EU-HYBNET

UPDATED DISSEMINATION, COMMUNCIATION AND EXPLOITATION PLAN

DELIVERABLE 5.3

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

D5.3 UPDATE OF THE DISSEMINATION COMMUNICATION AND EXPLOITATION PLAN

Deliverable number	**D5.3**	
Version:	**VO.1**	
Delivery date:	**26/10/2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**ready**	
Nature:	**Report**	
Main authors:	**Elodie Reuge, Maguelone Laval**	**EOS**
Contributors:	**All partners**	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

Version	Date	Authors	Changes
V0.1	30/09/2021	EOS	First draft
V0.2	11/09/2021	EOS	Update following task leaders and partners feedbacks
V0.3	18/10/2021	MoD	Peer Review
V0.3	18/10/2021	EOS	Integration of the comments
V0.4	20/10/2021	LAU, PPHS	Peer Review
V0.9	21/10/2021	EOS	Final version
V1	26/10/2021	LAU	Final review and submission of the D5.3 to the EC

DISCLAIMER

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

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

TABLE OF CONTENT

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

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 is achieved by defining the common requirements of European practitioners' and other relevant actors in the field of hybrid threats. Ultimately, this can fill knowledge gaps, deal with performance needs, and enhance capabilities or research, innovation and training endeavours concerning hybrid threats.

EU-HYBNET monitors developments in research and innovation activities as applied to hybrid threats; so 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 60 months. 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.

D5.1 addressed the relevant stakeholders through several channels: social networks (LinkedIn and Twitter already put in place at M1), the website (ready since M3), information sharing platforms (eDuuni, TUOVI, Innovation Arena) the "Innovation and Knowledge Exchange" workshops, the "Future Trends" workshops, Annual Workshops, Gaps and Needs events, trainings and exercises as well project documentation and public reports.

D5.3 (Updated Dissemination, Communication and Exploitation Strategy) consists of the update of the First DCE Strategy 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, constitute the basis for the update of the DCE Plan.

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

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 the paragraph below, on overview of benefits, starting from a general vision and concluding with a more specific and coherent approach to EU-HYBNET is presented.

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."**Error! Reference source not found.***

Accordingly, the Hybrid CoE characterises hybrid threat as:

- *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."**Error! Reference source not found.***

The hybrid threats ecosystem is a very sensitive and complex sector, involving every kind of organisations and activities The fight against hybrid threats is starting to gain more priority in modern societies. As an adequate awareness and understanding of the concept must be ensured, Europe needs a systematic approach to better manage evolving risks and vulnerabilities. The involvement of relevant stakeholders is crucial to manage the dissemination of the project results.

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

Stakeholder engagement is the first step to achieve the crucial goal of a global optimum for a systemic secure society[1]. 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 the stakeholders, the objectives of countering hybrid threats will be optimised, and it will allow existing resources to connect gaps and dots coherently in the innovation solutions and research landscape. The result will be 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 proper knowledge when it comes to hybrid threats. Indeed, it became a necessity to start most of the project's event with an introduction to the concept in order to make sure there is a consensus on what the project partners will be covering in their analysis. Therefore, it has been agreed that the next cycle (M18-M34) will focus on providing EU-HYBNET network members with brochures and a video focusing on the definition of hybrid threats. This task will be accomplished with the assistance of Hybrid CoE who has already developed a significant amount of educational content.

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]

[1] For further details related to Secure Societies, please see : https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

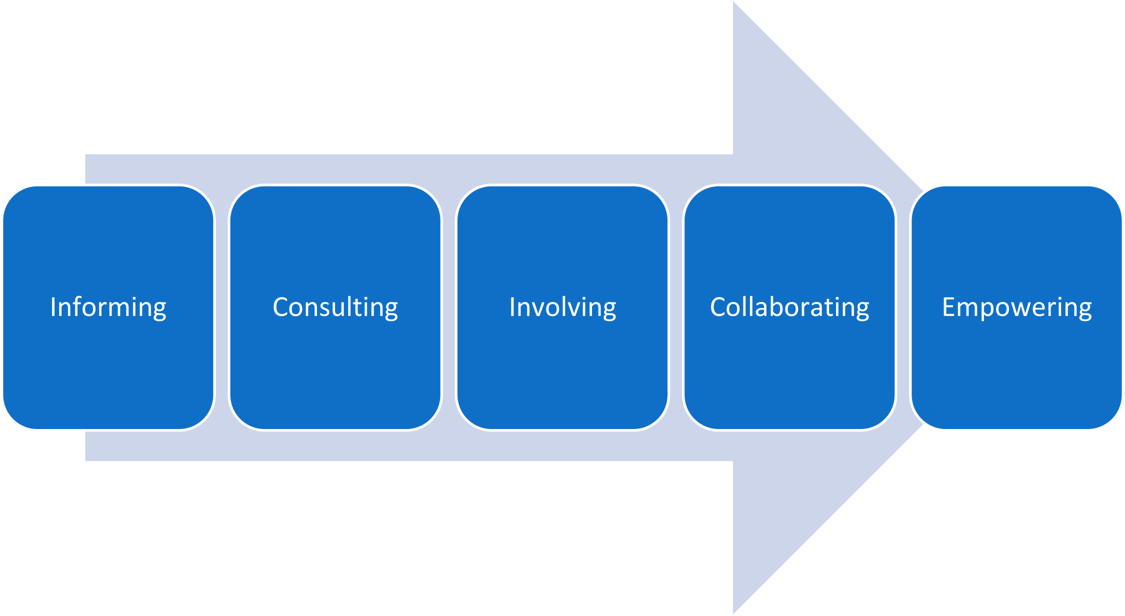


Figure 1: IAP2 Spectrum of Public Participation

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

	Informing	**Consulting**	**Involving**	**Collaborating**	**Empowering**
Public Participation objective	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
Promises made to the Public	Keep the public informed about the outcomes of EU-HYBNET ** Information shared on the website, on*	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 **Possibility for the public to share advices and*	Implement what the public decides within and through EU-HYBNET **Until then no decision have implemented*

	the social media channels and during the events organised	taken within EU-HYBNET * _Information shared on the website, on the social media channels and during the events organised_	*_Floor opened to registered people during events organised in the frame of EU-HYBNET_	_recommendations during events. Floor opened to discussions with the public_	

3. STAKEHOLDERS’ ENGAGEMENT

To maximise the engagement of the stakeholders, the key point here was to clearly define the categories of stakeholders, their needs and the priority group they belong. After this analysis, EU-HYBNET started building the EU-HYBNET network. The tables below show the members of the network as well as the organisations with which interaction has been and will be made. Of course these lists will be updated throughout the project.

3.1 INDENTIFICATION OF STAKEHOLDER CATEGORIES

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

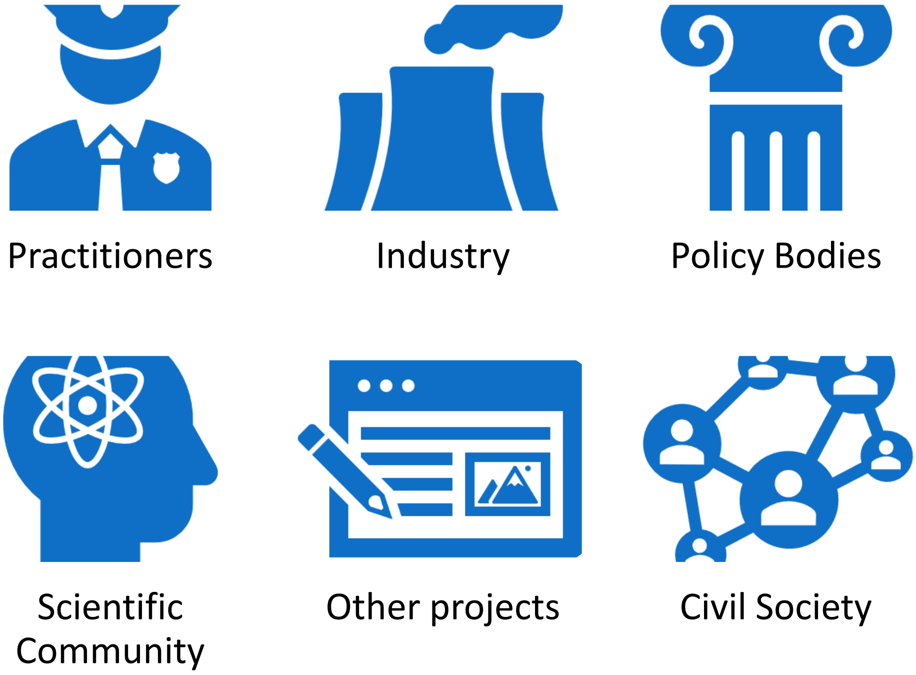


Figure 2 EU-HYBNET stakeholders' categories

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.

EU-HYBNET consortium has stuck to this wide approach of the concept of practitioners. The table below list 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.

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

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 second cycle of the project.

Table 3 Industry and SME within the EU-HYBNET network

Organisation	Country
European Organisation for Security (partner)	Belgium
SATWAYS (partner)	Greece
Systematic (Stakeholders Group)	France
Expertsystem	France
Ardanti	France
Soprasteria	France
Norsecon	Sweden
Enersec Technology	Romania
Smartlink Communications	Romania
Geostrategic Intelligence Group	Finland
Mira Technologies Group SRL	Romania
Sectyne AB	Sweden

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. EU-HYBNET Consortium identify and get in contact with the relevant people and invite the actors to the project events and workshops. The relevant files related to the hybrid threats subject under discussion were also identified and their development monitored by the Consortium. If necessary and when possible, they are discussed with policy makers.

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

Network	Target audience

EU Level	
DGs of the EC	DG Home (Directorate ISE: Industry, Synergies & enabler directorate/Directorate RTI: Research, technology & Innovation directorate/ Corporate services Directorates, Unit HOME.F Audit & Situational Awareness) DG Connect (Directorate A: Strategy and General Affairs/ Directorate Media Policy Directorate D: Security), DG MOVE, DG DEFIS, DG MARE, DG ECHO, DG Competition (Directorate C Market and cases II Information, Communication and Media, DG Grow, DG Trade, DG for Communication Networks, Content and Technology of the EC, DG Communication (Directorate C Representation & Communication in the Member States, DG EAC (Education, Youth, Sport and Culture – EAC. B Youth, Education and Erasmus+)
Agencies/Bodies of the EC	European Defence Agency, The European Border and Coast Guard Agency (EBCGA/ FRONTEX), European Union Agency for Cybersecurity (ENISA), The European Aviation Safety Agency (EASA), European Maritime Safety Agency (EMSA), The European Aviation Crisis Coordination Cell (ECCC) (created by the EC, Eurocontrol and the EASA), The Computer Emergency Response Team for the EU institutions (CER-TU), EU-LISA, EUROPOL and their innovation Lab
European Parliament	Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, AFET Committee, SEDE Sub-Committee, Committee on Culture and Education, Committee on the Internal Market and Consumer Protection
EEAS	Division Security and Defence Policy SECDEFPOL1 – Hybrid Threats, Hybrid Fusion Cell, EAST-STRATCOM Taskforce
The Council's Friends of Presidency Group on Countering Hybrid Threats (FoP)	Council of the European Union (General Secretariat)
European Committee of the Regions	Commission for Citizenship, Governance, Institutional and External Affairs, ECON: Commission for Economic Policy, Commission for Social Policy, Education, Employment, Research and Culture (SEDEC)
Council of Europe	Congress of Local and Regional Authority Secretary General
Internal Fact Checking Network	
Members of the High Level Group on Fake news and Online Disinformation	
European Data Protection Board	
The European Reference Network for Critical Infrastructure Protection (ERNCIP)	
Council of European Municipalities and Regions (CEMR)	
European Digital Media Observatory	
Independent Networks	Assembly of European Regions
European Economic and Social Committee	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 of the concept of hybrid threats. EU-HYBNET aims to impact the scientific community by expanding the existing knowledge of hybrid threats. Academics and researchers in hybrid threats are dedicated to thinking of unsolved problems, and 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 Tromsoe (partner)	Norway
RISE Research Institutes of Sweden Ab (partner)	Sweden
KEMEA (partner)	Greece
Lietuvos Kibenetiniu 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 Agademy (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

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 environment needs to be aligned with EU-HYBNET's approach, avoiding possible overlap and enhancing complementary synergies.

EU-HYBNET engages with a wide range of EU Initiatives and EC projects and, already identified during the preparation phase and throughout Cycle I of the project. In the following table there is an exemplification of the links already developed:

Table 6 Existing related initiatives

	EU-HYBNET partners involved	**Improvements and benefits that EU-HYBNET will deliver**
The landscape of Hybrid Threats: A Conceptual Model	Hybrid CoE, JRC	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. Reuse: For all EU-HYBNET activities, this report will provide the basis for understanding the phenomenon of hybrid threats.
Workshop on EU/NATO cooperation in civil protection	Hybrid CoE	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.
Scenario-based policy discussions	Hybrid CoE	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. Reuse: empowering the European network with new high level actors and audience interest.
Participation in NATO Science and Technology working groups related to Hybrid Threats	TNO, MoD NL	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.
Countering Hybrid Threats: Lessons Learned from Ukraine	MVNIA	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." 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.
Security in the Black Sea Region. Shared Challenges, Sustainable Future Program	MVNIA	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 and an informal platform of practitioners in the Black Sea Region.

Table 7 Existing related projects

Project instrument	**EU-HYBNET Partners**	**EU-HYBNET Outputs feed to following projects**	**Activity**	**Field of action**
H2020-GM	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
H2020 ICT	LAU, L3CE, RISE	ECHO, SPARTA, CONCORDIA	Research and Innovation hubs’ cyber network	Cyber security research and innovation, situational awareness tools, 5G security
H2020 INFRA	EOS, KEMEA, SATWAYS, LAU	SATIE, SAFECARE, PRECINCT, SAFETY4RAILS	Research and Innovation	Security, cyber security research and innovation
H2020-BES	KEMEA, SATWAYS, LAUREA, EOS	CIVILNEXT, AI ARC	Research and Innovation	Information systems, Maritime and border surveillance situational awareness
H2020 DRS	MVNIA, UCSC, SATWAYS, PLV, EOS	LINKS, RISKPACC	Research and Innovation	Man-made and natural disasters, CBRN, disaster response and preparedness risk management
H2020 FCT	KEMEA	SHUTTLE,	EU toolkit for trace analysis, economical& psychological aspects leading criminal activities	EU forensic laboratories, Citizens interaction, technologies, Social Media, economics and psychology

H2020 INT	MVNIA	ESEENTIAL	Ad-Hoc security research	Complex security environment
ISFP	L3CE, MVNIA, KEMEA, PPHS	SENTER, ARMOuR, SAFFRON	Network in Cybercrime critical communications	Cybercrime, resilience, detection of foreign fighters

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 the society.

A wide range of NGOs are listed below as members of the EU-HYBNET network:

Table 8: Non-governmental Organisations within the EU-HYBNET Network

Organisation	Country
Polish Platform for Homeland Security (partner)	Poland
Asociación Maldita (partners)	Spain
European Values Centre for Security Policy	Czech Republic
GLOBSEC	Slovakia
Vilnius Institute for Policy Analysis	Lithuania
Polish Association for National Security	Poland
Friends of Europe	Belgium
Euclid Institute	France
Demagog Association	Poland
The Kosciuszko Institute Association	Poland
Baltic Centre for Media Excellence	Latvia
Fondazione SAFE - Security and Freedom for Europe	Italy
Avoin yhteiskunta ry	Finland

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 are something more than a 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

EU-HYBNET DCE defines priority groups for its dissemination and communication activities.

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 and the EU-HYBNET practitioners are categorised as follows:

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

The second group is formed by European projects relevant to EU-HYBNET. The main focus is on the Commission Network of Practitioners (NoP) funded projects (funding Horizon2020-Secure Socities-General Matters -call). The NoP projects can be divided to two different categories. Naturally both project types are important to the EU-HYBNET project cooperation. The projects that have geographical focus for disaster resilience and security are: ARCSAR, MEDEA, DAREnet. The projects with a thematic focus area: FIRE-IN, ILEAnet, NO-FEAR, PEN-CP, E-notice, Exeter, ENCIRCLE, INCLUDING. In addition, the EU-HYBNET is focusing on cooperation with other relevant European projects and their funding instrument may vary E.G. EDA, DGs. Furthermore, the national projects focusing on hybrid threats are included to the second group.

The third group consists of organisations and actors engaged in related research areas of EU-HYBNET. The organizations in focus are EU Agencies and Offices E.G. eu-LISA, ENISA, EDA. 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. It is Crucial to mention that they might not be aware of the existence of EU-HYBNET or might not realize its importance:

- Public bodies / policy bodies including, EU DGs (such as DG HOME, DG MOVE, DG CONNECT, DG DEFIS, DG MARE, DG ECHO), Agencies of the EU (such as EDA, ENISA, EBCGA, EMSA, EASA), Organs of the EU (the European Parliament, EEAS with the EU-HYBRID Fusion cell), The Council’s Friend of Presidency on Countering Hybrid Threats

- Scientific community in order to supper the establishment of regulation mechanisms
- Private sector: industry, including SMEs. The consortium with its network with the European security industry is in the position of promoting EU-HYBNET and raises awareness to those stakeholders.

The consortium flagged any relevant opportunity with the following stakeholders for communicating EU-HYBNET outputs:

- Key actors of the projects dealing with closed topics to ensure visibility and uptake of results, providing opportunities to receive feedback, discuss similar issues that may occur
- Internal network/ audience of the 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

Messages to be shared with the stakeholders are key in terms of engagement. To create a proper and long standing relationship with the stakeholders, the 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 9 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
WP1 Coordination and Project Management							
Objectives related to the Project Management							
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
WP2 Gaps and Needs of European actors against Hybrid Threats							
Objectives related to the Gaps and Needs of European actors against Hybrid Threats							
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
WP3 Surveys to Technology, Research and Innovations							
Objectives related to the Surveys to Technology, Research and Innovations							
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 attends 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
WP4 Recommendations for Innovations Uptake and Standardization							

Objectives of the recommendations for Innovations Uptake and Standardization							
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 on the market	To be aware of the recommendations as input for potential follow up action when needed	To be aware of the recommendations	To be aware of the recommendations	To be aware of the recommendations	To be aware of the recommendations
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
WP5 Dissemination, Communication and Exploitation							
Objectives of the Communication, Dissemination and Exploitation Activities							
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	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

			improve actual policy				
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
WP6 Ethics							
No objectives to share with the stakeholders							

5.DISSEMINATION, COMMUNICATION AND EXPLOITATION MEANS TOWARDS ENGAGEMENT

5.1 MAIN DISSEMINATION MEDIUMS

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 MEDIUMS

EU-HYBNET WEBSITE

Since M3, EU-HYBNET has its own dedicated website (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 since more than 7,000 visits were recorded. During the project's main events (such as IKEW, FTW or Annual Workshop), 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 can be achieved with frequent publication of articles, podcasts and other interactive methods engaging the project's partners and network.

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 three 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.

- EU-HYBNET Network

This section is divided into 4 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. The first policy brief 'Framing the information domain vulnerabilities' was posted in June 2021 in the dedicated sub-section.

- 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 visited when participants have to register for the event.

- News

This section is used when additional documents are uploaded on the website. After every event, a dedicated page provides an update on the event and a press release is attached. In the same way, the project's newsletters are also published in this section.

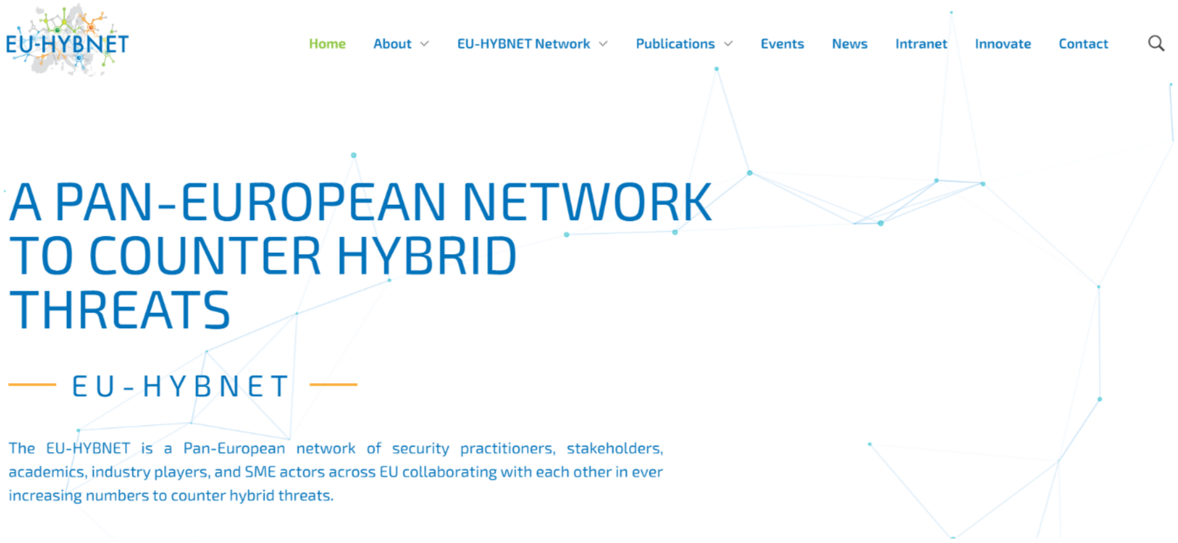
- Intranet

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



A PAN-EUROPEAN NETWORK TO COUNTER HYBRID THREATS

— EU-HYBNET —

The EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academics, industry players, and SME actors across EU collaborating with each other in ever increasing numbers to counter hybrid threats.

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 UAS since M5 and will continue running until M60. The Innovation Arena focuses on solving 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:

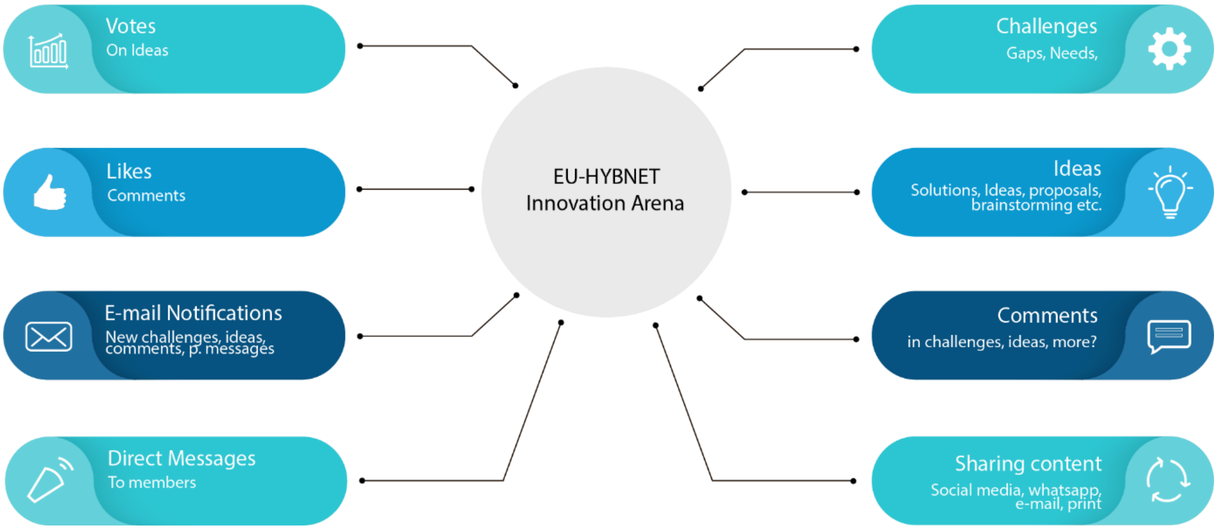

Votes
On Ideas
Challenges
Gaps, Needs,
Likes
Comments
EU-HYBNET
Innovation Arena
Ideas
Solutions, Ideas, proposals, brainstorming etc.
E-mail Notifications
New challenges, ideas, comments, p. messages
Comments
in challenges, ideas, more?
Direct Messages
To members
Sharing content
Social media, whatsapp, e-mail, print

Figure 4: Innovation Arena use cases

The two main contents of the Innovation Arena are Challenges and Ideas. These content types works 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.

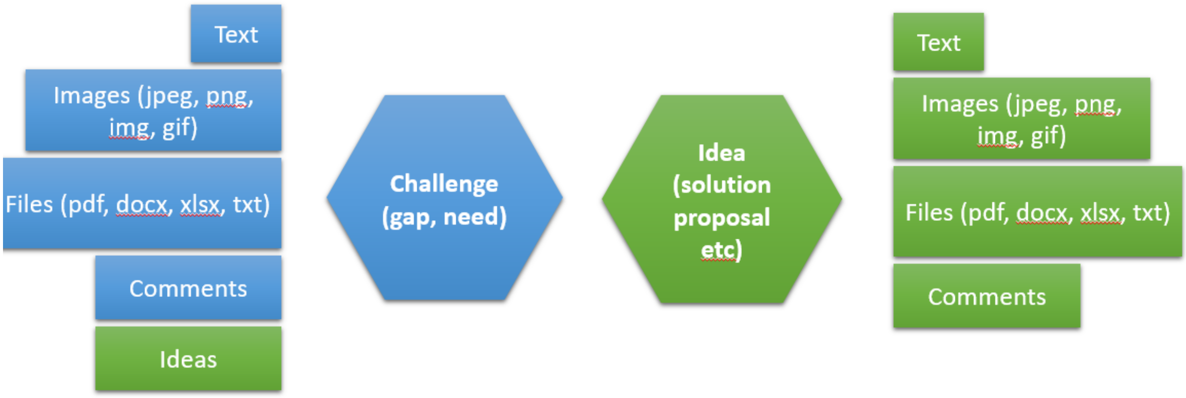

Text
Images (jpeg, png, img, gif)
Files (pdf, docx, xlsx, txt)
Comments
Ideas
Challenge (gap, need)
Idea (solution proposal etc)
Text
Images (jpeg, png, img, gif)
Files (pdf, docx, xlsx, txt)
Comments

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.

TUOVI

In order to support the EU-HYBNET Dissemination, Communication and Exploitation strategy, Laurea UAS 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.

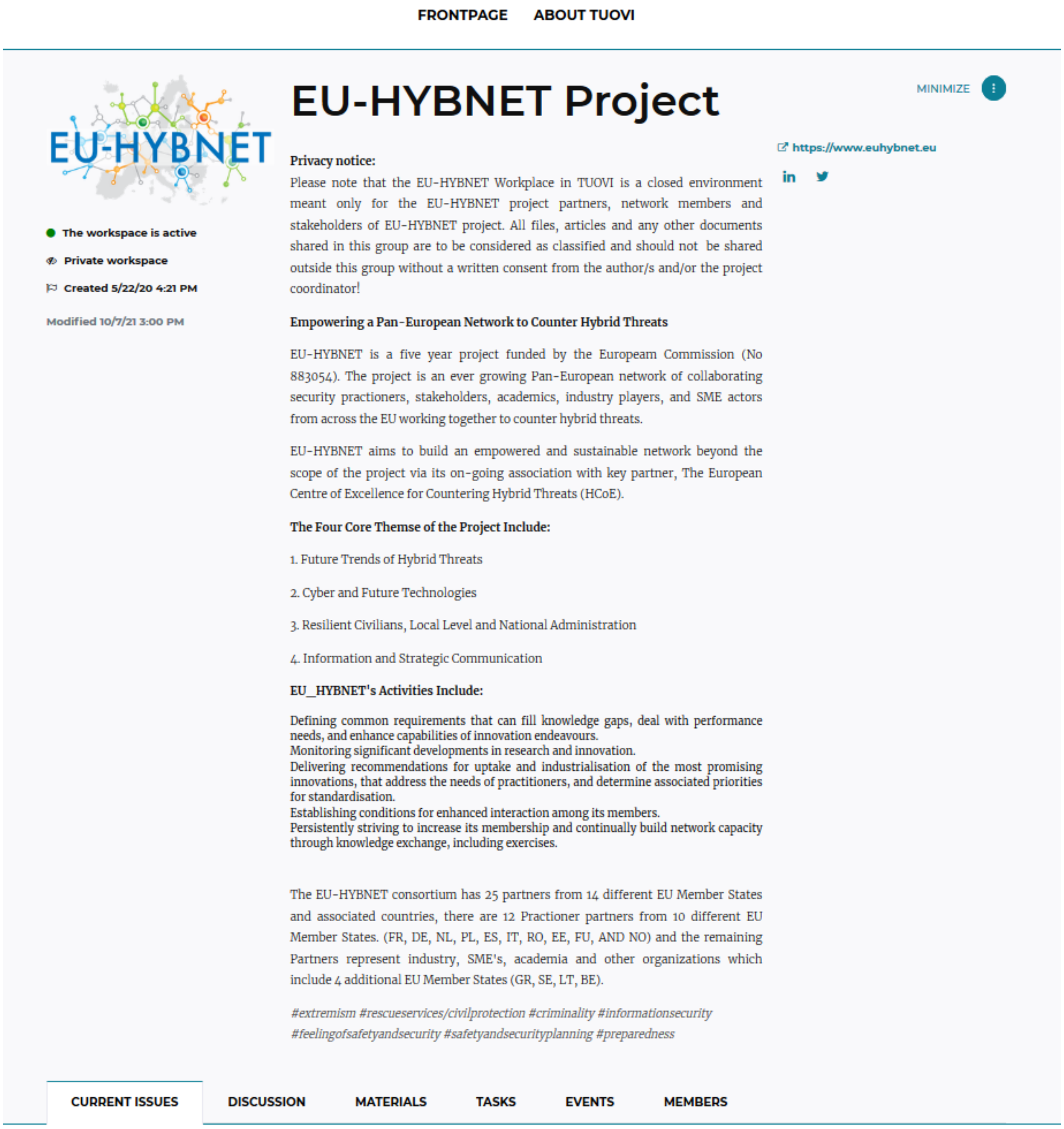
Unlike the EU-HYBNET web page, the TUOVI is available only for consortium partners, stakeholders and network members and provides the platform for restricted material sharing, secure communication, networking, and collaborating between the EU-Hybnet network members (Consortium partners, Stakeholder Group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

Throughout the life of the project (M1-60) Laurea UAS will manage all daily aspects of the TUOVI portal/ EU-HYBNET working space 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 UAS 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:



● The workspace is active

Private workspace

Created 5/22/20 4:21 PM

Modified 10/7/21 3:00 PM

EU-HYBNET Project

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 Europeam Commission (No 883054). The project is an ever growing Pan-European network of collaborating security practioners, 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, FU, 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

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 Communication, Dissemination 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 OFF-LINE DISSEMINATION MEDIUMS

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).

PROJECT PUBLICATIONS

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

STRATEGY ON MASS MEDIA

Such a strategy are put in place to support the partners in the organization of the three main types of events: the Innovation, Knowledge Exchange event and Future Trends Workshops and Annual Workshops. The mass media campaign needs to be linked to the social media strategy that it is describe below in the document.

5.1.3 DISSEMINATION THROUGH EVENTS

INNOVATION AND KNOWLEDGE EXCHANGE EVENTS

Three Innovation and Knowledge Exchange workshops are being 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 PLB (at M43)

These workshops are 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 19th 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. (Annex XI)

FUTURE TRENDS WORKSHOPS

The objectives of the 5 Future Trend workshop 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 Workshop 1 was hosted online by Hybrid CoE on the 31st of March 2021 (M11) (Annex XII for the agenda).

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.
68 participants from 44 organisations took part in the 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.

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 (see Annex XIII for the agenda) on the 19th 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.

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)

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.

The trainings and exercises will be delivered at M12, M29 and M46.

For these events, the plan is the following:

- Action 1: defining a yearly workshop/event plan (to be started at M4)
- Action 2: preparing, organizing, post-analysing and reporting on the workshops/events according the yearly plans
- Action 3: ensuring a proper interaction between the events/workshops and the Tasks and WPs, the idea being the results from EU-HYBNET.
- Action 4: making sure to organize at least one out-of-the-box event.

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.

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 3 CERIS events and will participate to a fourth one on the 29th of November[2].

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 infa& 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)

5.2 COMMUNICATION MEANING

'Communication is a way to keep all partners actively involved in the project'[4] 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 is 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

[2] At the time the writer work on the document, the fourth CERIS event still did not happen.

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.

5.2.2 EU-HYBNET WEBSITE

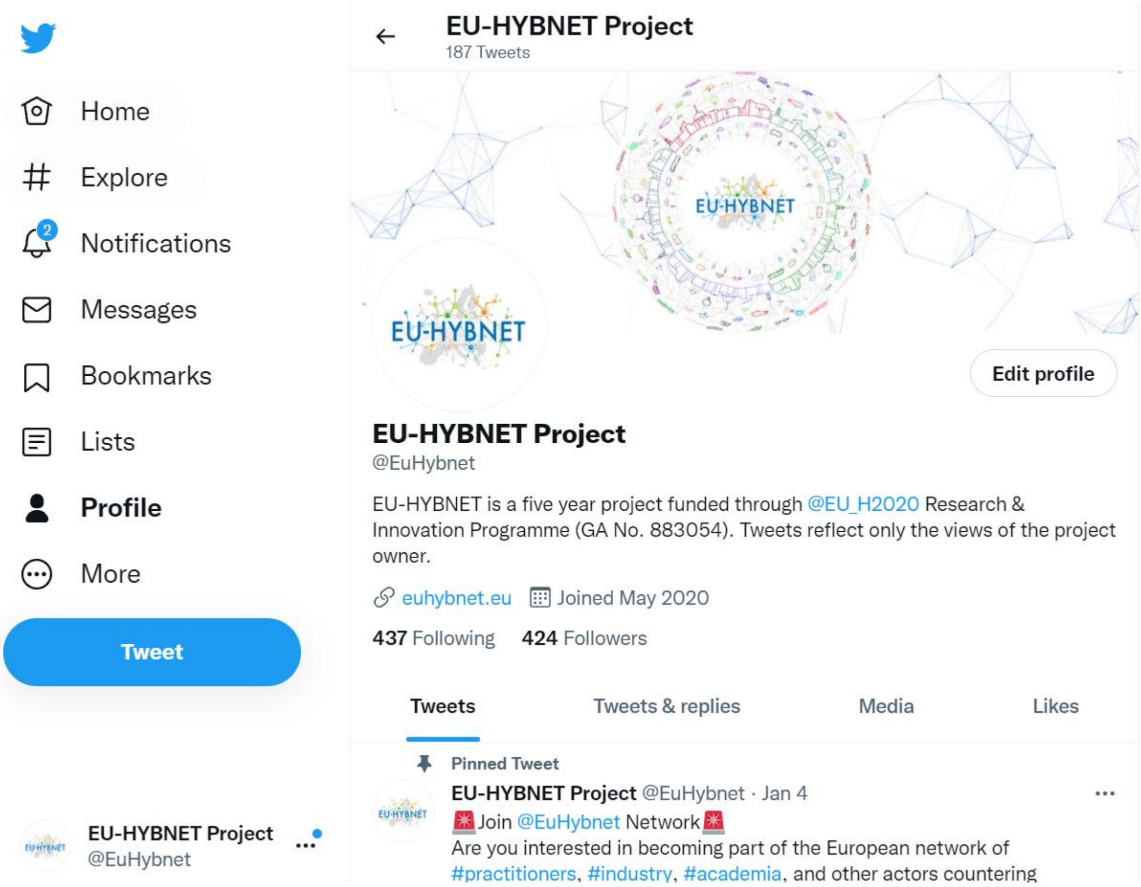
As explained above, the website is accessible since M3.

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.



EU-HYBNET Project
@EuHybnet

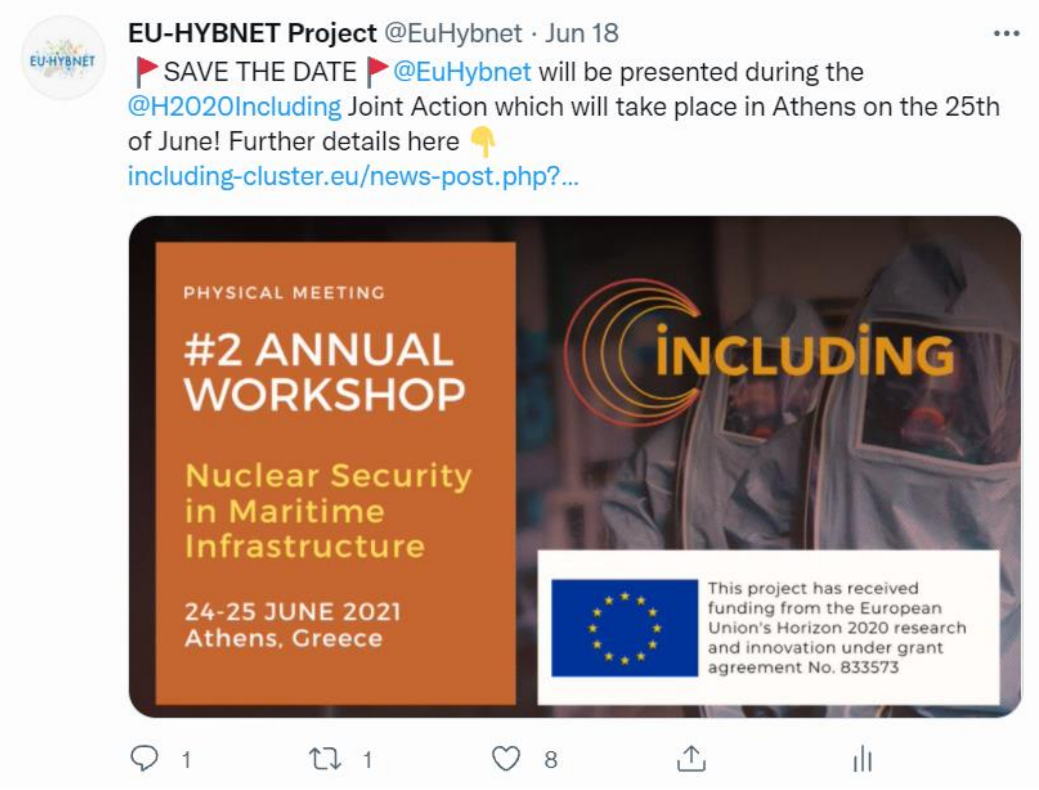
EU-HYBNET is a five year project funded through @EU_H2020 Research & Innovation Programme (GA No. 883054). Tweets reflect only the views of the project owner.

euhybnet.eu Joined May 2020

437 Following 424 Followers

EU-HYBNET Project @EuHybnet · Jan 4
🚨Join @EuHybnet Network🚨
Are you interested in becoming part of the European network of #practitioners, #industry, #academia, and other actors countering

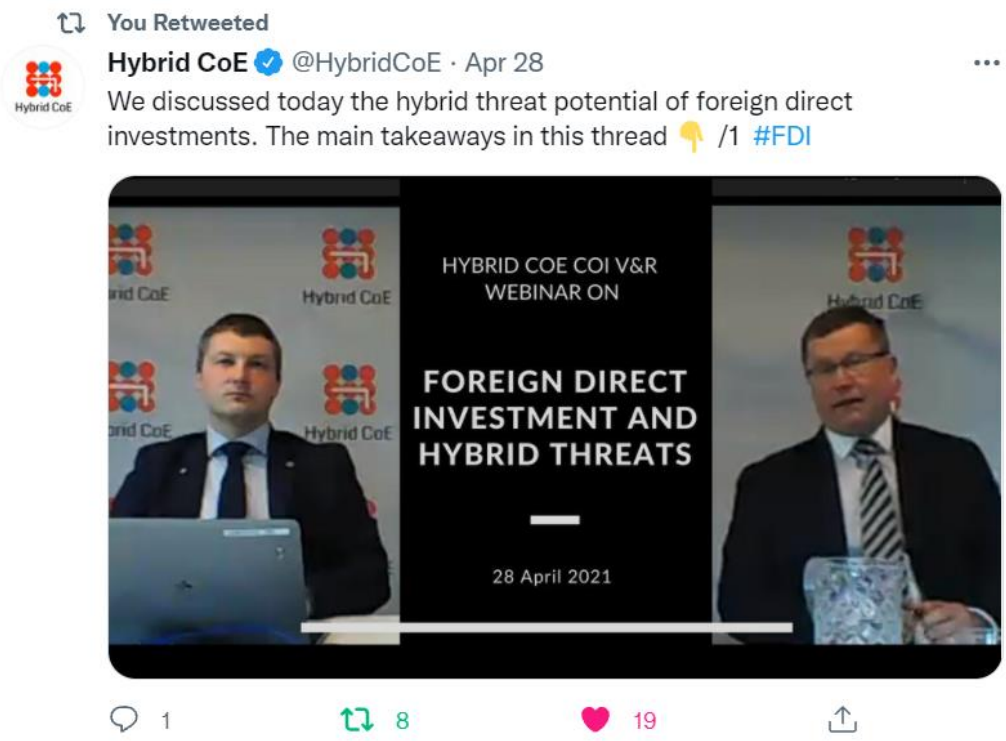
Figure 7: EU-HYBNET Twitter account homepage


EU-HYBNET
PHYSICAL MEETING
#2 ANNUAL WORKSHOP
Nuclear Security in Maritime Infrastructure
24-25 JUNE 2021
Athens, Greece
INCLUDING
This project has received funding from the European Union's Horizon 2020 research and innovation under grant agreement No. 833573
1
1
8

EU-HYBNET Project @EuHybnet · Jun 18

🚩SAVE THE DATE 🚩@EuHybnet will be presented during the @H2020Including Joint Action which will take place in Athens on the 25th of June! Further details here 👇
including-cluster.eu/news-post.php?...

Figure 8: Tweet to inform about an INCLUDING workshop



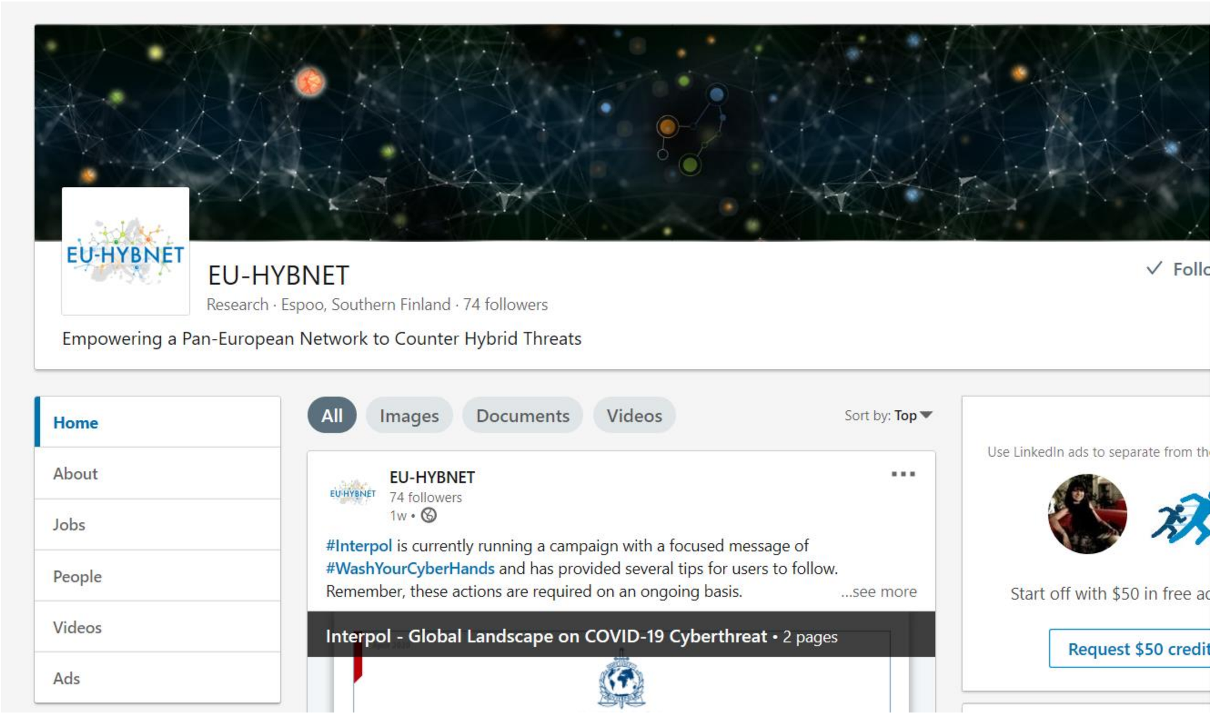
You Retweeted

Hybrid CoE @HybridCoE · Apr 28

We discussed today the hybrid threat potential of foreign direct investments. The main takeaways in this thread 👇 /1 #FDI

Figure 9: Retweet of Hybrid CoE

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



EU-HYBNET

Research · Espoo, Southern Finland · 74 followers

Empowering a Pan-European Network to Counter Hybrid Threats

EU-HYBNET
74 followers
1w •

#Interpol is currently running a campaign with a focused message of #WashYourCyberHands and has provided several tips for users to follow. Remember, these actions are required on an ongoing basis. ...see more

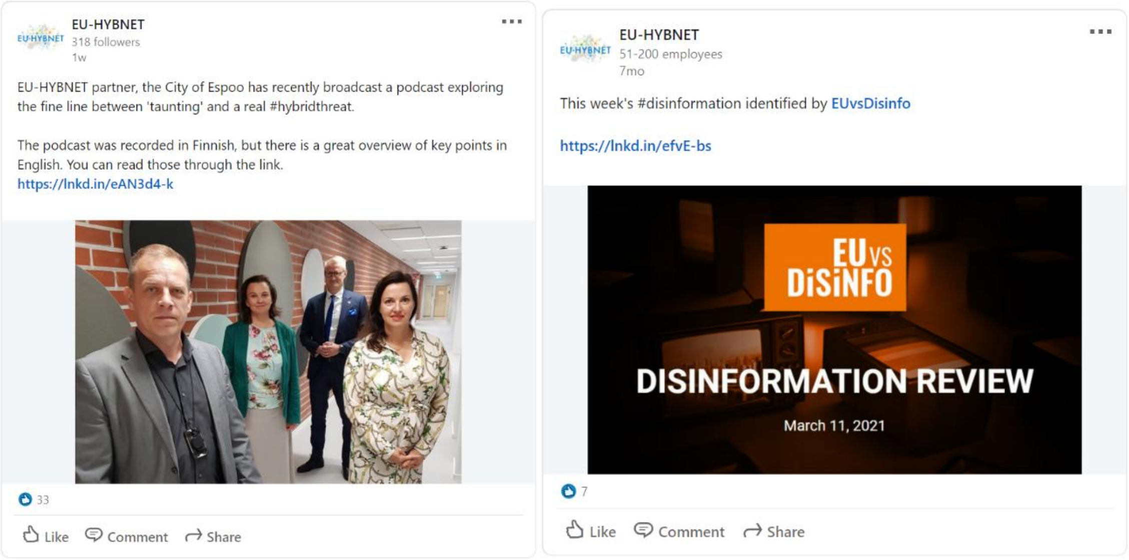
Interpol - Global Landscape on COVID-19 Cyberthreat • 2 pages

Use LinkedIn ads to separate from th

Start off with $50 in free ac

Figure 10: 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.



EU-HYBNET
318 followers
1w

EU-HYBNET partner, the City of Espoo has recently broadcast a podcast exploring the fine line between 'taunting' and a real #hybridthreat.

The podcast was recorded in Finnish, but there is a great overview of key points in English. You can read those through the link.
https://lnkd.in/eAN3d4-k

33

Like Comment Share

EU-HYBNET
51-200 employees
7mo

This week's #disinformation identified by EUvsDisinfo

https://lnkd.in/efvE-bs

7

Like Comment Share

Figure 11: 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.

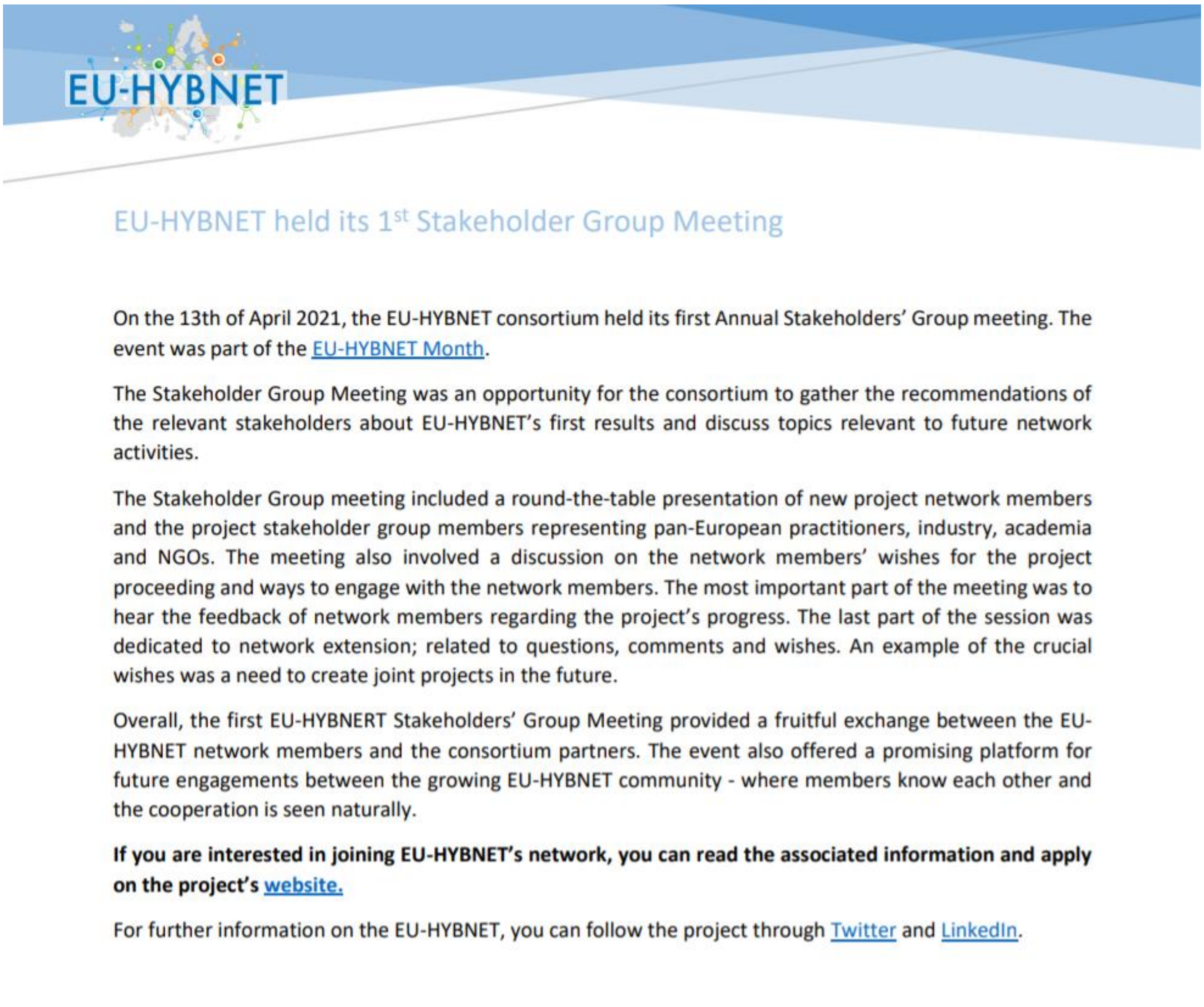
The First three project's newsletters were sent to almost 200 recipients, with a good opening rate. Each Newsletter provides the reader with results achieved by each Work Package. Recipients are aware of the past and upcoming events and an highlight of future objectives is given.

Figure 12: EU-HYBNET Newsletter April 2021

For the upcoming months, the DCE Team will seek to enrich furthermore the list of recipients so that the newsletter will have an even stronger impact.

5.2.5 PRESS RELEASE

Press releases are tools that will be shared to communicate about the project activities. The first press release was prepared by Hybrid CoE the day of the Kick-off-Meeting and was shared among the network of the consortium partners. Plus Laurea has produced two additional press releases at M7 and M12. The consortium will continue producing them on a necessary basis.



EU-HYBNET held its 1st Stakeholder Group Meeting

On the 13th of April 2021, the EU-HYBNET consortium held its first Annual Stakeholders' Group meeting. The event was part of the EU-HYBNET Month.

The Stakeholder Group Meeting was an opportunity for the consortium to gather the recommendations of the relevant stakeholders about EU-HYBNET's first results and discuss topics relevant to future network activities.

The Stakeholder Group meeting included a round-the-table presentation of new project network members and the project stakeholder group members representing pan-European practitioners, industry, academia and NGOs. The meeting also involved a discussion on the network members' wishes for the project proceeding and ways to engage with the network members. The most important part of the meeting was to hear the feedback of network members regarding the project's progress. The last part of the session was dedicated to network extension; related to questions, comments and wishes. An example of the crucial wishes was a need to create joint projects in the future.

Overall, the first EU-HYBNERT Stakeholders' Group Meeting provided a fruitful exchange between the EU-HYBNET network members and the consortium partners. The event also offered a promising platform for future engagements between the growing EU-HYBNET community - where members know each other and the cooperation is seen naturally.

If you are interested in joining EU-HYBNET's network, you can read the associated information and apply on the project's website.

For further information on the EU-HYBNET, you can follow the project through Twitter and LinkedIn.

Figure 13: Press release of the 1rst Stakeholder Group Meeting

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.

Before any communication, EU-HYBNET partners need to get in touch with EOS (as coordinator of the WP5), PPHS and LAUREA (as main contributors of WP5).

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:

Table 10 Partners Exploitation Strategies

LAU	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
PPHS	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.
UiT	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.
RISE	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
KEMEA	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 (20202027). As well, KEMEA will promote the EU-HYBNET project in European related events and workshops in which regularly takes part.
L3CE	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.
URJC	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.
MTES	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.
EOS	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.
TNO	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.
SATWAYS	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.
ESPOO	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 threads 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 threads in the local community.
UCSC	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.
JRC	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.
MVNIA	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
HCoE	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
MOD	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.
ICDS	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.
PLV	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.
ABW	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).
DSB	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
RIA	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.
MALDITA	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.

ZITiS	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.
COMTESSA	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 messages expressed in the 4th part 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:

- EU-HYBNET Twitter and LinkedIn Account (M1)
- TUOVI platform (M2)
- Promotional materials (M3)
- EU-HYBNET Website (M3)
- Events/workshop Plan (M5 and then every year)
- EU-HYBNET Newsletter (at M6 and then every six months)
- Additional press release written by partner organisations
- Attendance to EC events such as CERIS or other additional events with other EC funded projects
- 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 run until M56

Who: all the stakeholders developed 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 of the Innovation Arena and the day to day communication activities (moderation of the social media channels, feeding of the website, creation of publication).

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

Involvement:

The 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 the final 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 during the first 17 months. The initial KPIs are still available in D5.1 and D5.2.

Table 11 EU-HYBNET KPIs (update)

Key Performance Indicators			Target at M13			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 M32	140-300 per month 1400-3000 at M13	More than 300 per month More than 3000 at M32	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 M32	300-500 per month 4000-5000 at M32	More than 500 per month More than 5000 at M32	
	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 Statistics dashboard	Less than 200 at M32	200-400 at M32	More than 400 at M13	Responsible: PPHS Accountable: Laurea, EOS Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of posts on LinkedIn		Less than 150 at M32	150-250 at M32	More than 200 at M32	

	Number of Twitter followers	Twitter analytics	Less than 400 at M32	400-450 at M32	More than 450 at M32	Responsible: EOS Accountable: PPHS, Laurea Consulted:ESPOO, TNO, PLV, HCoE Informed: All other Partners
	Number of tweets per month		Less than 10	10-15	More than 15	
	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	Less than 1	1	More than 1	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, HCoE Informed: All other Partners
Brochures	Number of brochures distributed (conditional to the improvement of the sanitary situation)		200 brochures at M32	300 brochures at M32	400 brochures at M32	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	0-1 per month (starting at M3)	1-2 per month (starting at M3)	More than 2 per month (starting at M3)	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 M32	5-12 at M32	More than 12 at M32	
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	
	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 10	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 25	
	Number of cooperation activities (common events and other clustering activities)	Proceedings	Less than 1	2-5	More than 5	

Link to the Community of Users	Number of EU-HYBNET presentations made during plenary meetings and thematic workshops	Proceedings	1 every three events	1 every two events + organisation of 1 external cooperation workshop	1 per event + organisation of more than 1 external cooperation workshop	Responsible: Laurea Accountable: EOS, PPHS Consulted: ESPOO, TNO, HCoE, PLV Informed: All other partners
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 70	70-85	More than 85	Responsible: Laurea Accountable: EOS, PPHS, HCoE Consulted: ESPOO, TNO, PLV Informed: All other Partners

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 every partners are being appointed (or are about to be), the online presence of EU-HYBNET (e.g. the webpage, social media accounts etc.) are all 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 as crucial within EU-HYBNET, and moreover taken into consideration within the D5.1. The Work Package 6 (Ethical Requirements) together with Work Package 1 (Management) treat in more details these kind of issues.

However, two issues must be highlighted here. The first is related more with the project dissemination, and the second more with 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)

ANNEX I: GLOSSARY AND ACRONYMS

Table 12 Glossary and Acronyms

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

SATWAYS	SATWAYS
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
UCSC (UNICAT)	Universita Cattolica del Sacro Cuore
JRC	JRC - Joint Research Centre - European Commission
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
HCoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NLD MoD	Ministry of Defence/NL
ICDS	International Centre for Defence and Security, Estonia
PLV	Ayuntamiento de Valencia / Valencia Local Police
ABW	Polish Internal Security Agency
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
UniBW	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 20th of May 2010

[3] The definition of "practitioner" was rretrieved 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

ANNEX III : EU-HYBNET LOGO

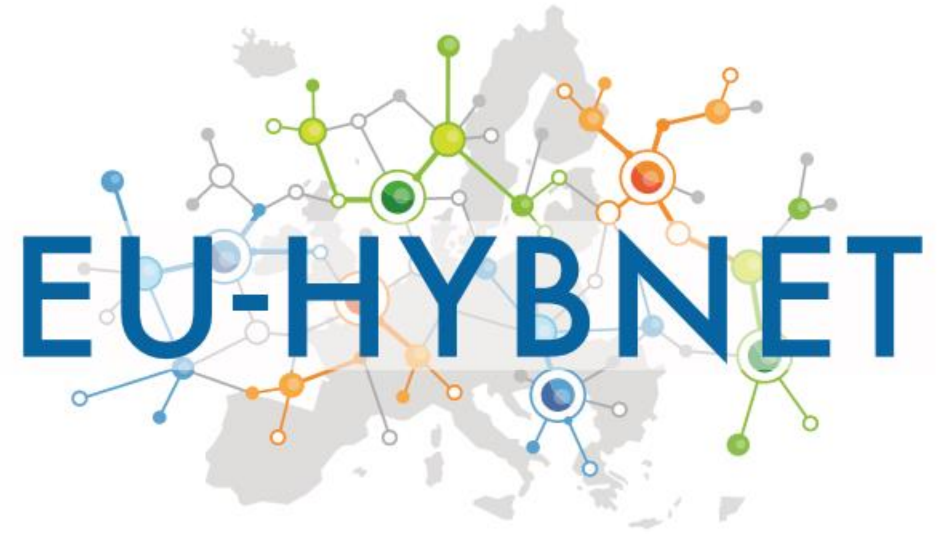
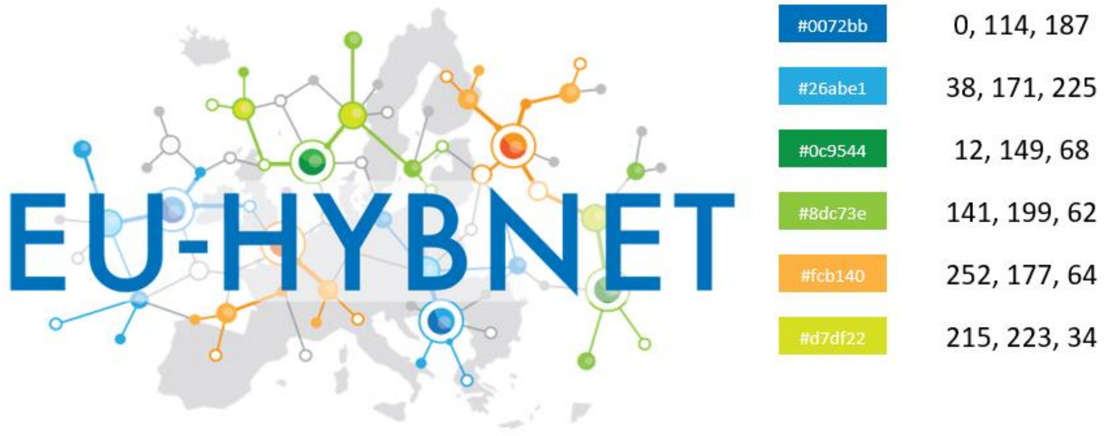


Figure 14: EU-HYBNET logo

ANNEX IV : EU-HYBNET COLOR CODES



#0072bb	0, 114, 187
#26abe1	38, 171, 225
#0c9544	12, 149, 68
#8dc73e	141, 199, 62
#fcb140	252, 177, 64
#d7df22	215, 223, 34

Figure 15: EU-HYBNET Color code

ANNEX V: LIST OF EXTERNAL RELEVANT EVENTS FOR EU-HYBNET

Table 13 List of external events relevant for EU-HYBNET

Name of the Event	Description of the Event	Date of the Event	Location of the Event (Town and Country)
ENISA Telecom Security Forum	focuses on emerging issues related to telecom security across Europe and aims to bring together telecom security experts from national authorities, national and European bodies and the telecom industry to : 1) Share good practices and experience on coping with the latest security threats 2) Discuss the latest developments on EU Telecom Security Framework and other legislative initiatives in a European but also national levels and exchange views on identified implementation and issues; 3) Get in touch with emerging technologies and relevant initiatives.	13th October 2021	Athens, Greece
Berlin Security Conference	The Berlin Security Conference is one of the largest European security and defence policy events. The Berlin Security Conference is a forum aimed at promoting the Common Security and Defence Policy. It focuses on issues concerning the European Parliament, the Commission and the Council as well as national parliaments and ministries. The emphasis is on proposing and discussing concrete solutions aimed at improving European and transatlantic political, operational and tactical cooperation. The goal is to develop ways to mitigate the frictions caused by insufficient capabilities, inadequate standardisation, the lack of interoperability, differences in the levels of support and national restrictions.	24-25 November 2021	Berlin, Germany
10th Cyber Investor Days	The most promising European cybersecurity start-ups and SMEs will have a chance to pitch their innovative cybersecurity solutions and hold B2B meetings with the leading investors and corporates from Europe and beyond.	1-2 December 2021	Helsinki, Finland

Munich Security Conference	The Munich Security Conference is the world's leading forum for debating international security policy. It is a venue for diplomatic initiatives to address the world's most pressing security concerns. The MSC's objective is to build trust and to contribute to the peaceful resolution of conflicts by sustaining a continuous, curated and informal dialogue within the international security community. Today, the MSC is the world's leading forum for debating international security policy.	Annual Conference usually taking place in February-March (TBD)	Munich, Germany
EC CERIS INFRA	EC Community of European Research and Innovation Security event focusing on Critical Infrastructure protection, inc. Hybrid threats	End of November 2021 (exact day TBC soon)	Telco or Brussels, Belgium
The 1st Nord Workshop on Hybrid Threats and Regional Response	The Workshop will focus on hybrid threats and regional response in Norway, best practices& way forward in comprehensive response to hybrid threats in society. In addition new project proposal will be under discussion to Horizon Europe program and Norwegian Research Council.	13-14/10	Oslo, Norway
DG HOME - Synergies between the use of EU funding for security Research and Innovation, and the complementary HOME Affairs Funds	The Workshop will collect feedback from EC funded projects, incl. EU-HYBNET, on future research topics to EC HOME Affairs Funds. EU-HYBNET will present what it sees as most new research topics in order to empower European response to hybrid threats	14/10	telco
FAKENEWS project launch	The FAKENEWS project was recently funded with 1,2 mil euro, examining civilian vulnerabilities and resilience during the 2020-2021 (and ongoing) COVID 19 pandemic and the 2015 migration crisis. FAKENEWS will be launched in november 2021 with a two day conference including project partners. Open to other interested parties (at own expense)	November 2021	Tromsø, Norway
TERRIFIC Final Public workshop	TERRIFIC (EC project "Accelerated CBRN Response") Final Public Workshop where to present the most promising innovation to CBRNE response. TERRIFIC is NoP project like EU-HYBNET and hence cooperation is very welcome. Goal is to learn about possible innovations beneficial for EU-HYBNET as well.	13/10/2021	Hybrid format: Telco and in-person meeting in Aix in Provence

ANNEX VI: EU-HYBNET PARTNERS SOCIAL MEDIA ACCOUNT

Table 14 EU-HYBNET Partners' Social Media Account

Partners	LinkedIn		Twitter	
	Account	Subscribers	Account	Followers
LAUREA	LAUREA	18,261	@Laureauas	3,369
PPHS	Polska Platforma	279	@PolishPlatform	271
UIT	UIT The Artic Universtiy of Norway	28442	@UiTromso	11,3 K
RISE	RISE	45464	@RISEsweden	5,384
KEMEA	N/A	N/A	N/A	N/A
L3CE	L3CE	3	@L3CE1	1
URJC	Universidad Juan Carlos	143,623	@URJC	53,8K
MTES	Ministère de la Transition écologique et solidaire	108569	@Ecologie_Gouv	180000
EOS	EOS LinkedIn	1369	@EOS_EU	1019
TNO	TNO	84828	@TNO-nieuws	3258
SATWAYS	SATWAYS	352	@SatwaysLtd	225
ESPOO	City of Espoo	17006	@locateinespoo	339
USCS	Universita Cattolica Del Sacro Cuore	210 167	@unicatt	19262
JRC	JRC	528123	@EU_ScienceHub	42.8k
MVNIA	NA	N/A	N/A	N/A
HCoE	N/A	N/A	@HybridCoE	5557
ICDS	ICDS-Tallinn	767	@ICS_Tallinn	3975
PLV	N/A	N/A	@policialocalvlc	38.2k
ABW	N/A	N/A	N/A	N/A
DSB	DSB	8671	@dsb.no	21.3 K
RIA	RIA	713	N/A	N/A
MALDITA	MALDITA	989	@maldita_es @malditobulo	102K 277K
ZITTIS	N/A	N/A	N/A	N/A
COMTESSA	COMTESSA	10333	@unibw	75

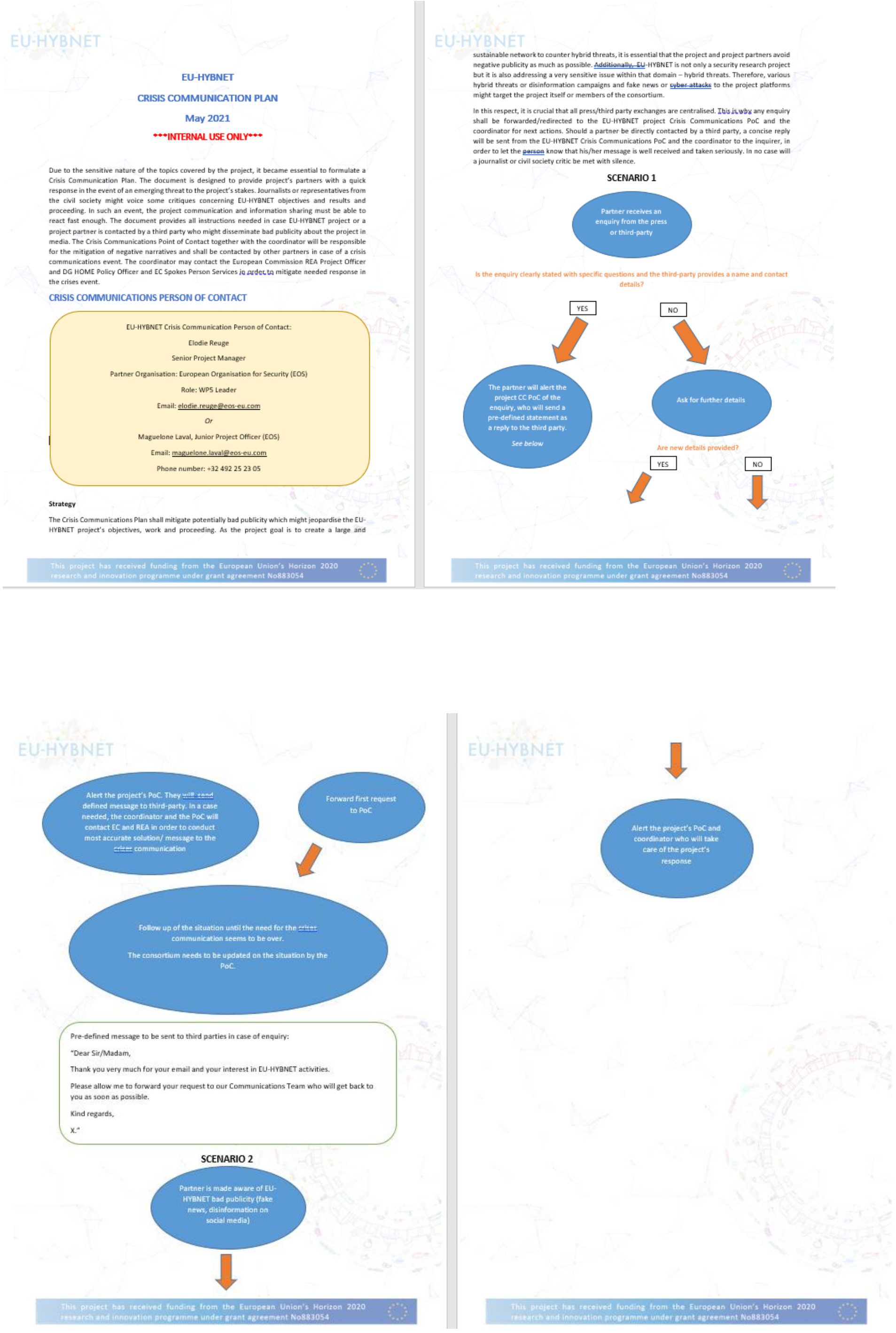
ANNEX VII: DISSEMINATION AND COMMUNICATION POINTS OF CONTACT

Table 15 D&C PoC

Partners	Names	Email
LAUREA	Paivi Mattila	Paivi.mattila@laurea.fi
	Artmir Galica	Artmir.galica@laurea.fi
PPHS	Rashel Talukder	rashel.tamlukder@ppbw.pl
	Bartek Ostrowski	Bartek.ostrowski@ppbw.pl
	Steven Ormston	Steven.ormston@ppbw.pl
	Magda Okuniewska	Magda.okuniewska@ppbw.pl
UIT	Guihild Hoogensen Gjorv	Gunhild.hoogensen.giorv@uit.no
RISE	Rolf Blom	Rolf.blom@ri.se
KEMEA	Maria Kampa	M.kampa@kemea-research.gr
	Panagiota Benekou	p.benekou@kemea-research.gr
L3CE	Egidija Versinskiené	egidija@l3ce.eu
	Ruta Ziberkinene	rutzib@mruni.eu
	Evaldas Bruze	evaldas@l3ce.eu
URJC	Ruben Arcos	Ruben.arcos@urjc.eu
MTES	Antoine-Tristan Mocilnikar	antoine-tristan.mocilnikar@developpement-durable.gouv.fr
	Christian Desprès	christian.despres@developpement-durable.gouv.fr
	Géraldine Ducos	geraldine.ducos@developpement-durable.gouv.fr
EOS	Maguelone Laval	Maguelone.laval@eos-eu.com
	Elodie Reuge	Elodie.reuge@eos-eu.com
TNO	Carolina van Weerd	Carolina.vanweerd@tno.nl
	Rick Meesen	rick.meessen@tno.nl
SATWAYS	Georgia Moutsou	g.Moutsou@satways.net
	Souzana Sofou	S.sofou@satways.net
ESPOO	Patri Hakkinen	petri.hakkinen@espoo.fi
USCS	Daniele Gui	Daniele.Gui@unicatt.it
	Rachele Brancaleoni	Rachele.brancaleoni@unicatt.it
JRC	Nina Kajander	Nina.KAJANDER@ec.europea.eu
MVNIA	Ileana Surdu	Ileana.surdu@animv.ro
HCoE	Päivi Tampere	paivi.tampere@hybridcoe.fi
	Emma Lappalainen	emma.lappalainen@hybridcoe.fi
	Maxime Lebrun	Maxime.lebrun@hybridcoe.fi
ICDS	Ivo Juurvee	Ivo.juurvee@icds.ee

	Ramon Loik	Ramon.loik@icds.ee
	Dmitri Teperik	Dmitri.tepereik@icds.ee
PLV	Susana Sola	Ssola@valencia.es
	PLV Corporate email	proyectosplv@valencia.es
ABW	Beata Gostomczyk	b.gostomczyck.cpt@abw.gov.pl
DSB	Orjan Karlsson	Orjan.Karlsson@dsb.no
RIA	Märt Hiietamm	mart.hiietamm@ria.ee
	Ege Tamm	Ege.tamm@ria.ee
MALDITA	Stéphane M. Grueso	steph@maldita.es
	Pablo Hernandez	phernandez@maldita.es
ZITTIS	Jessica Steinberger	Jessica.Steinberger@zitis.bund.de Eu-hybnet@zitis.bund.de
COMTESSA	Stefan Pickl	stefan.pickl@unibw.de
	Son Pham	son.pham@unibw.de

ANNEX VIII: CRISIS COMMUNICATION PLAN



EU-HYBNET

EU-HYBNET

CRISIS COMMUNICATION PLAN

May 2021

INTERNAL USE ONLY

Due to the sensitive nature of the topics covered by the project, it became essential to formulate a Crisis Communication Plan. The document is designed to provide project's partners with a quick response in the event of an emerging threat to the project's stakes. Journalists or representatives from the civil society might voice some critiques concerning EU-HYBNET objectives and results and proceeding. In such an event, the project communication and information sharing must be able to react fast enough. The document provides all instructions needed in case EU-HYBNET project or a project partner is contacted by a third party who might disseminate bad publicity about the project in media. The Crisis Communications Point of Contact together with the coordinator will be responsible for the mitigation of negative narratives and shall be contacted by other partners in case of a crisis communications event. The coordinator may contact the European Commission REA Project Officer and DG HOME Policy Officer and EC Spokes Person Services in order to mitigate needed response in the crises event.

CRISIS COMMUNICATIONS PERSON OF CONTACT

EU-HYBNET Crisis Communication Person of Contact:

Elodie Reuge

Senior Project Manager

Partner Organisation: European Organisation for Security (EOS)

Role: WP5 Leader

Email: elodie.reuge@eos-eu.com

Or

Maguelone Laval, Junior Project Officer (EOS)

Email: maguelone.laval@eos-eu.com

Phone number: +32 492 25 23 05

Strategy

The Crisis Communications Plan shall mitigate potentially bad publicity which might jeopardise the EU-HYBNET project's objectives, work and proceeding. As the project goal is to create a large and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

EU-HYBNET

sustainable network to counter hybrid threats, it is essential that the project and project partners avoid negative publicity as much as possible. ~~Additionally, EU~~-HYBNET is not only a security research project but it is also addressing a very sensitive issue within that domain – hybrid threats. Therefore, various hybrid threats or disinformation campaigns and fake news or ~~cyber attacks~~ to the project platforms might target the project itself or members of the consortium.

In this respect, it is crucial that all press/third party exchanges are centralised. This is why any enquiry shall be forwarded/redirected to the EU-HYBNET project Crisis Communications PoC and the coordinator for next actions. Should a partner be directly contacted by a third party, a concise reply will be sent from the EU-HYBNET Crisis Communications PoC and the coordinator to the inquirer, in order to let the ~~person~~ know that his/her message is well received and taken seriously. In no case will a journalist or civil society critic be met with silence.

SCENARIO 1

Partner receives an enquiry from the press or third-party

Is the enquiry clearly stated with specific questions and the third-party provides a name and contact details?

YES

NO

The partner will alert the project CC PoC of the enquiry, who will send a pre-defined statement as a reply to the third party.

See below

Ask for further details

Are new details provided?

YES

NO

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

EU-HYBNET

Alert the project's PoC. They ~~will send~~ defined message to third-party. In a case needed, the coordinator and the PoC will contact EC and REA in order to conduct most accurate solution/ message to the ~~crises~~ communication

Forward first request to PoC

Follow up of the situation until the need for the ~~crises~~ communication seems to be over.

The consortium needs to be updated on the situation by the PoC.

Pre-defined message to be sent to third parties in case of enquiry:

"Dear Sir/Madam,

Thank you very much for your email and your interest in EU-HYBNET activities.

Please allow me to forward your request to our Communications Team who will get back to you as soon as possible.

Kind regards,

X."

SCENARIO 2

Partner is made aware of EU-HYBNET bad publicity (fake news, disinformation on social media)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

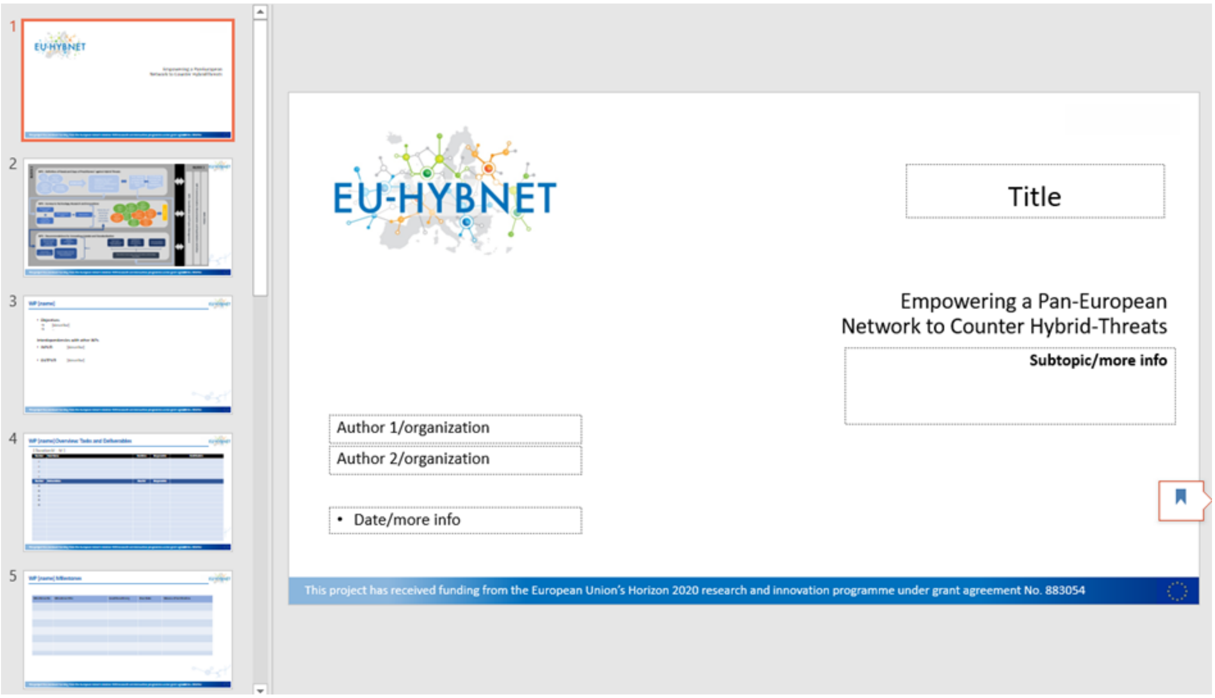
EU-HYBNET

Alert the project's PoC and coordinator who will take care of the project's response

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Figure 16: EU-HYBNET Crisis Communication Plan

ANNEX IX : EU-HYBNET PRESENTATION TEMPLATE



EU-HYBNET

Title

Empowering a Pan-European
Network to Counter Hybrid-Threats

Subtopic/more info

Author 1/organization

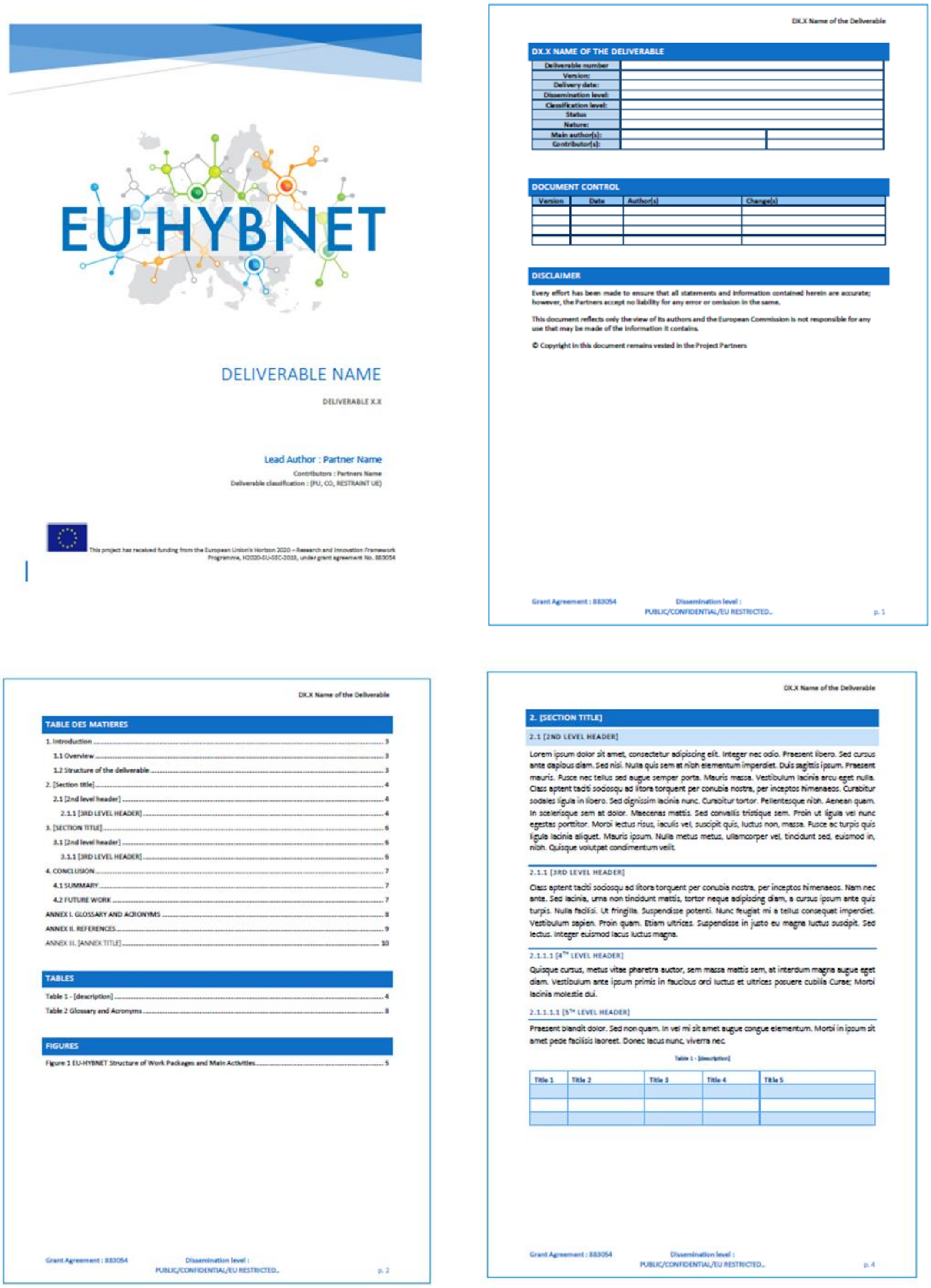
Author 2/organization

- Date/more info

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

Figure 17: EU-HYBNET Presentation Table

ANNEX X : EU-HYBNET DELIVERABLE TEMPLATE



EU-HYBNET

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, H2020-SU-SEC-2018, under grant agreement No. 883054

DX.X Name of the Deliverable

DX.X NAME OF THE DELIVERABLE

Deliverable number		
Version:		
Delivery date:		
Dissemination level:		
Classification level:		
Status		
Nature:		
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

DX.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

DX.X Name of the Deliverable

2. [SECTION TITLE]

2.1 [2ND LEVEL HEADER]

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. Praesent mauris. Fusce nec tellus sed augue semper porta. Mauris massa. Vestibulum lacinia arcu eget nulla. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur sodales ligula in libero. Sed dignissim lacinia nunc. Curabitur tortor. Pellentesque nibh. Aenean quam. In scelerisque sem at 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, nibh. Quisque volutpat condimentum velit.

2.1.1 [3RD LEVEL HEADER]

Class aptent taciti sociosqu 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 facilisi. 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.

2.1.1.1 [4TH LEVEL HEADER]

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.

2.1.1.1.1 [5TH LEVEL HEADER]

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.

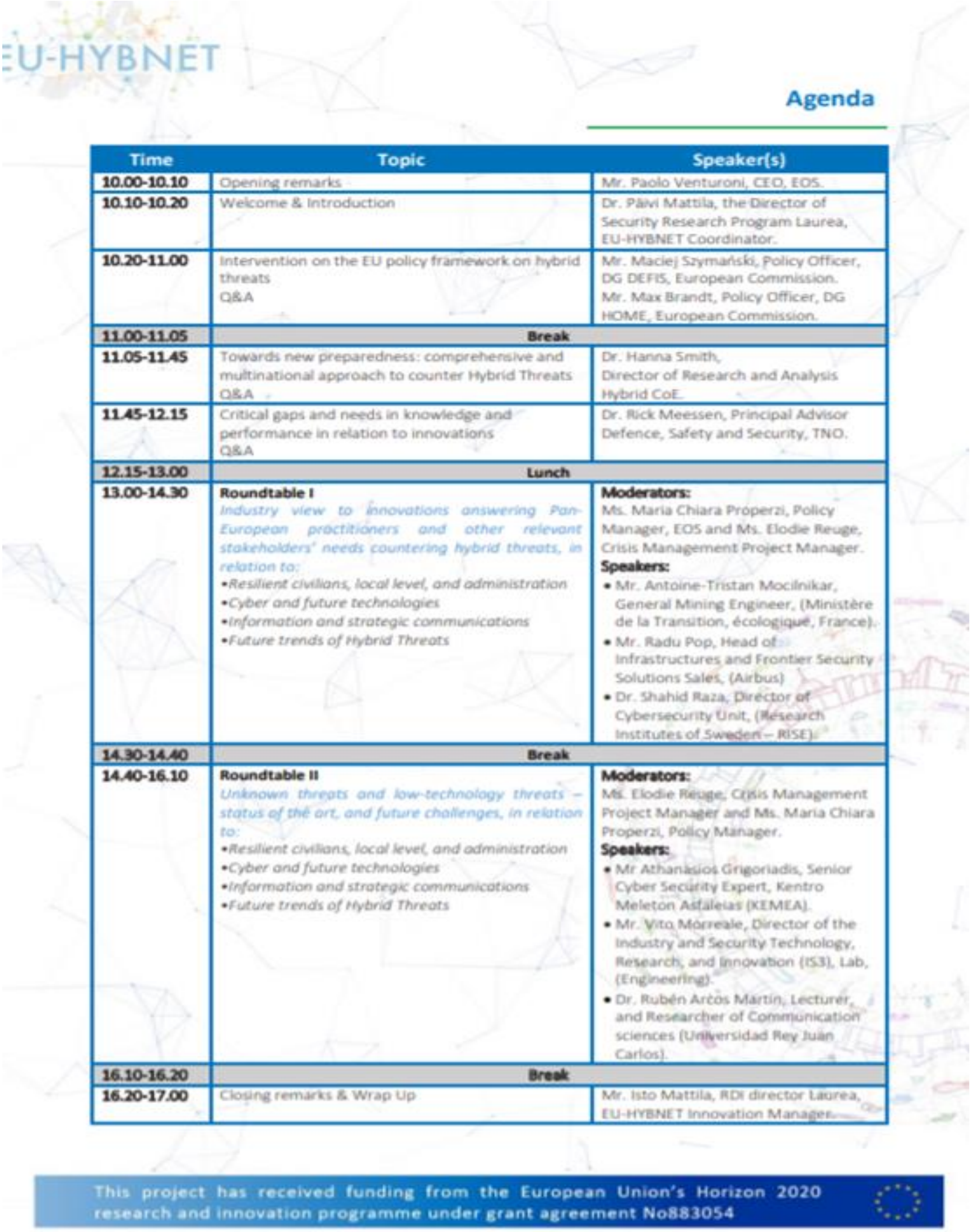
Table 1 - [description]

Title 1	Title 2	Title 3	Title 4	Title 5

Grant Agreement : 883054 Dissemination level : PUBLIC/CONFIDENTIAL/EU RESTRICTED.. p. 4

Figure 18: EU-HYBNET Deliverable template

ANNEX XI: AGENDA OF THE IKEW



EU-HYBNET

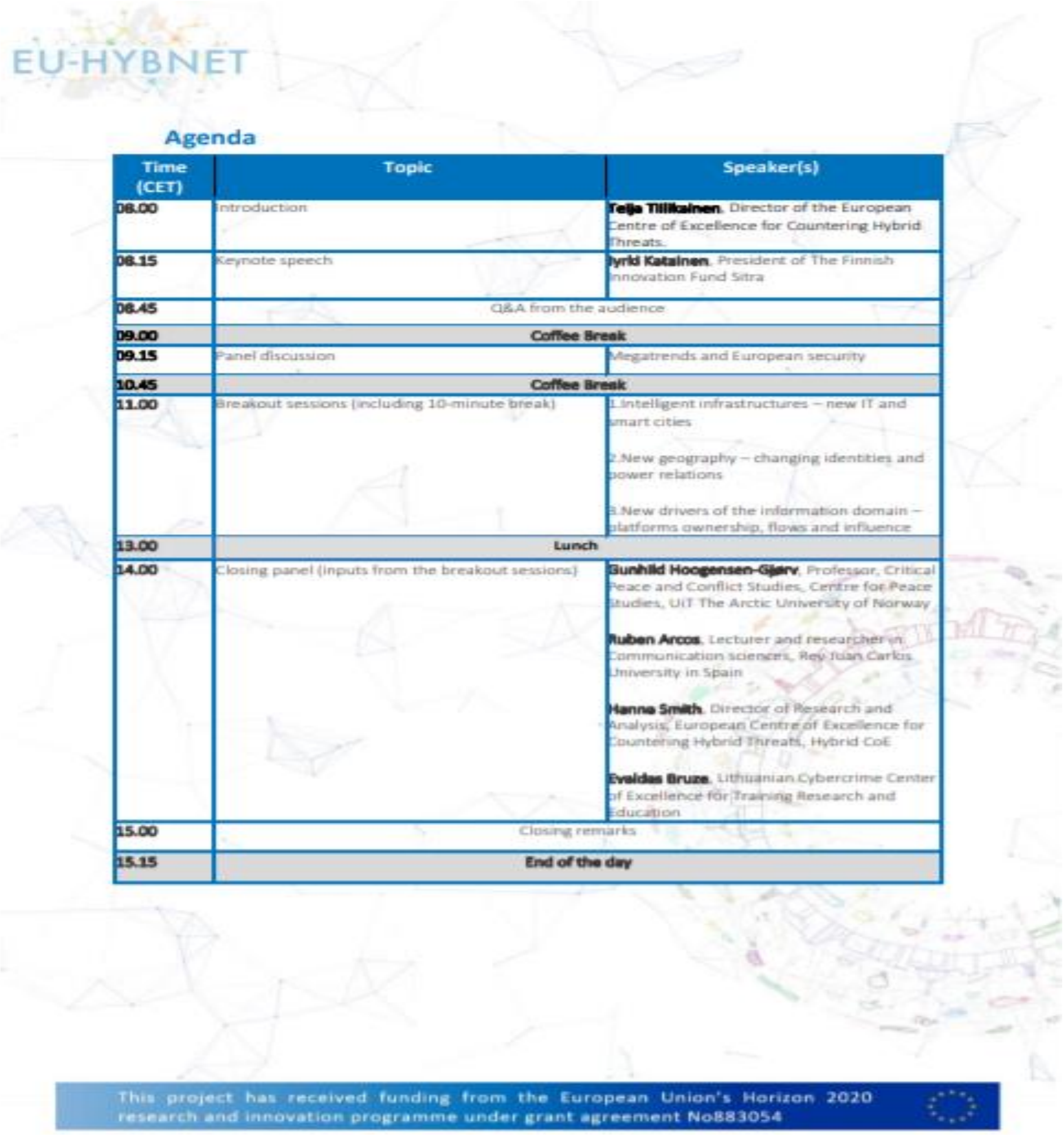
Agenda

Time	Topic	Speaker(s)
10.00-10.10	Opening remarks	Mr. Paolo Venturoni, CEO, EOS.
10.10-10.20	Welcome & Introduction	Dr. Päivi Mattila, the Director of Security Research Program Laurea, EU-HYBNET Coordinator.
10.20-11.00	Intervention on the EU policy framework on hybrid threats Q&A	Mr. Maciej Szymański, Policy Officer, DG DEFIS, European Commission. Mr. Max Brandt, Policy Officer, DG HOME, European Commission.
11.00-11.05	**Break**	
11.05-11.45	Towards new preparedness: comprehensive and multinational approach to counter Hybrid Threats Q&A	Dr. Hanna Smith, Director of Research and Analysis Hybrid CoE.
11.45-12.15	Critical gaps and needs in knowledge and performance in relation to innovations Q&A	Dr. Rick Meessen, Principal Advisor Defence, Safety and Security, TNO.
12.15-13.00	**Lunch**	
13.00-14.30	**Roundtable I** *Industry view to innovations answering Pan-European practitioners and other relevant stakeholders' needs countering hybrid threats, in relation to:* •*Resilient civilians, local level, and administration* •*Cyber and future technologies* •*Information and strategic communications* •*Future trends of Hybrid Threats*	**Moderators:** Ms. Maria Chiara Properzi, Policy Manager, EOS and Ms. Elodie Reuge, Crisis Management Project Manager. **Speakers:** • Mr. Antoine-Tristan Mocilnikar, General Mining Engineer, (Ministère de la Transition, écologique, France). • Mr. Radu Pop, Head of Infrastructures and Frontier Security Solutions Sales, (Airbus) • Dr. Shahid Raza, Director of Cybersecurity Unit, (Research Institutes of Sweden – RISE).
14.30-14.40	**Break**	
14.40-16.10	**Roundtable II** *Unknown threats and low-technology threats – status of the art, and future challenges, in relation to:* •*Resilient civilians, local level, and administration* •*Cyber and future technologies* •*Information and strategic communications* •*Future trends of Hybrid Threats*	**Moderators:** Ms. Elodie Reuge, Crisis Management Project Manager and Ms. Maria Chiara Properzi, Policy Manager. **Speakers:** • Mr Athanasios Grigoriadis, Senior Cyber Security Expert, Kentro Meleton Asfaleias (KEMEA). • Mr. Vito Morreale, Director of the Industry and Security Technology, Research, and Innovation (IS3), Lab, (Engineering). • Dr. Rubén Arcos Martin, Lecturer, and Researcher of Communication sciences (Universidad Rey Juan Carlos).
16.10-16.20	**Break**	
16.20-17.00	Closing remarks & Wrap Up	Mr. Isto Mattila, RDI director Laurea, EU-HYBNET Innovation Manager.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Figure 19 : Agenda of the IKEW

ANNEX XII: AGENDA OF THE 1ST FTW



EU-HYBNET

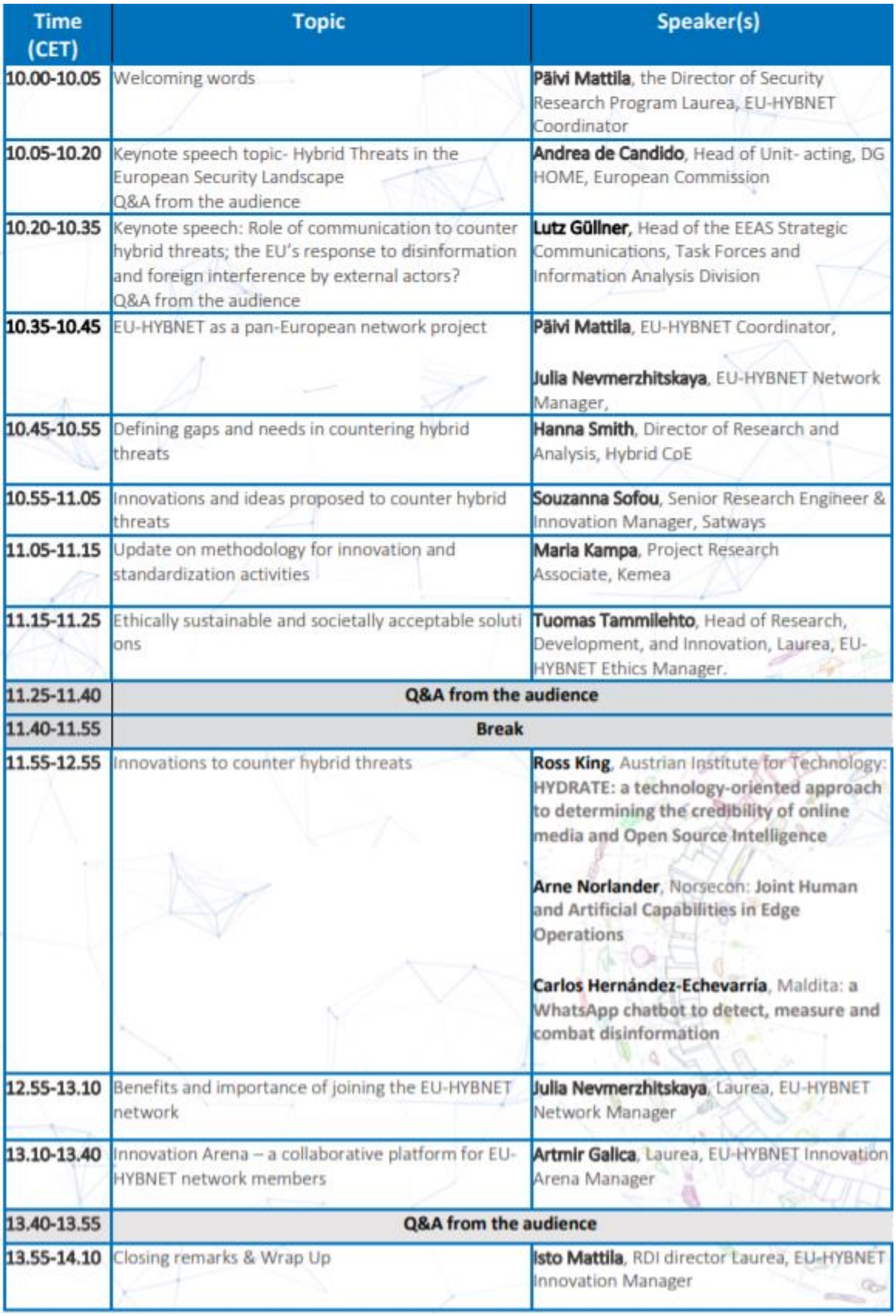
Agenda

Time (CET)	Topic	Speaker(s)
08.00	Introduction	**Teija Tiilikainen**, Director of the European Centre of Excellence for Countering Hybrid Threats.
08.15	Keynote speech	**Jyrki Katainen**, President of The Finnish Innovation Fund Sitra
08.45	Q&A from the audience	
09.00	**Coffee Break**	
09.15	Panel discussion	Megatrends and European security
10.45	**Coffee Break**	
11.00	Breakout sessions (including 10-minute break)	1.Intelligent infrastructures – new IT and smart cities 2.New geography – changing identities and power relations 3.New drivers of the information domain – platforms ownership, flows and influence
13.00	**Lunch**	
14.00	Closing panel (inputs from the breakout sessions)	**Gunhild Hoogensen-Gjørv**, Professor, Critical Peace and Conflict Studies, Centre for Peace Studies, UiT The Arctic University of Norway **Ruben Arcos**, Lecturer and researcher in Communication sciences, Rey Juan Carlos University in Spain **Hanna Smith**, Director of Research and Analysis, European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE **Evaldas Bruze**, Lithuanian Cybercrime Center of Excellence for Training Research and Education
15.00	Closing remarks	
15.15	**End of the day**	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Figure 20: Agenda of the FTW

ANNEX XIII: AGENDA OF THE ANNUAL WORKSHOP



Time (CET)	Topic	Speaker(s)
10.00-10.05	Welcoming words	**Päivi Mattila**, the Director of Security Research Program Laurea, EU-HYBNET Coordinator
10.05-10.20	Keynote speech topic- Hybrid Threats in the European Security Landscape Q&A from the audience	**Andrea de Candido**, Head of Unit- acting, DG HOME, European Commission
10.20-10.35	Keynote speech: Role of communication to counter hybrid threats; the EU's response to disinformation and foreign interference by external actors? Q&A from the audience	**Lutz Güllner**, Head of the EEAS Strategic Communications, Task Forces and Information Analysis Division
10.35-10.45	EU-HYBNET as a pan-European network project	**Päivi Mattila**, EU-HYBNET Coordinator, **Julia Nevmerzhitskaya**, EU-HYBNET Network Manager,
10.45-10.55	Defining gaps and needs in countering hybrid threats	**Hanna Smith**, Director of Research and Analysis, Hybrid CoE
10.55-11.05	Innovations and ideas proposed to counter hybrid threats	**Souzanna Sofou**, Senior Research Engineer & Innovation Manager, Satways
11.05-11.15	Update on methodology for innovation and standardization activities	**Maria Kampa**, Project Research Associate, Kemea
11.15-11.25	Ethically sustainable and societally acceptable soluti ons	**Tuomas Tammilehto**, Head of Research, Development, and Innovation, Laurea, EU-HYBNET Ethics Manager.
11.25-11.40	**Q&A from the audience**	
11.40-11.55	**Break**	
11.55-12.55	Innovations to counter hybrid threats	**Ross King**, Austrian Institute for Technology: HYDRATE: a technology-oriented approach to determining the credibility of online media and Open Source Intelligence **Arne Norlander**, Norsecon: Joint Human and Artificial Capabilities in Edge Operations **Carlos Hernández-Echevarría**, Maldita: a WhatsApp chatbot to detect, measure and combat disinformation
12.55-13.10	Benefits and importance of joining the EU-HYBNET network	**Julia Nevmerzhitskaya**, Laurea, EU-HYBNET Network Manager
13.10-13.40	Innovation Arena – a collaborative platform for EU-HYBNET network members	**Artmir Galica**, Laurea, EU-HYBNET Innovation Arena Manager
13.40-13.55	**Q&A from the audience**	
13.55-14.10	Closing remarks & Wrap Up	**Isto Mattila**, RDI director Laurea, EU-HYBNET Innovation Manager

Figure 21: Agenda of the Annual Workshop