POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

DELIVERABLE 4.16

Lead Author: Hybrid CoE

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme, H2020-SU-SEC-2019, under grant agreement No. 883054

D4.12 1ST POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

Deliverable number:	**D4.16**	
Version:	**V 1.0**	
Delivery date:	**29/04/2025**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	**Hybrid CoE**	**Maxime Lebrun**
Contributors:	**Hybrid CoE**	**Hanne Dumur-Laanila & Sophie Bujold**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	25.04.2025	Maxime Lebrun/ Hybrid CoE	First draft
0.2	25.04.2025	Hanne Dumur-Laanila & Sophie Bujold/Hybrid CoE	Comments
0.3	29.4.2025	Isto Mattila / Laurea	Review
1.0	29.4.2025	Tiina Haapanen / Laurea	Submission to EC

DISCLAIMER

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

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project delivers a series of policy papers, recommendations and briefs on a variety of issues relevant to countering hybrid threats and for different levels of practitioners as appropriate. It is part of WP4, Task 4.4 consolidates the results of WPs 2,3 and 4 in order to present some of the issue findings and area-specific considerations.

The main objective of this document is to collate the different summaries of the policy briefs submitted during the course of the EU-HYBNET project. This report is made of collations of parts of the policy briefs and for administrative purposes only. As such, the responsibility of findings and summaries rests solely with the authors of the policy briefs in question.

The project picture below describes the importance of T4.4 in the flow of project work and results delivery for wider knowledge of pan-European stakeholders.

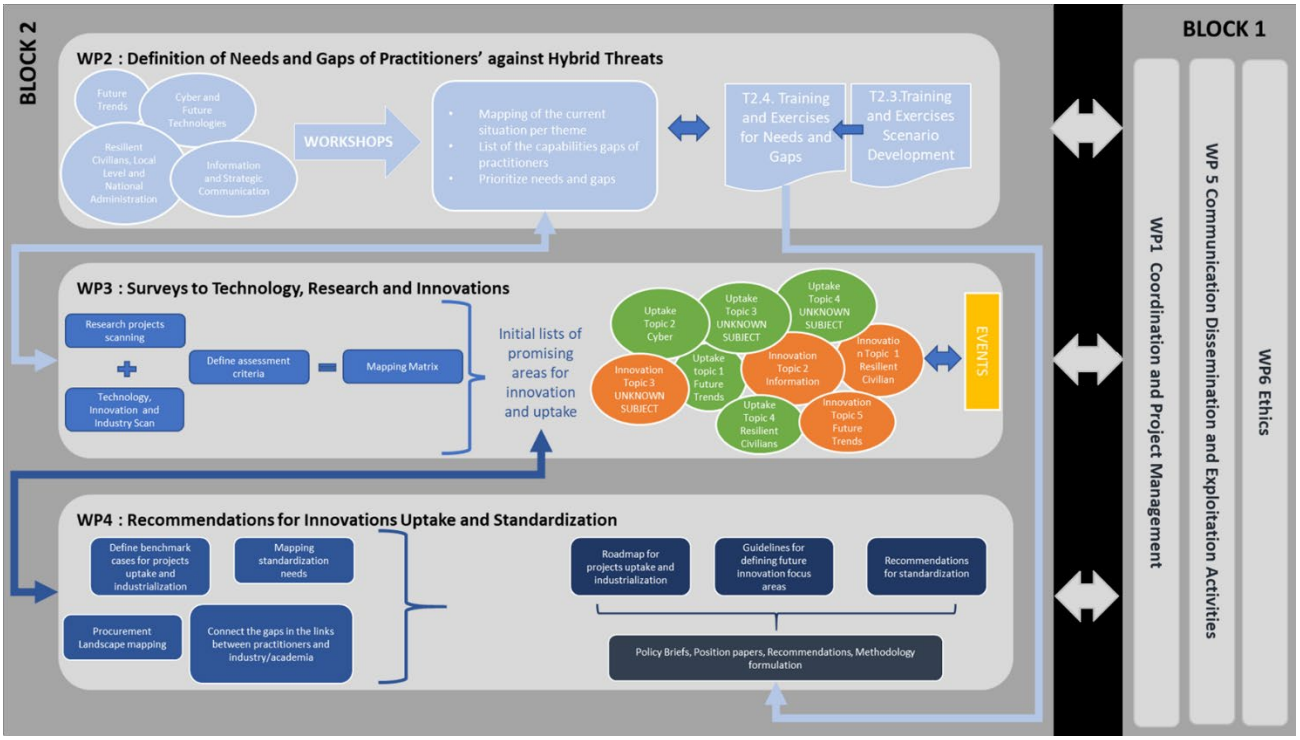

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

This deliverable and in particular the policy briefs delivered by the EU-HYBNET project fulfil following project objective:

OB4: To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats			
Goal		**KPI description**	**KPI target value**
4.4	To facilitate policy dialogues on future European research and innovation focus areas supporting innovation uptake	Policy related briefs written up on core research and innovation actions	-At least 7 policy briefs over 5 years for wider audiences and policy makers

2. SUMMARIES OF THE POLICY BRIEFS

2.1 FRAMING THE INFORMATION DOMAIN VULNERABILITIES, JUNE 2021

Exposing disinformation requires a thorough work on definition of what constitutes harmful content and a solid categorization of manipulative practices in information circulation. The use of algorithms to help identify disinformation in real time requires a thorough ethical approach and standards. Debunking and fact checking must rely on scale and networks constituted from pools of experts. Fact checking should be decentralized to take advantage of and connect expertise, while retaining a margin of manoeuvre for proactive approaches. The horizon of debunking fake news is necessarily reactive, resource consuming and can give unintended audience to fake content and their producers. An anticipatory approach should be privileged instead, whereby target groups could be warned of their being potentially subject to information manipulations.

2.2. COUNTERING HYBRID THREATS: AREAS FOR IMPROVEMENT AND DEVELOPING INNOVATIONS, DECEMBER 2021

Currently identified solutions and innovations focus on enhancing resilience and defensive capabilities. Offensive capabilities to deter or counteract hybrid threats remain a sensitive topic in democracies. However, it might be interesting to also look into this direction in order to broaden the counter hybrid capability portfolio. Citizen trust in government is an essential baseline upon which to improve resilience against hybrid threats. In absence of such trust, the effectiveness of solutions and innovations that involve citizen participation will be low. Policymakers play a vital role in creating and monitoring the frameworks through which possible solutions are developed and implemented, such as frameworks that define legal conditions, privacy regulations and standards for international cooperation.

2.3. INFORMATION MANIPULATION AND INTERFERENCE, FEBRUARY 2022

Develop an IMI taxonomy, which comprises common definitions and required terminology to adequately and precisely describe the IMI threats and approaches. Develop standards for IMI information exchange. Such as standard could take the STIX standard (Standard Threat Information Expression) as a starting point and extend it to cover relevant but missing IMI aspects. STIX allows sharing of information about incidents including actors, vulnerabilities, TTPs etc., in a machine-readable format. Develop a distributed networking solution for IMI information sharing and analysis. The networking solution could take e.g., the European Maritime Security Authority (EMSA) Maritime CISE (Common Information Sharing Environment) networking solution format as a starting point and extend it with capabilities for joint automatic or semi-automatic analysis of IMI data. The networking solution must include functionality which gives the information owner control of which information that is shared with whom. It should also ensure that systems currently in use by different stakeholder for IMI situational awareness and analysis can be accommodated. Initiate research and development in the area of automatic and / or semi-automatic IMI analysis tools. Such tools will be required to cope with the increasing amount of information that has to be monitored, scanned and analysed for IMI activities and/or attacks. As sharing of information related to IMI may be sensitive and block sharing of IMI information, a remedy would be to base joint analysis efforts on federated machine learning methods. Furthermore, it should be considered to

develop AI tools based on behaviour-based AI techniques as they may provide a more reliable solution which also is privacy and freedom-of-speech protecting. Initiate an EU task force investigating how to build trust between private and public sector stakeholders with the aim to make IMI information sharing available, i.e., analyse and propose solution for how to enable participation of private sector stakeholders in IMI information sharing and analysis networks. Issues at hand are how private ownership/control of assets should influence possibilities to participate, trust issues in general and barriers against sharing of secret or sensitive information, etc.

2.4. FAME ON SOCIAL MEDIA, A NEW CURRENCY OF CYBERCRIME? FEBRUARY 2023

The novel exposure of cybercriminal groups in the public space brings with it a brand-new set of challenges and opportunities From 2013 to the present, ransomware attacks have become more sophisticated, and cybercriminals have set up groups that work just like any company, diversifying its products and selling them to third parties The emergence of public dissemination channel claiming attacks, polling leaks and disseminating technical advice elicits commentary and publicity which creates a social media pressure. State sponsored cyberwarfare on an unprecedented scale is an unexpected consequence of the Russian invasion of Ukraine. The public attention that these attacks are getting, and the normalization of cybercrime as a valid, publicly lauded, even state sponsored activity is also attracting users from a younger generation. A strong and fast answer to this new reality is needed, where technical expertise must go hand in hand with timely communication, flexible strategies to attract new talent and, above all else, a true information exchange platform at European level that can be used as a knowledge repository.

2.5. ON INFORMATION SHARING BETWEEN CRITICAL ENTITIES FOR EARLY AND EFFICIENT DETECTION AND MITIGATION OF HYBRID THREATS, DECEMBER 2024

Hybrid threats are complex challenges that exploit societal weaknesses and undermine democratic societies. These threats combine traditional, unconventional, and cyber tactics, often causing cascading effects across different domains. Current protection strategies focus on asset protection, neglecting interdependencies and risks. This policy brief, based on the WINS methodology, proposes enhancing resilience through effective information sharing. The European Union's Critical Entities Resilience (CER) Directive emphasizes the need for comprehensive risk assessments and measures to ensure uninterrupted essential services. To manage hybrid threats, early detection and information sharing between critical entities is crucial. The brief recommends identifying essential information, termed Indicators of Hybrid Threats (IoHT), and using privacy-preserving technologies for secure data sharing and analysis. These steps will enable rapid detection and mitigation of hybrid threats, fostering resilience across various sectors and domains.

2.6. REFLECTIONS ON THE USE OF THE DTAG METHODOLOGY FOR EU-HYBNET TRAININGS (2020-2025), FEBRUARY 2025

The EU-HYBNET project was designed to have three full cycles (with a fourth cycle that is a wrap-up of all project components), each starting with the identification of European practitioners' gaps and needs in countering hybrid threats and ending with recommendations for innovation up-take and standardization2. One of the components of each cycle were the Training and Exercise activities, which were considered essential to increase participants' (such as industry, practitioners, academia, law enforcement agencies experts, etc.) knowledge about hybrid threats and how to counter them. Innovations were selected based on the project findings, and the most promising ones were then integrated into the training scenario. The goal, in addition to increasing participants' understanding of hybrid threats and testing the chosen innovations, was to present participants with the existing technological and non-technical solutions that can increase their knowledge of the potential of using innovations in countering hybrid threats. Further, the trainings were also beneficial in facilitating dialogue as well as the exchange of best practice and ideas among participants.

3. CONCLUSIONS

With six policy briefs published over the course of 5 years, the project has almost achieved its Key Performance Indicator on task 4.4. Policy briefs consolidated results from project proceedings and were authored by Consortium partners as well as network members. This task thus helped getting the network to work together in a collaborative fashion.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU -HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats
EU	European Union
CER	Critical Entities Resilience
IoHT	Indicators of Hybrid Threats
IMI	Information Manipulation and Interference
STIX	Standard Threat Information Expression
CISE	Common Information Sharing Environment
EMSA	The European Maritime Security Authority
OB	Objective
T	Task
WP	Work Package
WINS	What Information Needs to be Shared
KPI	Key performance Indicator
DTAG	Disruptive Technology Assessment Game