



# EU-HYBNET

## UPDATED DISSEMINATION, COMMUNICATION AND EXPLOITATION PLAN 3

DELIVERABLE 5.5

Lead Author: European Organisation for Security (EOS)

Contributors : All partners  
Deliverable classification : Public (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

**D5.5 UPDATE OF THE DISSEMINATION COMMUNICATION AND EXPLOITATION PLAN 3**

<b>Deliverable number</b>	<b>D5.5</b>	
<b>Version:</b>	<b>V1.0</b>	
<b>Delivery date:</b>	<b>08/01/2025</b>	
<b>Dissemination level:</b>	<b>Public (PU)</b>	
<b>Classification level:</b>	<b>PU</b>	
<b>Status</b>	<b>Final</b>	
<b>Nature:</b>	<b>Report</b>	
<b>Main authors:</b>	<b>Vincent Perez de Leon-Huet</b>	<b>EOS</b>
<b>Contributors:</b>	<b>All partners</b>	Laurea, MTES, URJC, Hybrid CoE, PPHS, UiT, RISE, KEMEA, L3CE, TNO, Satways, Espoo, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, Maldita, ZITiS, COMTESSA

**DOCUMENT CONTROL**

<b>Version</b>	<b>Date</b>	<b>Authors</b>	<b>Changes</b>
0.1	15/12/2024	Vincent Perez de Leon-Huet (EOS)	First draft
0.2	20/12/2024	Petteri Partanen (LAU) ; Jari Rasanen (LAU)	Comments and minor changes
0.3	23/12/2024	Vincent Perez de Leon-Huet (EOS)	Corrections and preparation for submission
1.0	08/01/2025	Tiina Haapanen (LAU)	Final text editing and submission to EC

**DISCLAIMER**

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

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

© Copyright in this document remains vested in the Project Partners

## TABLE OF CONTENT

1. Introduction .....	5
1.1 Overview .....	5
1.2 Structure of the deliverable .....	6
2. Engaging with the hybrid threats ecosystem .....	8
2.1 Objectives for engaging.....	8
2.1.1 General objectives for engaging.....	8
2.1.2 Specific objectives for engaging with hybrid threats ecosystem .....	8
2.1.3 Specific objectives for engaging with the hybrid threats ecosystem in the frame of EU-HYBNET .....	8
2.2 Level of engagement .....	9
3. Stakeholders' Engagement.....	12
3.1 Identification of stakeholder categories .....	12
3.1.1 Practitioners .....	12
3.1.2 Industry, including smes.....	14
3.1.3 Policy bodies.....	15
3.1.4 Scientific community .....	16
3.1.5 Other categories.....	18
3.1.6 Civil society.....	21
3.2 Stakeholders' needs .....	22
Practitioners .....	22
Industry, including SMEs .....	23
Public / Policy bodies .....	23
Scientific community.....	23
Other categories.....	23
3.3 Identification of priority groups .....	24
3.3.1 Priority groups.....	24
3.3.2 Other Stakeholders .....	24
4. Key messages to be shared .....	26
5. dissemination, communication and exploitation means towards engagement .....	29
5.1 Main dissemination MEANS.....	29
5.1.1 Online dissemination MEANS.....	29
5.1.2 Other dissemination MEANS.....	35
5.1.3 Dissemination through events .....	35
5.1.4 relationship with other relevant projects .....	40
5.2 Communication meaning .....	40
5.2.1 Visual materials .....	40

5.2.2 EU-HYBNET website .....	41
5.2.3 EU-HYBNET social network and social media strategy.....	41
5.2.4 Newsletter.....	45
5.2.5 Press releases .....	46
5.2.6 Communication policy.....	49
5.3 exploitation of results .....	50
6. Engagement roadmap.....	54
6.1 Launch Phase: creating awareness .....	54
6.2 Implementation phase: engagement in eu-hybnnet and information about the outcomes of eu-hybnnet ..	54
6.3 Sustainable phase: evaluating, sustaining and disseminating the final results.....	54
7. Monitoring and evaluation process to apply .....	55
8. DCE: Other Relevant Issues .....	61
8.1 General Data Protection Regulation (GDPR).....	61
8.2 Ethical Matters .....	61
8.3 Security Matters.....	62
8.4 Crisis Communication Plan.....	62
9. Conclusions .....	62
9.1 Summary .....	62
ANNEX I: GLOSSARY AND ACRONYMS .....	63
ANNEX II: REFERENCES.....	65
ANNEX III : EU-HYBNET LOGO.....	66
ANNEX IV : EU-HYBNET Color codes.....	67
ANNEX V: EU-HYBNET Partners social media Account.....	68
ANNEX VI : Updated Crisis Communication Plan .....	69
ANNEX VII : EU-HYBNET UPDATED PRESENTATION TEMPLATE .....	70
ANNEX VIII : EU-HYBNET DELIVERABLE TEMPLATE .....	71
ANNEX IX: Agenda of the 3 <sup>rd</sup> IKEW .....	72
ANNEX X: Agenda of the 2 <sup>nd</sup> ISW.....	73
ANNEX XI: AGENDA of the 3 <sup>rd</sup> ISW .....	75
ANNEX XII: Agenda of the 3 <sup>rd</sup> FTW .....	78
Annex XIII: Agenda of the 4 <sup>th</sup> FTW .....	80
ANNEX XIV: Agenda of the 3 <sup>rd</sup> AW .....	82
ANNEX XV: Agenda of the 4 <sup>th</sup> Aw .....	83

## TABLES

Table 1 Level of engagement following the Spectrum of the Public Participation .....	10
--	----

Table 2 Revised list of Practitioners within the EU-HYBNET Network .....	13
Table 3 Industry and SME within the EU-HYBNET network .....	14
Table 4 Key Policy Bodies for EU-HYBNET .....	15
Table 5 Academia and researcher within the EU-HYBNET Network .....	17
Table 6 Pre-existing related initiatives .....	18
Table 7 Related projects .....	20
Table 8 Examples of Cooperation with Security Research Projects .....	21
Table 9 Non-governmental Organisations within the EU-HYBNET Network .....	22
Table 10 Key messages for targeted groups .....	26
Table 11 Partners Exploitation Strategies .....	50
Table 12 EU-HYBNET KPIs (2nd update) .....	55
Table 13: KPIs for M52-M60 .....	58
Table 14 Glossary and Acronyms .....	63
Table 15 EU-HYBNET Partners' Social Media Accounts .....	68

## FIGURES

Figure 1: IAP2 Spectrum of Public Participation .....	10
Figure 2 EU-HYBNET stakeholders' categories .....	12
Figure 3: Current website homepage .....	31
Figure 4: Innovation Arena use cases .....	32
Figure 5: Innovation Arena Content Types .....	32
Figure 6: TUOVI Front Page .....	34
Figure 7: EU-HYBNET Twitter account homepage .....	42
Figure 8: Tweet to inform about the inclusion of EU-HYBNET in the TRAUMA OGGI Event .....	43
Figure 9: EU-HYBNET LinkedIn Profile .....	44
Figure 10: Examples of updates from EU-HYBNET LinkedIn account .....	45
Figure 11: EU-HYBNET Newsletter April 2021 .....	46
Figure 12: Press release of the 4 <sup>th</sup> FTW .....	49
Figure 13: EU-HYBNET logo .....	66
Figure 14: EU-HYBNET Color code .....	67
Figure 15: EU-HYBNET Crisis Communication Plan .....	69
Figure 16: EU-HYBNET Presentation Table .....	70
Figure 17: EU-HYBNET Deliverable template .....	71
Figure 18 : Agenda of the 3rd IKEW .....	73
Figure 19: Agenda of the 2nd ISW .....	75
Figure 20: Agenda of the 3rd ISW .....	77

Figure 21: Agenda of the 3 <sup>rd</sup> FTW .....	79
Figure 22: Agenda of the 4 <sup>th</sup> FTW .....	81
Figure 23: Agenda of the 3 <sup>rd</sup> AW .....	83
Figure 24: Agenda of the 4 <sup>th</sup> Annual Workshop .....	85

## 1. INTRODUCTION

### 1.1 OVERVIEW

The EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) project aims at enriching the existing European networks countering hybrid threats and ensuring long term sustainability. This will be achieved by defining the common requirements of European practitioners' and other relevant actors in the field of hybrid threats. Ultimately, the project is filling knowledge gaps, deals with performance needs, and enhances capabilities, research, innovation and training endeavours concerning hybrid threats.

EU-HYBNET monitors developments in research and innovation activities as applied to hybrid threats; so as 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.

EU-HYBNET is establishing conditions for enhanced interactions with practitioners, industry, and academia for a meaningful dialogue and for increasing membership in the network. The defined objectives of the project are:

- Objective 1: To enrich the existing network countering hybrid threats and ensure long term sustainability;
- Objective 2: 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;
- Objective 3: To monitor developments in research and innovation activities as applied to hybrid threats;
- Objective 4: 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;
- Objective 5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network;
- Objective 6: To foster capacity building and knowledge exchange on countering hybrid threats; and
- Objective 7: To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats.

Finally, EU-HYBNET fosters increased capacity of European practitioners' and other relevant actors in the field of hybrid threats – helping to build knowledge and encourage valuable exchange on countering hybrid threats. The project is creating a basis for establishing effective synergies with

existing European, national, and sub-national networks of practitioners and other actors countering hybrid threats.

The Dissemination, Communication and Exploitation Strategy (DCE – Deliverable (D) 5.1) introduced the overall engagement approach that EU-HYBNET will follow and respect for the 60 months of its lifecycle. The main purpose of D5.1 was to ensure that:

- **Project outputs and outcomes are widely disseminated to the right target audiences**, respecting an appropriate and defined timing, through intelligible channels and tools,
- **Stakeholders can contribute to the outputs development, evaluation and exploitation**. Thus, they should be identified and encouraged from the start to proactively interact with the consortium partners on a systematic basis.

The objectives of EU-HYBNET require first an understandable stakeholders' engagement approach - a key point of the DCE. The primary step of knowing what has to be reached and understand why it must be reached, helps with the implementation of the engagement process in a significant way. These efforts define the appropriate messages for the relevant stakeholders, selects adequate tools and uses suitable channels, respecting a defined timing.


In order to ensure that the DCE plan remains relevant and up to date, the plan undergoes reviews by the WP5 leaders (EOS) to update it based of the evaluations by URJC. The first update of the plan was D5.3 (Updated Dissemination, Communication and Exploitation Plan), following the first phase of implementation of the project. At M18 (October 2021), the project's first cycle ended providing the DCE Team with valuable lessons learned. Moreover, D5.2 'Midterm Project Dissemination Impact Assessment Report 1' was successfully submitted at M16 (August 2020). These two elements, along with the project's first review, constituted the basis for the first update of the DCE Plan (D5.3 Updated Dissemination, Communication and Exploitation Plan, M18). With the second cycle of the project concluding in M34 (February 2023), D5.4 (Updated Dissemination, Communication and Exploitation Plan 2) was the second update of the plan based on D5.6 "Midterm Project Dissemination Impact Assessment Report 2" submitted at M35 (March 2023), the lessons learned from the second cycle, and the comments from the 2<sup>nd</sup> project review.

Currently, EU-HYBNET is on its fourth and final cycle. Following the submission on D5.7 "Midterm Project Dissemination Impact Assessment Report 2" (aimed for M58, December 2024), D5.5 will be the final Dissemination, Communication and Exploitation plan submitted by the consortium. This plan will adjust the plan based on the findings of D5.7, but also focus on the sustainability measures that can be implemented post-project by consortium members.

## 1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 2 presents EU-HYBNET general strategy for engaging with the hybrid threats ecosystem;
- Section 3 defines the stakeholders that will be targeted by the project's dissemination team in order to foster engagement;
- Section 4 presents key messages that will be shared throughout the project;

- Section 5 highlights introduces the reader to the dissemination, communication and exploitation means aiming to engagement;
  - Section 6 defines an Engagement Roadmap;
  - Section 7 lists the monitoring and evaluation means that will be applied
  - Section 8 consists in data management, ethical, security guidelines and the Crisis Communication Plan
  - Section 9 outlines the conclusions.
- 



## 2. ENGAGING WITH THE HYBRID THREATS ECOSYSTEM

### 2.1 OBJECTIVES FOR ENGAGING

Understanding the logic behind stakeholder engagement is the first step for a well-defined engagement strategy, including the selection of appropriate tools to be used. In this section, an overview of objectives, starting from a general vision and concluding with a more specific and coherent approach to EU-HYBNET is presented. After many midterm assessments, the objectives remain unchanged as they are fit for purpose.

#### 2.1.1 GENERAL OBJECTIVES FOR ENGAGING

- **Extend and enhance EU-HYBNET's reputation:** communicating about EU-HYBNET will improve its image and gain stakeholders' trust;
- **Boost awareness of EU-HYBNET's** objectives and outcomes at local, national, European and international levels;
- **Intensify EU-HYBNET's impact:** efficient and personalized communication with stakeholders will support the uptake of the project's outcomes and increase their relevance;
- **Gather information:** about EU-HYBNET stakeholders' needs and requirements.

#### 2.1.2 SPECIFIC OBJECTIVES FOR ENGAGING WITH HYBRID THREATS ECOSYSTEM

*"Hybrid threats are methods and activities that are targeted towards vulnerabilities of the opponent. Vulnerabilities can be created by many things, including historical memory, legislation, old practices, geostrategic factors, strong polarisation of society, technological disadvantages or ideological differences. If the interests and goals of the user of hybrid methods and activity are not achieved, the situation can escalate into hybrid warfare where the role of military and violence will increase significantly."*[1]

Accordingly, Hybrid CoE identifies as a hybrid threat:

- *Coordinated and synchronised action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means.*
- *The activities exploit the thresholds of detection and attribution as well as the different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy).*
- *The aim of the activity is to influence different forms of decision making at the local (regional), state, or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target."*[1]

The hybrid threats ecosystem is very sensitive and complex, involving various organisations and activities. The fight against hybrid threats is continues being a priority in modern societies. An adequate awareness and understanding of the concept must be reached to ensure Europe adopts a systematic approach to better manage evolving risks and vulnerabilities. The EU-HYBNET project and the dissemination of its results with the involvement of all relevant stakeholders is crucial in that regard.

#### 2.1.3 SPECIFIC OBJECTIVES FOR ENGAGING WITH THE HYBRID THREATS ECOSYSTEM IN THE FRAME OF EU-HYBNET

Stakeholder engagement is a crucial first step for a systemic secure society. Enhancing the EU's resilience to hybrid threats by creating a state-of-the-art network and ensuring synergies with other European, subnational and national networks, specifically with security practitioners, academia and industry, NGO and other EU-funded projects, will help deliver this goal.

By identifying and considering the needs and concerns of all relevant stakeholders, the general objectives in countering hybrid threats will be further specified to meet the needs of the project in a way that connects the gaps and needs of practitioners and policymakers with innovative solutions and the research landscape. In that way the project can lead to an increase of the EU's awareness and capabilities established to detect and counter hybrid threats.

Engaging with relevant stakeholders in EU-HYBNET ensures the coherence of future innovations and solutions in the domain of technical and social research, and of their results on e.g., cognitive/informational aspects, attitude manipulation and behavioural effects of overt and covert disinformation and propaganda campaigns. These results are being disseminated to the Hybrid Threats stakeholders through the establishment of multi communication channels.

Following EU-HYBNET's first cycle, the DCE Team noticed the lack of knowledge when it comes to hybrid threats. Indeed, most project events began with an introduction to the concept in order to make sure there is a consensus on definitions. In the second cycle (M18-M34), information around hybrid threats phenomena was further specified and refined to meet the needs of all audiences, e.g., through brochures targeting SMEs or practitioners, and a video on the definition of hybrid threats, created by Hybrid CoE and shared with the consortium.

As the third cycle began, it was apparent that the consortium and network, as well as external stakeholders are well aware of the definition of hybrid threats. For this reason, the DCE team focused on revamping communication materials to share the project's results and added value in a simplified manner, allowing wider audiences to digest what EU-HYBNET was producing and raise awareness about hybrid threats. Additionally, the DCE focused on engaging a more diverse audience of stakeholders, including the European Parliament and other DGs and agencies of the EC.

For the fourth and final cycle, the aim of the DCE team is to highlight the final results of the project and summarise the 5-year project of EU-HYBNET. To achieve this, the DCE team will structure the final events of the project to present the results in this manner, as well as develop dissemination and communication materials for the event that encompass all of EU-HYBNETs results.

## 2.2 LEVEL OF ENGAGEMENT

Like other EU funded projects, EU-HYBNET follows the Spectrum of Public Participation which has been developed by the International Association of Public Participation (IAP2): **informing** (providing the public with balanced and objective information to assist them in understanding the problem, alternatives, opportunities and/or solutions), **consulting** (obtaining public feedback on analysing, alternatives and/or decisions), **involving** (working directly with the public, throughout the process to ensure that public concerns and aspirations are consistently understood and considered), **collaborating** (partnering with the public in each aspect of the decision including the development of alternatives and the identification of the preferred solution) and **empowering** (placing final decision making in the hands of the public).[2]

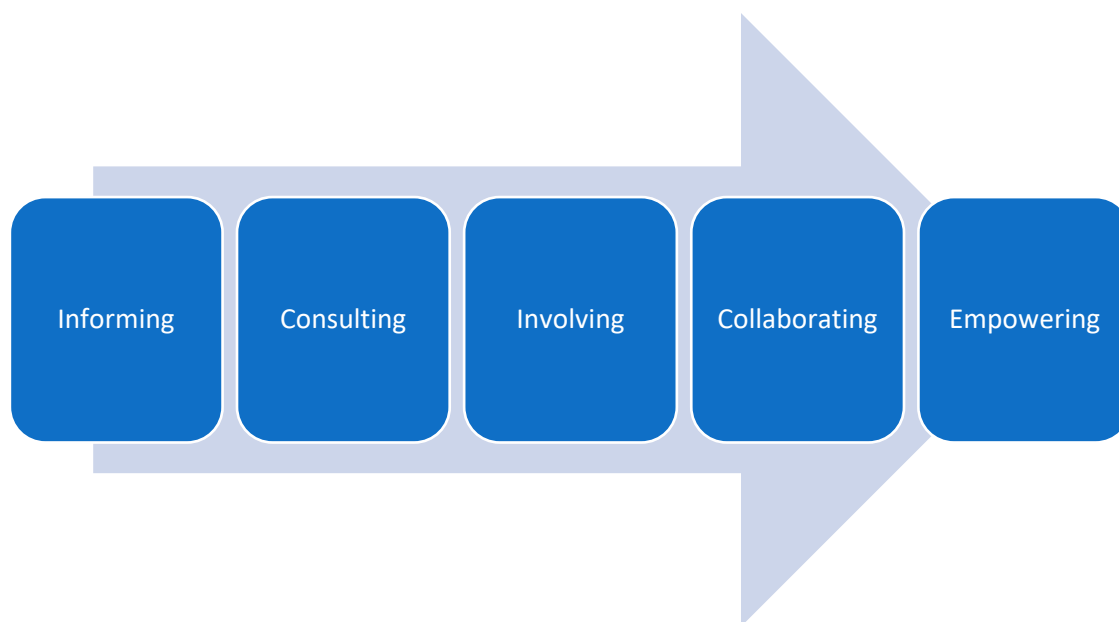


Figure 1: IAP2 Spectrum of Public Participation

With the table below, the consortium illustrates the meaning of the steps within the process and its use within EU-HYBNET:

Table 1 Level of engagement following the Spectrum of the Public Participation

	<b>Informing</b>	<b>Consulting</b>	<b>Involving</b>	<b>Collaborating</b>	<b>Empowering</b>
<b>Public Participation objective</b>	Provide the public with relevant and constructive information, the purpose being the public to understand the goals of EU-HYBNET and the concept of hybrid threats	Get the public's feedback on decisions taken within EU-HYBNET	Ensure that the public concerns and aspirations regarding EU-HYBNET are well-received and taken into consideration by the consortium	Partner with the public in several aspects of EU-HYBNET	Place decision making in the hand of the Public
<b>Promises made to the Public</b>	Keep the public informed about the outcomes of EU-HYBNET <i>* Information shared on the website, on</i>	Keep the public informed, of its concerns and provide feedback on how its input influenced a decision	Make sure that its concerns are reflected in the alternatives developed and provide feedback on how its input influenced the decision taken	Work closely with the public in incorporating its advice and recommendations into the decisions <i>*Possibility for the public to share advices and</i>	Implement what the public decides within and through EU-HYBNET <i>*Feedback from the network is</i>

	<i>the social media channels and during the events organised</i>	<p>taken within EU-HYBNET</p> <p>*</p> <p><i>Information shared on the website, on the social media channels and during the events organised</i></p>	<p><i>*Floor opened to registered participants during EU-HYBNET events to discuss their concerns, ask for more information as well as provide feedback on the project</i></p>	<i>recommendations during events. Floor opened to discussions with the public</i>	<i>taken into account for improving EU-HYBNET activities.</i>
--	--	--	---	---	---

### 3. STAKEHOLDERS' ENGAGEMENT

To maximise the engagement of the stakeholders, D5.1 clearly defined the categories of stakeholders, their needs and their priority for the project. Based on this analysis, EU-HYBNET started building its network. In this document, the tables below show the members of the network as well as the organisations with which interaction has been and will be made. These lists are continuously updated throughout the project.

#### 3.1 IDENTIFICATION OF STAKEHOLDER CATEGORIES

The different stakeholders' categories identified for EU-HYBNET purposes are the following:

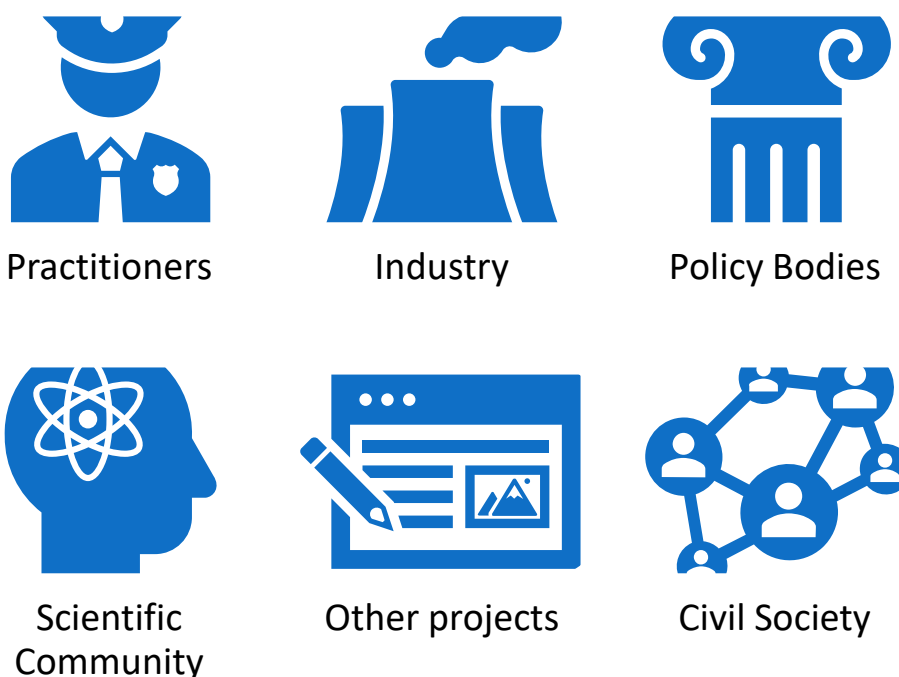


Figure 2 EU-HYBNET stakeholders' categories

The following list takes into account EU-HYBNET's successful Network expansion since the beginning of the project.

##### 3.1.1 PRACTITIONERS

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.”[3] 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.

Accordingly, EU-HYBNET practitioners are categorized as follows:

- Ministry level (administration);
- Local Level (cities and regions); and
- Support functions to ministry and local levels (including Europe's third sector).

EU-HYBNET includes practitioners from all of these levels and the project's primary focus is on security issues. EU-HYBNET partners include the following areas of expertise: internal and external security issues, law enforcement, civil protection and CBRN, forensic information analysis and cyber security, national and regional resilience and support functions.

The EU-HYBNET consortium has stuck to this wide approach of the concept of practitioners. The table below lists the EU-HYBNET network (Partners of the consortium included) belonging to the Practitioners category:

**Table 2 Revised list of Practitioners within the EU-HYBNET Network.**

<b>Organisation</b>	<b>Country</b>
<b>Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secretaria (partner)</b>	France
<b>Espoon Kaupunki / Region and city of Espoo (partner)</b>	Finland
<b>European Center of Excellence for Countering Hybrid Threats (partner)</b>	Finland
<b>Ministry of Defence (partner)</b>	Netherlands
<b>International Centre for Defence and Security (partner)</b>	Estonia
<b>Valencia local Police (partner)</b>	Spain
<b>Norwegian Directorate for Civil Protection (partner)</b>	Norway
<b>Estonian Information System Authority (partner)</b>	Estonia
<b>Zentrale Stelle für Informationstechnik im Sicherheitsbereich (partner)</b>	Germany
<b>Finish Border Guard (Stakeholders Group)</b>	Finland
<b>Ministry of Justice and Security in the Netherlands (Stakeholders Group)</b>	Netherlands
<b>Tromsø Police District Tromsø (Stakeholders Group)</b>	Norway
<b>Ministry of the Interior (Stakeholders Group)</b>	Finland
<b>Nato HQ joint Force Command</b>	Spain
<b>ENEA</b>	Italy
<b>Cyber - and Information Domain Service HQ</b>	Germany
<b>National Security Authority</b>	Slovakia
<b>Presidium of Police Force</b>	Slovakia
<b>Institute for Strategic Research</b>	France
<b>Ministry of Foreign Affairs</b>	Poland
<b>Swedish Police Authority/ National Forensic Centre</b>	Sweden
<b>Government Centre for Security</b>	Poland
<b>Office of the National Security Council of Georgia</b>	Georgia
<b>National Police Headquarters</b>	Poland
<b>Ministry of Foreign and European affairs, Directorate of Defence</b>	Luxembourg
<b>Luxinnovation</b>	Luxembourg
<b>Romanian Ministry of Economy, Entrepreneurship and Tourism</b>	Romania
<b>Ministry of Interior of the Slovak Republic</b>	Slovakia

<b>LEPL Cyber Security Bureau under the Ministry of Defence of Georgia</b>	Georgia
<b>Ministry of Foreign Affairs</b>	Netherlands
<b>The Polish Financial Supervision Authority</b>	Poland
<b>National Counterterrorism, Extremism and Cybercrime Agency</b>	Czechia
<b>Stad Geel</b>	Belgium
<b>Tilt</b>	Netherlands
<b>National Security Analytical Centre (NBAC)</b>	Slovakia
<b>CIN Consult GmbH</b>	Austria
<b>City of Imatra</b>	Finland
<b>Vilnius City Municipality Administration</b>	Lithuania
<b>Home Office</b>	United Kingdom

### 3.1.2 INDUSTRY, INCLUDING SMES

Industrial players, being the security industry or the suppliers of security solutions, having an interest in hybrid threats, have a key role to play in building the network of EU-HYBNET.

Being invited to attend events and workshops of EU-HYBNET, their opinion has been given the consortium an oriented idea of what is possible to be done in terms of innovative solutions. This network is invited to attend events and workshops of EU-HYBNET and receives all supportive documents needed. Through the European Organisation for Security, an additional effort will be given to more intensively include this category within the EU-HYBNET network during the next cycles of the project.

**Table 3 Industry and SME within the EU-HYBNET network**

<b>Organisation</b>	<b>Country</b>
<b>European Organisation for Security (partner)</b>	Belgium
<b>SATWAYS (partner)</b>	Greece
<b>Systematic (Stakeholders Group)</b>	France
<b>Expertsystem</b>	France
<b>Ardanti</b>	France
<b>Soprasteria</b>	France
<b>Norsecon</b>	Sweden
<b>Enersec Technology</b>	Romania
<b>Smartlink Communications</b>	Romania
<b>Geostrategic Intelligence Group</b>	Finland
<b>Mira Technologies Group SRL</b>	Romania
<b>Sectyne AB</b>	Sweden
<b>G4S</b>	Belgium
<b>Combitech AB</b>	Sweden
<b>HENSOLDT analytics</b>	Austria
<b>Hybrd Core BV</b>	Belgium

<b>The Hague Centre for Strategic Studies</b>	Netherlands
<b>SIGNALALERT SARL</b>	France
<b>Maltego Technologies GmbH</b>	Germany
<b>Safetech INNOVATIONS SA</b>	Romania
<b>Ridgeway Information EU B.V.</b>	Netherlands
<b>Traversals Analytics and Intelligence GmbH</b>	Germany
<b>DLTCode</b>	Spain
<b>Zetta Cloud</b>	Romania
<b>Datasense Labs Ltd.</b>	Hungary
<b>Correcta</b>	Spain
<b>ISR Nederland BV</b>	Netherlands
<b>CyberEcoCul Global Services</b>	Cyprus
<b>Greensoft SRL</b>	Romania
<b>Prosegur Research</b>	Spain
<b>EFE Verifica – Agencia EFE</b>	Spain
<b>Fingrid Oyj</b>	Finland
<b>Seeders</b>	Greece
<b>GraphAware</b>	United Kingdom
<b>Logically</b>	United Kingdom

### 3.1.3 POLICY BODIES

In this category, experts or organizations working in the public or policy sector and using EU-HYBNET findings for the achievement of their duties to help the society are targeted. The EU-HYBNET Consortium continuously identifies and gets in contact with the relevant stakeholders and invite them to project events and workshops. The consortium also monitors all relevant EU files and discussions related to hybrid threats, including legislation and other instruments on disinformation (e.g., the Digital Services Act, and the Code of Practice for Disinformation), cybersecurity (e.g., the NIS2 Directive), critical infrastructure protection (e.g., CER Directive) and discussions on hybrid threats (e.g., the hybrid threats toolbox, the JRC work on the conceptual model together with Hybrid CoE). If necessary and when possible, they are discussed with policy makers.

Member State experts and policymakers (e.g., in National ministries) are also targeted, but the project has included them in the category of practitioner, based on the definition used.

Below a table recapitulating the main target of the policy bodies category included in the EU-HYBNET Discussion:

**Table 4 Key Policy Bodies for EU-HYBNET**

<b>Network</b>	<b>Target audience</b>
<b>EU Level</b>	



<b>DGs of the EC</b>	Main targets for EU-HYBNET DCE activities: DG HOME, DG CONNECT, DG MOVE, DG DEFIS, DG MARE, DG ECHO,  DGs to additionally target include DG COMP, DG GROW, DG TRADE, DG COMM, DG EAC
<b>Agencies/Bodies of the EC</b>	EUROPOL and their innovation Lab, the European Union Institute for Security Studies (EUISS), the EU Joint Research Centre (JRC), the European Research Executive Agency (REA), the European Centre for Disease Control (ECDC), the European Defence Agency (EDA), The European Border and Coast Guard Agency (FRONTEX), European Union Agency for Cybersecurity (ENISA), the European Aviation Safety Agency (EASA), the European Maritime Safety Agency (EMSA), the European Aviation Crisis Coordination Cell (ECCC), the Computer Emergency Response Team for the EU institutions (CER-TU), EU-LISA
<b>European Parliament</b>	Special Committee on foreign interference in all democratic processes in the European Union, including disinformation, and the strengthening of integrity, transparency and accountability in the European Parliament (ING2), AFET Committee, SEDE Sub-Committee, Committee on the Internal Market and Consumer Protection (IMCO), ITRE Committee, LIBE Committee, DG SAFE
<b>EEAS</b>	Division Security and Defence Policy SECDEFPOL1 – Hybrid Threats, Hybrid Fusion Cell, EAST-STRATCOM Taskforce
<b>Council of the European Union</b>	Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats
<b>European Committee of the Regions</b>	Commission for Citizenship, Governance, Institutional and External Affairs, ECON: Commission for Economic Policy, Commission for Social Policy, Education, Employment, Research and Culture (SEDEC)
<b>Council of Europe</b>	Congress of Local and Regional Authority Secretary General
<b>European Data Protection Board</b>	
<b>The European Reference Network for Critical Infrastructure Protection (ERNICIP)</b>	
<b>Council of European Municipalities and Regions (CEMR)</b>	
<b>European Digital Media Observatory</b>	
<b>Independent Networks</b>	Assembly of European Regions
<b>European Economic and Social Committee</b>	TEN Section for Transport, Energy, Infrastructure and the Information Society, Section for Single Market, Production and Consumption, Section for Employment, Social Affairs and Citizenship (SOC)

### 3.1.4 SCIENTIFIC COMMUNITY

This category, composed by researchers and academics in the domain of hybrid threats is crucial in terms of understanding the concept of hybrid threats. EU-HYBNET aims to make an impact on the scientific community by expanding the existing knowledge of hybrid threats. Academics and researchers in hybrid threats are dedicated to exploring unsolved problems, and looking for new avenues for research or opportunities to validate approaches.

Table 5 Academia and researcher within the EU-HYBNET Network

Organisation	Country
Laurea (Coordinator of the EU-HYBNET Project)	Finland
University of Tromsøe (partner)	Norway
RISE Research Institutes of Sweden Ab (partner)	Sweden
KEMEA (partner)	Greece
Lietuvos Kibernetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras (partner)	Lithuania
University Rey Juan Carlos (partner)	Spain
TNO (partner)	Netherlands
University Cattolica del Sacro Cuore (partner)	Italy
JRC - Joint Research Centre - European Commission (partner)	Belgium
The Romanian National Intelligence Agency (partner)	Romania
University der Bundeswehr München (partner)	Germany
Fraunhofer-IVI (Stakeholders Group)	Germany
SafeCluster (Stakeholders Group)	France
Tecnoalimenti (Stakeholders Group)	Italy
CeSI - Centro Studi Internazionali (Stakeholders Group)	Italy
European Security and Defence College (Stakeholders group)	Belgium
European Health Management Association (Stakeholders Group)	Belgium
CSIC - Spanish National Research Council, Research group on Cryptology and Information Security (Stakeholders Group)	Spain
Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence (Stakeholders Group)	Ukraine
Bulgarian Defence Institute	Bulgaria
Nord University	Norway
Police University College	Finland
CRIMEDIM - NO-FEAR Project	Italy
AIT Austrian Institute of Technology	Austria
Institut Choiseul	France
Vesalius College VZW, part of the Brussels School of Governance and Vrije Universiteit Brussel (VUB)	Belgium
The School of Social Sciences ( of the University of Georgia )	Georgia
EFFECTUS - Entrepreneurial Studies - University College	Croatia
Faculty of Military Sciences	Netherlands
European Institute for Counter Terrorism and Conflict Prevention	Austria
Academic Centre for Strategic Communication	Poland
Defence Institution Building School	Georgia
International Cyber Academy	Poland
Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine	Ukraine
Center for the study of democracy	Romania

<b>Universidad Isabel I de Castilla</b>	Spain
<b>SAPIENZA University of Rome - Department of Human Neuroscience - Interpersonal Violence Research Lab (InterViRe)</b>	Italy
<b>FORTH - Foundation for Research and Technology - Hellas - Institute of Computer Science</b>	Greece
<b>SINTEF Digital, Dept. of Software Engineering, Safety and Security</b>	Norway
<b>University of Dubrovnik</b>	Croatia
<b>Marshall Center</b>	Germany
<b>Helmut-Schmidt-Universität / Universität der Bundeswehr Hamburg</b>	Germany
<b>Carol I National Defence University</b>	Romania
<b>Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering "Traian Lalescu"</b>	Romania
<b>Institute of Legal Personnel Training for the Security Service of Ukraine Yaroslav Mudryi National Law University</b>	Ukraine
<b>Polytechnic Institute of Setubal - School of Technology</b>	Portugal
<b>UCD Centre for Cybersecurity and Cybercrime Investigation</b>	Ireland
<b>Risk and Crisis Centre Mid-Sweden University</b>	Sweden
<b>National Cybersecurity Directorate</b>	Romania
<b>OPEWI</b>	Belgium
<b>Universidad Cardenal Herrera CEU</b>	Spain
<b>VIU - Universidad Internacional de Valencia</b>	Spain
<b>Fraunhofer FOKUS</b>	Germany
<b>University of Turku</b>	Finland
<b>Ghent University BIGDATPOL</b>	Belgium
<b>Elcano Royal Institute for International and Strategic Studies</b>	Spain

### 3.1.5 OTHER CATEGORIES

#### RELATED PROJECTS AND INITIATIVES

Related projects or initiatives are a crucial vector for the development of EU-HYBNET. They are an important stakeholder category, as their work needs to be aligned with EU-HYBNET's approach, avoiding possible overlap and enhancing complementary synergies.

EU-HYBNET has engaged with a wide range of EU Initiatives and EC projects some of which were already identified during the preparation phase and throughout last cycles of the project.

In the following tables, there is an explanation of the links already developed:

Table 6 Pre-existing related initiatives

	<b>EU-HYBNET partners involved</b>	<b>Improvements and benefits that EU-HYBNET delivers</b>
--	------------------------------------	--

<b>The landscape of Hybrid Threats: A Conceptual Model</b>	Hybrid CoE, JRC	<p>Reusable results: This JRC forthcoming technical report is expected to provide a point for reference for the policy making community at national and EU levels, it will facilitate common understanding and raise the awareness of the relevant authorities around the issue of hybrid threats.</p> <p>Reuse: For all EU-HYBNET activities, this report will provide the basis for understanding the phenomenon of hybrid threats.</p>
<b>Workshop on EU/NATO cooperation in civil protection</b>	Hybrid CoE	<p>Reusable results: Hybrid CoE jointly with Romanian MoI organised a dynamic workshop for stocktaking of the EU and NATO requirements and methods for civil protection. Workshop featured a table-top exercise based on medical-based scenario with an embedded hybrid threat. Reusable results: the best practices from the training can be put forward in the EU-HYBNET project.</p>
<b>Scenario-based policy discussions</b>	Hybrid CoE	<p>Reusable results: During the Finnish Presidency of the Council of the European Union, Hybrid CoE was involved in the preparations of scenario-based discussions at ministerial levels.</p> <p>Reuse: empowering the European network with new high level actors and audience interest.</p>
<b>Participation in NATO Science and Technology working groups related to Hybrid Threats</b>	TNO, MoD NL	<p>TNO and MoD NL participate in the NATO Science and Technology Organisation, at all levels (Steering committee, Panels and working groups). TNO will feed results from particular working groups into the EU HYBNET project, if relevant and feasible. One specific ongoing activity that has utmost relevance for EU HYBNET is the working group on Digital and Social Media Assessment for Effective Communication and Cyber. MoD NL can use their voting membership to steer and to stimulate new hybrid threats research within the NATO Science and technology working groups.</p>
<b>Countering Hybrid Threats: Lessons Learned from Ukraine</b>	MVNIA	<p>MVNIA, in partnership with „Bogdan Intemeietorul” National Intelligence and Security Institute from the Republic of Moldova, has organised in August 2015 the workshop “Countering Hybrid Warfare: Lessons Learned from Ukraine.”</p> <p>Reusable results: The event has led to the publication of a book under the aegis of the NATO SPS programme, and to the creation of an informal network of practitioners, academics and security experts.</p>
<b>Security in the Black Sea Region. Shared Challenges, Sustainable Future Program</b>	MVNIA	<p>MVNIA organises, in partnership with Harvard University and National Intelligence University in the US, a training programme for diplomats, security experts and intelligence officers. The latest 4 editions (2015-2019) have had a dedicated section for debates, lectures and exercises related to countering hybrid threats. Reusable results include a database of exercises and simulations, a network of academics</p>

		and an informal platform of practitioners in the Black Sea Region.
<b>European Cluster for Securing Critical Infrastructures (ECSCI)</b>	All partners	<p>EU-HYBNET joined the ECSCI cluster in 2021. The cluster, product of the FINSEC project, is to create synergies and foster emerging disruptive solutions to security issues via cross-projects collaboration and innovation. Research activities will focus on how to protect critical infrastructures and services, highlighting the different approaches between the clustered projects and establishing tight and productive connections with closely related and complementary H2020 projects. To promote the activities of the cluster, ECSCI will organize international conferences, and national or international workshops, involving both policy makers, industry and academic, practitioners, and representatives from the European Commission.</p> <p>Reusable results: EU-HYBNET will be able to use the cluster to promote its results and exploit the networks of other projects to expand its own network.</p>

Table 7 Related projects

Project instrument	EU-HYBNET Partners	EU-HYBNET Outputs feed to following projects	Activity	Field of action
<b>H2020-GM</b>	LAU, EOS, PPHS, L3CE, TNO, KEMEA, SATWAYS, UCSC	MEDEA, I-LEAD ; ARCSAR, EXETER, FIRE-IN, INCLUDING, NO- FEAR	Network extension	LEA cooperation, Search and Rescue, Fire and Rescue, Radiological and nuclear, emergency medical systems
<b>H2020 ICT</b>	LAU, L3CE, RISE	ECHO, SPARTA, CONCORDIA	Research and Innovation hubs' cyber network	Cyber security research and innovation, situational awareness tools, 5G security
<b>H2020 INFRA</b>	EOS, KEMEA, SATWAYS, LAU	SATIE, SAFECARE, PRECINCT, SAFETY4RAILS	Research and Innovation	Security, cyber security research and innovation
<b>H2020-BES</b>	KEMEA, SATWAYS, LAUREA, EOS	CIVILNEXT, AI ARC	Research and Innovation	Information systems, Maritime and border surveillance situational awareness
<b>H2020 DRS</b>	MVNIA, UCSC, SATWAYS, PLV, EOS	LINKS, RISKPACC	Research and Innovation	Man-made and natural disasters, CBRN, disaster response and preparedness risk management
<b>H2020 FCT</b>	KEMEA	SHUTTLE,	EU toolkit for trace analysis, economical& psychological aspects leading	EU forensic laboratories, Citizens interaction, technologies, Social Media, economics and psychology

			criminal activities	
<b>H2020 INT</b>	MVNIA	ESEENTIAL	Ad-Hoc security research	Complex security environment
<b>ISFP</b>	L3CE, MVNIA, KEMEA, PPHS	SENER, ARMOuR, SAFFRON	Network in Cybercrime critical communications	Cybercrime, resilience, detection of foreign fighters

Table 8 Examples of Cooperation with Security Research Projects

Project	Event/Action	Date
<b>InfraStress, SmartResilience, SecureGas</b>	CERIS DRS content planning & delivery with InfraStress, SmartResilience, SecureGas	November 2022
<b>i-LEAD</b>	EU Procurement landscape mapping, results sharing	October 2022
<b>Notiones</b>	Contribution to the EU-HYBNET Ethics Workshop in Critis2022	September 2022 to January 2023
<b>INCLUDING</b>	Contribution to Newsletter content	July 2022
<b>7SHIELD, PRAETORIAN</b>	Presented in EU-HYBNET ISW – best practices, LL on innovations standardization	June 2022
<b>PRECINCT</b>	PRECINCT 1 <sup>st</sup> Stakeholder Engagement Workshop – EU-HYBNET presentation on Hybrid Threats in the context of CI	May 2022
<b>7SHIELD, PRECINCT, MEDEA, ALIGNER</b>	7SHIELD, PRECINCT, MEDEA, ALIGNER invited to AW – presentations on promising innovations	April 2022
<b>ILEAnet</b>	ILEAnet Final Workshop, participation to Panel “Way forward”	April 2022
<b>ECHO</b>	ECHO Cyber Morning – presentation on HT	April 2022
<b>ECSCI Cluster</b>	ECSCI Cluster – 3 EU-HYBNET presentations in 3 day Conference	April 2022
<b>CYCLOPES</b>	CYCLOPES presentation in EU-HYBNET Annual Workshop	April 2023
<b>NO-FEAR</b>	NO-FEAR conference presentation from EU-HYBNET	March 2023
<b>EU-CIP</b>	EU-CIP Annual Conference / ECSCI Cluster Workshop, booth participation	November 2024

### 3.1.6 CIVIL SOCIETY

The civil society is also a crucial stakeholder category directly linked to the development of EU-HYBNET as the objectives of the project environment have to be aligned with the needs of society.

A wide range of NGOs are listed below as members of the EU-HYBNET network. Their contribution is often sought and offered in EU-HYBNET events.

**Table 9 Non-governmental Organisations within the EU-HYBNET Network**

<b>Organisation</b>	<b>Country</b>
<b>Polish Platform for Homeland Security (partner)</b>	Poland
<b>Asociación Maldita (partners)</b>	Spain
<b>European Values Centre for Security Policy</b>	Czech Republic
<b>GLOBSEC</b>	Slovakia
<b>Vilnius Institute for Policy Analysis</b>	Lithuania
<b>Polish Association for National Security</b>	Poland
<b>Friends of Europe</b>	Belgium
<b>Euclid Institute</b>	France
<b>Demagog Association</b>	Poland
<b>The Kosciuszko Institute Association</b>	Poland
<b>Baltic Centre for Media Excellence</b>	Latvia
<b>Fondazione SAFE - Security and Freedom for Europe</b>	Italy
<b>Avoin yhteiskunta ry</b>	Finland
<b>Beyond the Horizon ISSG</b>	Belgium
<b>Istituto Affari Internazionali (IAI)</b>	Italy
<b>VOST Portugal</b>	Portugal
<b>New Strategy Center</b>	Romania
<b>Hybrid Warfare Research Institute</b>	Croatia
<b>SECURE IDENTITY TECHNOLOGIES SL (IDBOTIC)</b>	Spain
<b>Strategic Analysis</b>	Slovakia
<b>Center for East European Policy Studies (CEEPS)</b>	Latvia
<b>Foreign Affairs Institute (FAINST)</b>	Greece
<b>IRI Europe ASBL (International Republican Institute)</b>	Belgium

### 3.2 STAKEHOLDERS' NEEDS

The identification of the stakeholders is a crucial point as EU-HYBNET is delivering targeted messages which could differ from one category to another.

#### PRACTITIONERS

Due to the wide definition of practitioners given in EU-HYBNET, it is easy to say that their needs differ from one to another. Indeed, for some practitioners the identification of the risks and their understandings seem to come first, for others the risks are well-known, and they only need to plan their measures directly. In all the cases, the practitioners must be able to reach a well-informed

decision driven by the access of reliable information to be integrated in their daily work. Their behaviour needs to be adapted to the state of security that they aim to reach. For example, in case of event or crisis, the communication must be understood. It is also important to say that hybrid threats go beyond the definition of crisis. It can include the silent and low-visibility-influencing of decision making, and the use of many different domains in parallel to reach a long-term goal.

---

## INDUSTRY, INCLUDING SMES

The Security Industry group need insight into risks, context and environment of the hybrid threats that may occur. It also requires opportunities to validate novel security solutions in such eco-systems.

---

## PUBLIC / POLICY BODIES

Public bodies have to identify and deploy a global security model for a better understanding of the situation created by hybrid threats. A security model dedicated to hybrid threats must be imagined at the national and European levels. Public policies might want to identify the opportunities of getting innovative tools that could be integrated to the strategy, it is also crucial for them to receive the correct information and then to act accordingly. Because of that, public bodies should be aware of results and outputs produced throughout EU-HYBNET.

The needs that can be taken into consideration for the public bodies are quite wide and advice coming from the scientific community, must also consider the impact of these actions on the civil society. The integration of inputs coming from diverse stakeholders can also be used to support the implementation of related projects and initiatives.

---

## SCIENTIFIC COMMUNITY

EU-HYBNET can be relevant for the scientific community in the domain of hybrid threats. The latest developments occurring in this domain should be analysed from the scientific perspective, the main idea being to aim at an advanced state-of-art of legal literature, and improving the already existing knowledge with respect to hybrid threats. The idea would be to:

- Provide guidance in terms of the interpretation of legal requirements in scope,
- Identify the main gaps of the relevant regulations that may be addressed.

The results of such an action will be interesting for the scientific community but also for all other stakeholders identified that may access the relevant information.

---

## OTHER CATEGORIES

---

### RELATED PROJECTS AND INITIATIVES

This category of stakeholders needs to be perfectly aware of what is happening within EU-HYBNET. Their feedback on the outputs of EU-HYBNET and their participation to events and workshops is crucial for a better understanding of the project and also to establish synergies and create a wider impact than a project would do alone.

---

### CIVIL SOCIETY



The main need of this type of category is to get a better understanding of the concept of hybrid threats to be able to propose a relevant and coherent response to various types of crisis, vulnerabilities in society and also to increase awareness of hybrid threats.

### 3.3 IDENTIFICATION OF PRIORITY GROUPS

The priority groups and the specific action plans for the project activities of each target group are provided. EU-HYBNET's consortium has identified three different priority groups:

#### 3.3.1 PRIORITY GROUPS

The first group includes the stakeholders directly linked with the overall concept of EU-HYBNET, its objectives and expected outcomes. Dissemination activities with this group need to be launched at the start of the project and continue for 60 months.

The first group consists of practitioners which are categorised as follows:

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

Together with practitioners in this cycle, the project greatly focused its efforts in engaging with the industry and notably SMEs. That is because the industry and in particular EU SMEs are now actively developing innovative solutions that can help practitioners counter hybrid threats and enhance EU security.

The second group is formed by European projects relevant to EU-HYBNET. The main focus is on the EC Network of Practitioners (NoP) funded projects (funding Horizon2020-Secure Societies-General Matters -call) and these include ARCSAR, MEDEA, DAREnet, FIRE-IN, ILEAnet, NO-FEAR, PEN-CP, E-notice, Exeter, ENCIRCLE, INCLUDING, NOTIONES, EU-CIP, i-LEAD, iProcureNet. In addition, EU-HYBNET is also aiming to cooperate with other relevant European projects (regardless of their funding instrument) that could be working on areas relevant to hybrid threats practitioners: PRECINCT, CYCLOPES, PRAETORIAN, FINSEC, RESISTO, ECHO, 7SHIELD, ALIGNER, DOMINOES, CRESCENT, CRITERIA, EU-CIP.

The third group consists of organisations and actors engaged in related research areas of EU-HYBNET. The organizations in focus are EU Agencies and bodies e.g., EUROPOL, FRONTEX, EMSA, eu-LISA, ENISA, EDA, EEAS. Furthermore, an important EU actor is Commission hosted Community of Users (CoU) group, which now called the Community of European Research and Innovation Security (CERIS). In addition, relevant national and sub-national networks and actors are in the scope of EU-HYBNET.

#### 3.3.2 OTHER STAKEHOLDERS

This group of stakeholders could have an interesting impact on EU-HYBNET, however they might not be aware of the existence of EU-HYBNET or might not realize its importance:

- Public bodies / policy bodies including, EU DGs (outside of DG HOME, such as DG MOVE, DG CONNECT, DG DEFIS, DG MARE, DG ECHO), Institutions of the EU, as well as The Council's Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats

- Scientific community

The consortium continues to flag any relevant opportunity for communicating EU-HYBNET outputs, notably with:

- Key actors of projects to ensure visibility and uptake of results, providing opportunities to receive feedback, discuss similar issues that may occur;
- Internal network/ audience of consortium partners can be seen as important too and adequate internal communication must ensure that EU-HYBNET has a high profile.

#### 4. KEY MESSAGES TO BE SHARED

To create a proper and long-standing relationship with the stakeholders, the project's key messages have to be adapted to get their interest, present a clear and simple structure and straight to the point they aim to reach.

The communicable objectives are hereby presented per work packages with a proposition for every target group:

Table 10 Key messages for targeted groups

	Practitioners	Industry including SMES	Public / Policy Bodies	Research and scientific community	Related Projects and Initiatives	Civil Society	LEAs and ERAs
<b>WP1 Coordination and Project Management</b>							
<b>Objectives related to the Project Management</b>							
Achieve EU-HYBNET objectives	To get access to the achievement of EU-HYBNET Objectives	To get access to the opportunities to further improve EU-HYBNET outputs	To gain a better understanding of EU-HYBNET for future influence on Policies	To get the opportunity to give feedback on EU-HYBNET outputs	To get a better understanding of EU-HYBNET, enhance collaboration and avoid overlap	To gain a better understanding of EU-HYBNET for future influence of Policies	To gain a better understanding of EU-HYBNET for future influence of Policies
<b>WP2 Gaps and Needs of European actors against Hybrid Threats</b>							
<b>Objectives related to the Gaps and Needs of European actors against Hybrid Threats</b>							
To identify Gaps and Needs	To be able to give feedback on the identification Gaps and Needs	To have a better understanding of the G&N	To have access to the G&N identified	To have access and give feedback to the G&N identified	To be aware of the G&N identified	To have access to the G&N identified	To have access to the G&N identified
To increase European Stakeholders' knowledge of the hybrid threats	To get knowledge on Hybrid threats	To get knowledge on hybrid threats	To get knowledge on hybrid threats	To get knowledge on hybrid threats	To get knowledge on hybrid threats	To get knowledge on hybrid threats	To get knowledge on hybrid threats
To test Innovation to enhance European Stakeholders measures against hybrid Threats	To be aware of the test and give feedback on Innovation	To be aware of the test and to be able to take a position on the market	To be aware of the test as input for potential follow up action when needed	To be aware of the results of the tests and use them	To be aware of the test	To be aware of the test	To be aware of the test and be able to give feedback

To support the extension of actors in the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats	To be part of the European Network against hybrid threats
<b>WP3 Surveys to Technology, Research and Innovations</b>							
<b>Objectives related to the Surveys to Technology, Research and Innovations</b>							
To map the needs for innovations: results to be populated via the IA	To be aware of the mapping	To be aware of the mapping	To be aware of the mapping	To be aware of the mapping	To be aware of the mapping	To be aware of the mapping	To be aware of the mapping
To monitor and select available innovative solutions for measures against hybrid threats	To be aware of the selected solutions	To be aware of the selected solutions as input for potential follow up action when needed					
To arrange events	To be aware of the events and attend them	To be aware of the events and attend them	To be aware of the events and attend them	To be aware of the events and attend them	To be aware of the events and attend them	To be aware of the events and attend them	To be aware of the events and attend them
<b>WP4 Recommendations for Innovations Uptake and Standardization</b>							
<b>Objectives of the recommendations for Innovations Uptake and Standardization</b>							
To build a concrete roadmap on innovation uptake	To be aware of the roadmap	To be aware of the roadmap and see its potential influence on the market	To be aware of the roadmap	To be aware of the roadmap	To be aware of the roadmap	To be aware of the roadmap	To be aware of the roadmap
To compile recommendations for standardisation activities	To be aware of the recommendations	To be aware of the recommendations and see their potential influence	To be aware of the recommendations as input for potential follow up action	To be aware of the recommendations	To be aware of the recommendations	To be aware of the recommendations	To be aware of the recommendations

		on the market	when needed				
To deliver Policy Briefs, Position Papers and Recommendations	To be aware of the documents	To be aware of the documents produced	To be aware of the documents produced as input for potential follow up action when needed	To be aware of the documents needed	To be aware of the documents needed	To be aware of the documents needed	To be aware of the documents needed
<b>WP5 Dissemination, Communication and Exploitation</b>							
<b>Objectives of the Communication, Dissemination and Exploitation Activities</b>							
To disseminate results and interact with other related networks	To be aware of the main results and objectives of EU-HYBNET	To be aware of the main results and take a position on the market	To be aware of the main results of EU-HYBNET To have the opportunity to improve actual policy	To be aware of the mail results of EU-HYBNET	To be aware of the main results of EU-HYBNET	To be aware of the main results of EU-HYBNET	To be aware of the main results of EU-HYBNET
To create conditions for better interaction with industry, research and academia Enrich existing network against hybrid threats with academics, practitioners, stakeholders and industry actors across Europe	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network	To be part of the EU-HYBNET Network
<b>WP6 Ethics</b>							
No objectives to share with the stakeholders							

## 5. DISSEMINATION, COMMUNICATION AND EXPLOITATION MEANS TOWARDS ENGAGEMENT

### 5.1 MAIN DISSEMINATION MEANS

The objectives of the dissemination means are the creation of awareness and the engagement of stakeholders already identified above in this document.

Channels and tools which are being used for EU-HYBNET are described below:

#### 5.1.1 ONLINE DISSEMINATION MEANS

##### EU-HYBNET WEBSITE

Since M3, EU-HYBNET has its own dedicated website ([www.euhybnet.eu](http://www.euhybnet.eu)), to be seen as both a promotional and information tool. Its establishment was crucial in terms of communication as such a tool had an impact on the visibility and enhances stakeholders' engagement as it is widely accessible.

The website has the same graphical identity as the communication tools which are used within EU-HYBNET. It is one of the main tools of the Dissemination, Communication and Exploitation plan. The website is meant to be modern and present an attractive style. Google analytics was added by LAUREA which was in charge of establishing the website.

Whenever necessary, the content of the website is updated to share the relevant upcoming events, the latest news of the main achievements of EU-HYBNET. The website also makes project resources and deliverables available to the public.

The website launch can be considered a success. For 2024, there were 25,000 page views were recorded, with a total of 9.2k users (an increase of 700 users compared to D5.4). During the project's main events (such as Innovation & Knowledge Exchange Workshops, Future Trends Workshops or Annual Workshops), the website was particularly visited. Taking this feature into account, the DCE team's objective will be to maintain a high number of visits even when there is no project's event. This could be achieved with frequent publication of articles describing the project's results.

With the aim to be user-friendly, the website is divided into several categories:

- Home

The project's home page presents the main objectives of the project. A definition of its general approach is also provided. Thanks to LAUREA efforts the website presents an eye-pleasing and interactive view.

- About

The about section has four sub-sections. "The Project" contains an overview of EU-HYBNET, its objectives and present the project's Four Core Themes. "Management Structure" introduces the reader to the different management entities of the project and their relation. "Project Partners" consists in the presentation of EU-HYBNET consortium Members. Finally, "Synergies" lists the different

Horizon 2020/Europe projects that EU-HYBNET is cooperating with in terms of joint-DCE activities, participating in events and exchanging knowledge.

- EU-HYBNET Network

This section is divided into 5 subsections including a direct link to the TUOVI platform used by the consortium and a list of all Network Members.

- Publications

This section contains all EU-HYBNET papers that are public. Consortium partners had already co-written articles that are very relevant for the project's audience. There, the website visitor can as well find all press releases published after the project's events. Five policy briefs have been posted, with the latest being "On Information Sharing between Critical Entities for early and efficient detection and mitigation of Hybrid Threats" in December 2025.

- Events

In this section, visitors can find all information about past and upcoming events. For every event, a 'Save the Date' is created and displayed on the website. A countdown is also displayed for every upcoming event. The event pages are particularly updated and visited when events are approaching.

- News

This section was removed, following the duplication of other communication efforts (X, LinkedIn).

- Intranet

This section redirects the visitor to the Eduuni platform that is used by EU-HYBNET consortium for project's management.

- Innovate

The section redirects the visitor to the Innovation Arena (see below).

- Contact

This section provides a contact form that will allow people to get in touch with the project team, namely the coordinator and DCE team



Figure 3: Current website homepage

## INNOVATION ARENA

The project dissemination and communication plan also includes the creation of the Innovation Arena (IA) platform, carried out by LAUREA since M5 and will continue running until M60. The Innovation Arena focuses on finding the best technical solution for use cases, logic of content relations, the added value of IA to the project content and input, security and data protection issues.

The core usefulness of the IA platform is that it enables project partners and other network members to provide input to identified challenges (gaps & needs), that will ultimately support WP3 and WP2 and eventually WP4 to deliver the recommendations of the most promising innovations uptake (incl. industrialisation).

The IA is a social Idea management platform as it will have also social elements integrated into it such as; Members, Votes, Likes, Discussions, Sharing of content, private messages between members, e-mail notifications and more.

The main use cases of the IA is, as illustrated in the figure (IA use cases) below:

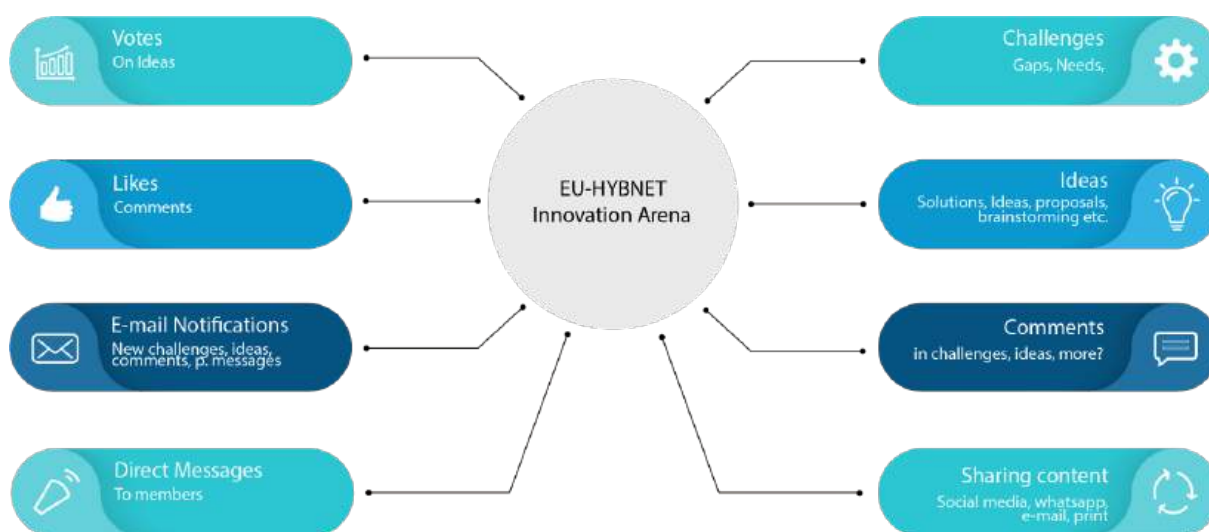




Figure 4: Innovation Arena use cases

The two main contents of the Innovation Arena are Challenges and Ideas. These content types work interlinked with one another. I.e. Ideas can exist within challenges or on their own as standalone solutions to unidentified challenges. Here with Challenges we are referring to issues such as gaps and needs while with ideas we refer to solutions to challenges (gaps and needs) i.e. ideas for improvement, new technologies and so on. Furthermore, both content types have the possibility to contain illustrative images, documents, active time, discussions and so on.

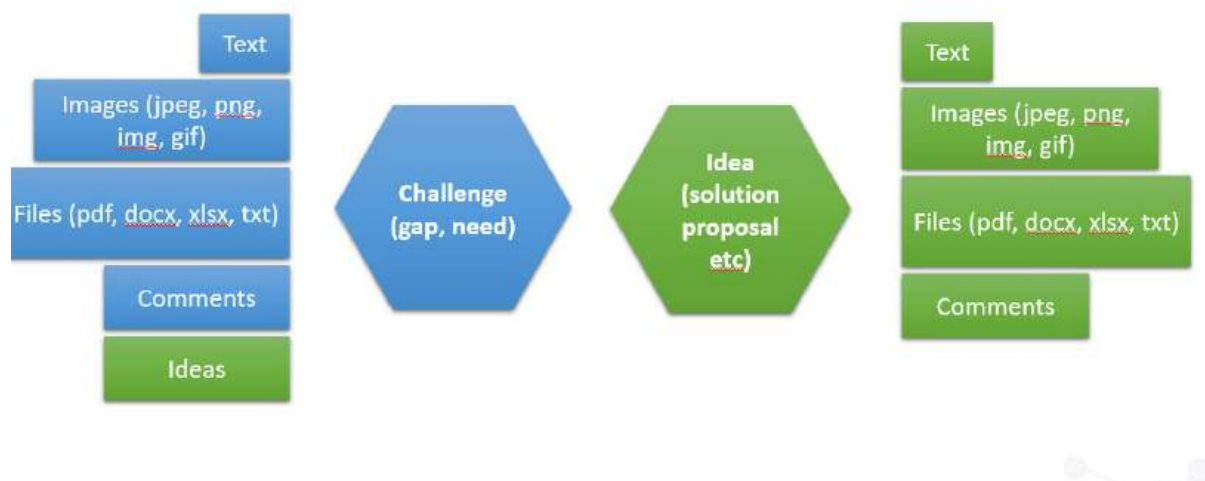


Figure 5: Innovation Arena Content Types

The IA has a central role in the EU-HYBNET innovation mapping. In short, by building an on-line Innovation Arena (IA) Platform the project provides an arena for project partners, (esp. practitioners) and those who will join via the project to the European Network against Hybrid Threats, to announce their needs for new innovations (technical and social/non-technical). In addition, in IA those projects and network members (esp. industry, SMEs, academics) who may provide possible solutions to announced innovation needs may tell about their solutions and what is reasonably expected, and according to which timetable. The project uses the IA discussion between those who need and those who may deliver innovations (technical and social) in Work Package (WP) 3 and WP2 for their research and analysis activities in order to find the most promising and potential innovations that answer to practitioners' needs and can be recommended to the standardisations process. EU-HYBNET partners are currently discussing how to improve the Innovation Arena to ensure it meets the needs of the project and EU-HYBNET network and maximise its impact.

## TUOVI

In order to support the EU-HYBNET Dissemination, Communication and Exploitation strategy, LAUREA has coordinated the use of a secure online portal named TUOVI where EU-HYBNET has own working space for EU-HYBNET Stakeholder Group/ EU-HYBNET Network members. TUOVI is hosted by the Finnish Ministry of Interior and EU-HYBNET has agreed with the Ministry on the use of TUOVI. Link to [TUOVI](#).

Unlike the EU-HYBNET web page, the TUOVI is available only for consortium partners, stakeholders and network members and provides the platform for restricted material sharing, secure communication, networking, and collaborating between the EU-HYBNET network members (Consortium partners, Stakeholder Group members and network members).

Throughout the life of the project (M1-60) LAUREA will manage all daily aspects of the EU-HYBNET working space in the TUOVI platform and will continually add relevant project information available for use by all EU-HYBNET Network members, including Advisory Board members.

The TUOVI platform serves as a useful and enduring means of secure communication, networking, and collaborating between existing (present EU-HYBNET Stakeholder Group members) and new, accepted members of the EU-HYBNET network. All EU-HYBNET Network members can see each other's profiles and are able to contact each other via email if they wish or discuss or exchange ideas about the project or other matters involving hybrid threats within the platform.

Within TUOVI there are many unique workspaces where all TUOVI users collaborate. LAUREA has created a private EU-HYBNET workspace which is available for all approved members. There are two main areas of the TUOVI workspace; a front page which provides basic information about the EU-HYBNET project, project social media links (Linkedin and Twitter), when the workspace was created and a link to the official EU-HYBNET webpage. At the bottom of this main page is an area with tabs that navigate to customized folders containing additional information about the project. All information related to the project will be organized with these tabs and located within customized folders. TUOVI folders contains general project information as well as information about EU-HYBNET events, press releases and other marketing and project promotional materials. Of note, the TUOVI platform will remain active after the EU-HYBNET project has ended and management will be transferred to the European Center of Excellence for Countering Hybrid Threats (HCoE) in order to keep the network active and to regularly communicate and provide content relevant to hybrid threats. In short, TUOVI platform provides sustainability for the EU-HYBNET Network cooperation.

The TUOVI front page with tabs identified is illustrated in the figure below:

[FRONTPAGE](#)   [ABOUT TUOVI](#)



● The workspace is active  
🔒 Private workspace  
📅 Created 5/22/20 4:21 PM  
🕒 Modified 10/7/21 3:00 PM

## EU-HYBNET Project

MINIMIZE ⌵

<https://www.euhybnet.eu>  
[in](#) [tw](#)

**Privacy notice:**  
Please note that the EU-HYBNET Workplace in TUOVI is a closed environment meant only for the EU-HYBNET project partners, network members and stakeholders of EU-HYBNET project. All files, articles and any other documents shared in this group are to be considered as classified and should not be shared outside this group without a written consent from the author/s and/or the project coordinator!

**Empowering a Pan-European Network to Counter Hybrid Threats**

EU-HYBNET is a five year project funded by the European Commission (No 883054). The project is an ever growing Pan-European network of collaborating security practitioners, stakeholders, academics, industry players, and SME actors from across the EU working together to counter hybrid threats.

EU-HYBNET aims to build an empowered and sustainable network beyond the scope of the project via its on-going association with key partner, The European Centre of Excellence for Countering Hybrid Threats (HCoE).

**The Four Core Themse of the Project Include:**

1. Future Trends of Hybrid Threats
2. Cyber and Future Technologies
3. Resilient Civilians, Local Level and National Administration
4. Information and Strategic Communication

**EU\_HYBNET's Activities Include:**

Defining common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavours.  
Monitoring significant developments in research and innovation.  
Delivering recommendations for uptake and industrialisation of the most promising innovations, that address the needs of practitioners, and determine associated priorities for standardisation.  
Establishing conditions for enhanced interaction among its members.  
Persistently striving to increase its membership and continually build network capacity through knowledge exchange, including exercises.

The EU-HYBNET consortium has 25 partners from 14 different EU Member States and associated countries, there are 12 Practioner partners from 10 different EU Member States. (FR, DE, NL, PL, ES, IT, RO, EE, FI, AND NO) and the remaining Partners represent industry, SME's, academia and other organizations which include 4 additional EU Member States (GR, SE, LT, BE).

*#extremism #rescueservices/civilprotection #criminality #informationsecurity  
#feelingofsafetyandsecurity #safetyandsecurityplanning #preparedness*

CURRENT ISSUES
DISCUSSION
MATERIALS
TASKS
EVENTS
MEMBERS

Figure 6: TUOVI Front Page

The TUOVI platform has a central role in the expansion of the EU-HYBNET network and in creating additional opportunities for project communication. The TUOVI platform provides an arena for the network members of the European Network against Hybrid Threats to announce discuss project innovations, and potentially new hybrid threats. In addition, network members may provide any feedback to the project or recommend new members to the network. In addition, TUOVI can be used as discussion arena on new research and project initiatives in the field of hybrid threats.

## ONLINE MEDIA STRATEGY

Knowing that the main objective of the Dissemination, Communication and Exploitation plan is to increase the project's awareness across the Hybrid threats ecosystem and enhance the general understanding, the promotion of EU-HYBNET results to the online media is the second key point of the present document.

The idea here is to raise interest among the hybrid threats community and the civil society in general.

---

### 5.1.2 OTHER DISSEMINATION MEANS

Most of the deliverables are public within EU-HYBNET. These documents are crucial and contain detailed descriptions of the results. After the official approval of the public deliverables by the EC, they are open to CORDIS and can be found online on the website. On that purpose a list of online media is established and regularly updated by the consortium partners (including local, national, regional and international, general or specialized media).

---

### EXTERNAL CHANNELS

EU-HYBNET results are also shared on several external websites. These websites are listed below:

- EU-HYBNET's partners' websites and social networks
- EC and EU website and social networks

---

### 5.1.3 DISSEMINATION THROUGH EVENTS

---

#### INNOVATION AND KNOWLEDGE EXCHANGE EVENTS

Three Innovation and Knowledge Exchange workshops were organized in the frame of EU-HYBNET:

- Event 1: Introduction to EHYBNET project and existing Network in Brussels by EOS (at M9)
- Event 2: Innovation and Knowledge Exchange workshop in The Hague by TNO (at M26)
- Event 3: Innovation and Knowledge Exchange workshop in Valencia by PLV (at M43)

These workshops were meant to be nonconformist, requiring creative thinkers to attend, the aim being to find new threats or manifestations of hybrid threats.

The First Innovation and Knowledge Exchange Workshop (IKEW) was held online (due to the COVID-19 situation) on the 19<sup>th</sup> of January. The event gathered 88 people and introduced participants to the EU-HYBNET project, its existing network and the EC's interest to extend network as a Pan-European hybrid platform for Member States' needs. It aimed to provide practitioners, industry, SMEs and academia with an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to counter them. Of course the consortium needed to adapt the organisation of the events to the COVID-19 situation.

On the 14<sup>th</sup> of June 2022, the EU-HYBNET consortium held its 2nd Innovation and Knowledge Exchange Workshop #IKEW in a hybrid format. As with the previous IKEW, its aim was to provide practitioners, industry, SMEs, and academia an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to answer them. During the 2nd IKEW, consortium partners and external participants (practitioners, industry, academia and NGOs) discussed the project's latest Innovation Assessment results and exchanged new ideas regarding how the innovations could be further improved to counter hybrid threats. The 2nd IKEW, organised by TNO, included morning plenary sessions, two tracks of break-out sessions – one track offered live in The Hague and one catered for online participants – and afternoon plenary sessions.

The 3<sup>rd</sup> and Final IKEW (see agenda in annex XX) was held in Valencia, Spain in a hybrid format. The workshop was attended by approximately 60 representatives of the EU-HYBNET consortium and

network, as well as other stakeholders from industry, practitioner and policymaking organisations. 90 people also followed the workshop online through Youtube. The workshops centred around four innovations based on the gaps and needs identified and assessed by the consortium over the past year. These innovations were also mapped to the four core themes of the project and were mainly from other EU-funded projects, demonstrating how EU-funded security research is responding to the issue of hybrid threats in an innovative manner.

---

## FUTURE TRENDS WORKSHOPS

The objectives of the 5 Future Trend workshops are to disseminate project findings to a large number of stakeholders, and to ensure vivid interactions with industry, academia and other providers of innovative solutions outside of the consortium with a view to assessing the feasibility of the project findings and possible recommendations to innovation uptake and standardization.

- Workshop 1: In Brussels by HCoE (at M12)
- Workshop 2: in Rome by UCSC (at M24)
- Workshop 3: In Bucharest by MVNIA (at M36)
- Workshop 4: In Valencia by PLV (at M48)
- Workshop 5: In Ispra by JRC (at M58)

The first Future Trends Workshop was hosted online by Hybrid CoE on the 31st of March 2021 (M11).

This workshop also marked the start of the EU-HYBNET month, which gathered the consortium and EU-HYBNET network around several interesting virtual events until the 28th of April 2021. It provided practitioners, industry, SMEs and academia with an opportunity to learn from the different speakers about Megatrends and European Security and measures to counter hybrid threats. The event was able to gather 68 participants from 44 organisations to the (virtual) table and participate in this event. The objective of the event was to gather information from participants on what they think were the most important elements that could impact the future context in which hybrid threats will manifest, twenty years on. These reflections will support future assessment of EU-HYBNET gaps, needs, solutions and innovations.

The second Future Trends Workshop was hosted in-person and online on the 4<sup>th</sup> of April 2022 (M24) in Rome, Italy.

The objective for the second Future Trends Workshop was the same as the first one: to gather information from participants on what they think were the most important elements that could impact the future context in which hybrid threats will manifest, twenty years on. Differently from the first workshop, the event was focused on 3 trends: Changing populism, Instrumentalization of social networks, and the constitution of international groups. A total of 56 organizations (96 participants) registered for the event with most of them deciding to participate online. 15 EU countries were represented and 3 non-EU countries (namely Georgia, Turkey and UK). Most of the organization represented the academic world while 14 the practitioners' side, 8 organizations were SMEs and 7 represented NGOs.

The EU-HYBNET consortium successfully held its 3rd Future Trends Workshop in Bucharest, Romania on the 19<sup>th</sup> of April, 2024. The workshop was attended by approximately 90 representatives of the EU-

HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations. The topic of the 3<sup>rd</sup> FTW addressed “Hybrid Threats in the EU Neighbourhood – Implications for the future of EU security” and served as a platform of interaction for all stakeholders to discuss hybrid threats in the EU’s neighbourhood, implications for the future of EU security and innovations to counter them. The 3<sup>rd</sup> FTW allowed for the EU-HYBNET project and their stakeholders to engage in topical debates as well as discuss the role of the project, such as finding various solutions by looking into one dimension of a multidimensional problem.

The 4<sup>th</sup> FTW was held on the 23<sup>rd</sup> of April 2024, The workshop was attended by approximately 85 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations in person, with another 67 views on the streaming platform. The 4<sup>th</sup> iteration of the FTW focused on “Border Management to Counter Hybrid Threats”, focusing on recent hybrid threat trends that have challenged the strength of EU borders as a way to disrupt society and create divisions. The event centred on the question of can effective border management counter such hybrid threats.

At the time of writing, the [5<sup>th</sup> and Final EU-HYBNET Future Trends Workshop](#) on “Rising Foreign Interferences” is currently being planned for the 13<sup>th</sup> of February, 2025 in Brussels. Additionally, the agendas for FTW 3 and 4 can be found in the annexes of this document.

---

#### ANNUAL WORKSHOP

The consortium organises several Annual Workshops where to disseminate project findings for large scale of stakeholders and to ensure vivid interaction with industry, academia and other providers of innovative solutions outside of the consortium with a view to assessing the feasibility of the project findings and possible recommendations to innovations uptake (incl. industrialisation) and standardisation.

Moreover, Annual Workshops have to foster network activities, raise awareness of the project and bring together relevant practitioners and stakeholders who may to join to the EU-HYBNET network and its activities.

Due to COVID-19 situation, the first Annual Workshop was organised online by Hybrid CoE on the 19<sup>th</sup> of April. The event presented the initial project findings and progress to the project consortium members, EUHYBNET network members and pan European stakeholders; made up of practitioners, industry, academia, and NGOs. The programme included the project’s initial results, overview of each Work Package, network membership, and an introduction to the Innovation Arena platform. Additionally, the workshop hosted a handful of presenters introducing their unique innovation ideas to counter hybrid threats.

The second Annual Workshop was held in Rome and organised by UCSC on the 5<sup>th</sup> of April 2023. The Annual Workshop, hosted by UCSC and co-organized with LAUREA, included three high-level keynote speeches, the project’s results and network activities from the second project year. Additionally, the workshop hosted a handful of presenters and European projects introducing their unique innovation ideas to counter hybrid threats.



Since the previous DCE plan, EU-HYBNET has held 2 Annual Workshops, the 3<sup>rd</sup> AW in Bucharest, Romania on the 20<sup>th</sup> of April 2023 with approximately 80 participants and the 4<sup>th</sup> AW in Valencia, Spain on the 24<sup>th</sup> of April with 82 in person and 27 online participants. Both events presented the results of the project from the year and included keynote speakers as well as pitches of innovations to counter hybrid threats (see agenda in the annexes).

At the time of writing this report, the planning of the 5<sup>th</sup> and Final Annual Workshop is underway and will take place in a hybrid format in Brussels, Belgium on the 12<sup>th</sup> of February.

---

#### WORKSHOP FOR INNOVATION STANDARDIZATION

Three workshops for Innovation and standardization will be organized to help map the current status and identify the needs and possibilities for standardization and share them with relevant stakeholders. Each workshop will focus on a given theme during the standardization session:

- Standardization Workshop 1: In The Hague by TNO (at M26)
- Standardization Workshop 2: In Valencia by PLV (at M43)
- Standardization Workshop 3: In Brussels by LAUREA (at M56)

The 1st Innovation and Standardisation Workshop organised by PPHS gathered input and recommendations from consortium partners, network members and external participants (practitioners, industry, academia and NGOs) on standardisation requirements for innovations to counter hybrid threats.

- During Working Group 1 – Standardisation measures in the context of critical infrastructure protection and innovations to enhance information sharing’, standardisation experts and pan-European security practitioners presented their views on current standards, needs and future possibilities for standardisation in the field of critical infrastructure protection in of light the challenges deriving form hybrid threats.
- During Working Group 2 – Innovations in disinformation and media literacy, participants discussed standardisation best practices and innovative solutions answering security practitioners’ needs to counter information manipulation and interference, disinformation and media literacy.

The 2<sup>nd</sup> ISW as organized by PPHS and hosted by PLV on November 8<sup>th</sup>, 2023 in Valencia, Spain. this edition allowed participants to discuss standardisation recommendations and case studies for countering hybrid threats in two thematic areas, Foreign Information Manipulation and Interference (FIMI) & Protection of Critical Infrastructure.

The 3<sup>rd</sup> and Final ISW was organised by PPHS and hosted by LAUREA at the EU Helsinki Office In Brussels, Belgium on the 22<sup>nd</sup> of October, 2024. The workshop brought together approximately 40 participants, including consortium members, EU-HYBNET network members, industry representatives, practitioners, and policymakers and was divided into four thematic sessions. Each session was dedicated to one of the innovations identified during the 3rd cycle of the EU-HYBNET project:

- Session 1 – Innovation: Citizen – Responder Platform for Information Sharing in a case of an Emergency and Crises (CRP) EU-HYBNET core theme: Resilient Civilians, Local Level and National Administration

- Session 2 – Innovation: Local Media Hybrid Threats Tracker (LMHTT) EU-HYBNET core theme: Information and Strategic Communication
- Session 3 – Innovation: Citizens Reporting Tool on Suspicious Signs (CiReTo) EU-HYBNET core theme: Cyber and future technologies
- Session 4 – Innovation: STARLIGHT and Innovation testing best practices EU-HYBNET core theme: Future Trends and Hybrid Threats

The event was also accompanied by a keynote speech on innovation implementation and a closing speech on the procurement process.

---

#### TRAININGS AND EXERCISES FOR NEEDS, AND SOLUTIONS FOR GAPS

L3CE leads the organization and deliver with the support of the contributors of WP2 the trainings and exercises for the identified needs and gaps. The objectives here are to enhance European actors' capacity, knowledge and competence on measures against hybrid threats by delivering training and exercises to participants (C.30-40 persons) with various backgrounds, and to gain new knowledge and skills to enhance their measures against hybrid threats.

Three training events were held:

- The first training event was held online on the 22<sup>nd</sup> and 29<sup>th</sup> of April, 2021
- The second training event was held in Vilnius on the 21<sup>st</sup> & 30<sup>th</sup> of September, 2022
- And the last training event was held in Vilnius on the 18<sup>th</sup> & 19<sup>th</sup> of January, 2024

Due to the closed nature of the events, it is not possible to go into further detail regarding the contents apart from the fact that each trainings were based of the identified gaps and needs and innovations and used the DTAG methodology. L3CE, the organiser of the events, also released a short video for the EU-HYBNET network discussing the training.

---

#### GAPS AND NEEDS WORKSHOPS

Every EU-HYBNET project cycle starts with a Gaps and Needs Event, which in practice means a series of workshops among the stakeholders (EU-HYBNET Network members and Stakeholders group members) and consortium members. The goal of the gaps and needs workshops is to gain information on European actors gaps and needs to counter hybrid threats. In addition, in the gaps and needs events participant are to share information with other participants about issues they consider vulnerabilities, existing capabilities to tackle these vulnerabilities, needs that they have to mitigate the vulnerability from escalating, and gaps that need to be addressed before these needs can be met. In the gaps and needs event, the participants have a chance to provide further reading and examples to support the information in the tables, and to gain information about each other's vulnerabilities and the shared understanding of the hybrid threat environment. The workshops also provide a valuable insight into participants' understanding of what hybrid threats are. The information from the events is in the core of each project cycle because the events deliver information on the most important and present gaps and needs and vulnerabilities among European actors to counter hybrid threats. The information is then processed by other project tasks: innovation mapping to gaps and needs, research activities and delivery of innovation recommendations and standardization needs during the project cycle.



The final Gaps & Needs Event was hosted by URJC and organised by URJC and HCoE in Madrid on June 12<sup>th</sup>, 2024.

---

### THIRD PARTY EVENTS

EU-HYBNET also needs to be present at other events organized by other projects or initiatives or by the EC. EU-HYBNET partners attend events according to their field or expertise and take the chance of enhancing the networking part of the project. For example, EU-HYBNET already attended many of the CERIS events, the latest event being the CERIS FCT/INFRA Annual Event on December 15<sup>th</sup>, 2023.

---

#### 5.1.4 RELATIONSHIP WITH OTHER RELEVANT PROJECTS

The main aim here is to increase EU-HYBNET's visibility and allowing interesting exchange with other relevant initiatives. The avoidance of work duplication is also extremely important, this can be addressed by sharing experience and expertise.

The relationship between EU-HYBNET and other projects needs to be seen as a mutual promotion of news, mutual invitation to participate and present project workshops or organize joint events. A support for standardization activities and surveys related to this subject is also foreseen between EU-HYBNET and its projects partners.

EU-HYBNET has already had vivid cooperation with many EC funded security projects and the list below highlights the volume of the events alike the project with whom the cooperation has been established:

- CERIS Critical INFRA & Hybrid threats WG content delivery with STOP-IT, RESISTO, FINSEC (June 2021)
- Hybrid threats elements to a training scenario to be used in INCLUDING training (June 2021)
- Cooperation to solve EU procurement landscape with I-LEAD (April 2021)
- Participation to procurement event of MEDEA (March 2021)
- Event on network extension (Oct 2020) & presentation in Brokerage Event of SPARTA (Dec 2021)
- Network extension and presentation in Closing Seminar of LION DC (May 2021)
- Second ECSCI Cluster Workshop (April 2022)
- PRECINCT stakeholder engagement workshops (May & November 2022)
- NO-FEAR Workshop on Ethics (March 2023)
- EU-CIP, PAVED, GEMS, and AHEAD participation in the EU-HYBNET 4<sup>th</sup> AW (April 2024)
- STARLIGHT participation in EU-HYBNET's ISW (October 2024)

EU-HYBNET also has a synergies tab on the website that lists the different relationships that EU-HYBNET has been able to establish, such as with NOTIONES, PRECINCT and more.

## 5.2 COMMUNICATION MEANING

'Communication is a way to keep all partners actively involved in the project'[3] The Communication part of a project clearly requires targeted measures used by the entire consortium for communicating about the project objectives and results.

---

### 5.2.1 VISUAL MATERIALS

The visual identity is well defined by the project's logo (created at the time of the submission) and by the document templates (deliverables and standard PowerPoint presentation provided at M1 by PPHS and EOS).

A promotional package has been ready since M3 and includes:

- Flyers / Brochures to be disseminated during events in general, both in soft and hard copies
- EU-HYBNET roll-up banners to be used during project events and events EU-HYBNET will attend.
- Pens, bags and notepads to be distributed during project events

All communication materials, like the flyers, brochures and roll-up, will be updated according to the needs of the consortium, and in order to update information according to project developments and successes. The most recent update includes an updating of the powerpoint template by PPHS in M35. The update was aimed at modernising the image of the project and making information easier to digest when project partners are presenting EU-HYBNET activities, results, etc.

---

#### 5.2.2 EU-HYBNET WEBSITE

As explained above, the website is accessible since M3.

---

#### 5.2.3 EU-HYBNET SOCIAL NETWORK AND SOCIAL MEDIA STRATEGY

Having a proper social network and social media strategy is crucial to get easily access to the security actors.

Next to the website, two social media platforms are in place and ensure a more concrete level of exchange.

A Twitter Account, called EU-HYBNET project has been created before the Kick-off-meeting at M1. The main objective is to share and promote EU-HYBNET activities with the several stakeholders connected. During the first 18 months of the project, the Twitter account reached great results in terms of followers, posts per month and retweets. The Twitter account has been particularly active during the project's events. The DCE Team informed the project's contacts of the event in live and reposted content provided by project's partners.

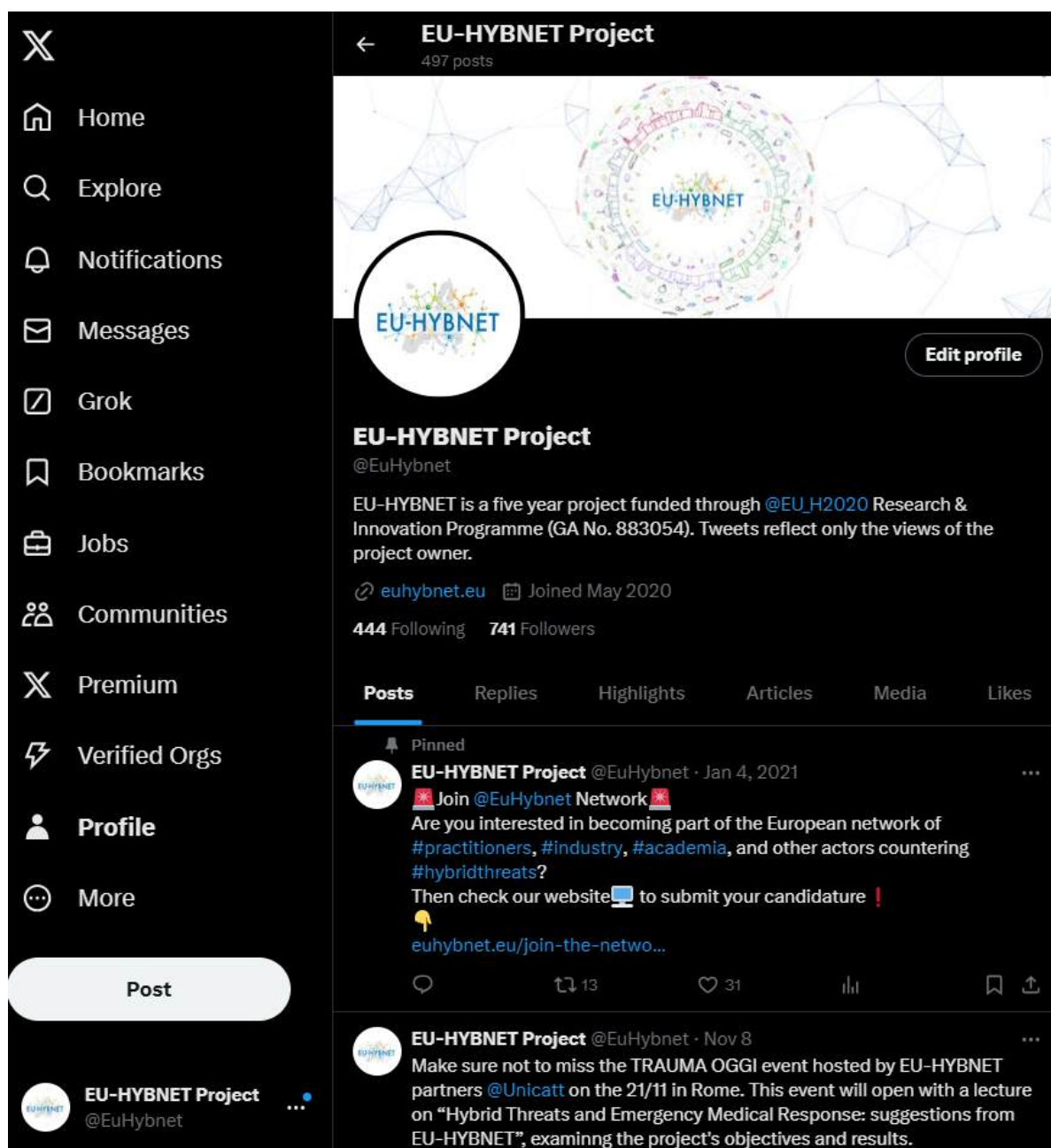


Figure 7: EU-HYBNET Twitter account homepage

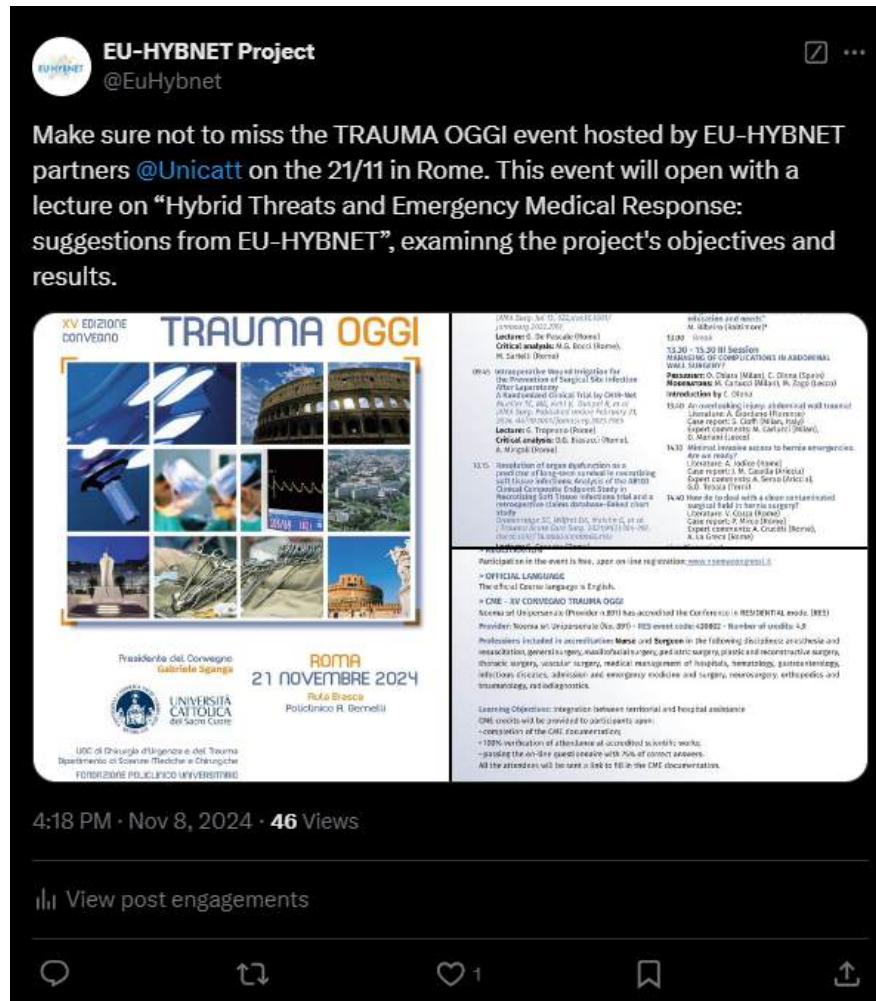


Figure 8: Tweet to inform about the inclusion of EU-HYBNET in the TRAUMA OGGI Event

With the same objective a LinkedIn Profile has been create at M1 as well:

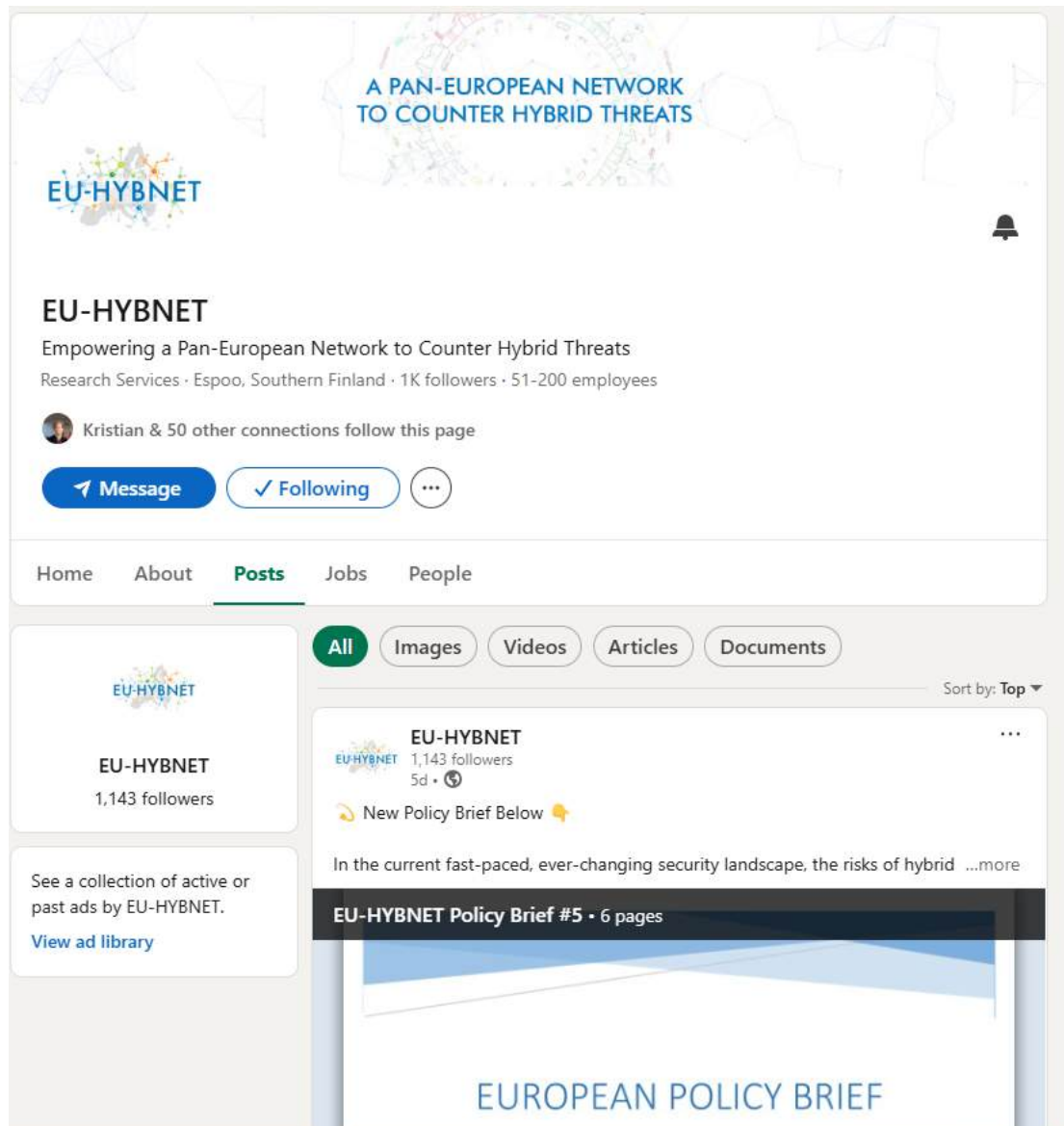


Figure 9: EU-HYBNET LinkedIn Profile

The LinkedIn account follows the same objectives. It benefits from the relevance of the platform contents which can feed the account's updates. The EU-HYBNET page is also used to disseminate the



project's papers and podcasts in order to reach a wide audience.



Figure 10: Examples of updates from EU-HYBNET LinkedIn account

## 5.2.4 NEWSLETTER

Twice a year the consortium shares a newsletter updating the stakeholders about what has happened in the past six months and what will happen in the six months to come. The document of course follows the design of the website and is shared in two ways: via Sendinblue (an account was created at M6) and via the wide networks of the consortium partners.

The First three project's newsletters were sent to almost 200 recipients, with a good opening rate. Each Newsletter provides the reader with results achieved by each Work Package. Recipients are aware of the past and upcoming events and an highlight of future objectives is given.



Press releases are tools that will be shared to communicate about the project activities. After each event involving EU-HYBNET, a press release has been posted summarising the event and discussions. Since the end of the 2<sup>nd</sup> cycle, it has been a goal to ensure that the press releases dive deeper into the content discussed (if the event allows i.e. if it is open to the public) instead of simply being a summary. In total there are 23 press releases available on the website, the latest one from June 2024.



## EU-HYBNET held its 4<sup>th</sup> Future Trends Workshop, #FTW2024

On the 23<sup>rd</sup> of April 2024, the EU-HYBNET consortium successfully held its 4<sup>th</sup> **Future Trends Workshop** in Valencia Spain. The workshop was attended by approximately 85 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations in person, with another 67 views on the streaming platform.

Building on the project findings from the last four years, the workshop addressed “Border Management to Counter Hybrid Threats” and served as a platform of interaction for all stakeholders to discuss recent hybrid threats or trends that have challenged EU border management and how effective border management can be used to counter future hybrid threats.



In this fourth iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and current analytical models and dive deeper in the topic of hybrid threats, in what way it is related to border management and border security, and how the EU and member states can adapt to be prepared for what comes next. The workshop’s aim was to highlight various ways border management could be used to counter hybrid threats and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

### Changing the way we think about hybrid threats, foresight activities, and preparing for the unmanned futures – key points and conclusions from the Plenary session

The workshop included a plenary session with a keynote speech from the Belgian General Intelligence and Security Service outlining various conceptual models to analyse the hybrid threat landscape as well as a panel discussion on Border Management to counter future hybrid threats from the Finnish Ministry of Interior, Laurea University of Applied Sciences, Europol Innovation Lab and Satways.

Through this session, it became apparent that **the different conceptual models used to analyse conflicts, events, or threats all have built in biases or levels and therefore can skew understanding in a way that renders a common situational awareness difficult.** The question then arises how to move past these issues in a complex and multi-level environment such as border management where multiple actors are involved. Some suggestions offered to participants to think about were multi-faceted taxonomies or the standardisation of models to remove blind spots.

Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don’t pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to understand how



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054.

Page | 1





## EU-HYBNET

technology can be used in new ways to undermine border security or slow down border management processes.

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by refining conceptual models and participating in foresight activities when possible** (even based on the gaps and needs identified by consortium and network practitioners). We welcome the feedback of additional practitioners and look forward to welcoming them into our network, among other hybrid threats stakeholders.

### What are the future trends of hybrid threats? – Key points and conclusions from the Break-out sessions

In the second part of the workshop, participants were split into four break-out sessions based on the project's core themes in an attempt to discuss and draw conclusions on the key trends for the future of border related hybrid threats in:

**Future Trends in Cyber and Future Technologies:** The session examined the future trends in cyber and future technologies. It allowed participants to think about the future threats arising from AI, Cyber-attacks, and Blockchain technologies. AI's exponential growth promises transformative advancements across industries, enabling automation, predictive analytics, and personalized experiences. However, with this innovation comes the looming threat of AI-driven cyber-attacks, leveraging sophisticated algorithms to orchestrate malicious activities such as deepfakes and automated phishing campaigns. Simultaneously, blockchain technology offers unprecedented transparency and security through decentralized ledgers, revolutionizing sectors like finance and supply chain management. As these technologies continue to shape the digital landscape, interdisciplinary collaboration and proactive strategies will be imperative to harness their potential while mitigating emerging cyber risks, ensuring a secure and resilient future for society.

**Weaponisation of Migration: Analysing the weaponisation of migration as part of hybrid threats** using the CORE Model shows that the majority of the 13 domains are concerned. For example, it affects diplomacy as it is a political issue and the response requires a calculated answer, infrastructure can be overwhelmed if an influx happens, etc. It also touches upon the Core Foundation of Democracy, as decision-making is mainly targeted through the weaponization of migration. 4 case studies were identified as examples and demonstrates that this will continue to be a tool used by hybrid threat actors to destabilise the EU. Additionally, Network Member ICDS gave an example of how Estonia increases its resilience to counter hybrid attacks from abroad.

**Code of Practice on Disinformation and FIMI during the European Elections:** A comprehensive framework aimed at **safeguarding the integrity of democratic processes** within the European Union. The session allowed participants learn all about a nuanced understanding of FIMI and its role as a tool in the upcoming European elections of June 2024. The session **emphasized transparency, accountability, and collaboration among all parties involved**, urging platforms to enhance their detection mechanisms for identifying and removing disinformation promptly.

### Securing the EU's borders to 2040 – Thinking about the security landscape:

Using the futures triangle to **understand the push of the present, the pull of the future, and the weight of the past**, participants were able to highlight possible future trends of how borders may be affected by hybrid threats. Trends identified were **digitalisation**, and how the reliance on digital systems and the automation of borders could lead to new vulnerabilities in case of a coordinated cyber attack, **climate change**, which will cause more and open new routes of migration, which could be weaponised by hybrid



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054.

Page | 2



threat actors and **the weaponisation of migrants in general** continuing in the future as part of hybrid threat campaigns.

The next Future Trends Workshop will be held in February 2025.

If you would like to stay updated on the work and conclusions of the project and attend future events, you're welcome to [join the EU-HYBNET network](#); you can read the associated information and apply on the project's [website](#). For further information on EU-HYBNET, you can follow the project through [Mastodon](#), [Twitter](#) and [LinkedIn](#).



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054.

Page | 3

Figure 12: Press release of the 4<sup>th</sup> FTW

## 5.2.6 COMMUNICATION POLICY

The communication objectives need to be reached according to a strategic and well-defined approach.

Partners are asked to communicate with interested stakeholders with the final objective of serving EU-HYBNET interest. Any communication activity led by specific partners has to reflect its own view, and that neither the EC nor the REA is responsible for any use that may be made of the information it contains.

Any communication activity should be reported in the updated DCEs, to be submitted as per DoA. All external communications should refer to the Grant Number (883054) and use the project visual identity and the European flag.

EU-HYBNET partners are recommended to get in touch with EOS (coordinator of WP5), PPHS and LAUREA (as main contributors of WP5) before posting on the social media channels of EU-HYBNET.

### 5.3 EXPLOITATION OF RESULTS

EU-HYBNET's plan for the exploitation of the results demonstrates how the proposed measures help achieving the expected impact. Exploitation of the results is key to maximizing their impact. An exploitation strategy per partner is outline below. Apart from the individual exploitation plans, which have already helped EU-HYBNET results spread, the consortium has already begun discussing the sustainability of the network as well as undertaken opportunities to take advantage of the EU-HYBNET lessons learned and proceed with new project proposals that would continue to raise awareness on the importance of hybrid threats.

**Table 11 Partners Exploitation Strategies**

<b>LAU</b>	Laurea will exploit the project's research findings and results in its Security Manager education programme, where students will be exposed to the latest knowledge related to European measures countering hybrid threats, which will be incorporated in graduate theses and disseminated to society at large. These same students will go on to eventually take on leading security positions in Finland or other European countries. The EU-HYBNET will also support Laurea to participate to new hybrid threats theme related European project proposals and projects, and hence share the information on the EU-HYBNET results further in the future. Laurea will also share information on the project's results in its national and international security, industry and education networks in order to increase general knowledge of measures countering hybrid threats in general
<b>PPHS</b>	PPHS will exploit the project's results within skills development and training programmes and various forms of educational degree programmes. These efforts will raise awareness of the challenges related to dealing with hybrid threats within public and private institutions in Poland and across Europe. More specifically, PPHS will exploit the project's results within training activities it conducts in Poland, and through conferences and workshops it organises through national and international networks, where PPHS is engaged. Significantly, it will also use the new knowledge acquired in assessments of needs and requirements related to technologies and services, to develop and exploit these further in the future, and in cooperation with industry and science.
<b>UiT</b>	UiT is stepping up its student programmes (bachelors, masters, PhD and post-doc), and will exploit the project's results through its focus on future project development on hybrid threats by developing new innovative solutions countering hybrid threats in Europe. What is more, with its local and regional practitioners in northern Norway, is currently engaged in and further developing a focused, community-based research agenda that aims to impact general awareness raising on hybrid threats within society.

<b>RISE</b>	RISE through its wide network, will exploit the outcomes of EU-HYBNET by promoting results to relevant authorities, industry and other interested organisations. It will also exploit these results in its cyber range training programmes for industry, as well as in the development of security solutions requested by the practitioner community
<b>KEMEA</b>	The exploitation of the results of EU-HYBNET is a top priority for KEMEA. Having strong links to ministries and agencies, KEMEA will promote EU-HYBNET results especially to Ministry Agencies and the Hellenic Ministry of Defence. Additionally, the above actions may lead to the development of new commercial project ideas related to the National Programme for the Internal Security Fund for the period 2020-2027, the Anti-Criminal Policy Program of Hellenic Police, and the new National Strategic Reference Framework (2020-2027). As well, KEMEA will promote the EU-HYBNET project in European related events and workshops in which regularly takes part.
<b>L3CE</b>	L3CE has demonstrated strong exploitation capabilities in the transfer of scientific and research results to security practitioners. L3CE has a solid network of EU Centres of Excellence and local governments, which will be used to exploit the project's outputs: LT Armed Forces Stratcom, Ministry of Defence, National Cybersecurity Centre of Lithuania, and Ministry of Interior. In addition to transferring knowledge to local authorities, critical results and technologies tested and evaluated by EU-HYBNET will be presented to regional law enforcement agencies that are in close collaboration with L3CE to maximise the possibility of project outputs being used by security practitioners in Baltic countries.
<b>URJC</b>	URJC will exploit the research findings to strengthen national knowledge networks involving stakeholders addressing hybrid threats in its different aspects, boosting research lines on hybrid threats within the university in the activities associated with its postgraduate programme of Specialist in Strategic Communication, Hybrid Threats, and Security and the research Group Ciberimaginario a7d events like the StratComES Conference.
<b>MTES</b>	MTES The exploitation of project's results is top priority for MTES, and it will exploit outcomes in particular with regard to the operators it works with, and in the management of hybrid threats, and it will define efficient means to ensure acceptance and uptake by practitioners of their methods and solutions. The outcomes of the EU HYBNET project will be fed into governmental policy and decision making processes in energy, water, environmental, industry and transportation sectors. Finally, its association with the French Security Industry, will allow for new knowledge to be promoted regarding industrial solutions at national and European levels.
<b>EOS</b>	EOS will promote the results of the project through its wide network of 45 members, extending from industry to academic institutions, research centres, and related organisations. EOS is committed to promoting policies that would support practitioners in countering hybrid threats among others also through the innovative solutions developed by the industry. The results of the project are already feeding into the EOS Working Group on Cyber and Physical Security which also covers hybrid threats.
<b>TNO</b>	TNO will exploit EU-HYBNET results in cooperation with its most prolific partners as regards issues of Dutch resilience to hybrid threats, namely, with the ministries of Security & Justice and Defence (respectively, a stakeholder and practitioner of EU-HYBNET). Also, by regularly keeping the ministry of Foreign Affairs abreast of EU HYBNET's progress, it is guaranteed that the outcomes of the EU-HYBNET project will be fed directly into governmental policy and decision making processes on hybrid threats in the Netherlands.
<b>SATWAYS</b>	SATWAYS will enhance its expertise and exploit the new knowledge arising from EU-HYBNET for further research and development. By expanding the company's network in academia, industry sectors and practitioners' groups, Satways will extend its reach into other related research and innovative projects.
<b>ESPOO</b>	ESPOO (2. largest city in Finland) will use and share project learnings within the organisation and with local security authorities to increase knowledge on hybrid threats and on measures countering them in the local community. As cities and municipalities in Finland are responsible in providing social, health and educational services to its residents, the impacts of hybrid attacks



	are potentially wide. Having a better understanding of where vulnerabilities lie within possible target services enables the city to develop measures making city services less vulnerable. The project's Europe-wide network provides the city with latest research information to support city decision-making. The project training activities will build capacity among city staff. Espoo as trusted source of reliable information, will also raise awareness on hybrid threats in the local community.
<b>UCSC</b>	UCSC will leverage project outcomes to design a specific course on "Cyber risks and Hybrid Threats in Medicine and Hospital Management." As coordinator of PANACEA (people-centric security in health care), UCSC aims at connecting the outcomes of EU-HYBNET into the PANACEA toolkits. Cross-border emergencies such as pandemics are managed through Public Health and WHO and ECDC directives, however the direct non mediated exposure of Hospitals during a pandemic will not protect these first-line response systems from pandemic threats that may be inflated by hybrid attacks. USCS plans to involve other MS and international Hospitals, medical and non-medical staff in the project training activities through conjunct exercises. USCS will exploit project results through seminars within the Hospital premises to raise awareness among staff of the complexity and inter-sectorial connection of hybrid threats.
<b>JRC</b>	JRC will exploit the results of the EU-HYBNET project to refine the focus of its hybrid-related research activities. Direct and continuous connection with practitioners and industry is expected to create spill-over effects to multiple security related areas, especially 1) Information Society 2) Safety and Security, and 3) Standards.
<b>MVNIA</b>	MVNIA will incorporate the project's research findings and information into its MA & PhD research programmes, such as the MA dedicated to the Management of Intelligence for National Security. As students come from diverse areas (security practitioners, legal, media, private business), the impact of exploitation of this information will reach a wide audience, not to mention that EU-HYBNET training materials will also be employed to enhance capabilities of experts and practitioners in the fight against hybrid threats
<b>HCoE</b>	Hybrid CoE (HCoE) hopes to enlarge its collection of networks, receive input from analysis of capability gaps, horizon scan of technologies and behavioural innovation. Synergies between scenarios, trainings and exercises are expected to strengthen exploitation activities. HCoE hopes to inspire partners and be inspired. Upon project completion HCoE intends to continue the coordination of the European Network against Hybrid Threats empowered in the EU-HYBNET and contribute to innovation uptake in the field of hybrid threats
<b>MOD</b>	MOD will use and share project learnings within the NL MoD organisation and with national partner security organisations to increase knowledge on hybrid threats and on measures countering them both within the NL MoD department and where possible cross-departmentally. In addition, the close relation and cooperation with TNO will enable the NL MoD to guide and steer further research nationally, based on the outcomes and findings from EU-HYBNET, both during the project and beyond.
<b>ICDS</b>	ICDS will enhance its capabilities related to security and resilience. Capability gap analysis competence will be further deployed as a contractor for government agencies. Policy recommendations may contribute to ICDS policy briefs and direct advisory role for the government.
<b>PLV</b>	PLV will apply and integrate EU-HYBNET's results into its training curricula in order to improve police skills and consequently the services the police officers are providing to the community in terms of crime prevention and security enhancement. PLV has a vast network of contacts in European law enforcement authorities (LEA). Consequently, PLV will contribute to exploiting the project's outputs to potential EU LEAs.
<b>ABW</b>	ABW On the basis of best practices, methods and solutions identified within the project, ABW will identify disinformation experts, data analysts, outreach officers and hybrid intelligence analysts at national levels to exchange knowledge regarding the latest hybrid threat strategies employed by adversaries, and thus tackle disinformation head-on by raising awareness about its dangers. ABW will exploit the project's research findings to enhance cooperation between national institutions and service providers, as well as with national authorities, industry and civil

	society and media to engage in a coordinated response to disinformation, and improving societal resilience to threat onslaughts (in particular among diplomats and public administration employees).
<b>DSB</b>	DSB (a directorate with strong links to both the national and the regional level) will use and share project learnings with both line agencies and counties in Norway. The aim is to increase our knowledge on hybrid threats and how they could impact on different levels. Population aspect with regards to the long term effect of fake news/disinformation (best practices for mitigation/gaps in knowledge) is a prioritised work stream and something DSB will hope to gain more insight in, both through our participation in the project and as part of our engagement with other HYBNET partners and the empowered European Network against Hybrid Threats
<b>RIA</b>	RIA will exploit participation in the project by designing and upgrading various services. Trainings and scenario-based exercises will be used as a testing ground for cyber security solutions in countering hybrid threats.
<b>MALDITA</b>	MALDITA will exploit the results of EU-HYBNET to develop better techniques in countering disinformation by streamlining their methodologies, disseminating the new knowledge in their training curricula and exchanges with other fact checkers around the world.
<b>ZITiS</b>	ZITiS will use and share the information gained in this project in training and education events for its customers (German federal authorities with security tasks with regard to information technology capabilities) to increase their knowledge on European measures countering hybrid threats. ZITiS will use the new knowledge derived from EUHYBNET's needs and gaps analyses in the area of hybrid threats to develop tailored cyber security solutions to support the work of the German federal authorities. Furthermore, ZITiS will contribute to the development of recommendations for standardisation in selected areas of crucial importance.
<b>COMTESSA</b>	COMTESSA ensures effective exploitation of project's results. It will use an exploitation strategy that is linked to the European safety & defence development exploitation model that is geared towards acceptance by various professional stakeholders in public and private sectors and that exploits the strengths of the partners in the consortium in relation to civil applications. The key players involved are: Government agencies& public/private security operators at local, regional, national or international levels; Industry, esp. safety & security solution providers; Universities & research institutions. For each of these groups, a tailor-made exploitation strategy will be employed: 1)media releases, interviews, presentations, workshops, lectures& discussions, 2) joint cooperation/joint proposals for future work or projects, 3)concrete application of results by stakeholders.

## 6. ENGAGEMENT ROADMAP

The key messages from Section 4 are being displayed throughout the EU-HYBNET timeline.

### 6.1 LAUNCH PHASE: CREATING AWARENESS

#### **Informing:**

Phase 1 was about creating an awareness among the targeted stakeholders.

- When: The launch phase started at M1 (May 2020) and was running for 6 months until M7 (October 2020).
- Who: During this phase all the targeted stakeholders were reached.
- What: DCE activities to launch in this phase:
  - o EU-HYBNET Twitter and LinkedIn Account (M1)
  - o TUOVI platform (M2)
  - o Promotional materials (M3)
  - o EU-HYBNET Website (M3)
  - o Events/workshop Plan (M5 and then every year)
  - o EU-HYBNET Newsletter (at M6 and then every six months)
  - o Additional press release written by partner organisations
  - o Attendance to EC events such as CERIS or other additional events with other EC funded projects
  - o Creation of a pod cast by the Espoo partner

### 6.2 IMPLEMENTATION PHASE: ENGAGEMENT IN EU-HYBNET AND INFORMATION ABOUT THE OUTCOMES OF EU-HYBNET

#### **Consulting:**

The implementation is the core phase of the project. It is the time to receive feedback of the stakeholders.

- When: The phase 2 started at M8 and runs until M56
- Who: all the stakeholders identified in the previous sections, using the system of prioritization.
- What: the main activities in terms of the DCE within this phase will be the organization of the EU-HYBNET several events, the creation and use of the Innovation Arena and the day to day communication activities (moderation of the social media channels, feeding of the website, creation of publications).

### 6.3 SUSTAINABLE PHASE: EVALUATING, SUSTAINING AND DISSEMINATING THE FINAL RESULTS

#### **Involvement:**

This is the final phase of the project. It will also be the one requiring the highest involvement from the stakeholders.

- When: the final phase will start at M57 and run until M60.
- Who: All the stakeholders described in the previous sections
- What: the most important activity will be the final Annual and Future Trends workshops to be held at M58 in Ispra by the JRC.

## 7. MONITORING AND EVALUATION PROCESS TO APPLY

It is now important to present the Key Performance Indicators (KPIs) defined in the DCE Plan. The KPIs will be analysed and updated in each update of the DCE, if needed.

These KPIs strictly follow the seven project objectives in line with the GM-01 call:

- Objective 1: To enrich the existing network countering hybrid threats and ensure long term sustainability
- Objective 2: 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
- Objective 3: To monitor developments in research and innovation activities as applied to hybrid threats
- Objective 4: To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardization for empowering the Pan-European network to effectively counter hybrid threats
- Objective 5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network
- Objective 6: To foster capacity building and knowledge exchange on countering hybrid threats
- Objective 7: To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats

The Table below is an updated list of the KPIs taking into account the project's developments up until M52. The initial KPIs are still available in D5.1, D5.2, D5.3 and D5.6.

Table 12 EU-HYBNET KPIs (2nd update)

Key Performance Indicators			Target at M52			Partners involved
			Level of performance			
Dissemination and Communication tools	Definition of the indicator	Type of data required	Poor	Good	Excellent	
Project Website	Number of visits per month	Google analytics	Less than 140 per month Less than 1400 at M52	140-300 per month 1400-3000 at M52	More than 300 per month More than 3000 at M52	Responsible: EOS Accountable: Laurea, PPHS Consulted: ESPOO, TNO, PLV, HCoE Informed: All other partners
	Page views per month		Less than 300 per month Less than 3000 at M52	300-500 per month 4000-5000 at 52	More than 500 per month More than 5000 at M52	
	Average time spent on website		Less than 30 seconds	30 seconds -1.5 min	More than 1.5 min	
Social Media	Subscribers of the LinkedIn Page	LinkedIn Group	Less than 600 at M52	600-800 at M52	More than 800 at M52	Responsible: PPHS Accountable: Laurea, EOS Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of posts on LinkedIn	Statistics dashboard	Less than 150 at M52	150-250 at M52	More than 200 at M52	
	Number of Twitter followers	Twitter analytics	Less than 600 at M52	600-800 at M52	More than 800 at M52	



## D5.5 Updated Dissemination, Communication and Exploitation Plan 3

	Number of tweets per month		Less than 10	10-15	More than 15	Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of retweets per month		Less than 3	3-7	More than 7	
	Number of tweets liked per month		Less than 10	10-25	More than 25	
Biannual Newsletter	Number of Newsletters published	Proceedings	0	1	More than 1	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
Brochures <sup>1</sup>	Number of brochures distributed (conditional to the improvement of the sanitary situation)		180 brochures at M52	250 brochures at M52	400 brochures at M52	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
Contributions to external events	Number of external events in which EU-HYBNET participates	Proceedings	0-3 per year	3-5 per year	More than 5 per year	Responsible: EOS, PPHS Accountable: Laurea Consulted: ESPOO, TNO, HCoE, PLV Informed: All other partners
	Number of abstracts/papers submitted and selected		Less than 5 at M52	5-12 at M52	More than 12 at M52	
Innovation and Knowledge workshop	Number of workshops organized	Events timeline	5			Responsible: EOS, TNO, PLV Accountable: Laurea, PPHS Consulted: HCoE, ESPOO Informed: All other partners
	Number of participants	Proceedings	Less than 60	60-80	More than 80	
	Number of registered participants	Proceedings	Less than 80	80-120	More than 120	
	Number of Tweets during a workshop	Twitter analytics	Less than 4	5-8	More than 8	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	
Future Trends workshop	Number of workshops organized	Events timeline	5			Responsible: HCoE, HSCS, MVNIA, PLV, JRC Accountable: EOS, Laurea, PPHS Consulted: ESPOO, TNO Informed: All other Partners
	Number of participants	Proceedings	Less than 60	60-80	More than 80	
	Number of registered participants	Proceedings	Less than 80	80-120	More than 120	
	Number of Tweets during a workshop	Twitter analytics	Less than 4	5-8	More than 8	

<sup>1</sup> For the brochures, the KPIs were lowered for a few reasons, not only because the measure of this KPI is quite difficult in practice, but also because COVID has changed brochures, as they cannot be given to online participants and for health concerns, they were handed out less during the course of the pandemic. Additionally, as environmental concerns start to become more prominent, the handing out of brochures has become less common. Online brochures have become more commonplace, but once again these are difficult to measure.

### D5.5 Updated Dissemination, Communication and Exploitation Plan 3

	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	
Gaps and needs workshops	Number of workshops organized	Events timeline	4			Responsible: HCoE Accountable: EOS, Laurea, PPHS Consulted: ESPOO, TNO, PLV Informed: All other partners
	Number of participants	Proceedings	Less than 40	40-55	More than 55	
	Number of registered participants	Proceedings	Less than 40	40-60	More than 60	
	Number of Tweets during a workshop	Twitter analytics	Less than 2	2-5	More than 5	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	
Annual Workshop	Number of workshops organised	Events Timeline	5			Responsible: LAUREA Accountable: PPHS, EOS Consulted: HCoE, TNO, KEMEA, Satways Informed: all partners
	Number of participants	Proceedings	Less than 60	60-80	More than 80	
	Number of registered participants	Proceedings	Less than 80	80-100	More than 100	
	Number of Tweets during a workshop	Twitter analytics	Less than 5	5-8	More than 8	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	
Liaison activities and synergies	Number of relevant projects/initiatives identified and contacted/invited at project events	List of attendees	Less than 4	4-10	More than 12	Responsible: EOS, PPHS Accountable: Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of relevant organisations/communities/experts identified and contacted/invited at project events		Less than 12	12-25	More than 30	
	Number of cooperation activities (common events	Proceedings	Less than 1	2-5	More than 5	

## D5.5 Updated Dissemination, Communication and Exploitation Plan 3

	and other clustering activities)					
Link to the Community of Users	Number of invitations to EU-HYBNET to join and to contribute to CERIS in a role of a speaker or panellist or creator of content to the event (e.g. scenario etc)	Proceedings	1 time in a year	Two times in a year	3 or more times in a year	Responsible: Laurea Accountable: EOS, PPHS Consulted: all consortium partners to join according to their interests and expertise
Impact towards Policy Makers	Number of bilateral meetings with Policy makers	Agenda	0-1	2-4	More than 4	Responsible: EOS, Laurea Accountable: PPHS Consulted: ESPOO, TNO, HCoE, PLV Informed: All other Partners
	Presentations made during events gathering policy makers	Proceedings	Less than 2	2-4	More than 4	
Stakeholders Board	Numbers of members	Proceedings	Less than 40	40-55	More than 55	Responsible: Laurea Accountable: EOS, PPHS, HCoE Consulted: ESPOO, TNO, PLV Informed: All other Partners

Following the assessment of the KPIs under D5.7, it became clear that the KPIs above could not be fully transferred for monitoring until the end of the project. While EU-HYBNET did quite well during the assessment (Most KPIs were excellent while others were good. Only minimal poors), the KPIs were assessed over the course of around 1.5 years and certain aspects such as Gaps and Needs workshops are over; therefore, the table below proposes targets for DCE for the last 5 months of the project based on the current situation.

Table 13: KPIs for M52-M60

Key Performance Indicators			Target at M52			Partners involved
			Level of performance			
Dissemination and Communication tools	Definition of the indicator	Type of data required	Poor	Good	Excellent	
Project Website	Number of visits per month	Google analytics	Less than 140 per month Less than 1400 at M52	140-300 per month 1400-3000 at M52	More than 300 per month More than 3000 at M52	Responsible: EOS Accountable: Laurea, PPHS Consulted: ESPOO, TNO, PLV, HCoE Informed: All other partners
	Page views per month		Less than 300 per month Less than 3000 at M52	300-500 per month 4000-5000 at 52	More than 500 per month More than 5000 at M52	
	Average time spent on website		Less than 30 seconds	30 seconds -1.5 min	More than 1.5 min	
Social Media	Subscribers of the LinkedIn Page		1 145 by M60	1 145 – 1 200 by M60	1 200+ by M60	Responsible: PPHS Accountable: Laurea, EOS

## D5.5 Updated Dissemination, Communication and Exploitation Plan 3

	Number of posts on LinkedIn	LinkedIn Group Statistics dashboard	Average of 1 post per month from M52-M60	Average of 3 post per month from M52-M60	Average of 6 post per month from M52-M60	Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of Twitter followers	Twitter analytics	Less than 745 at M60	750 by M60	More than 750 by M60	Responsible: EOS Accountable: PPHS, Laurea Consulted:ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of tweets per month		Less than 3	3-6	More than 6	
	Number of retweets per month		Less than 3	3-7	More than 7	
	Number of tweets liked per month		Less than 10	10-25	More than 25	
Biannual Newsletter	Number of Newsletters published	Proceedings	0	1	More than 1	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
Contributions to external events	Number of external events in which EU-HYBNET participates	Proceedings	0-3 per year	3-5 per year	More than 5 per year	Responsible: EOS, PPHS Accountable: Laurea Consulted: ESPOO, TNO, HCoE, PLV Informed: All other partners
	Number of abstracts/papers submitted and selected		5 by M60	5-12 at M60	More than 12 at M60	
5 <sup>th</sup> Future Trends workshop						Responsible: HCoE, HSCS, MVNIA, PLV, JRC Accountable: EOS, Laurea, PPHS Consulted: ESPOO, TNO Informed: All other Partners
	Number of participants	Proceedings	Less than 60	60-80	More than 80	
	Number of registered participants	Proceedings	Less than 80	80-120	More than 120	
	Number of Tweets during a workshop	Twitter analytics	Less than 4	5-8	More than 8	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	
5 <sup>th</sup> Annual Workshop						Responsible: LAUREA Accountable: PPHS, EOS Consulted: HCoE, TNO, KEMEA, Satways Informed: all partners
	Number of participants	Proceedings	Less than 60	60-80	More than 80	
	Number of registered participants	Proceedings	Less than 80	80-100	More than 100	
	Number of Tweets during a workshop	Twitter analytics	Less than 5	5-8	More than 8	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-4	More than 4	

## D5.5 Updated Dissemination, Communication and Exploitation Plan 3

Liaison activities and synergies	Number of relevant projects/initiatives identified and contacted/invited at project events	List of attendees	0 from M52-M60	1 from M52-M60	3+ from M52-M60	Responsible: EOS, PPHS Accountable: Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of relevant organisations/communities/experts identified and contacted/invited at project events		2 from M52-M60	5 from M52-M60	6+ from M52-M60	
	Number of cooperation activities (common events and other clustering activities)	Proceedings	Less than 1 from M52-M60	2 from M52-M60	3+ from M52-M60	
Impact towards Policy Makers	Number of bilateral meetings with Policy makers	Agenda	0 from M52-M60	1 from M52-M60	More than 1 from M52-M60	Responsible: EOS, Laurea Accountable: PPHS Consulted: ESPOO, TNO, HCoE, PLV Informed: All other Partners
	Presentations made during events gathering policy makers	Proceedings	0 from M52-M60	1 from M52-M60	More than 1 from M52-M60	

## 8. DCE: OTHER RELEVANT ISSUES

### 8.1 GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR issues are taken into consideration within the DCE Strategy. For example, the Data Protection Officers of all partners have been appointed, the online presence of EU-HYBNET (e.g. the webpage, social media accounts etc.) is in accordance with GDPR.

Perhaps the most critical in what comes to GDPR and DCE is the principle of consent. This includes both individuals being part of the activities as participants and as receivers of information. In the first case, for example, the participants are always asked for consents for publishing any comments or interviews, and no pictures are taken without any permission. This has been the policy and practice from the start of the project. The relevant consent forms together with the information sheets are prepared and stored in projects online documents repository (Eduuni) for the use of the whole consortium.

As information receivers, everyone is entitled to cancel, for example, any receiving of newsletters or such, and they can opt out from social media channels. Naturally, any personal data that is stored for dissemination purposes is processed securely by necessary means of appropriate technical and organisational measures, and used only for the purposes the data was originally collected.

Another guiding principle is avoiding revealing personal data (direct or indirect) altogether, especially if it is not adding any value to the dissemination or exploitation. For example, if a news story on the project can be written without disclosing any personal information.

Finally, visitors or users of the EU-HYBNET online platforms i.e. Website, Tuovi and Innovation Arena, have the right to request to know the data we hold on them and for its destruction upon request. However, some data such as IP address, location, device used, timestamp etc. of offending visitors performing suspicious actions on the website, may be held for security purposes.

### 8.2 ETHICAL MATTERS

Ethical matters are considered crucial within EU-HYBNET, and moreover taken into consideration within D5.1. Work Package 6 (Ethical Requirements) together with Work Package 1 (Management) treat in more details these issues.

However, two issues must be highlighted here. The first is related more to project dissemination, and the second more to exploitation, but the issues are not limited to one or another. The issues are limiting possible harm and ethically sustainable and societally acceptable use of the EU-HYBNET outcomes.

In short, EU-HYBNET aims in all action, including dissemination and exploitation, to avoid doing harm. In dissemination harm might be for example tarnished reputation caused by inaccurate or inappropriate communication. Thus, special emphasis must be put into accurate and proper communication actions, use of material (not revealing anything that should not be revealed), and also, for example, prompt corrections if any inaccuracies occurs. Although few if any of EU-HYBNET participants are professional journalist, their ethical guidelines are advised to follow when disseminating. (A list of them can be found in <https://accountablejournalism.org/ethics-codes/europe>).

What comes to the exploitation, that too, perhaps even more pivotally, must be ethical. Thus, for example, benefitting from the work done in WP1 (D1.17 and D1.18 Social Impact reports) and in WP6 (especially deliverables on misuse and dual use) the exploitation activities must be done taking ethics into considerations as well. The exploitation plans must also touch the whole ecosystem and business and governance models in which the end-results of EU-HYBNET (including the network itself) will so that at the end, EU-HYBNET can deliver something truly positive and meaningful.

Naturally, the Ethics Advisory Group is providing guidance for dissemination and exploitation too throughout the project.

### 8.3 SECURITY MATTERS

Security issues are also well assessed in DCE activities. Every kind of information is evaluated before any publication. The fake news issue is well apprehended within EU-HYBNET. Furthermore, a Security Advisory Board has been settled and handles any security matters. For example, hacking and malicious harm doing related to dissemination and exploitation are possible risks, especially related with online material and social media accounts.

### 8.4 CRISIS COMMUNICATION PLAN

A Crisis Communication Plan was established in May 2021. Due to the sensitive topics covered by EU-HYBNET, the formulation of such a document became crucial. It establishes persons of contact and strategy of mitigation (as this is essential that EU-HYBNET avoids bad publicity). (See Annex 7).

After an incident in late 2022 that required the activation of the Crisis Communication Plan, the Crisis Communication Plan was updated to reflect the lessons learned from this experience. The latest version is from October 2022.

## 9. CONCLUSIONS

### 9.1 SUMMARY

D5.5 has been the third and final update of EU-HYBNET's DCE plan. The update took into account the actions that were listed to be taken in the previous update (D5.4) from M35, what was done in reality, and the conclusions/analysis from the latest Midterm Project Dissemination Impact Assessment report (D5.7). EU-HYBNET has been quite active over the course of the entire project lifetime and involved in many events (both internal and external). This updated DCE plan now includes all of the dissemination actions that EU-HYBNET has undertaken since the beginning of the project until M52. Additionally, the KPI's have been updated based on D5.7, and will now constitute the KPIs to reach until the end of the project. This plan now replaces the previous report (D5.4) as the main document to lead future EU-HYBNET dissemination and communication work.

The DCE measures and to be undertaken by the project partners after the project lifetime will be determined by HCoE internal DCE policies, as they will be taking over the network after the project ends.

## ANNEX I: GLOSSARY AND ACRONYMS

Table 14 Glossary and Acronyms

<b>DCE</b>	<b>Dissemination, Communication and Exploitation</b>
<b>DCE Team</b>	Dissemination, Communication and Exploitation Team (WP5 Tasks Leaders : EOS, PPHS and LAUREA)
<b>DG</b>	Directorate General
<b>DoA</b>	Document of Action
<b>EASA</b>	European Aviation Safety Agency
<b>EBCGA</b>	European Boarder and Coast Guard
<b>EC</b>	European Commission
<b>EDA</b>	European Defense Agency
<b>EEAS</b>	European Union External Action Service
<b>EMSA</b>	European Maritime Safety Agency
<b>ERA</b>	Emergency Responses Agencies
<b>EU</b>	European Union
<b>GA</b>	Grant Agreement
<b>GDPR</b>	General Data Protection Regulation
<b>IA</b>	Innovation Arena
<b>KPIs</b>	Key Performance Indicators
<b>LEA</b>	Law Enforcement Agency
<b>REA</b>	Research Executive Agency
<b>RUSI</b>	Royal United Services Institute
<b>WP</b>	Work Package
<b>TUOVI</b>	Platform hosted by the Finnish Ministry of the Interior
<b>eDuuni</b>	Platform hosted by Laurea and used to the EU-HYBNET consortium internal information sharing
<b>Moi FI</b>	Finnish Ministry of the Interior
<b>LAUREA</b>	Laurea-ammattikorkeakoulu Oy
<b>PPHS</b>	Polish Platform for Homeland Security
<b>UiT</b>	Universitetet i Tromsø
<b>RISE</b>	RISE Research Institutes of Sweden Ab
<b>KEMEA</b>	Kentro Meleton Asfaleias
<b>L3CE</b>	Lietuvos Kibernetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
<b>URJC</b>	Universidad Rey Juan Carlos
<b>MTES</b>	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
<b>EOS</b>	European Organisation for Security Scrl
<b>TNO</b>	Nederlandse Organisatie voor Toegepast Natuureenschappelijk Onderzoek TNO



<b>SATWAYS</b>	SATWAYS
<b>ESPOO</b>	Espoon Kaupunki / Region and city of Espoo, Finland
<b>UCSC (UNICAT)</b>	Universita Cattolica del Sacro Cuore
<b>JRC</b>	JRC - Joint Research Centre - European Commission
<b>MVNIA</b>	Academia Nationala de Informatii Mihai Viteazul / The Romanian National Intelligence Academy
<b>HCoE</b>	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
<b>NLD MoD</b>	Ministry of Defence/NL
<b>ICDS</b>	International Centre for Defence and Security, Estonia
<b>PLV</b>	Ayuntamiento de Valencia / Valencia Local Police
<b>ABW</b>	Polish Internal Security Agency
<b>DSB</b>	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
<b>RIA</b>	Riigi Infosüsteemi Amet / Estonian Information System Authority
<b>MALDITA</b>	MALDITA
<b>ZITIS</b>	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
<b>UniBW</b>	Universitaet der Bundeswehr München

## ANNEX II: REFERENCES

- [1] Hybrid Threats, HCoE, Available here: <https://www.hybridcoe.fi/hybrid-threats/>
- [2] IIAP2 is the international organization advancing the practice of public participation which the mission to advance and extend the practice of public participation through professional development, certification, standards of practice, core values, advocacy and key initiatives with strategic partners around the world. <https://www.iap2.org/mpage/Home> - Consulted on the 20<sup>th</sup> of May 2010
- [3] The definition of “practitioner” was retrieved by the following website <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156>
- [4] Jan Willem Gunnink, project coordinator, COMET, in [https://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-guide-comm\\_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-guide-comm_en.pdf)

ANNEX III: EU-HYBNET LOGO



Figure 13: EU-HYBNET logo

## ANNEX IV: EU-HYBNET COLOR CODES

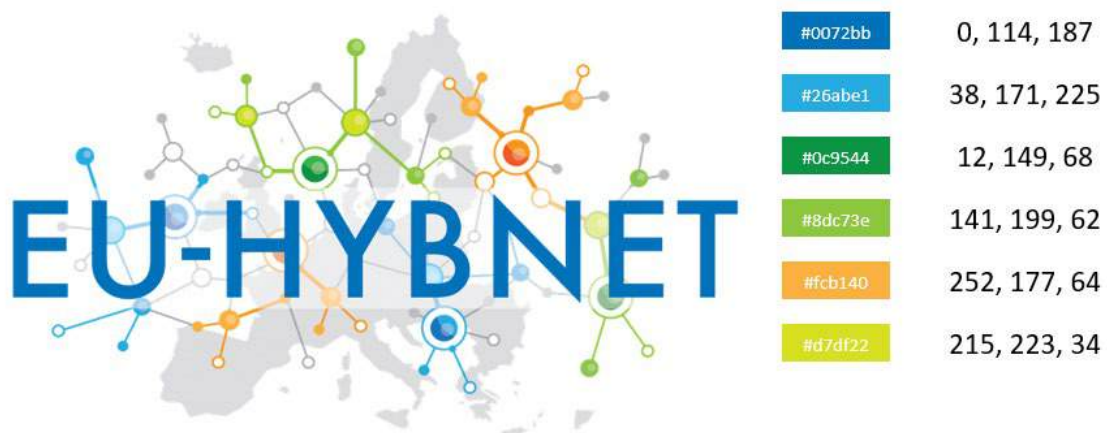


Figure 14: EU-HYBNET Color code

## ANNEX V: EU-HYBNET PARTNERS SOCIAL MEDIA ACCOUNT

Table 15 EU-HYBNET Partners' Social Media Accounts

	Linkedin	Twitter
LAUREA	<a href="#">LAUREA</a>	@Laureauas
PPHS	<a href="#">Polska Platforma</a>	<a href="#">@PolishPlatform</a>
UIT	<a href="#">UIT The Arctic University of Norway</a>	@UiTromso
RISE	<a href="#">RISE</a>	@RISEsweden
KEMEA	N/A	N/A
L3CE	<a href="#">L3CE</a>	@L3CE1
URJC	<a href="#">Universidad Juan Carlos</a>	@URJC
MTES	<a href="#">Ministère de la Transition écologique et solidaire</a>	@Ecologie_Gouv
EOS	<a href="#">EOS LinkedIn</a>	<a href="#">@EOS_EU</a>
TNO	<a href="#">TNO</a>	@TNO-nieuws
SATWAYS	<a href="#">SATWAYS</a>	@SatwaysLtd
ESPOO	<a href="#">City of Espoo</a>	@locateinespoo
USCS	<a href="#">Universita Cattolica Del Sacro Cuore</a>	@unicatt
JRC	<a href="#">JRC</a>	@EU_ScienceHub
MVNIA	NA	N/A
HCoE	N/A	@HybridCoE
ICDS	<a href="#">ICDS-Tallinn</a>	@ICS_Tallinn
PLV	N/A	@policialocalvlc
ABW	N/A	N/A
DSB	<a href="#">DSB</a>	@dsb.no
RIA	<a href="#">RIA</a>	N/A
MALDITA	<a href="#">MALDITA</a>	@maldita_es @malditobulo
ZITTIS	N/A	N/A
COMTESSA	<a href="#">COMTESSA</a>	@unibw

## ANNEX VI : UPDATED CRISIS COMMUNICATION PLAN



## ANNEX VII: EU-HYBNET UPDATED PRESENTATION TEMPLATE

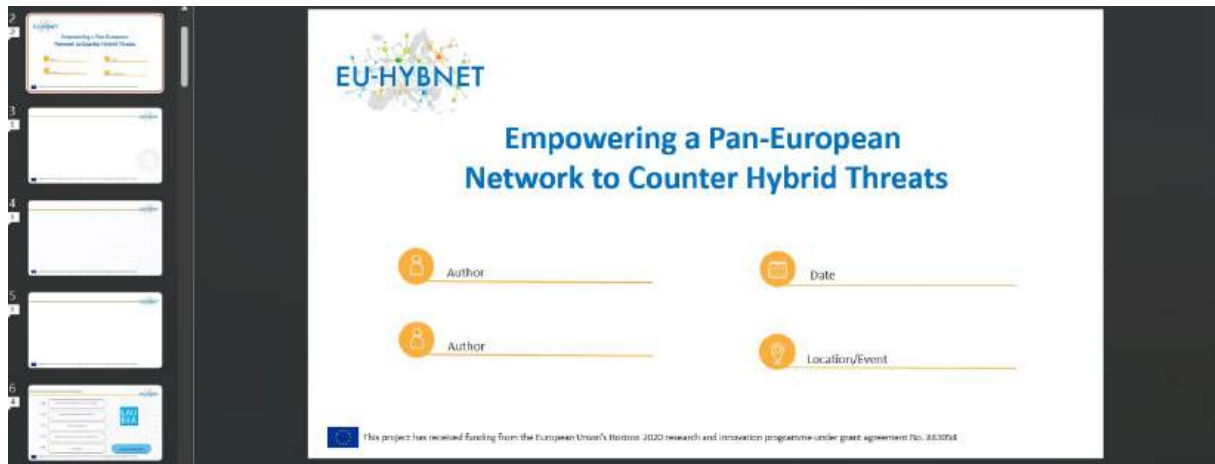



Figure 16: EU-HYBNET Presentation Table

## ANNEX VIII : EU-HYBNET DELIVERABLE TEMPLATE




**DELIVERABLE NAME**

DELIVERABLE X.X

Lead Author : Partner Name

Contributors : Partners Name

Deliverable classification : (PU, CO, RESTRAINT UE)



This project has received funding from the European Union's Horizon 2020 - Research and Innovation Framework Programme, 101019-01-001-001, under grant agreement No. 883054

DK.X Name of the Deliverable

DK.X NAME OF THE DELIVERABLE	
Deliverable number	
Version	
Delivery date	
Dissemination level	
Classification level	
Status	
Subject	
Main author(s)	
Contributor(s)	

DOCUMENT CONTROL			
Version	Date	Author(s)	Change(s)

**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.

Grant Agreement : 883054
Dissemination level : PUBLIC/CONFIDENTIAL/EU RESTRICTED..
p. 1

DK.X Name of the Deliverable

TABLE DES MATIERES	
1. Introduction	3
1.1 Overview	3
1.2 Structure of the deliverable	3
2. [Section title]	4
2.1 [2nd level header]	4
2.1.1 [3RD LEVEL HEADER]	4
3. [Section title]	6
3.1 [2nd level header]	6
3.1.1 [3RD LEVEL HEADER]	6
4. CONCLUSION	7
4.1 SUMMARY	7
4.2 FUTURE WORK	7
ANNEX I. GLOSSARY AND ACRONYMS	8
ANNEX II. REFERENCES	9
ANNEX III. [ANNEX TITLE]	10

TABLES	
Table 1 - [description]	4
Table 2 Glossary and Acronyms	8

FIGURES	
Figure 1 EU-HYBNET Structure of Work Packages and Main Activities	5

Grant Agreement : 883054
Dissemination level : PUBLIC/CONFIDENTIAL/EU RESTRICTED..
p. 2

DK.X Name of the Deliverable

2. [SECTION TITLE]				
2.1 [2ND LEVEL HEADER]				
<p style="font-size: x-small;">Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi. Nulla quis sem at nibh elementum imperdiet. Duis sagittis ipsum. Praeent mauris. Fusce nec tellus sed augue semper porta. Mauris massa. Vestibulum lacinia arcu eget nulla. Class aptent taciti sodosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur sodales ligula in libero. Sed dignissim lacinia nunc. Curabitur tortor. Pellentesque nish. Aenean quam. In scelerisque sem et dolor. Maecenas mattis. Sed convallis tristique sem. Proin ut ligula vel nunc egestas porttitor. Morbi lectus risus, iaculis vel, suscipit quis, luctus non, massa. Fusce ac turpis quis ligula lacinia aliquet. Mauris ipsum. Nulla metus metus, ullamcorper vel, tincidunt sed, euismod in, nish. Quisque volutpat condimentum velit.</p>				
2.1.1 [3RD LEVEL HEADER]				
<p style="font-size: x-small;">Class aptent taciti sodosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nam nec ante. Sed lacinia, urna non tincidunt mattis, tortor neque adipiscing diam, a cursus ipsum ante quis turpis. Nulla facilis. Ut fringilla. Suspendisse potenti. Nunc feugiat mi a tellus consequat imperdiet. Vestibulum sapien. Proin quam. Etiam ultrices. Suspendisse in justo eu magna luctus suscipit. Sed lectus. Integer euismod lacus luctus magna.</p>				
2.1.1.1 [4TH LEVEL HEADER]				
<p style="font-size: x-small;">Quisque cursus, metus vitae pharetra auctor, sem massa mattis sem, at interdum magna augue eget diam. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Morbi lacinia molestie dui.</p>				
2.1.1.1.1 [5TH LEVEL HEADER]				
<p style="font-size: x-small;">Praesent blandit dolor. Sed non quam. In vel mi sit amet augue congue elementum. Morbi in ipsum sit amet pede facilisis laoreet. Donec lacus nunc, viverra nec</p>				
Table 1 - [description]				
Title 1	Title 2	Title 3	Title 4	Title 5

Figure 17: EU-HYBNET Deliverable template



ANNEX IX: AGENDA OF THE 3<sup>RD</sup> IKEW

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	José Vicente Herrera Arrando Chief of the PLV Jesús Carbonell Aguilar City Council Member representative of the PLV
09:15-09:30	Keynote Speech #1: Considerations on “Innovation Uptake”	Giannis Skiadaresis SSRI Area Coordinator, DG HOME, European Commission
09:30-09:45	Keynote Speech #2	Francisco Alonso Batuecas Head of ICT Infrastructure and Security, Security Technology Centre (CETSE), Secretary of State for Security
09:45-10:15	Results of Innovations Mapping and Assessment (3rd EU-HYBNET Cycle)	Souzanna Sofou, SATWAYS Okke Lucassen, TNO
10:15-10:30	Audience Q&A	Moderator: José L. Diego Head of the Innovation & Project Management Division, Valencia Local Police
10:30-10:45	Coffee Break	
Parallel Breakout Sessions		
10:45-12:15	Breakout Session #1: Cyber and future technologies  Innovation: STARLIGHT EU Project – way forward with AI transformative impact on security domain	Moderator & Presenter: Evaldas Bružė Deputy Director, Head Innovations' Architect, Lithuanian Cybercrime Center of Excellence for Training, Research & Education (L3CE)
	Breakout Session #2: Information and strategic communications  Innovation: VIGILANT EU Project	Eva Power VIGILANT Project Manager, ADAPT Centre, Trinity College Dublin  Oisín Carroll VIGILANT Technical Coordinator, ADAPT Centre, Trinity College Dublin  Moderator: Päivi Mattila EU-HYBNET Project Coordinator, Laurea UAS

12:15-13:15	Lunch Break	
Parallel Breakout Sessions		
13:15-14:45	<b>Breakout Session #3:</b> Resilient civilians, local level, and administration <b>Innovation:</b> CONNECTOR EU Project	<i>Javier Moreno García</i> Maritime Officer, Customs and Coast Guard, Spain (DAVA-AEAT) <b>Moderator:</b> <i>Gunhild Hoogensen Gjørsv</i> The Arctic University of Norway (UiT) <i>Isto Mattila</i> EU-HYBNET Innovation Manager, Laurea UAS
	<b>Breakout Session #4:</b> Future trends of Hybrid Threats <b>Innovation:</b> AI transformative implications on security research and emerging security practitioners' needs	<b>Moderator &amp; Presenter:</b> <i>Evaldas Bružė</i> Deputy Director, Head Innovations' Architect, Lithuanian Cybercrime Center of Excellence for Training, Research & Education (L3CE)
14:45-15:00	Coffee Break	
15:00-16:00	Break-out session outcomes	Break-out session moderators in conversation with: <ul style="list-style-type: none"><li>• Europol Innovation Lab Representative</li><li>• <i>Rashel Talukder</i> Managing Director of the Polish Platform for Homeland Security</li><li>• <i>José L. Diego</i> Head of the Innovation &amp; Project Management Division, Valencia Local Police</li></ul>
16:00-16:10	Audience Q&A	
16:10-16:25	Linking innovation providers and practitioners	<i>Eva Škruba</i> Capability Manager, EACTDA
16:25-16:30	Closing remarks	<i>José L. Diego</i> Head of the Innovation & Project Management Division, Valencia Local Police
16:30-18:00	Round table discussion: EU-HYBNET post-project topics	<i>Päivi Mattila</i> , LAUREA <i>Christian Despres</i> , MTES <i>Gunhild Hoogensen-Gjorv</i> , UiT <i>Souzanna Sofou</i> , SATWAYS <i>Julian Theron</i> , JRC

Figure 18 : Agenda of the 3rd IKEW

ANNEX X: AGENDA OF THE 2<sup>ND</sup> ISW

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	<i>José L. Diego</i> Head of the Innovation & Project Management Division, Valencia Local Police
09:15-09:30	<b>Keynote Speech #1</b> Protecting Critical Infrastructure in a changing world – a government perspective	<i>Kimini Delfos, Kiki van Setten</i> Dutch Ministry of Infrastructure and Water Management
09:30-09:45	<b>Keynote Speech #2</b> Unlocking sustainable networked defence against FIMI: The key role of standards	<i>Daniel Fritz</i> European External Action Service
09:45-10:00	<b>Keynote Speech #3</b> Whole of government approach to countering hybrid threats: lessons learned and challenges from Slovakia (focus on non-technical innovation in terms of coordination of actors, setting up structures, joint analytical outputs and monitoring of information space)	<i>Daniel Mila</i> Centre for Countering Hybrid Threats, Institute for administrative and security analysis, Ministry of Interior of the Slovak Republic
10:00-10:15	Audience Q&A	<b>Moderator:</b> <i>Iván Luis Martínez Villanueva</i> Valencia Local Police
10:15-10:45	Coffee Break	
Parallel Breakout Sessions		
	<b>Breakout Session #1:</b> Foreign Information Manipulation and Interference (FIMI)	<b>Breakout Session #2:</b> Protection of Critical Infrastructure
10:45 - 11:15	<b>Keynote speech:</b> Foreign Information Manipulation and Interference: Strategic Threats on the Rear  <i>Julien Théron</i> Joint Research Centre (JRC)  <b>Moderator:</b> <i>Rashel Talukder</i> Polish Platform for Homeland Security (PPHS)  Audience Q&A 11:00 – 11:15	<b>Keynote speech:</b> <i>Georgios Kolliarakis</i> German Council on Foreign Relations (DGAP)  <b>Moderator:</b> <i>Isto Mattila</i> Laurea  Audience Q&A 11:00 – 11:15
11:15 – 12:30	<b>#1 case study presentation &amp; discussion</b> Antagonising Poles and Ukrainians through disinformation – challenges and responses	<b>#1 case study presentation &amp; discussion</b> Hybrid activities aimed at Polish Critical Infrastructure (CI). Case study based on a transportation system



	<p><i>Paula Rejkiewicz</i> Ministry of Foreign Affairs Republic of Poland, Strategic Communication and Countering Disinformation Unit</p> <p><b>Moderator:</b> <i>Rashel Talukder</i> Polish Platform for Homeland Security (PPHS)</p>	<p><i>Karolina Wojtasik</i> Government Centre for Security (RCB), Polish Association for National Security (PTBN)</p> <p><b>Moderator:</b> <i>Isto Mattila</i> Laurea</p>
12:30 – 13:30	Lunch Break	
13:30 – 14:30	<p><b>#2 case study presentation &amp; discussion</b> (F)IMI &amp; Innovative solutions for detection: A case study of online coordinated inauthentic campaigns from 'pro-Iranian' and 'pro- Palestinian' accounts on Twitter / X</p> <p><i>Esther Jacobs</i> TILT Insights</p> <p><b>Moderator:</b> <i>Rashel Talukder</i> PPHS</p>	<p><b>#2 case study presentation &amp; discussion</b> Hybrid threats against Critical infrastructures and the case of Italy</p> <p><i>Paola Tessari</i> IAI Istituto Affari Internazionali</p> <p><b>Moderator:</b> <i>Isto Mattila</i> Laurea</p>
14:30 – 15:30	<p><b>#3 case study presentation &amp; discussion</b> Addressing the challenges of the early detection of advanced manipulation campaigns</p> <p><i>David Arroyo</i> Spanish National Research Council (CSIC)</p> <p><b>Moderator:</b> <i>Rashel Talukder</i> PPHS</p>	
15:00 – 15:15	Coffee Break	
15:15 – 15:45	<p>Breakout sessions outcomes Audience Q&amp;A</p>	<p><b>Moderator:</b> <i>Isto Mattila</i> Laurea and <i>Rashel Talukder</i> PPHS</p>
15:45 – 16:00	<b>Closing remarks</b>	<p><i>José Vicente Herrera Arrando</i> Comisario Principal Jefe de la Policía Local de Valencia <i>Jesús Carbonell Aguilar</i> Concejal Delegado de la Policía Local de Valencia</p>

Figure 19: Agenda of the 2nd ISW

ANNEX XI: AGENDA OF THE 3<sup>RD</sup> ISW

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	LAUREA, Polish Platform for Homeland Security, Helsinki EU Office
09:15-09:30	<b>Keynote Speech #1</b> <b>Giannis Skiadaresis (DG Home)</b> Hybrid Threats innovation uptake in the future	
09:30-09:40	Audience Q&A	<b>Moderator:</b> EU-HYBNET Coordinator Prof. Isto Mattila
9:40 – 10:40	<b>Session 1 – Innovation: Citizen – Responder Platform for Information Sharing in a case of an Emergency and Crises (CRP),</b> <ul style="list-style-type: none"> <li>- Presentation of the innovation: Citizen – Responder Platform (CRP), <b>EU-HYBNET Innovation Manager Petteri Partanen, LAUREA</b> (9:40 – 9:45)</li> <li>- Standards in European and international level in the field of security, <b>Pertti Woitsch, Woitsch Consulting</b> (9:45 – 10:05)</li> <li>- Expert view to Hybrid threats and the CRP Innovation, <b>Austrian Red Cross</b> (10:05 – 10:25) <b>tbc</b></li> <li>- Discussion (10:25 – 10:40)</li> </ul>	<b>Moderator:</b> EU-HYBNET Coordinator, Prof. Isto Mattila
10:40-11:00	Coffee Break	
11:00 – 12:00	<b>Session 2 – Innovation: Local Media Hybrid Threats Tracker (LMHTT)</b> <ul style="list-style-type: none"> <li>- Presentation of the innovation: Local Media Hybrid Threats Tracker (LMHTT), <b>Polish Platform for Homeland Security</b> (11:00 – 11:05)</li> <li>- Topic, <b>Philip Starz, Travelsals</b> 11:05 – 11:25) <b>tbc</b></li> <li>- Fact-checking, media literacy, <b>Karina Stasiuk-Krajewska, CEDMO / SWPS University</b> (11:25 – 11:45)</li> <li>- Discussion (11:45 – 12:00)</li> </ul>	<b>Moderator:</b> Polish Platform for Homeland Security, Rashel Talukder
12:00 – 13:00	<b>Session 3 – Innovation: Innovation: Citizens Reporting Tool on Suspicious Signs (CiReTo)</b> <ul style="list-style-type: none"> <li>- Presentation of the innovation: Citizens Reporting Tool (CiReTo), <b>Rolf Blom, RISE</b> (12:00 – 12:05)</li> <li>- Topic, <b>Polish Police</b> (12:05- 12:25)</li> <li>- Police's view to tools used by citizens to announce suspicious actions – room for AI to support data analysis and to pin point critical cases, <b>Tomas Divis, Police of the Czech Republic</b> (12:25 – 12:45)</li> <li>- Discussion (12:45 – 13:00)</li> </ul>	<b>Moderator:</b> RISE, Rolf Blom
13:00 – 14:00	Lunch Break	
14:00 – 15:00	<b>Session 4 – Innovation: STARLIGHT and Innovation testing best practices</b>	<b>Moderator:</b> L3CE



	<ul style="list-style-type: none"> <li>- Presentation of the innovation: STARLIGHT and Innovation testing best practices, <b>L3CE</b> (14:00 – 14:05)</li> <li>- Topic, <b>Nikolaos Gkalelis, EUROPOL Innovation Lab</b> (14:05 – 14:25)</li> <li>- <b>STARLIGHT Project, Speaker</b> (14:25 – 14:45) <b>tbc</b></li> <li>- Discussion (14:45 – 15:00)</li> </ul>	
<b>15:00 – 15:30</b>	<b>Jorge Garzon, French Ministry of Interior, iProcureNet Project</b> Audience Q&A	<b>Moderator:</b> Satways, Dr Souzanna Sofou
<b>15:30 – 16:00</b>	Workshop outcomes & Closing Remarks	EU-HYBNET Coordinator, Prof. Isto Mattila;

Figure 20: Agenda of the 3rd ISW

ANNEX XII: AGENDA OF THE 3<sup>RD</sup> FTW

Time EEST	Topic	Speaker
08.30-09.00	Registration	
Plenary session (Room: Ramada Europe)		
09.00-09.15	Welcome & Practical Information	Dr. Päivi Mattila, EU-HYBNET Coordinator, Laurea Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy
09.15-09.30	<b>Keynote Speech #1:</b> "Hybrid threats in the Black Sea Region and implications for European security"	Mr. Ovidiu Raetchi, President, Euro-Atlantic Resilience Centre
09.30-09.45	<b>Keynote Speech #2</b>	Mr. Dan Cîmpean, National Directorate for Cyber Security, Romania
09.45-10.00	<b>Keynote Speech #3:</b> "EU Maritime Security Strategy"	Mr Thierry Segers, Policy Officer, Directorate-General for Maritime Affairs and Fisheries, European Commission - <b>online speaker</b>
10.00-10.15	Audience Q&A	<b>Moderator:</b> Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea
10.15-10.35	Coffee Break (at Foyer Plaza)	
10.35 – 12:00	<b>Panel Discussion:</b> Hybrid threats in the EU's neighbourhood shaping the future of EU security	<b>Chair:</b> Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy  <b>Panel speakers:</b> <ul style="list-style-type: none"> <li>• Dr. Iulian Fota, State Secretary for Strategic</li> </ul>



		Affairs, Ministry of Foreign Affairs, Romania <ul style="list-style-type: none"><li>• Ms. Liudmyla Buimister, Member of Parliament, Ukraine</li><li>• Dr. Orlando Cenciarelli, European Centre for Disease Prevention and Control</li><li>• Dr. Souzanna Sofou, Senior Research and Innovation Manager, SATWAYS</li></ul>
12:00 – 13:15	Lunch Break (at Red Pepper)	
Parallel Breakout Sessions		
13:15-14:45	<b>Breakout Session #1:</b> Cyber & Future Technologies <i>Room: Ramada Africa</i>	Evaldas Bruze (L3CE)
	<b>Breakout Session #2:</b> Resilient Civilians, Local Level and National Administration <i>Room: Ramada Asia</i>	Gunhild Hoogensen Gjörv (UIT)
	<b>Breakout Session #3:</b> Information & Strategic Communication <i>Room: Ramada Europa</i>	Rubén Arcos (URJC) Irena Chiru (MVNIA)
14:45-15:00	Coffee Break (at Foyer Plaza)	
15:00-15:30	<b>Panel Discussion:</b> Future Trends for EU security	<b>Chair:</b> Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea  <b>Panel speakers:</b> <ul style="list-style-type: none"><li>• Evaldas Bruze (L3CE)</li><li>• Gunhild Hoogensen Gjörv (UIT)</li><li>• Dr. Rubén Arcos (URJC)</li></ul>
15:30-15:45	Audience Q&A	
15:45 - 16.00	<b>Closing Keynote Speech:</b> The role of the Common Information Sharing Environment (CISE) for EU Maritime Security	Mr. Gianluca Luraschi, Project Officer, Department 2 - Safety, Security and Surveillance at European Maritime Safety Agency (EMSA)
16.00-16.05	Closing remarks	Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy

Figure 21: Agenda of the 3<sup>rd</sup> FTW

ANNEX XIII: AGENDA OF THE 4<sup>TH</sup> FTW

Time EEST	Topic	Speaker
09.00-09.30	Registration	
Plenary session		
09.30-09.45	Welcome & Practical Information	Mr Jesús Carbonell Aguilar, City Councillor, representative of the Valencia Local Police Mr José Vicente Herrera Arrando, Chief Constable of the Valencia Local Police
09.45-10.00	<b>"Models for Conflict Analysis &amp; Some Critical Remarks on Dealing with Hybrid Threats"</b>	Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces
10.00-10.30	Audience Q&A	<b>Moderator:</b> Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police
10.30-10.45	Coffee Break	
10.45 – 12:15	Border Management to Counter Future Hybrid Threats	<b>Chair:</b> Isto Mattila, EU-HYBNET Innovation Manager  <b>Panel speakers:</b> <ul style="list-style-type: none"><li>• Dr. Souzanna Sofou, Satways</li><li>• Dr. Jarmo Puustinen, Finnish Mol</li><li>• Europol Innovation Lab Representative</li></ul>
12:15 – 13:15	Lunch Break	
Parallel Breakout Sessions		
13:15-14:15	<b>Breakout Session #1: Future Trends in Cyber and Future Technologies</b> Core Theme: Cyber and Future Technologies	Evaldas Bružė, Analyst and Consultant in Commercial Development at L3CE.
	<b>Breakout Session #2: Weaponization of Migration</b>	Dr. Julien Theron, Researcher in Hybrid Threats at the JRC

	Core Theme: Resilient civilians, local level and national administration	
<b>14:15-14:30</b>	Coffee Break	
	<b>Breakout Session #3: Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats</b> Core Theme: Information & Strategic Communication	Jorge Gomez (VOST Europe)
<b>14:30-15:30</b>	<b>Breakout Session #4: Securing the EU's borders to 2040 – Thinking about the security landscape</b> Core Theme: Future Trends of Hybrid Threats	Maxime Lebrun, Deputy Director R&A at The European Centre of Excellence for Countering Hybrid Threats Hanne Dumur-Laanila, Analyst at the The European Centre of Excellence for Countering Hybrid Threats
<b>15:30-15:45</b>	Conclusions of the BOS & Audience Q&A	
<b>15:45 – 16:00</b>	<b>"FRONTEX's View on the Future of Hybrid Threats in Relation to Border Management"</b>	Mr. Dinesh Rempling, Head-of Capability Programming Office at FRONTEX
<b>16:00 – 16:10</b>	Closing remarks & Practical Information for Annual Workshop	Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police
<b>16:10 – 17:10</b>	EU-HYBNET Societal Impacts Workshop	Tuomas Tammilehto, EU-HYBNET Ethics Manager

Figure 22: Agenda of the 4th FTW

ANNEX XIV: AGENDA OF THE 3<sup>RD</sup> AW

Time EET	Topic	Speakers
<b>Welcome and registration</b> <i>Room: Ramada Europe</i>		
8:30-9:00	Registration	
9:00-9:10	Welcome & Practical information	Dr. Päivi Mattila, <i>EU-HYBNET Coordinator, Laurea</i> Dr. Cristina Ivan, <i>Mihai Viteazul National Intelligence Academy</i>
9:10-9:20	<b>Keynote Speech #1:</b> "NIS2 and the way forward"	Ms Svetlana Schuster, <i>European Commission, DG CONNECT, Head of Sector Implementation and Review of the NIS Directive</i>
9:20-9:30	<b>Keynote Speech #2:</b> "Bolstering efforts to counter foreign interference"	Dr. Nad'a Kovalčíková, <i>Senior Analyst, European Union Institute for Security Studies</i>
9:30-9:50	Audience Q&A	<b>Host:</b> Dr. Cristina Ivan, <i>Mihai Viteazul National Intelligence Academy</i>
<b>EU-HYBNET's latest findings and results</b> <i>Room: Ramada Europe</i>		
9:50-10:50	Round Table Discussion: EU-HYBNET 3 <sup>rd</sup> year, latest findings and results to countering hybrid threats on <ul style="list-style-type: none"> <li>- Gaps &amp; Needs findings, research focus</li> <li>- Promising innovations for counter measures</li> <li>- Innovation uptake recommendations</li> <li>- Network activities</li> </ul>	<b>Round Table experts:</b> <ul style="list-style-type: none"> <li>- <i>EUROPOL Innovation Lab</i></li> <li>- Dr. Teemu Tammikko, <i>Policy Officer, European External Action Service/Hybrid Threats Sector, Security and Defence Policy Division of the European External Action Service</i></li> <li>- Mr. Juraj Majcin, <i>Program Manager, Friends of Europe</i></li> </ul> <b>EU-HYBNET Consortium:</b> <ul style="list-style-type: none"> <li>- Mr. Evaldas Bruze/ <i>L3CE</i></li> <li>- Dr. Souzanna Sofou, <i>Satways</i></li> </ul>



		<ul style="list-style-type: none"><li>- Mr. Alex Koniaris, Ms Vanessa Papapkosta, Dr. Athanasios Kosmopoulos, KEMEA</li><li>- Dr. Rolf Blom, Research Institutes of Sweden</li><li>- Mr. Rashel Talukder, Polish Platform for Homeland Security</li><li>- Mr. Jari Räsänen/ Laurea</li></ul>
10.50-11.00	Audience Q&A	<b>Host:</b> Mr. Paolo Venturoni, CEO European Organization for Security
11.00-11.20	Coffee break (at Foyer Plaza)	
Pitches - Innovation and ideas to counter hybrid threats by organizations and projects Room: Ramada Europe		
11.20-11.30	"Countering Disinformation with Maltego"	Mr. Stefan Iwan, Maltego
11.30-11.40	"TrustServista – AI-powered Content Analytics and Verification Platform"	Mr. George Bara, TrustServista
11.40-11.50	"CRITERIA - Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks"	Dr. Aitana Radu, University of Malta
11.50-12.00	Innovations from CYCLOPES EC funded project	Rashel Talukder, Coordinator of Fighting Cyber Crime – Law Enforcement Practitioners' Network (CYCLOPES), Polish Platform for Homeland Security
12.00-12.10	Innovation from CRESCent-DOMINOES EC funded project	Dr. Ruben Arcos, Rey Juan Carlos University, Spain Mr. Alberto Sanchez, Rey Juan Carlos University, Spain
12.10-12.40	Audience Q&A	<b>Host:</b> Mr. Okke Lucassen, TNO
12.40-13.40	OpenCTI/DDS-Alpha Innovation to Counter Hybrid Threats in the Information Domain	Ms. Chiara Pacenti, European External Action Service – Strategic Communication Division
13.30-13.40	Audience Q&A	Host: Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea
13.40-13.50	Closing remarks	Dr. Päivi Mattila, EU-HYBNET Coordinator, Laurea Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy
13.50-14.30	Lunch Break (at Red Pepper)	

Figure 23: Agenda of the 3rd AW

ANNEX XV: AGENDA OF THE 4<sup>TH</sup> AW

Time CET	Topic	Speakers
<b>Welcome and registration</b>		
<b>8:30-9:00</b>	Registration	
<b>9:00-9:10</b>	Welcome & Practical information	José L. Diego, Inspector, Head of Innovation & Project Management Division, PLV Päivi Mattila, EU-HYBNET Coordinator, Laurea
<b>9:10-9:20</b>	Keynote Speech "From analysis to (re)action – a framework for networked defence"	Chiara Pacenti Information Systems Officer European External Action Service (EEAS)/ Strategic Communications and Information Analysis
<b>9:20-9:30</b>	Keynote Speech "The EU approach to countering hybrid threats"	Torben Fell, Policy Officer EEAS/SECDEFPOL.2, Hybrid Threats and Cyber, Hybrid Threats Sector
<b>9:30-9:40</b>	Keynote Speech "European elections 2024 and hybrid threats"	Manuel Rodríguez Vico Director for Technologies and Information, DG SAFE – European Parliament
<b>9:40-10:10</b>	Audience Q&A	<b>Host:</b> José L. Diego, PLV
<b>EU-HYBNET's latest findings and results</b>		
<b>10:10-11:10</b>	Round Table Discussion on "EU-HYBNET 4 <sup>th</sup> year findings and results to counter hybrid threats" – topics: <ul style="list-style-type: none"> <li>• "Findings on present pan-European security practitioners' gaps&amp;needs/ threats to counter hybrid threats"</li> <li>• "Identified promising innovations to counter hybrid threats"</li> <li>• "Innovation uptake recommendations"</li> </ul>	<b>EU-HYBNET Consortium:</b> <ul style="list-style-type: none"> <li>- Hanne Dumur-Laanila, Analyst, Research &amp; Analyses, European Center of Excellence for Countering Hybrid Threats</li> <li>- Evaldas Bruze, L3CE</li> </ul>

	<ul style="list-style-type: none"><li>• "EU-HYBNET Network activities and sustainability"</li></ul>	<ul style="list-style-type: none"><li>- Souzanna Sofou, Senior Research and Innovation Manager, Satways</li><li>- Julien Theron, Researcher in Hybrid Threats, Joint Research Centre (JRC)</li><li>- Päivi Mattila, EU-HYBNET Coordinator, Laurea</li></ul>
11.10-11.20	Audience Q&A	<b>Hosts:</b> Tiina Haapanen, EU-HYBNET Project Manager, Laurea  Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, PLV
11.20-11.50	Coffee break	
Pitches		
Innovations and solutions to counter hybrid threats by organizations and projects		
11.50-12.00	Denial-of-service/DDOS / attack on infrastructures critical to population livelihood - Pitch	Marios Thoma, Director, CyberEcoCul Global Services
12.00-12.10	Smart City -Pitch	Marina Galiano Botella, CSIRT-CV
12.10-12.20	Resilience Assessment Tool (R/VAT) -Pitch	Vazha Sopromadze, The University of Georgia Security, Policy and Nationalism Center
12.20-12.30	Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats - Pitch	David Arroyo, The Spanish National Research Council
12.30-12.40	"European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection" (EU-CIP), Horizon project	EU-CIP coordinator Emilia Gugliandolo, Senior Researcher, ENGINEERING
12.40-12.50	"Toward Sustainable Foresight Capabilities for Increased Civil Security" (AHEAD), Horizon project	Laure Brévignon-Dodin, Head of Office, Directorate for International Security Cooperation, Ministry of the Interior in France
12.50-13.00	"Gaming Ecosystem as a Multi-Layered Security Threat" (GEMS), Horizon project	Bledar Feta, Hellenic Foundation for European and Foreign Policy
13.00-13.10	"Protecting our strategic Assets, Values and Economy against harmful Disinformation" (PAVED) project, initiative of France	Frederic Tatout, Anatase; Anne-Marie Duval, Ministry of Ecological Transition in France
13.10-13.40	Audience Q&A	<b>Host:</b> Isto Mattila, EU-HYBNET Innovation Manager, Laurea
13.40-13.50	Closing remarks	José L. Diego, PLV
13.50-15.00	Lunch	
15.00-16.30	EU-HYBNET General Assembly EU-HYBNET Consortium partners only	

Figure 24: Agenda of the 4<sup>th</sup> Annual Workshop