bring their contribution to the project by providing valuable inputs in different EU-HYBNET events, where the network members are invited. In addition, the network members have a possibility to contribute to the project's research activities and in its articulation of solutions to the gaps and needs identified. The engagement with the project consortium and network members is to ensure that the project addresses the needs and possible solutions from a wider European security audience.

The network members' contribution to EU-HYBNET project is relevant in the following areas:

- *To define* gaps and needs for pan-European practitioners and other relevant actors' measures to counter hybrid threats.
- *To define* and offer the most promising solutions, innovations (technical, non-technical) to pan-European practitioners and other relevant actors' measures to counter hybrid threats.

- *To test and to evaluate* technical and non-technical solutions identified to pan-European practitioners and other relevant actors' gaps and needs to counter hybrid threats.
- *To recommend* technical and non-technical solutions identified to pan-European practitioners and other relevant actors' gaps and needs to counter hybrid threats.
- Contribute to EU-HYBNET *research article writing* on the prioritized topics concerning hybrid threats.
- *To disseminate and exploit* EU-HYBNET project results and findings within own organization and work.

4.2 KEY TOOLS TO ENGAGE AND EXPAND THE NETWORK

The EU-HYBNET project arranges many different types of events and offers a variety of tools to engage with the network members, hence ensuring that the network members have their voice heard in the project and joint activities.

4.2.1 COLLABORATIVE PLATFORMS

The EU-HYBNET project offers the following platforms to EU-HYBNET Network members to engage with the EU-HYBNET consortium partners and to deliver their views to the project execution. The platforms are described in detail within EU-HYBNET public deliverable 1.15 "Established EU-HYBNET Network Platforms" and hence only a summary of the importance of the platforms is provided below.

- *Innovation Arena (IA)*
  IA is a platform for EU-HYBNET consortium partners and EU-HYBNET network members where members can announce gaps and needs to counter hybrid threats and also possible solutions and ideas to cover the gaps and needs.
- *TUOVI Platform*
  TUOVI platform is a platform where consortium partners and network members can work with each other and share information that supports knowledge of and measures to counter hybrid threats.
- *Project website, LinkedIn, Twitter*
  The project website provides general information, updates, achievements and context to network members, wider audiences and stakeholders alike. The website also works as an archive to find relevant research articles, policy documents and project deliverables.
  Additionally, EU-HYBNET Twitter and LinkedIn accounts serve as fast-track information sharing platforms that actively engage network members and stakeholders.

4.2.2 EU-HYBNET EVENTS

The network members will be invited to following EU-HYBNET project events and activities to ensure vivid interaction between the consortium and network members and to gain expert feedback from network members pertaining to the project's proceeding and results.

- *Gaps and Needs Event* (c. March 2023, June 2024)

Network members are invited to share their views on the current gaps and needs of pan-European practitioners and other key actors' measures to counter hybrid threats. The information is

analysed in the project to define the context for vulnerabilities, and to find the most critical gaps and needs and also possible solutions (technical or non-technical/ e.g. social science based) to best cover the gaps and needs.

- *Trainings and exercises* (c. February 2024)

Network members are invited to participate in EU-HYBNET trainings and exercises during which identified solutions (technical or non-technical/ e.g. social-sciences based) for the gaps and needs are tested and evaluated. In addition, the trainings and exercises will include lectures on hybrid threats and hence enhance the general knowledge and measures to counter hybrid threats.

- *Innovation and Knowledge exchange events* (c. December 2023)

These events are arranged especially for practitioners (and stakeholders in general) to facilitate the exchange of information regarding the most promising innovations and knowledge to counter hybrid threats. In addition, the events provide a forum for practitioners to engage with innovation (technical and social innovations) providers, in and outside of the consortium and to monitor solutions for identified gaps and needs to counter hybrid threats. In addition, the event is an arena where network members may assess the feasibility of the EU-HYBNET project activities and findings and provide recommendations for proceeding so that the project would serve the network's interest in the best possible way.

- *Future Trends workshop* (c. April 2023, April 2024, February 2025)

Network members are invited to Future Trends workshops that address expected future manifestations and evolutions of hybrid threats, so that the project and network members not only look into innovations and solutions for today but also for tomorrow.

- *Events on possibilities for innovation standardization* (c. November 2023, December 2024)

Network members who have the background and knowledge of innovation standardization are invited to specifically themed innovation and standardisation workshops to counter hybrid threats. From each session a report will be prepared, in which all of the defined needs and possibilities are listed in relation to the suggested innovations. This information supports the project to further identify innovations and standardisation possibilities. In the workshop, network members have an important role to share their experiences and views on the needs of innovation standardization and way forward.

- *Annual workshops for stakeholders* (c. April 2023, April 2024, February 2025)

Network members are invited to an Annual Workshop (AW) where project findings are disseminated for a large scale of stakeholders. The workshops are designed to enable vivid interaction with industry, academia and other providers of innovative solutions outside of the consortium with a view to assessing the feasibility of project findings and possible recommendations to innovations uptake (incl. industrialisation) and standardisation. Moreover, Annual Workshops will foster network activities, raise awareness of the project and bring together relevant practitioners and stakeholders who may to join the EU-HYBNET network and its activities. The goal of the AW is also to bolster the sustainability of the project activities and increase relevant

members in the network. The AW is important for the network members to review the project's proceeding and to share their wishes for future proceeding.

- *Other possible events e.g. workshops with other EC funded projects (tbc)*

Network members are also invited to other EU-HYBNET project events that might be arranged as a result of cooperation with other Commission funded projects or deriving from a wish of a network members to have a joint/combined event. These events deliver relevant information regarding measures to counter hybrid threats.

4.3 EU-HYBNET NETWORK ENGAGEMENT AND SUSTAINABILITY PLAN

The plan below details key activities that engage and maintain the network during the project's duration. A key feature of the sustainability plan is a joint responsibility of the EU-HYBNET project partners in disseminating, attracting and maintaining interactions with the network members via EU-HYBNET tasks and events described above in this Chapter. The overall responsibility for maintaining and sustaining the network during the project duration belongs to Laurea as EU-HYBNET coordinator organization.

Table 3 EU-HYBNET Network Sustainability Plan

Activity	Implementation schedule	Lead/involved partners
Engagement activities (creating interest, attracting new members)		
Raising Awareness	M1-M60 According to dissemination and communication activities plan	EOS/all partners
Publishing Application to join EU-HYBNET network	M8	Hybrid CoE/Laurea
Sending targeted invitations to join the network	M8-M60 On a continuous basis	Laurea/all partners
Promoting network during EU-HYBNET events	M1-M60 According to the EU-HYBNET events schedule	Laurea/all partners
Accepting new members	M10-M60 Bi-monthly	Laurea (PMB) and Hybrid CoE
Maintenance activities (maintaining interest and interactions among network members)		
Inviting network members to participate in EU-HYBNET events	M10-M60 According to the EU-HYBNET event schedule	EOS/all partners
Facilitating network interactions in TUOVI and IA	M10-M60 Monthly	Laurea
Promoting netwok member organizations via EU-HYBNET Social Media (e.g. tagging in tweets)	M1-M60 According to dissemination and communication activities plan	EOS/all partners
Encouraging and engaging network members to participate in joint EU-	M10-M60 According to cooperation events as described in section 4.2.2	Laurea/EOS, Hybrid CoE

HYBNET events with other projects and initiatives		

4.4 ASSESSMENT OF THE EU-HYBNET NETWORK ENLARGEMENT IN M1-M30

As mentioned before, the EU-HYBNET network currently has 81 members (& 25 consortium partners) and it represents a wide selection of European practitioners, SME's industry and research organisations, all deeply involved in the work of countering hybrid threats.

The network enlargement has progressed remarkably and the KPI target of reaching 30 new network members annually has been achieved.

The network continues to put a lot of effort in attracting key organisations in the field of hybrid threats. After the general project review from October 2021, the consortium has started to reach out to European SME's in order to complement the network structure.

The project has also started to actively engage its network partners and it has taken efforts to increase the participation in events now that Covid-19 pandemic has plateaued.

Extra steps in community building have also been taken in the form of roadshows during the Future trends workshop in April 2022 in Rome and in the Innovation and knowledge exchange workshop in June 2022 in the Hague.

Hybrid CoE has created a video on hybrid threats, and it has been shared on TUOVI platform, thereby increasing the network members' understanding hybrid threats.

5. NETWORK SUSTAINABILITY BEYOND THE PROJECT

Section 5 presents a sustainability plan for the network beyond the EU-HYBNET project lifecycle. The aim is to maintain and consolidate the well-established collaboration between different practitioners.

5.1 KEY ISSUES IN NETWORK SUSTAINABILITY

The EU-HYBNET network will be handed over to Hybrid CoE to host after the project term has ended. To ensure an easy transition, Hybrid CoE will develop a specific plan for the network hand-over. This plan will be designed within the last six months of the project, and it will be contained in the sustainability deliverable at Month 60, as an implementation of the principles outlined in the present deliverable.

During the project, the Hybrid CoE will look at the sustainability of the EU-HYBNET network from many different angles to ensure that the transition can be achieved in the best possible way and that all parties involved can benefit from the collaboration also after the project's lifecycle.

As stated in the KPI 1.4 of project objective 1, Hybrid CoE does not have to use the name EU-HYBNET after the project's completion in 2025. It is therefore useful to have a thorough assessment of the current project activities and tools and to keep in mind the essence of the network which is to connect resources, innovations and solutions to European practitioners' gaps and needs in countering hybrid threats.

5.2 MAIN PRINCIPLES FOR NETWORK SUSTAINMENT AFTER 2025

With due consideration of the Hybrid CoE Memorandum of Understanding, the main principles for sustainment of the network beyond 2025 are presented below:

Principles:

The Hybrid CoE will, upon the project's completion in 2025, invite EU-HYBNET network members to join its expert networks. This provides several benefits for the EU-HYBNET network members: joining an international, network-based organization promoting a whole-of-government and whole-of-society approach in countering hybrid threats. However, Hybrid CoE will reserve the right to review and screen the network members and also to deny accession, in particular in cases where the given network member would have been inactive or demonstrated a lack of competence during the project life cycle.

EU-HYBNET four core themes after the project's completion

The Hybrid CoE will seek to build a working methodology in order to fuse, where appropriate and in furtherance of the Hybrid CoE's yearly Work Programme, the input of the network members through the core theme "Future Trends of Hybrid Threats". The four core themes of the EU-HYBNET project ("Future Trends of Hybrid Threats", "Cyber and Future Technologies", "Resilient Civilians, Local Level and National Administration", "Information and Strategic Communication") are relevant to Hybrid CoE´s work.

Events

The EU-HYBNET Future Trends Workshop may possibly be continued after 2025 but the decision will be made towards the end of the EU-HYBNET project.

Platforms

The Hybrid CoE considers the future of project platforms TUOVI and Innovation Arena after 2025 with a view to assessing whether these platforms will be useful or duplicates from the engagement frameworks of the Hybrid CoE, within the framework of which the sustainability of the EU-HYBNET network of practitioners is conceived. In case they duplicate, the Hybrid CoE will maintain relevant engagement with the project members via its own platform.

5.3 PLAN FOR THE EU-HYBNET NETWORK AFTER 2025

Upon the end of the project's lifecycle, the Hybrid CoE will continue to host network members as part of its own expert networks, thereby maintaining and consolidating the existing collaboration between different practitioners.

The project events and activities will not be continued as such but by joining the Hybrid CoE expert network, the EU-HYBNET members will continue to be invited to a selection of events organized by Hybrid CoE. Other appropriate activities enabling a full use of the potential of Hybrid CoE's diversified networks can be planned.

6. NETWORK SUSTAINABILITY RISKS AND MITIGATION MEASURES

Network sustainability risks are closely related to the critical risks of the overall EU-HYBNET project implementation and include specifically, risks relating to networking and stakeholders as defined in the EU-HYBNET DoA and described in Table below.

Table 4 EU-HYBNET Network risks

EU-HYBNET Network Risks	Impact	Mitigation measures
Failure to enrich the EU-HYBNET network	**Low** – *Low*	Concerns for the dangers associated to hybrid threats are high and therefore opening possibility to join the network events and innovations will strengthen end user capabilities
Inability to establish enhanced interactions with practitioners and other actors	**High** – *Low*	-Platform for information exchange will be established -Community forums will be established and events held -Roadmap for increasing networking activities is created -Training events will be organised
Not achieving network sustainability	**Low** – *Low*	European Centre of Excellence for Countering Hybrid Threats will keep leadership in post-project activities for EU-HYBNET
Low attendance at events	**High** – *Medium*	- If attendance is weak, marketing and dissemination of events will be increased - Organisers will draw lessons learned after events (in form of workshop reports) where attendance and impact are assessed and draw from those throughout the project
– Not having the right participants attending workshops, e.g. subject matter experts	**Medium** – *Medium*	Clear instructions will be provided to potential participants, stating what is required of them when attending workshops, e.g. subject knowledge. Additionally, they will be provided with a list of activity objectives and required outcomes of the workshops, so they can make an informed decision on whether or not they should participate. This will be done in a timely manner in order to invite alternative participants when original participant is unable to fulfil the requirements
Trolling of the project	**Low** – *Low*	Precise project media monitoring processes in the Dissemination and Communication strategy, incl. measures to handle trolling
Inadequate access to stakeholders	**Medium** - *Medium*	-Already there is a strong representation of many EU countries in the EY-HYBNET consortium -Already committed external stakeholder groups are in place
Low interest in joining the European Network against Hybrid Threats and its activities	**High** - *Medium*	-Promptly planned measures for network extension -Increased dissemination activities and project partners' involvement to secure interest, and engage potentially new member candidates in the activities of the Network

In addition, the following risks related to the sustainability of the network have been identified by the project partners:

Table 5 Additional risks identified during the project

EU-HYBNET Network Sustainability Risks	Impact	Mitigation measures

Network will grow too big to stay active	**Low** – *Low*	- New members will be accepted on a continuous basis, taking into consideration existing network structure and balanced representation of organizations. If too many applications are received, decision will be made to limit accepted members to 30/year - Systematic engagement of the network members in the online (TUOVI, IA) and offline (events) activities will be performed at least once a month to facilitate active interactions
Nature of a network member changes in critical way	**Medium – Low**	- Acceptance of the new members will be done based on the Eligibility Criteria defined in D1.7, which minimizes possibilities of accepting legal entities that can be harmful to the network - Balanced representation of practitioners and other actors will be monitored and maintained - In case of any network member violating the network rules, they will be excluded from the network.
Network member(s) raise concerns due to passivity or misconduct	**Medium - Low**	- Any partner can raise concerns about a network participant. The concern will be evaluated by PMB and Hybrid CoE. A reason for exclusion includes passivity (does not do anything, does not respond to anything) and bad behavior (spreads disinformation, for example). An exclusion decision will be accomplished collectively during a PMB meeting, in cooperation with Hybrid CoE.

7. CONCLUSION

7.1 SUMMARY

In this document we have described the EU-HYBNET network sustainability plan and how the network will live on after the project's completion in 2025. Measures to keep the network active after 2025 were described. The final plan for network sustainability will be published in the final months of the project.

7.2 FUTURE WORK

D1.24 is an important deliverable for EU-HYBNET in that it outlines the principles for a sustainable approach to the EU-HYBNET Network's extension and its continuity beyond the project duration.

D1.24 lays the foundation for EU-HYBNET deliverable D1.25 "*EU-HYBNET Network Sustainability Final Report*" (project month 60/ April 2025).

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EC	European Commission
EU	European Union
EU MS	EU Member State
AC	EU Associated Countries
H2020	Horizon2020 Program
CSA	Coordination and Support Action
EU-HYBNET	A Pan-European Network to Counter Hybrid Threats project
NoP	Network of Practitioners project funded by EC
CoU	Community of Users, EC hosted group based on funded projects
GDPR	General Data Protection Regulation
DoA	Description of Action
D	Deliverables
WP	Work Package
T	Task
M	project month
MS	Milestone
NM	EU-HYBNET Network Manager
PMB	EU-HYBNET Project Management Board
SG	Stakeholder Group
IA/Innovation Arena	Platfrom for EU-HYBNET consortium and network members to use for gaps&needs and innovative solutions sharing
TUOVI	Platform for EU-HYBNET consortium and Network members to engage
Eduuni	Platfrom for EU-HYBNET consortium to internal project work
OB.	Objective
KPI	Key Performance Indicator
NGO	Non-governmental organization
LAUREA	Laurea-ammattikorkeakoulu Oy
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras

URJC	Universidad Rey Juan Carlos
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
EOS	European Organisation for Security Scrl
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
SATWAYS	SATWAYS
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
UCSC (UNICAT)	Universita Cattolica del Sacro Cuore
JRC	JRC - Joint Research Centre - European Commission
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NLD MoD	Ministry of Defence/NL
ICDS	International Centre for Defence and Security, Estonia
PLV	Ayuntamiento de Valencia / Valencia Local Police
ABW	Polish Internal Security Agency
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
COMTESSA	Universitaet der Bundeswehr München

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.