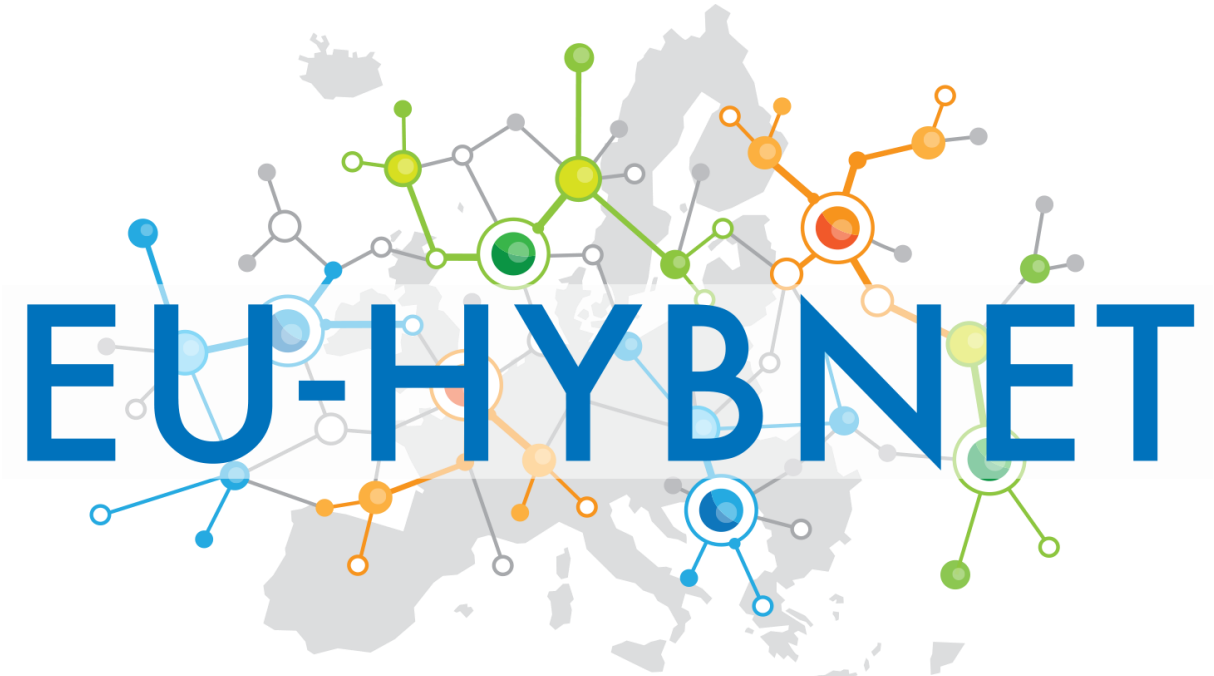

1ST POLICY BRIEFS, POSITION PAPERS, RECOMMENDATIONS REPORT

DELIVERABLE 4.12

Lead Author: Hybrid CoE

Contributors: KEMEA, TNO, EOS, Laurea, MTES
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

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

Deliverable number :	**D4.12**	
Version:	**V 1.0**	
Delivery date:	**28/2/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	**Hybrid CoE**	**Maxim Lebrun**
Contributors:	**KEMEA**	**Panagiota Benekou**
	EOS	**Elodie Reuge, Maguelone Laval**
	TNO	**Okke Lucassen, Rick Meessen**
	Laurea	**Päivi Mattila, Jari Räsänen**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	21.12.2021	Maxime Lebrun/ Hybrid CoE	First draft
0.2	4.1.2022	Panagiota Benekou/ KEMEA	Review
0.3	4.1.2022	Elodie Reuge and Maguelone Laval/ EOS	Review and comments for improvements
0.4	5.1.2022	Päivi Mattila/ Laurea	Review and comments for improvements
0.5	7.1.2022	Okke Lucassen, Rick Meessen/ TNO	Review and comments for improvements
0.6	17.2.2022	Jari Räsänen/ Laurea	Review and comments for improvements
0.7	17.2.2022	Géraldine Ducos, Antoine-Tristan Mocilnikar, Philippe Lorec, Christian Despres/ MTES	Review and comments for improvements
0.8	17.2.2022	Maxime Lebrun/ Hybrid CoE	Text editing
0.9	17.2.2022	Päivi Mattila/ Laurea	Review and comments for improvements
0.91	22.2.2022	Maria Soukkio/ Hybrid CoE	Text editing and document for submission
0.92	23.2.2022	Päivi Mattila/ Laurea	Text editing and final comments for Hybrid CoE
0.93	1.3.2022	Maria Soukkio/ Hybrid CoE	Text editing and document for submission
1.0	1.3.2022	Päivi Mattila/ Laurea	Final review and submission of the document to the EC.

DISCLAIMER

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

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

TABLE OF 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. 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 describe policy briefs, position papers and recommendations reports delivered in EU-HYBNET Work Package (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 proceeding. Three policy briefs will be highlighted in this document:

- *Patterns of information manipulations* (June 2021) by Hybrid CoE and KEMEA
- *Countering Hybrid Threats: Areas for Improvement and Developing Innovations* (December 2021) by TNO
- *Building Societal Resilience – Sharing Information Manipulation and Interference (IMI) Information* (February 2022) by RISE

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.

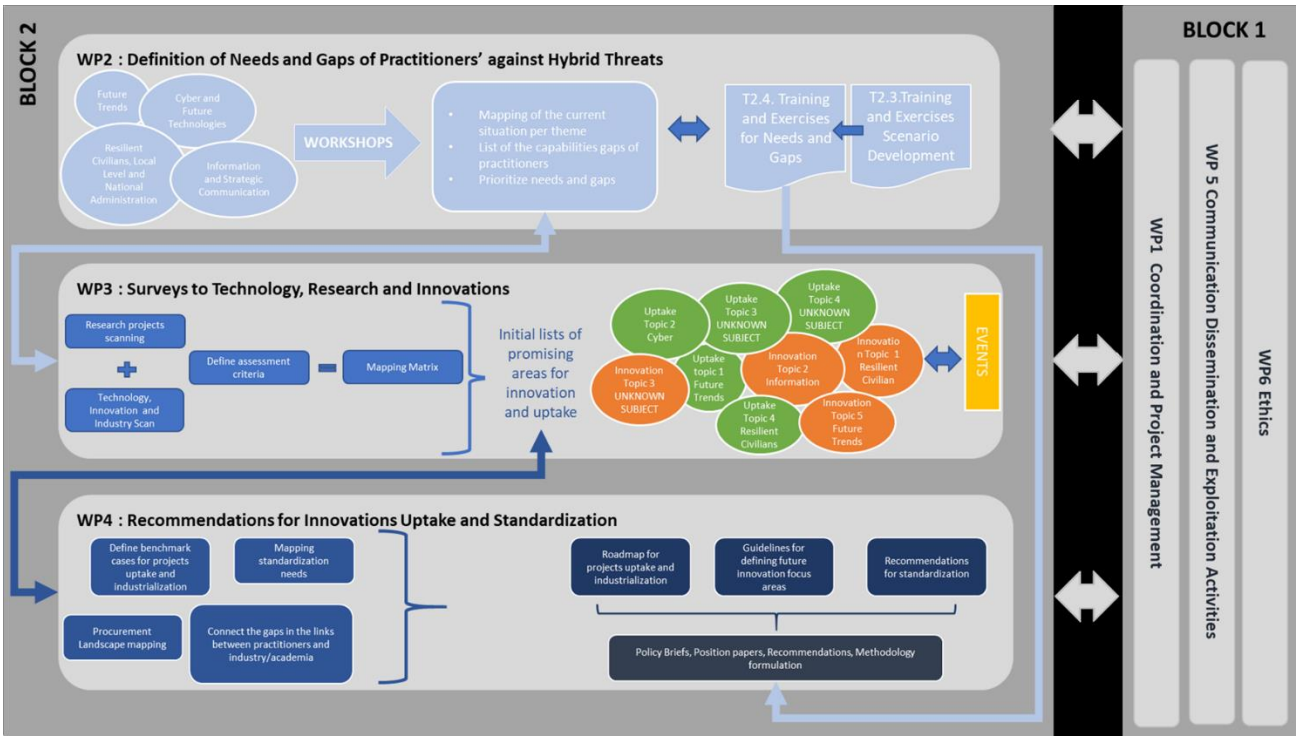

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

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

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 proper. This document includes the following sections:

- Section 1: In this section introduction to the D4.12 content is given.
- Section 2: Highlights the key findings of the 1st EU-HYBNET Policy Brief "*Framing the Information Domain Vulnerabilities*"
- Section 3: Describes the key findings of the 2nd EU-HYBNET Policy Brief "Co*untering Hybrid Threats: Areas for Improvement and Developing Innovations*"
- Section 4: Presents the key findings of the 3rd EU-HYBNET Policy Brief "*Sharing information manipulation and interference (IMI) information*
- Section 5: Describes the contribution of T4.4. and D4.12 to the "Three Lines of Actions" (LoA) of the project
- Section 6: Provides conclusion and way forward and future work

2. POLICY BRIEF ON FRAMING THE INFORMATION DOMAIN VULNERABILITIES

2.1 CONTENT AND FINDINGS

This policy brief collected a series of preliminary findings and ongoing work of the EU-HYBNET project in Work Packege 2, 3 and 4, in light of EU policy and regulatory developments in the field of digital platforms, information and cyber security. From the manifold insights gathered at this occasion, the following elements stand out the most.

2.1.1. THE WEAKENING OF THE BUSINESS MODEL OF JOURNALISM

Information circulation patterns in digital public spaces blur the separation between the steps of reception and conversation. Social media gives conversation a visible, public and potentially superseding character by comparison, to the content of the information itself. The diffusion of information on social media is unhinged, viral and undergoes little to no control mechanism.

2.1.2. THE SOCIAL DEMAND FOR DISINFORMATION, MISINFORMATION AND MANIPULATED INFORMATION

EU-HYBNET has identified social exclusion as a core vulnerability because the circulation of content associated with disinformation cannot solely be explained by irrationality or media illiteracy. Individual actors are empowered to offer and promote their opinion online and individuals tend to believe less in the information itself than to adhere to a worldview that corresponds to it.

2.1.3. THE DESTABILIZING AND DISPROPORTIONATE EFFECTS OF HYPER PERSONALIZED TARGETING

Individual behaviours became computable and predictable through the use of algorithms exploiting massive amounts of personal data, traces and signals online. This led to a significant possibility to anticipate, entice or discourage individual behaviour. The conjunction of advanced algorithms, computational power and massive amounts of data allows for the interpretation of the social world starting from individual levels.

3. COUNTERING HYBRID THREATS: AREAS FOR IMPROVEMENT AND DEVELOPING INNOVATIONS

3.1 CONTENT AND FINDINGS

This policy brief stems from an assessment of innovations and various solutions presented throughout the EU-HYBNET project thus far, analysed and compiled by TNO. In particular, it found that offensive capabilities remain a sensitive topic for development in countering hybrid threats. It identified that a strong bond of trust between citizens and their government is essential to remain resilient against hybrid threats. The report proceeds through six innovations.

3.1.1. FAKE NEWS EXPOSER

Using content and metadata via a software tool that could indicate the degree of fabrication of information pieces.

3.1.2. GUIDES TO IDENTITY FAKES

Public guides for the wider public information about verification and veracity methods in the reception of information.

3.1.3. DEBUNKING FAKE NEWS

Fake news exposer and guides to be used for feeding into an online platform as an independent crowdsourced analytical centre.

3.1.4. STRATEGIC PERSONALIZED ADVERTISING

The idea is to personally advertise the right information, for the right person at the right moment and especially the ways in which the information is trustful.

3.1.5. CROSS SECTOR CYBER THREAT INFORMATION SHARING

Lack of trust and sharing willingness create gaps in collaboration and therefore anticipation and countering of cyber-enabled hybrid threats.

3.1.6. PUBLIC PRIVATE INFORMATION SHARING GROUPS FOR COLLABORATIVE INVESTIGATIONS AND COLLECTIVE ACTION

Ethical and social acceptability questions as well as legal frameworks for devising solutions to aspects of hybrid threats are critical. Some of the solutions presented above present significant risks of blowback and could undermine the core of liberal democracies if implemented and abused.

4. BUILD SOCIETAL RESILIENCE – SHARING INFORMATION MANIPULATION AND INTERFERENCE (IMI) INFORMATION

This policy brief is based EU-HYBNET Task4.2 "Strategy for Innovation uptake and industrialization" and its results presented in project deliverable 4.4 "1st Innovation uptake, industrialisation and research strategy" by Research Institutes in Sweden (RISE).

4.1. CONTENT AND FINDINGS

The main question is how to build and improve societal resilience against national and foreign information manipulation and interference (IMI) activities and campaigns. This is a key basis for early detection and joint actions to counter IMI activities.

The policy paper stresses the need to:

- **Develop an IMI taxonomy**
- **Develop standards for IMI information exchange**.
- **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
- **Initiate research and development in the area of automatic and / or semi-automatic IMI analysis tools**.
- **Initiate an EU task force on building trust between private and public sector stakeholders** with the aim to make IMI information sharing available.

5. 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.

6. CONCLUSION

6.1 SUMMARY

While the policy brief of "*Framing the Information Domain Vulnerabilities*" highlighted a series of gaps and needs, common requirements for practitioners involved in the field of countering disinformation and misinformation, the policy briefs of "*Countering Hybrid Threats: Areas for Improvement and Developing Innovations*" and "*Sharing information manipulation and interference (IMI) information*" presented a series of findings which stemmed from the EU-HYBNET project proceeding, and especially in terms of evaluating the innovations and their associated needs.

6.2 FUTURE WORK

The next policy brief is planned to address ethical considerations in countering hybrid threats. It is an especially important topic since hybrid threat actors intend to discredit democratic systems, the rule of law and human rights in order to advance more authoritarian strategic objectives. The topic is also under EU-HYBNET's Ethics Advisory Group work and concern. The way in which democracies countering hybrid threats manage not to undermine their own values in response is a key stake of strategic importance. This policy brief is expected to be ready during 2022. The project will also deliver other policy briefs according to recognized key project findings important to be addressed in a policy brief or in a positon paper.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
LoA	Line of Action
OB	Objective
T	Task
WP	Work package
KPI	Key performance Indicator
IMI	Information Manipulation and Interference

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.

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/