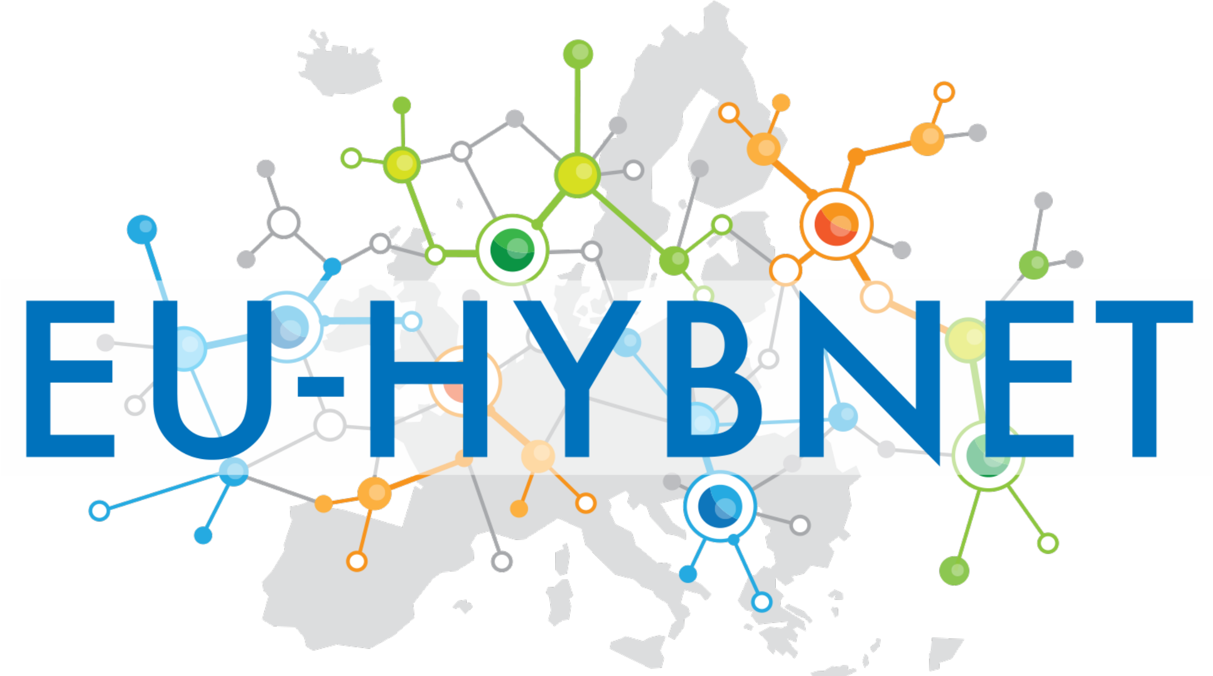

3RD POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

DELIVERABLE 4.14

Lead Author: Hybrid CoE

Contributors: RISE, Laurea

Deliverable classification: Public (PU)

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

D4.14 3RD POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

Deliverable number:	**D4.14**	
Version:	**v1.0**	
Delivery date:	**20.11.2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	**Hybrid CoE**	**Maxime Lebrun, Hanne Dumur-Laanila, Sophie Bujold**
Contributors	**RISE**	**Rolf Blom**
	Laurea	**Päivi Mattila, Isto Mattila, Jari Räsänen, Petteri Partanen**

DOCUMENT CONTROL

Version	Date	Authors	Changes
v0.1	17.10.2024	Hanne Dumur-Laanila	First draft
v0.2	25.10.2024	Maxime Lebrun	Editing
v0.3	25.10.2024	Hanne Dumur-Laanila	Editing
v0.4	28.10.2024	Hanne Dumur-Laanila & Sophie Bujold	Editing
v0.4	4.11.2024	Petteri Partanen, Jari Räsänen, Isto Mattila	Review
v0.5	18.11.2024	Tiina Haapanen	Text editing
v1.0	20.11.2024	Tiina Haapanen	Final text editing and submission to EC

DISCLAIMER

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

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

TABLE OF CONTENTS

FIGURES

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. This work is conducted as part of Work Package (WP) 4, Task 4.4, which 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 describe policy briefs, position papers, and recommendations reports delivered in EU-HYBNET WP 4 "Recommendations for Innovations Uptake and Standardization", Task (T) 4.4 "Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge" and their importance to the project. The project picture below describes the importance of T4.4 in the flow of project work and results delivery for increased knowledge of pan-European stakeholders.

This report will outline the policy brief "On Information Sharing between Critical Entities for Early and Efficient Detection and Mitigation of Hybrid Threats".

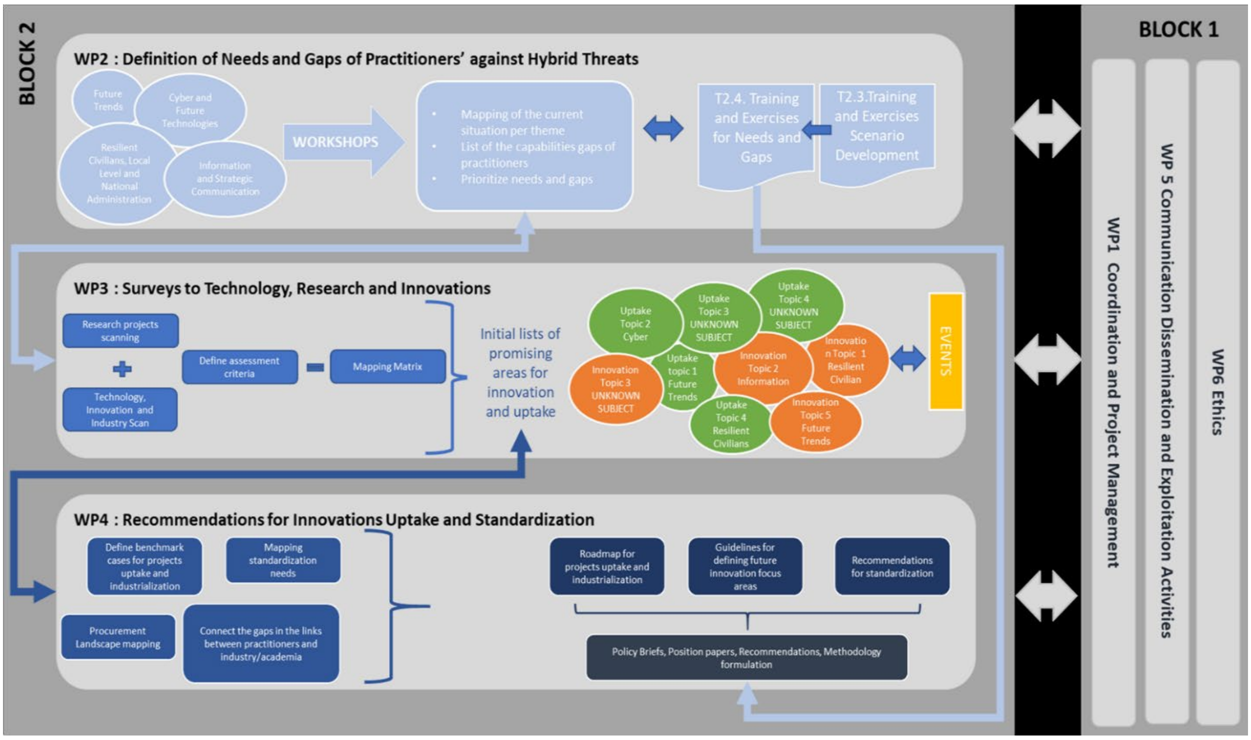
BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities gaps of practitioners
Prioritize needs and gaps
T2.4. Training and Exercises for Needs and Gaps
T2.3.Training and Exercises Scenario Development
WP3 : Surveys to Technology, Research and Innovations
Research projects scanning
Technology, Innovation and Industry Scan
Define assessment criteria
Mapping Matrix
Initial lists of promising areas for innovation and uptake
Uptake Topic 2 Cyber
Uptake Topic 3 UNKNOWN SUBJECT
Uptake Topic 4 UNKNOWN SUBJECT
Innovation Topic 3 UNKNOWN SUBJECT
Uptake topic 1 Future Trends
Innovation Topic 2 Information
Innovatio n Topic 1 Resilient Civilian
Uptake Topic 4 Resilient Civilians
Innovation Topic 5 Future Trends
EVENTS
WP4 : Recommendations for Innovations Uptake and Standardization
Define benchmark cases for projects uptake and industrialization
Mapping standardization needs
Procurement Landscape mapping
Connect the gaps in the links between practitioners and industry/academia
Roadmap for projects uptake and industrialization
Guidelines for defining future innovation focus areas
Recommendations for standardization
Policy Briefs, Position papers, Recommendations, Methodology formulation
BLOCK 1
WP1 Coordination and Project Management
WP 5 Communication Dissemination and Exploitation Activities
WP6 Ethics

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 the following project objective:

OB4: To indicate priorities for innovation uptake and industrialization and to determine priorities for standardization for empowering the Pan-European network to effectively counter hybrid threats			
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

1.2 STRUCTURE OF THE DELIVERABLE

This deliverable will only briefly introduce the key points of both policy briefs and will not duplicate those briefs at length. This document includes the following sections:

- Section 1: Describes the object of policy briefs in the project.
- Section 2: Provides an introduction of the policy brief this report is based on.
- Section 3: Highlights key findings of the fourth policy brief.
- Section 4: Describes the contribution of T4.4. and D4.12 to the “Three Lines of Actions” (LoA) of the project.
- Section 4: Provides conclusions.

2. POLICY BRIEF “ON INFORMATION SHARING BETWEEN CRITICAL ENTITIES FOR EARLY AND EFFICIENT DETECTION AND MITIGATION OF HYBRID THREATS”

Hybrid threats are complex challenges that exploit societal weaknesses and undermine democratic societies. Hybrid threats combine traditional, unconventional, and cyber tactics causing cascading effects across different domains. Current protection strategies focus on asset protection, neglecting interdependencies and risks. The policy brief *On Information Sharing between Critical Entities for Early and Efficient Detection and Mitigation of Hybrid Threats*, based on the WINS (What Information Needs to be Shared) methodology, proposes enhancing resilience through effective information sharing.

The policy brief was written by Rolf Blom from RISE and Päivi Mattila from Laurea. The goal of the current report is to present the main findings.

3. CONTENT AND FINDINGS

To better counter hybrid threats, early detection and information sharing between critical entities is crucial. The policy 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.

While the recent Critical Entities Resilience (CER) Directive stresses the importance of comprehensive risk assessments, *Indicators of Hybrid Threats* (IoHT) need to be identified using privacy-preserving technologies for secure data sharing and analysis. Critical entities must maintain a solid overview of the risks they face.

The policy brief recommends two key actions: (1) identify and define essential information that must be shared and (2) explore the implementation of privacy preserving techniques to facilitate such sharing. An efficient information-sharing solution enables rapid analysis using various AI methods, allowing for near-real-time detection of hybrid threats and facilitating early mitigation actions.

The first step in adopting this proposal should be entrusted to the research community for determining and validating the specific methods for sharing IoHT information to be used and the results that can be achieved. The subsequent steps would involve developing an efficient sharing platform and introducing it across EU Member States and critical entities.

4. THE THREE LINES OF ACTION

This deliverable and especially the reports serve the following two Lines of Action (LoA):

LOA 2 - common requirements as regards innovations that could fill in gaps and needs;

LOA 3 - priorities as regards of increasing knowledge and performance requiring standardization.

5. CONCLUSION

The policy brief suggests that the European Commission extends the CER Directive to include the near-real-time cross-domain sharing of IoHT. The European research community is asked to propose sets of sufficient and needed IoHT and validate that sharing this information would allow for the detection of hybrid threats with required performance measures; propose an architecture and tools for near-real-time analysis of the shared IoHT to detect hybrid threats, propose mitigating actions, and predict possible next step attacks and propose efficient privacy-enhancing technology for data sharing and analysis of the IoHT. Further, the policy brief suggests that the European Commission procures the implementation of a first live test and demonstration solution.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
AI	Artificial Intelligence
EU	European Union
CER	Critical Entities Resilience
IoHT	Indicators of Hybrid Threats
LoA	Line of Action
OB	Objective
T	Task
WP	Work Package
WINS	What Information Needs to be Shared
KPI	Key performance Indicator
Laurea	Laurea University of Applied Sciences
RISE	Research Institutes of Sweden

ANNEX II. REFERENCES

[1] European Commission Decision C (2014)4995 of 22 July 2014.

[2] Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.

6. ANNEX III. EU HYBNET PUBLISHED POLICY BRIEFS

EU-HYBNET Policy Brief No1. – Framing the Information Domain Vulnerabilities - June 2021. https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No2. – Countering Hybrid Threats: Areas for Improvement and Developing Innovations – December 2021 https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No3. – Sharing information manipulation and interference (IMI) information – February 2022 https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No4. – Fame on social media, a new currency of cybercrime? – February 2023 https://euhybnet.eu/policy-briefs/

EU-HYBNET Policy Brief No5. – On Information Sharing between Critical Entities for early and efficient detection and mitigation of Hybrid Threats – October 2024 https://euhybnet.eu/policy-briefs/