

DISSEMINATION, COMMUNCIATION AND EXPLOITATION PLAN

DELIVERABLE 5.1

Lead Author: European Organisation for Security (EOS)

Contributors: All

Deliverable classification: PU



D5.1 DISSEMINATION, COMMUNICATION AND EXPLOITATION STRATEGY				
Deliverable number	D5.1			
Version:	VO.1			
Delivery date:	M3			
Dissemination level:	PU			
Classification level:	PU			
Status				
Nature:	Report			
Main author(s):	Elodie Reuge, Maria Chiara Properzi	EOS		
Contributor(s):	ALL			

DOCUMENT CONTROL				
Version	Date	Author(s)	Change(s)	
V0.1	29/05/2020	EOS	No	
V0.2	02/05/2020	EOS	No	
V0.3	09/06/2020	LAU	Yes	
V0.3	11/06/2020	EOS	Yes	
V0.4	11/6/2020	LAU	Yes	
V0.5	30/6/2020	ALL	Yes	
V0.6	30/06/2020	EOS	Yes	
V0.7	08/07/2020	EOS	Yes	
V0.8	09/07/2020	LAU	Yes	
V0.9	13/07/2020	LAU	Yes	
V1.0	20/7/2020	KEMEA	Yes	
V1.1	21/07/2020	TNO	Yes	
V1.2	21/07/2020	LAUREA	Yes	
V1.3	22/07/2020	EOS	Yes	

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.

 $\hbox{$\mathbb C$}$ Copyright in this document remains vested in the Project Partners

TABLE OF CONTENT

1. Introduction	5
1.1 Overview	5
1.2 Structure of the deliverable	6
2. Engaging with the hybrid threats ecosystem	7
2.1 Objectives for engaging	7
2.1.1 General objectives for engaging	7
2.1.2 Specific objectives for engaging with hybrid threats ecosystem	7
2.1.3 Specific objectives for engaging with the hybrid threats ecosystem in the frame	e of EU-HYBNET 8
2.2 Level of engagement	8
3. Stakeholders' Engagement	10
3.1 Identification of stakeholder categories	10
3.1.1 Practitioners	10
3.1.2 Industry(including smes)	11
3.1.3 Public/Policy bodies	12
3.1.4 Scientific community	13
3.1.5 Other categories	14
3.2 Stakeholders' needs	17
Practitioners	17
Industry, including SMEs	17
Public / Policy bodies	17
Scientific community	18
Other categories	18
3.3 Identification of priority groups	18
3.3.1 Priority groups	18
3.3.2 Other Stakeholders	19
4. Key messages	20
5.Dissemination, communication and exploitation means towards engagement	24
5.1 Main dissemination media	24
5.1.1 Online dissemination mediums	24
5.1.2 Off-line dissemination mediums	28
5.1.3 Dissemination through events	29
5.1.4 Synergies with other relevant projects	31
5.2 Communication Strategy	31
5.2.1 Visual materials	32
5.2.2 EU-HYBNET website	32

5.2.3 EU-HYBNET social network and social media strategy	32
5.2.4 Newsletter	34
5.2.5 Press release	34
5.2.6 Communication policy	34
5.3 Exploitation of results	34
6. Engagement roadmap	38
6.1 Launch Phase	38
6.2 Implementation phase	38
6.3 Sustainable phase	38
7. Monitoring and evaluation process to apply	39
7. DCE: other relevant issues	42
7.1 General Data Protection Regulation (GDPR)	42
7.2 Ethical matters	42
7.3 Security matters	43
ANNEX I: GLOSSARY AND ACRONYMS	44
ANNEX II: REFERENCES	46
ANNEX III : EU-HYBNET LOGO	47
ANNEX IV : EU-HYBNET Color codes	48
ANNEX V: List of external relevant events for EU-HYBNET	49
ANNEX VI: Face-to-Face/bilateral Meetings	53
ANNEX VII: EU-HYBNET Partners social media Account	54
ANNEX VIII: Dissemination and communication points of contact	55
ANNEX IX : EU-HYBNET presentation template	57
ANNEX X : EU-HYBNET deliverable template	58
TABLES	
Table 1 Level of engagement following the Spectrum of the Public Participation	a
Table 2 Key Initial Practitioners for EU-HYBNET	
Table 3 Key Initial Industry and SME partners for EU-HYBNET	
Table 4 Key Public Bodies for EU-HYBNET	
Table 5 Existing related initiatives	
Table 6 Existing related projects	
Table 7 Key messages for targeted groups	
Table 8 Partners Exploitation Strategies	
Table 9 EU-HYBNET KPIs	
Table 10 Glossary and Acronyms	

Grant Agreement: 883054

D5.1.1 Dissemination, Communication and Exploitation Strategy

Table 11 List of external events relevant for EU-HYBNET	49
Table 12 example of face-to-face meeting held by EU-HYBNET Partners	53
Table 13 EU-HYBNET Partners' Social Media Account	54
Table 14 D&C PoC	55
FIGURES	
Figure 1 IAP2 Spectrum of Public Participation	8
Figure 2 EU-HYBNET stakeholders' categories	10
Figure 3 Current homepage of the website	25
Figure 4 Innovation Arena use Cases	26
Figure 5 Innovation Arena Content Types	26
Figure 6 EU-HYBNET Tuovi Front Page	28
Figure 7 EU-HYBNET Twitter account homepage	33
Figure 8 EU-HYBNET LinkedIn Profile	33
Figure 9 EU-HYBNET Presentation Template	57
Figure 10 EU-HYBNET Deliverable template	58

1. INTRODUCTION

1.1 OVERVIEW

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

EU-HYBNET will monitor developments in research and innovation activities as applied to hybrid threats; in order to indicate priorities for innovation uptake and industrialization and to determine priorities for standardization to empower the Pan-European network to effectively counter hybrid threats.

EU-HYBNET will establish conditions for enhanced interactions with practitioners, industry, and academia for a meaningful dialogue and for increasing the membership in the network.

Finally, EU-HYBNET will foster 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 will create 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) is introducing the overall engagement approach that EU-HYBNET will follow and respect for 60 months. The main purpose of D5.1 is 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.

The **Key audiences for EU-HYBNET**, as described in the DoA, are considered as the followings: the practitioners, the industry including SMEs, the policy makers and the scientific community and NGOs. The strategy will also include key messages and means of approaching the aforementioned stakeholders.

D5.1 will address the relevant stakeholders through several channels:

- Social networks (Twitter and LinkedIn);
- Website;

- Information sharing platforms (eDuuni, TUOVI, Innovation Arena);
- "Innovation and Knowledge Exchange" workshops;
- "Future Trends" workshops;
- Annual Workshops;
- Gaps and Needs events;
- Trainings and exercises, as well project documentation and public reports;
- Consortium partners own networks;
- EU-HYBNET network members.

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 2: Engaging with the hybrid threats ecosystem;
- Section 3: Stakeholder's engagement;
- Section 4: Key Messages to be shared;
- Section 5: Dissemination, communication and exploitation means towards engagement;
- Section 6: Engagement Roadmap; and
- Section 7: Security and Ethics.

2. ENGAGING WITH THE HYBRID THREATS ECOSYSTEM

2.1 OBJECTIVES FOR ENGAGING

Understanding the logic behind stakeholders' engagement is the first step for a well-defined engagement strategy; including the selection of appropriate tools to be used. In the paragraph below, an 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; and
- **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.**

Countering hybrid threats is a sensitive activity, involving every kind of organisations and sectors. The fight against hybrid threats is starting to gain more importance in modern societies. As an adequate comprehension of the concept must be ensured, Europe needs a systematic approach to better manage evolving risks, and vulnerabilities. The involvement of the 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. Enhancing the EU's resilience to hybrid threats by creating a network and ensuring synergies with other European, national and subnational networks, specifically with security practitioners, academia and industry and NGO 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 needs 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 will ensure 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 will be disseminated to the hybrid threats stakeholders through the establishment of multi communication channels.

2.2 LEVEL OF ENGAGEMENT

Like other EU funded projects, EU-HYBNET will follow the Spectrum of Public Participation which has been developed by the International Association of Public Participation (IAP2): **informing, consulting, involving, collaborating and empowering.**[2]

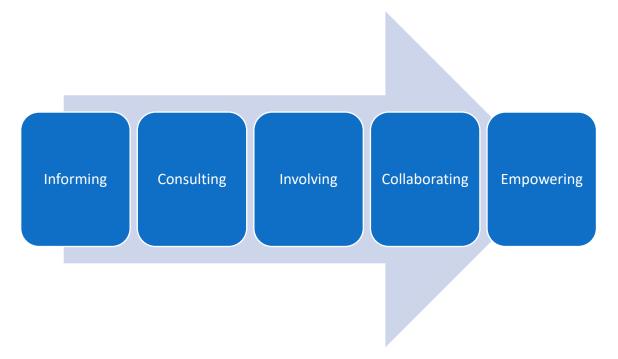


Figure 1 IAP2 Spectrum of Public Participation

In the table below, the consortium illustrates the meaning of such division 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	Get and evaluate the public feedback related to EU-HYBNET activities 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	Keep the public informed, of their concerns and provide feedback on how its input influenced a decision taken within EU-HYBNET	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 when plausible	Implement what the public decides within and through EU- HYBNET

3. STAKEHOLDERS' ENGAGEMENT

To maximise the engagement of the stakeholders, the key point is to clearly define the categories of stakeholders, their needs and the priority group they belong.

3.1 IDENTIFICATION OF STAKEHOLDER CATEGORIES

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



Figure 2 EU-HYBNET stakeholders' categories

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 these levels and the project's primary focus is on civilian 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 will follow this wide approach of the concept of practitioners and the target audience is depicted below :

Table 2 Key Initial Practitioners for EU-HYBNET

Network	Target audience
Ministry level	
Royal United Services Institute for Defence and Security Studies Defense and security services at Ministry level	Hybrid threats experts, security experts
	At MTES (France): Operational watch and alert agents; Experts taking part of the anticipation process
Local Level	
Resilient cities in the area of hybrid threats	City of Exeter, City of Helsinki, City of Bucharest
European Level	
ENLETS (European Network of Law Enforcement Technology Services	Law enforcement Agencies
Artic Coast Guard Forum (ACGF) ARCSAR	Artic and North-Atlantic Coast Guards and security and emergency response practitioners
National Security Analysts Network	Organisations supporting National Security policy
European Reference Network for Critical Infrastructure Protection: ERNCIP	CIP Stakeholders focusing particularly on the technical protective security solutions
Exeter centre for International Law	Researchers and practitioners in the field of human rights law, the law of armed conflict and international refugee law
CBRN CoE	EU Centres of Excellence on Chemical, Biological, Radiological and Nuclear Risk Mitigation
European Council on Foreign relations	Decision makers, Business Leaders, Civil Society Leaders, Senior IO officials, Academics, Journalists and influencers in the field of European foreign and security policy

3.1.2 INDUSTRY(INCLUDING SMES)

Industrial players represent 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 will give the consortium an oriented idea of what is possible to be done in terms of innovative solutions and advice on the innovation delivery obstacles (absence of needed infrastructure, legislation that could

hinder/accelerate the uptake) and share experiences on how to overcome them. The audience listed below will engage with its wide network (security industry, suppliers of security solutions). This audience will receive all supportive documents needed. Table 3 provides an initial list of networks that should be contacted by EU-HYBNET for disseminating and communicating Project's results. The list, however, is not definitive, but it will be further enriched throughout the project's life span.

Table 3 Key Initial Industry and SME partners for EU-HYBNET

Network	Target audience		
EU level			
EOS	European security industry		
ECSO	European cyber security stakeholders		
ASD	European aerospace, defence and security industry		
СЕЕМЕТ	European Tech and Industry employers		
SIINDA	Search and Information Industry		
UNIFE	European Rail Manufacturing Industry		
National level			
SAFECLUSTER	National security industry		
Security industry including SMEs	National Security industry operating in Europe		

3.1.3 PUBLIC/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 are targeted. EU-HYBNET Consortium will identify and get in contact with the relevant organisations and invite them to the project events and workshops, also via targeted web based communication (EU-HYBNET platforms, web-page, and other remote way of connecting Practitioners). The relevant files under discussion within these bodies will also be identified and their development monitored by the Consortium. If necessary and when possible, they will be discussed with policy makers.

Different public administration units, responsible for coherence and resilience in society, are in charge of first responses , in case of a major attack: rescue or police departments for example, like the International Association of Fire and rescue services. The interested part of these bodies is their overall responsibility to raise societal resilience as they can be called at any time and sent on spot in case of events.

Below a table recapitulating the main target of the public/policy bodies category:

Table 4 Key Public 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), DG Connect (Directorate A: Strategy and General Affairs/ Directorate D: Security), DG MARE, DG ECHO
Agencies/Bodies of the EC	European Defense Agency, The European Border and Coast Guard Agency (EBCGA/FRONTEX), 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), The European union institute for security study (EUISS)
European Parliament	Files on Hybrid Threats
EEAS	Division Security and Defence Policy SECDEFPOL1 – Hybrid Threats, Hybrid Fusion Cell
The Council's Friends of Presidency Group on Countering Hybrid Threats (FoP)	Council of the European Union (General Secretariat)
EAST-STRATCOM	Administration of the European Union, focused on proactive communication of EU policies and activities in the Eastern neighbourhood (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) and beyond (Russia itself)
National level	
National Ministries	National Ministries of Interior (i.e. Centre Against Terrorism and Hybrid Threats in Czech Republic), National Ministries of Foreign and European Affairs, National Ministries in charge of Defense

3.1.4 SCIENTIFIC COMMUNITY

This category, composed by researchers and academics in the area of hybrid threats is crucial in terms of understanding the concept of hybrid threats. EU-HYBNET aims to impact the scientific community by expanding the existing knowledge of hybrid threats. Academics in hybrid threats, and also researchers focused on other issues such as on IT, are keen on resolving unsolved problems, and also exploring new avenues for research or opportunities to validate approaches.

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 will engage with a wide range of EU Projects and European and national activities, already identified during the preparation phase. In the following table there is an exemplification of the links already developed:

Table 5 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. MVNIA, in partnership with "Bogdan
Countering Hybrid Threats: Lessons Learned from Ukraine	MVNIA	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.
International conference Intelligence in the Knowledge Society	MVNIA	MVNIA organises an international conference which combine three main categories of audience, involved in the intelligence and security field: academics and researchers, practitioners and experts. The latest edition (2018) included panels and experts debates on hybrid warfare, topics which will remain on the agenda for future editions.

Table 6 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, SAYSO	Network extension	LEA cooperation, Search and Rescue, Fire and Rescue, Radiological and nuclear, emergency medical systems
H2020 ICT	LAU, L3CE, RISE	ECHO, SPARTA, CONCORDIA, 5G- ENSURE	Research and Innovation hubs' cyber network	Cyber security research and innovation,

				situational awareness tools, 5G security
H2020-BES	KEMEA, SATWAYS, LAUREA	CIVILNEXT, MARISA, RANGER, ANDROMEDA	Research and Innovation	Information systems, Maritime and border surveillance situational awareness
H2020 DRS	MVNIA, UCSC, SATWAYS, PLV	CARISMAND, ENCIRCLE, IN-PREP, BE-AWARE	Research and Innovation	Man-made and natural disasters, CBRN, disaster response and preparedness risk management
H2020 TDS	UCSC	PANACEA	Research and Innovation	Cyber in health and wellbeing
H2020 FCT	KEMEA, MVNIA, TNO, EOS, PLV	SHUTTLE, CITYCOP, MEDI@4SEC, ROCSAFE, FORENSOR, TAKEDOWN, INSPEC2T	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
H2020-IBA	JRC	CF SEDSS II	Research and Innovation	Energy
FP7 GM	KEMEA	CRESCENDO, EU- SEC II	Coordination action with EU Security Research Networks	Risks, evolution of threats, Security at major events
FP7, security	EOS, TNO, KEMEA	DRIVER+, THE HOUSE,	Community of practice, security research	Crisis management, research coordination, border, impact assessment
EU Sec-2020	PPHS, EOS	MINDB4ACT	Ecosystem building	Terrorism, extremism, radicalization
ISFP-2014-2017	L3CE, MVNIA, KEMEA	SENTER, ARMOUR, SAFFRON	Network in Cybercrime critical communications	Cybercrime, resilience, detection of foreign fighters
EU-ECSEL- Council Regulation 2017	RISE	SECREDAS	Research and Innovation Joint undertaking	Safety, security and privacy in systems
ISEC-HOME- 2°13	L3CE	ECOPOL	Centre of excellence building	Hybrid threats, cyber disinformation operations
ERASMUS-2018	MVNIA, KEMEA, URJC	CRESCEnt	Integrated online platform	Education in communication
National funding	TNO	V1925	Resilience building, visualisation and modelling hybrid conflicts, hybrid conflict gaming, horizon	Hybrid threats

Grant Agreement: 883054

			scanning, capability research,	
Ministry for Education and Research (DE)	COMTESSA	RIKOV, REHSTRAIN	Identifying and analyzing terrorist risk, Simulation	Civil security, Terrorism, Critical infrastructures, Resilience

3.2 STAKEHOLDERS' NEEDS

The identification of the stakeholders is a crucial point as EU-HYBNET wants to deliver well-oriented 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 quite well known and they only need to plan their measures directly. In all cases, the practitioners must be able to reach the optimum decisions by accessing reliable information and integrate them 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 an event or crisis, the communication must be well received. 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.

The EU-HYBNET goal is to invite and bring together European practitioners in the same discipline of Hybrid Threats together and jointly with other core project stakeholders to define the needed measures to counter hybrid threats.

INDUSTRY, INCLUDING SMES

The Industry group can be divided into two sub categories; suppliers and providers.

- The suppliers need guidance into the security requirements and examples of security solutions
 proven to be effective in the targeted context to improve the security provided by their
 products and services.
- The *providers*, on their side, have to be aware of the potential threats and risks created by potential hybrid threats and implement appropriate security solutions to prevent the risks and to mitigate the impact of some crisis and vulnerabilities on the society.

Security Industry needs 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 projected at national and European levels. Public policies might intent 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 the 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, aiming at an advanced state-of-art of legal literature, and improving the already existing knowledge with respect to hybrid threats. More specifically the idea would be to:

- Provide guidance in terms of the interpretation of legal requirements in scope,
- Exchange research results, in order to efficiently use available resources
- 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 also for other stakeholders 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 its impact.

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 responses to various types of crisis and vulnerabilities in society.

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 types of 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 (those that will also form the core group of EU-HYBNET Network) are categorised as follows:

- Ministry level (administration);
- Local level (cities and regions); and
- 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 Societies-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.

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 CONNECT, DG MARE, DG ECHO), Agencies of the EU (such as EDA, EBCGA, EMSA, EASA), EU Institutions (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 support the establishment of regulation mechanisms
- Private sector: industry, including SMEs. The consortium with its network with the European security industry will be in the position of promoting EU-HYBNET and raise awareness to those stakeholders.

The consortium will need to flag 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;
- Key actors in innovation uptake and standardization; and
- Internal network/ audience of the consortium partners can be seen as important too and effective internal communication must ensure that EU-HYBNET has a high profile.

4. KEY MESSAGES

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 be straight towards the point they aim to reach.

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

Table 7 Key messages for targeted groups

				_	_	
	Practitioners	Industry including SMES	Public Policy Bodies	Research and scientific community	Related Projects and Initiatives	Civil Society
WP1 Coordination a						
Objectives related t						
Achieve EU- HYBNET objectives	To get access to the achievem ent of EU-HYBNET Objectives	To get access to the opportunit ies to further improve EU-HYBNET outputs and to join the network	To gain a better understan ding of EU-HYBNET for future influence on Policies	To get the opportunity to give feedback on EU-HYBNET outputs and to join the network	To get a better understanding of EU-HYBNET, enhance collaboration and avoid overlap	To get a better understanding of EU-HYBNET input to society
To support the	To be part o	f the Europea	n Network aga	inst hybrid threat	S	
extension of						
actors in the						
European						
Network against hybrid threats						
WP2 Gaps and Need	ds of Europea	n actors again	st Hybrid Thr	eats		
Objectives related t					hreats	
To identify Gaps and Needs	To be able to gather, analyse and deliver solutions on the identificati on Gaps and Needs	To have a better understan ding of G&N	To have a better understan	To have a better understanding of G&N identified	To be aware of G&N identified	To have a better understandi ng of G&N identified
To increase European Stakeholders' knowledge of the hybrid threats To test Innovation	To get know	rledge on Hybr	id threats To be	To be aware of	To be aware of	To be aware
to enhance	aware of	aware of	aware of	the results of	the test	of the test

		I	I	T.	I	1
European	the test	the test	the test as	the tests and		
Stakeholders	and give	and to be	input for	use them		
measures against	feedback	able to	potential			
hybrid Threats	on	take a	follow up			
.,	Innovatio	position on	action			
		the market	when			
	n	themarket				
			needed			
WP3 Surveys to Tec						
Objectives related t	to the Surveys	_	1			
To map the needs	To be	To be	To be aware	of the mapping		
for innovations:	aware of	aware of				
results to be	the	the				
populated via the	mapping	mapping				
IA		and to				
		provide				
		more				
		informatio				
	1					
To manufact t	T- '	n if needed	NASI::	Tuine	Ta martin d	Halada - 11
To monitor and	To be	To be	Making	Trigger new	To make them	Help the civil
select available	aware of	aware of	them	research in	aware of the	society to be
innovative	the	the	aware of	hybrid threats	developments	better aware
solutions for	selected	selected	new	application in	in EU-HYBNET,	of advanced
measures against	solutions	solutions	research	the most	so that other	hybrid
hybrid threats		as input for	and	promising	projects can	threats, and
,		potential	innovation	areas.	further	to advise on
		follow up	s, thus		advance	the
		action	increase		developed	response.
		when	readiness		knowledge.	тезропзе.
		_			_	
		needed	of		On the other	
			organizatio		hand EU-	
			ns to		HYBNET will	
			recognize		use	
			recognize		use	
			recognize new		use knowledge	
			recognize new threats and		use knowledge accumulated by other	
			recognize new threats and employ		use knowledge accumulated	
			recognize new threats and employ new		use knowledge accumulated by other	
			recognize new threats and employ new methods/t		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them.		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research		use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into		use knowledge accumulated by other	
To arrange events	To be aware	e of the events	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process.	nem	use knowledge accumulated by other	
			recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend th		use knowledge accumulated by other	
WP4 Recommendate	tions for Inno	vations Uptak	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the	dization	use knowledge accumulated by other projects.	
WP4 Recommendate Objectives of the re	tions for Inno	vations Uptak ons for Innova	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar tions Uptake	dization and Standardizat	use knowledge accumulated by other projects.	To be aware
WP4 Recommendate Objectives of the recommendate To build a	tions for Inno commendation	vations Uptak ons for Innova To be	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar tions Uptake To be	dization and Standardizat To be aware of	use knowledge accumulated by other projects.	To be aware
WP4 Recommendate Objectives of the recommendate To build a concrete roadmap	tions for Inno commendation To be aware of	vations Uptak ons for Innova To be aware of	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar tions Uptake To be aware of	dization and Standardizat To be aware of the roadmap	use knowledge accumulated by other projects.	of the
WP4 Recommendate Objectives of the reconcrete roadmap on innovation	tions for Inno commendation To be aware of the	vations Uptak ons for Innova To be aware of the	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar tions Uptake To be aware of the	dization and Standardizat To be aware of the roadmap and to	use knowledge accumulated by other projects.	
WP4 Recommendate Objectives of the recommendate To build a concrete roadmap	tions for Inno commendation To be aware of	vations Uptak ons for Innova To be aware of the roadmap	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar ntions Uptake To be aware of the roadmap	dization and Standardizat To be aware of the roadmap and to contribute to	use knowledge accumulated by other projects.	of the
WP4 Recommendate Objectives of the reconcrete roadmap on innovation	tions for Inno commendation To be aware of the	vations Uptak ons for Innova To be aware of the	recognize new threats and employ new methods/t echnologie s to mitigate them. Feed research results into the policy process. and attend the e and Standar tions Uptake To be aware of the	dization and Standardizat To be aware of the roadmap and to	use knowledge accumulated by other projects.	of the

	I					
		influence	input to it	relevant		
		on the	if possible.	knowledge		
		market	Moreover,			
			to			
			capitalise			
			on the			
			recommen			
			dations in			
			order to			
			formulate			
			the next			
			steps			
			against			
			Hybrid			
			threats in			
			EU Level.			
To compile	To be	To be	To be	To be aware of	To be aware of	To be aware
recommendations	aware of	aware of	aware of	the	the	of the
for	the	the	the	recommendati	recommendati	recommend
standardisation	recomme	recommen	recommen	ons	ons	ations
activities	ndations	dations	dations as			
		and see	input for			
		their	potential			
		potential	follow up			
		influence	action			
		on the	when			
		market	needed			
To deliver Policy	To be	To be	To be	To be aware of	To be aware of	To be aware
Briefs, Position	aware of	aware of	aware of	the	the	of the
Papers and	the	the	the	documents	documents	documents
Recommendation	document	documents	documents	needed and to	needed	needed
s	S	produced	produced	contribute to		
		and to	as input for	them if		
		contribute	potential	possible		
		to them if	follow up			
		possible	action			
			when			
			needed			
WP5 Dissemination						
Objectives of the Co	mmunication					
To disseminate	To be	To be	To be	To be aware of	To be aware of	To be aware
results and	aware of	aware of	aware of	the main	the main	of the main
interact with	the main	the main	the main	results of EU-	results of EU-	results of
other related	results	results and	results of	HYBNET and to	HYBNET and	EU-HYBNET
networks	and	take a	EU-	exploit them	to exploit	and to
	objectives	position on	HYBNET		them	exploit them
	of EU-	the market	To have			
	HYBNET		the			
	and to		opportunit			
	exploit		y to			
	them		improve			
			actual			
			policy			
To create	To be part o	f the EU-HYBN	IET Network			
conditions for						
better interaction						
with industry,						

Grant Agreement: 883054

D5.1.1 Dissemination, Communication and Exploitation Strategy

research and	
academia	
Enrich existing	
network against	
hybrid threats	
with academics,	
practitioners,	
stakeholders and	
industry actors	
across Europe	
WP6 Ethics	
No objectives to sha	are with stakeholders

Grant Agreement : 883054 Dissemination level :

PUBLIC p. 23

5.DISSEMINATION, COMMUNICATION AND EXPLOITATION MEANS TOWARDS ENGAGEMENT

5.1 MAIN DISSEMINATION MEDIA

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 will be used for EU-HYBNET are described below:

5.1.1 ONLINE DISSEMINATION MEDIUMS

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.

EU-HYBNET WEBSITE

Up from M3, EU-HYBNET will have its own dedicated website (www.euhybnet.eu), to be seen as both a promotional and information tool. Its establishment is crucial in terms of communication as such a tool has an impact on the visibility and enhances stakeholders' engagement as it will be widely accessible.

The website will have the same graphical identity as the communication tools which are used within EU-HYBNET. It will be 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 will be added by Laurea who is in charge of establishing it.

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

With the aim to be user friendly, the website will be divided into several sections. The sections are planned to be e.g. following: HOME – The project – Innovate with us – Network – News – Events – Results – Eduuni. The sections will include relevant information about the project content e.g. HOME and About. In addition, the plan is to have a section that will tell about the latest information about the project, e.g. News. Furthermore, some of the sections will describe the forthcoming and past project events e.g. Events. Some sections are planned to include information that will encourage to join the EU-HYBNET network and to gain more information about the network; e.g. Network, also News, Events. Moreover, relevant information on the project results (e.g. Deliverables) and EU-HYBNET project related latest research information is planned to be shared in a section e.g. Publications. In addition, the plan is to have a section that forwards project partners and network members to use project Innovation Arena. The innovation arena is a platform where project partners and network members will describe their needs and wishes to innovations that could fill capability gaps

to counter hybrid threats. In addition, Innovation Arena users may tell about existing innovation or research findings that could fill the capability gap. In short, the section "Innovate with us" is to support innovation mapping to the announced Pan-European Network's needs to counter hybrid threats. Lastly, the web page will include a category that links consortium partners to use the project intranet.

The webpage is also described with details in D5.8 that is submitted to the Commission in project month 3.



Figure 3 Current homepage of the website

INNOVATION ARENA

The project dissemination and communication plan includes the creation of the Innovation Arena (IA) platform, planned to be carried out by Laurea UAS in M5 and will continue running until M60. Since this deliverable/ IA is still in the design phase, at the moment the IA planning is ongoing and it 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 will enable 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 will be 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 will be as illustrated in the figure (IA use cases) below:

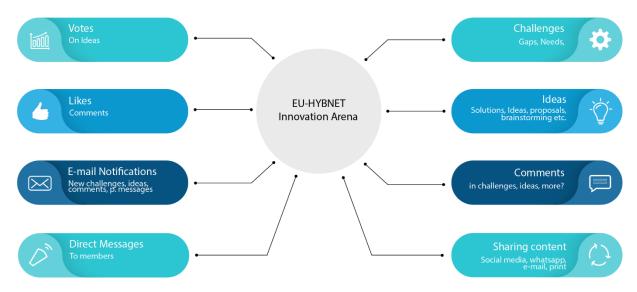


Figure 4 Innovation Arena use Cases

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



Figure 5 Innovation Arena Content Types

The IA will have 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 project 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 will use the IA discussion between those who need and those who may deliver innovations (technical and social) in Work Package WP3 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.[6]

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 will serve 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 will see each other's profiles and will 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 will be 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, contact information, project social media links (LinkedIn and Twitter), how many members the workspace has, 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 will contain general project information as well as information about EU-HYBNET events, press releases and other marketing and project promotional materials. As project newsletters and deliverables are accomplished these also will be uploaded to folders for access by all members. 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 (Hybrid CoE) 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 6:



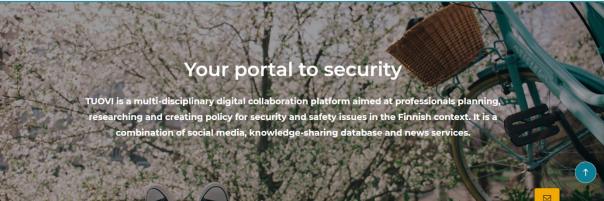


Figure 6 EU-HYBNET Tuovi Front Page

The TUOVI platform will have 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 existing, new and future members of the European Network against Hybrid Threats to announce discuss project innovations, and potentially new hybrid threats. In addition, network members may provide feedback to project deliverables 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.

TUOVI is described in details in D1.15 that is submitted to the Commission in project month 2.

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

DELIVERABLES

All deliverables (D) except D2.1-2.11 and D6.1-6.4 are public within EU-HYBNET — the non-public deliverables are Consortium Only (CO). These documents are crucial and will contain detailed descriptions of the results. After their submission, the title and a short description of the deliverables is put on the website, if the deliverables is "public". After their official approval by the EC, they are open to CORDIS and can be found online on the website in a case of "public". 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

The scientific publications produced within EU-HYBNET will be freely available, in order to maximize the impact of the project. OperAIRE can be used to select the proper open access repository and/or deposit publications. Journal (Journal of Defence and Security Technology)

EXTERNAL CHANNELS

EU-HYBNET results will also be 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
- Presentations of the project in scientific journals e.g. MVNIA's Romanian Intelligence Studies Review

STRATEGY ON MASS MEDIA

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

5.1.3 DISSEMINATION THROUGH EVENTS

INNOVATION AND KNOWLEDGE EXCHANGE EVENTS

Three Innovation and Knowledge Exchange workshops will be hosted in the frame of EU-HYBNET:

- Event 1: Introduction to EU-HYBNET project and existing Network in Brussels by EOS (at M9);
- Event 2: Innovation and Knowledge Exchange workshop in The Hague by TNO (at M26); and
- 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.

FUTURE TRENDS WORKSHOPS AND ANNUAL WORKSHOPS

Five Future Trends workshops, organized together with five annual workshops will address expected future manifestations and evolution of hybrid threats. The objectives of these workshops will be 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 Hybrid CoE (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); and
- Workshop 5: In Ispra by JRC (at M58).

Future Trends Workshops form an integral part of Task 3.4, which aims to deliver annual events for practitioners (and stakeholders in general) to facilitate exchange of information on innovations and knowledge and increase the likelihood of uptake. The first event will introduce the EU-HYBNET project and existing network as an innovation exchange arena for the extended network. It allows practitioners to become aware of innovation possibilities via the EU-HYBNET project and network activities. For this event the output from T3.1-3.3 will be used, in particular the mapping matrix of gaps/needs and research/innovations. For each event organised, the partners involved in T3.4 will make sure to provide interaction with industry, academia and other providers of innovative solutions (technical and social innovations) outside of the consortium with a view to assessing the feasibility of the EU-HYBNET project activities and findings (as requested in the GM-01 call, special conditions). Special attention is required for the unknown threats and the low-tech threats (based on surprising and creative tactics), which are often not in direct focus and attention of practitioners. Therefore a workshop in which also out-of-the-box, nonconformist and creative thinkers attend, will be organised, with the aim to find new threats or manifestations of hybrid threats.

WORKSHOP FOR INNOVATION STANDARDIZATION

Events on 'Innovation and Knowledge Exchange' will have different themes although noticing the project four core themes and will facilitate continuous mapping of needs, monitoring of solutions, and providing a forum where practitioners can engage with innovation providers. Innovation providers will be invited to explain and demonstrate innovative solutions that match with the event theme and interact with practitioners. Knowledge transfer will be incorporated in several ways: peer-to-peer practitioner learning, learning from EU MS national actors, and through workshops. Meetings will involve key personnel within organisations involved in measures against hybrid threats.

Three workshops for Innovation and standardization will be hosted 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); and
- Standardization Workshop 3: In Brussels by Laurea (at M56).

TRAININGS

L3CE in the partnership with WP2 contributors will lead the organization and delivery of the Trainings and Exercises (knowledge exchange events) for Needs and Solution 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 background 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, ensuring that trainings reflect knowledge advancements in EU-HYBNET project; and

• Action 4: making sure to organize at least one out-of-the-box event.

GAPS AND NEEDS EVENTS

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. 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 will attend events according to their field or expertise and take the chance of enhancing the network of the project.

Practitioners' engagement should also be considered, through face-to-face or bilateral meetings where EU-HYBNET Partners could disseminate the developments of the projects while visiting other police forces. This typology of meeting, implying a "Police to Police" communication could prove to be effective.

5.1.4 SYNERGIES WITH OTHER RELEVANT PROJECTS

The main aim 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.

5.2 COMMUNICATION STRATEGY

'Communication is a way to keep all partners actively involved in the project'[5]

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- and Word document template provided at M1 by PPHS and EOS – see Annex IX and X).

A promotional package is also meant to be ready at M3 and will include:

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

All communication materials, like the flyers, brochures and roll-up, will be updated according to the needs of the consortium, and in order to update information according to project developments and successes.

5.2.2 EU-HYBNET WEBSITE

As explained above, the website will be accessible at M3 and more detailed description is provided in D5.3 due month 3.

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.

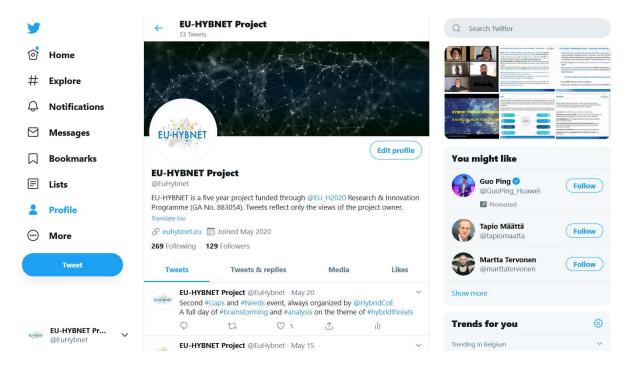


Figure 7 EU-HYBNET Twitter account homepage

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

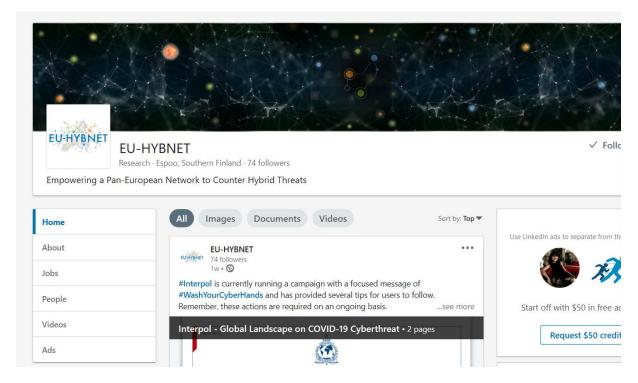


Figure 8 EU-HYBNET LinkedIn Profile

Both platforms will be used to promote events before and during them, as well to share relevant post related to Hybrid threats or the project outcomes. EOS (for Twitter) and PPHS (for LinkedIn) will be in charge of feeding the platforms with the support of the consortium's partners.

5.2.4 NEWSLETTER

Twice a year the consortium will share a newsletter updating the stakeholders and the EU-HYBNET network members about what has happened in the past six months and what will happen in the six months to come. The document will of course follow the design of the website and will be shared in two ways: via Mailchimp (an account will be created at M6) and via the wide networks of the consortium partners.

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. The consortium will continue producing them on a necessary basis, to promote an event for example.

5.2.6 COMMUNICATION POLICY

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

Partners will be 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).

The deliverable (D) 1.8 "EU-HYBNET Network Sustainability Plan" will describe the communication policy with the EU-HYBNET network from sustainability point of view in details.

5.3 EXPLOITATION OF RESULTS

EU-HYBNET's plan for the exploitation of the results demonstrates how the proposed measures support to achieve the expected impact. Exploitation of the results is key to maximizing their impact. An exploitation strategy per partner is outline below:

Table 8 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-

	HVRNET project will be fed directly into governmental policy and decision making processes on
	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 exploiting the experience of EU-HYBNET to ameliorate the Hospital's response to cyberthreats also taking into consideration that Hospitals are considered as critical infrastructures. 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. Cross-border emergencies such as pandemics are managed through Public Health and WHO and ECDC directives, and these agencies are a main object of hybrid threats, directly or indirectly. Awareness of this menace by major Hospitals is mandatory to better deal with immediate response. USCS plans to involve other MS and international Hospitals, medical and non-medical staff in the project training activities through conjunct exercises and pose itself as "leader" in this setting.
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
Hybrid CoE	Hybrid CoE (Hybrid CoE) 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. Hybrid CoE hopes to inspire partners and be inspired. Upon project completion Hybrid CoE 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 will be displayed throughout the EU-HYBNET timeline.

6.1 LAUNCH PHASE

Informing:

Phase 1 will be about creating an awareness among the targeted stakeholders.

<u>When</u>: The launch phase will start at M1 (May 2020) and run for 6 months until M7 (October 2020).

<u>Who</u>: During this phase all the targeted stakeholders will be 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); and
- EU-HYBNET Newsletter (at M6 and then every six months).

6.2 IMPLEMENTATION PHASE

Consulting:

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

When: The phase 2 will start at M8 and run until M56;

<u>Who</u>: all the stakeholders developed in the previous sections, using the system of prioritization; and

<u>What</u>: 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

Involvement:

The is the final phase of the project. It will also be the one requiring the highest involvement from the stakeholders. <u>When</u>: the final phase will start at M57 and run until M60.

Who: All the stakeholders described in the previous sections.

<u>What</u>: the most important activities will be the final Future Trends workshops and the project Annual Workshop to be held both in 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; 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.

The EU-HYBNET dissemination, communication and exploitation activities included more detailed KPIs which are described in the table below.

Table 9 EU-HYBNET KPIs

Key Performance Indicators		Target at M13			Partners involved	
		Level of performance				
Disseminat ion and Communic ation tools	Definition of the indicator	Type of data required	Poor	Good	Excellent	
Project Website	Number of visits per month Page views per month Average time	Google analytics	Less than 140 per month Less than 1400 at M13 Less than 300 per month Less than 3000 at M13 Less than 30 seconds	140-300 per month 1400-3000 at M13 300-500 per month 4000-5000 at M13	More than 300 per month More than 3000 at M13 More than 500 per month More than 5000 at M13	Responsible: EOS Accountable: Laurea, PPHS Consulted: ESPOO, TNO, PLV, Hybrid CoE Informed: All other partners
Social	spent on website Subscribers of the LinkedIn Page	LinkedIn Group	Less than 100 at M13	min 100-200 at M13	More than 200 at M13	Responsible: PPHS Accountable: Laurea, EOS
Media	Number of posts shared on LinkedIn	Statistics dashboard	Less than 15 at M13	15- 20 at M13	More than 20 at M13	Consulted: ESPOO, TNO, PLV, Hybrid CoE Informed: All other Partners

	Number of Twitter followers		Less than 200 at M13	200-400 at M13	More than 400 at M13	Responsible: EOS Accountable: PPHS, Laurea
	Number of tweets per month	- Twitter -	Less than 10	10-25	More than 25	Consulted:ESPOO, TNO, PLV, Hybrid CoE
	Number of retweets per month	analytics	Less than 3	3-10	More than 10	Informed: All other Partners
	Number of tweets liked per month		Less than 10	10-25	More than 25	
Biannual Newsletter	Number of Newsletters published	Proceedings	Less than 1	1-2	More than 2	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, Hybrid CoE Informed: All other Partners
Brochures	Number of brochures distributed		400 brochures at M13	600 brochures at M13	750 brochures at M13	Responsible: PPHS Accountable: EOS, Laurea Consulted: ESPOO, TNO, PLV, Hybrid CoE Informed: All other Partners
Contributio	Number of external events in which EU-HYBNET participates		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, Hybrid CoE, PLV
ns to external events	Number of abstracts/papers submitted and selected	Proceedings	Less than 3 at M13	3-10 at M13	More than 10 at M13	Informed: All other partners
	Copies of the brochure/factshe et distributed		Less than 300 at M13	300-800 at M13	More than 800 at M13	
	Number of workshops organized	Events timeline	5			Responsible: EOS, TNO, PLV Accountable: Laurea, PPHS Consulted: Hybrid CoE,
Innovation and	Number of participants	Proceedings	60	60-80	80-100	ESPOO Informed: All other partners
Knowledge workshop	Number of Tweets during a workshop	Twitter analytics	Less than 5	5-10	More than 10	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-5	More than 5	
Future Trends workshop	Number of workshops organized	Events timeline	eline 5 HSCS, MVNIA, P		Responsible: Hybrid CoE, HSCS, MVNIA, PLV, JRC Accountable: EOS, Laurea,	
	Number of participants	Proceeding	60	60-80	80-100	PPHS Consulted: ESPOO, TNO
	Number of Tweets during a workshop	Twitter analytics	Less than 5	5-10	More than 10	Informed: All other Partners
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-5	More than 5	
Gaps and needs workshops	Number of workshops organized	Events timeline	4			Responsible: Hybrid CoE Accountable: EOS, Laurea, PPHS
	Number of participants	Proceedings	30-40	40-55	55-65	Consulted: ESPOO, TNO, PLV Informed: All other partners

D5.1.1 Dissemination, Communication and Exploitation Strategy

	Non-lease CT 1	T . 200				
	Number of Tweets during a workshop	Twitter analytics	Less than 3	3-7	More than 7	
	Number of online articles making reference to the workshop	Google analytics	Less than 2	2-5	More than 5	
	Number of relevant projects/initiative s identified and contacted/invited at project events	List of	Less than 4	4-12	More than 12	Responsible: EOS, PPHS Accountable: Laurea Consulted: ESPOO, TNO, PLV, Hybrid CoE Informed: All other Partners
Liaison activities and synergies	Number of relevant organisations/co mmunities/expert s identified and contacted/invited at project events	List of attendees	Less than 12	12-30	More than 30	
	Number of cooperation activities (common events and other clustering activities)	Proceedings	Less than 1	2-5	More than 5	
Link to the Commun ity 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, Hybrid CoE, PLV Informed: All other partners
Impact towards	Number of bilateral meetings with Policy makers	Agenda	0-1	2-4	More than 4	Responsible: EOS, Laurea Accountable: PPHS Consulted: ESPOO, TNO, Hybrid CoE, PLV
Policy Makers	Presentations made during events gathering policy makers	Proceedings	Less than 2 a	2-5	More than 5	Informed: All other Partners
Stakehol ders Board	Numbers of members	Proceedings	30-40	40-55	55-70	Responsible: Laurea Accountable: EOS, PPHS, Hybrid CoE Consulted: ESPOO, TNO, PLV Informed: All other Partners

7. DCE: OTHER RELEVANT ISSUES

7.1 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, will 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.

7.2 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) will treated 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.

7.3 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 will handle 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.

ANNEX I: GLOSSARY AND ACRONYMS

Table 10 Glossary and Acronyms

DCE	Dissemination, Communication and Exploitation
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
D	Project deliverable
LEA	Law Enforcement Agency
REA	Research Executive Agency
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
Mol 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 Kibernetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras / Lithuanian Cybercrime Center of Excellence for Training, Research and Education
URJC	Universidad Rey Juan Carlos
MTES	Ministere 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	De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek
SATWAYS	SATWAYS

ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland			
UCSC (UNICAT)	Università Cattolica del Sacro Cuore			
JRC	JRC - Joint Research Centre - European Commission			
MVNIA	Academia Națională de Informații "Mihai Viteazul" / "Mihai Viteazul" National Intelligence Academy			
Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Centre 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	ASOCIACIÓN MALDITA CONTRA LA DESINFORMACIÓN, PERIODISMO, EDUCACIÓN, INVESTIGACIÓN Y DATOS EN NUEVOS FORMATOS			
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheisbereich			
UniBW	Universitaet der Bundeswehr München			

ANNEX II: REFERENCES

- [1] Hybrid Threats, Hybrid CoE, 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] Special attention is required for the unknown threats and the low-tech threats (based on surprising and creative tactics), which are often not in direct focus and attention of practitioners. Therefore a workshop in which also out-of-the-box, nonconfirmist and creative thinkers attend, will be organised, with the aim to find new threats or manifestations of hybrid threats. As described in the DoA.
- [4] The definition of "practitioner" was retrieved by the following website https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156
- [5] Jan Willem Gunnink, project coordinator, COMET, in https://ec.europa.eu/research/participants/data/ref/h2020/other/gm/h2020-guide-comm_en.pdf
- [6] Link to TUOVI: https://sisainenturvallisuus.fi/en/frontpage?p p id=missinglanguageversionnotification WAR languagevers iontoolportlet& missinglanguageversionnotification WAR languageversiontoolportlet missingLanguageVer sion=1

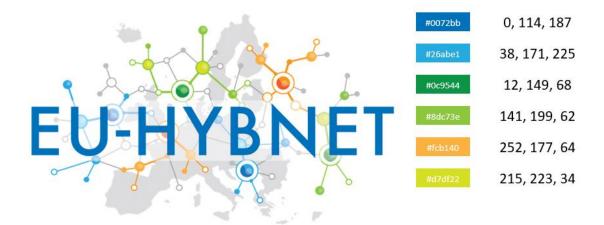
ANNEX III: EU-HYBNET LOGO



Grant Agreement : 883054 Dissemination level :

PUBLIC

ANNEX IV: EU-HYBNET COLOR CODES



PUBLIC

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

Table 11 List of external events relevant for EU-HYBNET

International/European External Events

Name of the Event	Description of the Event	Date of the Event	Location of the Event (Town and Country)
SBSR – Security in the Black Sea Region. Shared challenges, sustainable future Program	International training program organized by MVNIA for young leaders in the Black Sea Region, on countering security threats in the disinformation era	Annual event 3 rd September 2020	Bucharest, Romania
Intelligence in the Knowledge Society	International conference	Annual event	Bucharest, Romania
Security Research Event 2020	International conference	Annual event, 25th-26th November 2020 (tbc)	Bonn, Germany
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.	Annual event, 24th-25th November 2020	
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	Annual event	Munich, Germany

	leading forum for debating international security policy.		
CODE Conference	The conference is dedicated to the German EU Council Presidency and normally lasts for 3 days. On the first day, the focus of the CODE 2020 will be on politics and current cyber security issues in the EU. We look forward to exciting discussions and lectures by high-ranking EU representatives and experts. The second day will include interesting workshops on current cybersecurity relating issues as well as the half-day innovation conference 'Cyber and Information Technology', which is initiated by the German Federal Ministry of Defense. The third day is dedicated to research and our science track.	Annual event, 10th-12nd November 2020	Munich, Germany
Cybersecurity Summer BootCamp (Organised by INCIBE - Spanish National Institute of Cybersecurity)	International cybersecurity training initiative for LEAs and Policy Makers.	Annual event (Summer of each year)	On-line (COVID-19 exceptionality); on-site normally in Spain (Madrid).
International Event for Homeland Security and Civil Defence (Organised by MILIPOL Network)	International conference (a "Global Security Ecosystem" with conferences, exhibitors, official Delegations, etc.)	Annual event (i.e. Paris, 19th- 22nd October 2021)	Paris, France Doha, Qatar Marina Bay Sands, Singapore
European Police Congress	International LEAs Conference	Annual event, 9th-10th February 2021	Berlin, Germany
SMILE Conference	International Conference (The SMILE Conference is the leading training conference devoted to Social Media, the Internet and Law Enforcement initiatives).	Annual event, 14th-18th June 2021	Scottsdale AZ, USA
SICUR – International Security, Safety and fire exhibition	International event (trade fair, conferences)	Annual event, TBD	Madrid, Spain
EICC 2020 : European Interdisciplinary Cybersecurity Conference	International Conference	Annual event, TBD	Rennes, France
PSCE (Public Safety Communication Conference)	International Conference (Is Society Ready for IT? Or is IT Ready for Society? Exploring Societal Readiness for PPDR Innovation)	Annual event, 8th-9th December 2020)	Brussels, Belgium

"Criminal Intelligence – New Trends in Analysis Conference 2020" (CINTIA 2020)	The aim of the conference is to enable knowledge transfer between representatives of agencies, providers of tools for conducting criminal analysis, and representatives of the world of science. By participating in the presentations of new technologies and becoming familiar with the results of research, representatives of law enforcement agencies will gain knowledge that will allow them to improve their criminal analysis process.	23rd-24th September 2020	Krakow, Poland
"Cybercrime.2 – Technologies" ("CP.2- Technologies")	The second edition of the conference addressed particularly to the representatives of Law Enforcement Agencies, public institutions, financial institutions, companies responsible for critical infrastructure protection, employees of the private security sector, academics and companies, as well as institutions dealing with security in cyberspace.	9th-10th November 2020	Warsaw, Poland
Research Day within i- LEAD project	The event provides a space for research initiatives and researchers to deliver presentations directly to security practitioners and procurement specialists from European law enforcement agencies (LEAs). The goal of the meeting is to foster cooperation, supporting an ongoing dialogue between LEAs and the research market.	8th October 2020	The Hague, Netherlands
Protect by training. The importance of awareness in terrorism prevention	International conference on the cooperation of ABW Poland / SOA Croatia special services within the framework of the EU financed project PO WER. In the first part of the conference, a training program for public administration servants on terrorism prevention will be presented. The methodology and tailored training itself was developed on expert knowledge gained from international partners, with whom we have managed to establish cooperation under the abovementioned EU project. The second part of the conference will be devoted to the role and	9th-10th September 2020	Warsaw, Poland

	function of the media, including social media in terrorism prevention.		
SPARTA Day International event, organised by SPARTA network TBD, February Specifically focused on research collaborations in cyber security area.			Brussels, Belgium
Community of Users on Secure, Safe and Resilient Societies (CoU)	CoU had been developed by DG Home (EC) since 2014. Aim of Thematic Workshops is to support to the development of the "Community of Users" needs is pursued through networking events (thematic1 workshops) and reinforcing links with existing international networks and national / regional initiatives.	14th-15th September 2020	Brussels, Belgium
Seminar on societal security at Inland Norway University of Applied Sciences	National training program: Security in the Cyber domain	Annual event, 7th October 2020	Rena, Norway
Disinformation and Fake news	Presentation at Nord University, MA grade.	1st September 2020	Bodø, Norway
European Maritime Day International event, organism the Commission, specific focused on maritime affairs		TBD, Spring 2021, yearly event	Den Helder, Netherlands
National Security Seminar	National event, organised by the Finnish Ministry of the Interior, specifically focused on research and internal security issues not forgetting internal and external security nexus	TBD, January 2021	Porvoo, Finland

ANNEX VI: FACE-TO-FACE/BILATERAL MEETINGS

Table 12 example of face-to-face meeting held by EU-HYBNET Partners

Name of the Events ¹	Date of the Event	Location of the Event (Town and Country)
PLV - Face to face meeting with the Bulgarian Police*	26/03/2018	Sofia, Bulgaria
PLV - Meeting with the Slovenian Ministry of the Interior*	11/12/2018	Ljubljana, Slovenia
PLV - Meeting with the San Sebastian Police*	15/01/2019	San Sebastián, Spain
PPHS - Workshop dedicated only to EU-HYBNET, organized for Polish government institutions	September/October 2020	Poland
TNO - Capability workshop Dutch programme 'Resilience against hybrid threats'. Relevant hybrid capabilities in the Dutch context with Dutch interdepartmental participation	September 2020	The Hague, Netherlands
TNO - Workshop Hybrid in the Artic	17 July 2020	Doorn, The Netherlands
Training program, National Liason officers National training program — Civil-military coordination / Total Defence	Annual event, 2-3 September 2020	Reitan, Norway

 $^{^{1}}$ As an example of national meetings; yearly, EU-HYBNET Partners carry on multiple bilateral meetings with the main LEAs representatives, at a national and/or regional level.

ANNEX VII: EU-HYBNET PARTNERS SOCIAL MEDIA ACCOUNT

Table 13 EU-HYBNET Partners' Social Media Account

Partners	LinkedIn		Twitter	
	Account	Subscribers	Account	Followers
LAUREA	<u>Laurea University of Applied Sciences</u>	18,261	@Laureauas	3,369
PPHS	Polska Platforma	150	@PolishPlatform	145
UIT	<u>UIT The Artic University of Norway</u>	28442	@UiTromso	11,3K
RISE	RISE – Research Institutes of Sweden	45 464	@RISEsweden	5,384
KEMEA	N/A	N/A	N/A	N/A
L3CE	L3CE	2	@L3CE1	
URJC	<u>Universidad Rey Juan Carlos</u>	121,310	@URJC	51,3K
MTES	Ministère de la Transition écologique et solidaire	108 569	@Ecologie_Gouv	180 000
EOS	EOS LinkedIn	957	@EOS_EU	916
TNO	TNO	69.159	@TNO-nieuws	11000
SATWAYS	Satways Ltd	200	@ SatwaysLtd	174
ESPOO	<u>Espoo</u>	13080	@ locateinespoo	339
USCS	<u>Università Cattolica Del Sacro Cuore</u>	183.144	@unicatt	19262
JRC	Joint Research Centre	528123	@EU ScienceHub	42.8k
MVNIA	N/A	N/A	N/A	N/A
Hybrid CoE	N/A	N/A	@HybridCoE	5557
ICDS	ICDS-Tallinn	767	@ICDS_Tallinn	3975
PLV	N/A	N/A	@policialocalvlc	38.2k
ABW	N/A	N/A	N/A	N/A
DSB	<u>Direktoratet for samfunnssikkerhet og bereds</u>	8.671	@dsb.no	21.3k
RIA	RIA	713	N/A	N/A
MALDITA	<u>MALDITA</u>	989	@maldita_es @malditobulo	102 K 277 K
ZITiS	N/A	N/A	N/A	N/A
COMTESSA	Universitaet der Bundeswehr Muenchen	10.333	@unibw	75

ANNEX VIII: DISSEMINATION AND COMMUNICATION POINTS OF CONTACT

Table 14 D&C PoC

Partners	Names	Email	
LAUREA	Paivi Mattila	Paivi.mattila@laurea.fi	
	Artmir Galica	Artmir.galica@laurea.fi	
PPHS	Rashel Talukder	rashel.talukder@ppbw.pl	
	Natalia Jarmuzek	Natalia.jarmuzek@ppbw.pl	
	Steven Ormston	Steven.ormston@ppbw.pl	
	Klaudia Kaczmarek	Klaudia.kaczmarek@ppbw.pl	
UIT	Gunhild Hoogensen Gjørv	Gunhild.hoogensen.giorv@uit.no	
RISE	Rolf Blom	Rolf.blom@ri.se	
KEMEA	Maria Kampa	M.kampa@kemea-research.gr	
	Mirela Rosgova	M.rosgova@kemea-research.gr	
L3CE	Egidija Versinskiené	egidija@l3ce.eu	
	Ruta Ziberkiene	rutzib@mruni.eu	
URJC	Rubén Arcos	ruben.arcos@urjc.es	
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	Maria Chiara Properzi	Maria.properzi@eos-eu.com	
	Elodie Reuge	Elodie.reuge@eos-eu.com	
TNO	Carolina van Weerd	Carolina.vanweerd@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	Gabriela Conțu	gabriela.contu@animv.ro	
Hybrid CoE	Päivi Tampere	paivi.tampere@hybridcoe.fi	
	Emma Lappalainen	emma.lappalainen@hybridcoe.fi	
ICDS	Ivo Juurvee	<u>lvo.juurvee@icds.ee</u>	
	Ramon Loik	Ramon.loik@icds.ee	
	Dmitri Teperik	Dmitri.tepereik@icds.ee	
PLV	Susana Sola	Ssola@valencia.es	
	PLV Corporate email	proyectosplv@valencia.es	

D5.1.1 Dissemination, Communication and Exploitation Strategy

ABW	Pawel Sapiecha	p.sapiecha.cpt@abw.gov.pl	
DSB	Orjan Karlsson	Orjan.Karlsson@dsb.no	
RIA	Märt Hiietamm	mart.hiietamm@ria.ee	
MALDITA	Stéphane M. Grueso	steph@maldita.es	
	Ximena Villagrán	xvillagran@maldita.es	
ZITTIS	Jessica Steinberger	Jessica.Steinberger@zitis.bund.de	
COMTESSA	Stefan Pickl	stefan.pickl@unibw.de	
	Son Pham	son.pham@unibw.de	

ANNEX IX: EU-HYBNET PRESENTATION TEMPLATE

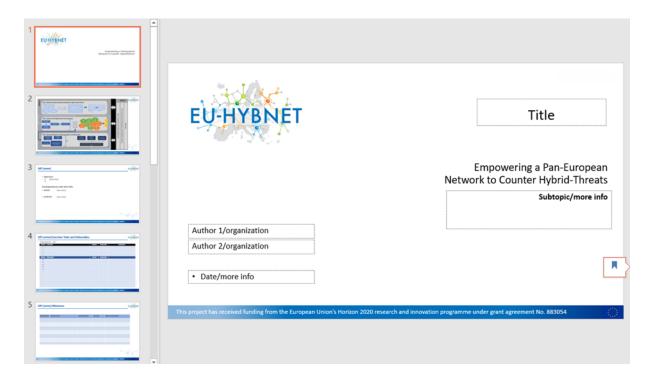
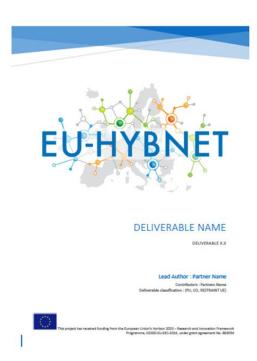
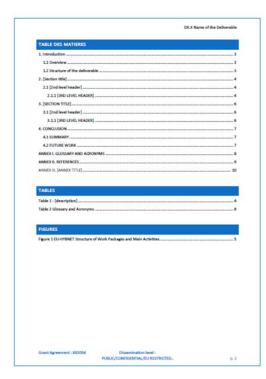


Figure 9 EU-HYBNET Presentation Template

ANNEX X: EU-HYBNET DELIVERABLE TEMPLATE









p. 58

Figure 10 EU-HYBNET Deliverable template