10TH SIX MONTH ACTION REPORT

DELIVERABLE 1.14

Lead Author: Laurea

Contributors: All partners
Deliverable classification: Public (PU)

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

D1.14 10TH SIX MONTH ACTION REPORT

Deliverable number:	**1.14**	
Version:	**1.0**	
Delivery date:	**30/04/2025**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	Isto Mattila	**Laurea**
Contributors:	Tiina Haapanen	**Laurea**
	Input to the report from all consortium partners due to their project work in various Tasks and events as contributors	**MTES, URJC, Hybrid CoE, PPHS, KEMEA, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, RISE, UCSC, Maldita, COMTESSA, ZITiS, L3CE, UiT**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	14/04/2025	Tiina Haapanen/Laurea	Deliverable template update and first draft
0.2	22/04/2025	Isto Mattila/Laurea	Drafting
0.3	24/04/2025	Isto Mattila/Laurea	Text editing
0.4	28/04/2025	Isto Mattila/Laurea	Text editing
0.5	29/04/2025	Tiina Haapanen/Laurea	Content delivery
0.6	30/04/2025	Isto Mattila/Laurea	Text editing
1.0	30/04/2025	Tiina Haapanen/Laurea	Final editing and document submission to the EC

DISCLAIMER

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

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

TABLE OF CONTENT

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The goal of the *Empowering a Pan-European Network to Counter Hybrid Threats* (EU-HYBNET) project deliverable (D) 1.14 "*Tenth Six Month Action Report*" in project month (M) 60/Apr 2025 is to describe how the project has proceeded from M55 until end of M60 of the project (November 2024 – April 2025). According to the European Commission (EC), *"three lines of action*" are mandatory to report according to the Horizon2020 Secure Societies Programme/General Matters-01-2019 funded projects. The *"three lines of action*", also mentioned in the EU-HYBNET Description of Action (DoA).

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1. Provides an overview of the document content.
- Section 2. Describes the project and its progress.
- Section 3. Describes how the project activities from the project months 55 - 60 (November 2024 – April 2025) have contributed to the EC's requested "three lines of action" activities.
- Section 4. Conclusions of the last six-month period of the project (November 2024 - April 2025).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.14 "*Tenth Six-Month Action Report*" is part of EU-HYBNET Work Package (WP) 1 «*Coordination and Project Management* » Task (T) 1.1 «*Administrative, Financial Planning and Coordination* ». Generally speaking, the EU-HYBNET six-month action reports are mandatory progress reports to the EC. The reports support both the EC and the project itself to estimate if the project delivers consistent results according to the project's core activities, the Grant Agreement (GA), and the Description of Action (DoA).

The EU-HYBNET six-month action reports, such as D1.14, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.14 is to provide a general update on how the project reaches the results mentioned in the project objectives and KPIs. We have highlighted this in the figure below, showing the role of WP1 to support and guide project WPs 2-4, where the main project activities take place, and the core project results are achieved.

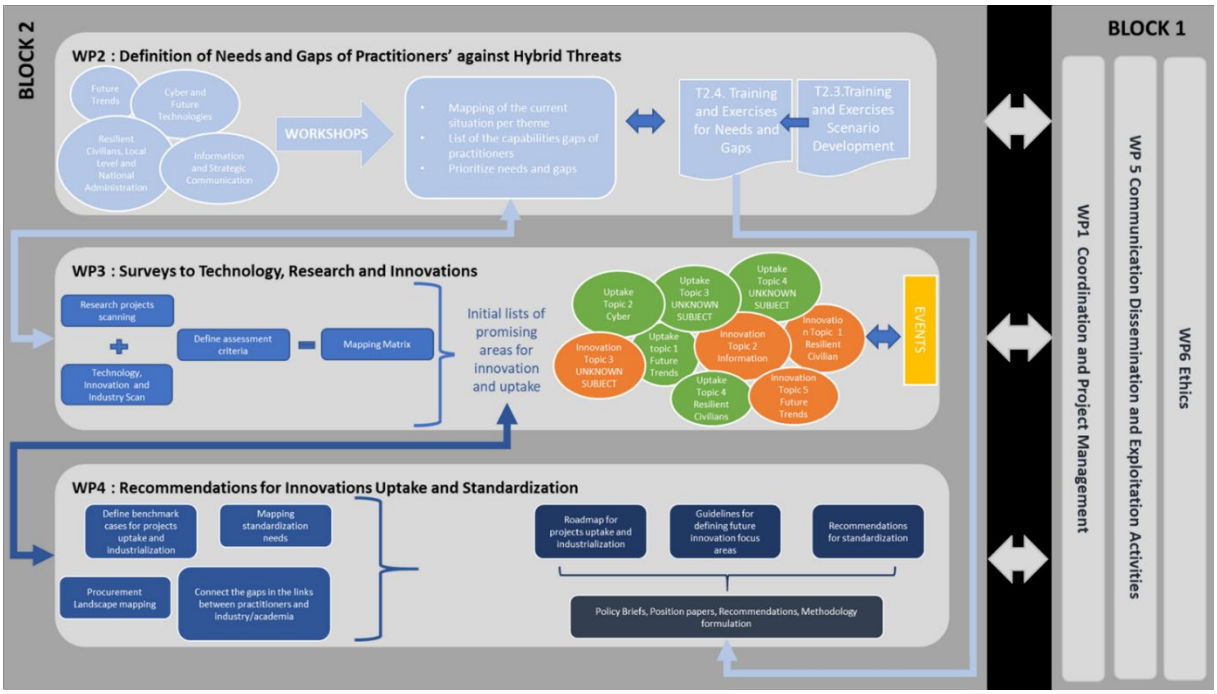

Figure 1: EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in EU-HYBNET Six-Month Action Reports are often linked to the project milestones (MS) achieved during the last six-month period. During D1.14 reporting period, project Milestones set for the project are as follows:

MS number.	MS action description
29	4th Policy briefs, Position Papers, or Recommendations documents are published
15	Final Gaps and Needs Evaluation
24	Strategy ready for innovation uptake and industrialisation
38	5th Annual workshop
25	Standardization Recommendation ready
30	Policy briefs, Position Papers, or Recommendations documents are published
9	5th EU HYBNET Project Management Board meeting
10	EU HYBNET Network Sustainability Final Report

Table 1: Milestones M55-M60

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The Tenth Six-Month Action Report (D1.14) main author is Laurea, the organization responsible for the delivery of D1.14. However, EU-HYBNET work package (WP) and task (T) leaders have also provided information on the tasks they are responsible for and have been working on during the sixth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager and Network Manager have contributed to D1.14 by providing general remarks on the project's general progress and innovation uptake.

3. PROJECT PROCEEDINGS

3.1 MONITORING OF RESEARCH AND INNOVATION PROJECTS WITH A VIEW TO RECOMMENDING THE UPTAKE OR THE INDUSTRIALISATION OF RESULTS

Final Gaps and Needs Evaluation

The first "Three Lines of Action" reporting is coming from the EU-HYBNET Task (T)2.1 "Final evaluation of Gaps and Needs (lead by Hybrid CoE). The overall goal of the Gaps and Needs events of the EU-HYBNET project has been to identify and understand what kind of gaps and needs European practitioners may have in countering hybrid threats so that the analysis would stem from concrete observations and experiences. In the EU-HYBNET project, "gaps" represent the space between the current and best practices and "needs" are the resources required to fill those gaps.

The methodology to collect data during each Gaps and Needs event has evolved each year after analysing the results. This approach should be considered as a natural process in a long-term project. The DoA provides enough space to make the necessary modifications, so that in the end, the project has data that expose the identified gaps and needs from multiple perspectives associated to the constantly evolving hybrid threat landscape.

Each event has produced new insights for the EU-HYBNET project to work with and fundamentally, each event has created a space for participants to gain a deeper understanding of hybrid threats and how they evolve over time. The Gaps and Needs events have also been a great networking opportunity, relating directly to one of the main project objectives, which is to facilitate a large, pan-European network consisting of diverse organizations and expertise.

The four core themes: *Cyber and Future Technologies* (led by L3CE), *Information and Strategic Communications* (led by URJC), *Resilient Civilians, Local and State Administration* (led by UiT), and *Future Trends of Hybrid Threats* (led by Hybrid CoE) have been an integral part of the T2.1 work throughout the project's life span.

In addition, *the Landscape of Hybrid Threats: A conceptual model*[1] and the *Hybrid Threats: A Comprehensive Resilience Ecosystem (CORE) model*[2] have played an important part in all EU-HYBNET work since its publication in 2023 but especially under T2.1. The CORE model was used for the first time during the 3rd Gaps and Needs event intending to have a better understanding of which areas (governance space, civil space, services space) threats, gaps, and needs are located in.

GAPS and NEEDS Priority areas

The following priority areas guided the discussions in each core theme group to articulate the gaps that the priorities suggest, and the type of resources that are needed to fill in the identified gaps. The priority areas designate a field of inquiry to focus on to better characterize threats and their potentialities, but also responses and solutions for improved preparedness and anticipation. Priority areas need to be identified for a better understanding of specific gaps and needs. The priority areas highlight important observations that are relevant to consider in crafting responses to hybrid threat activity.

1. Core Theme 1: Future Trends of Hybrid Threats
2. Core Theme 2: Cyber and Future Technologies
3. Core Theme 3: Resilient Civilians, Local Level and National Administration
4. Core Theme 4: Information and Strategic Communications

The overall goal of the Gaps and Needs Events was to understand the different perspectives of the entities participating in EU-HYBNET. Concrete observations and experiences from the participants formed the bedrock of the work of analysis. This approach was selected as it was not possible to define the gaps and needs of each organization individually in countering hybrid threats. Adopting a cross-domain approach throughout the project has been a consistent need, as it proved unworkable to focus on specific organizational gaps and needs. Organizations were understandably unwilling to open up extensively on the operational challenges they would face at a working level. This has been an obvious limitation to the granularity of findings that could be expected at the onset of the project. It must be noted that this made it necessary to deviate from the expected output. Nevertheless, the successive gaps and needs methodologies have endeavoured to gather as many perspectives as possible qualitatively through in-depth discussions.

The final Gaps and Needs event in Madrid had an obvious stocktaking perspective (12.6.2024). This guided the delineation of the different priority areas and their shortlisting by the participants. Gaps and Needs analyses have provided a series of snapshots of disparate yet interconnected considerations to account for better responses to hybrid threats at the European level. The Gaps and Needs events, as well as the EU-HYBNET project, have had a positive impact on connecting diverse actors throughout activities, communication, and common work. The priority areas and potential gaps and needs stemming from them result from interactions and qualitative crowdsourced data collection with strong organizational and individual perspectives on them. The results of EU-HYBNET should be used to create indicators, among others, to craft better policies in countering hybrid threats. The pitfalls associated with the successive methodologies, which were crafted in a spirit of continual improvement, could also be of use for organizing similar crowdsourced data collection events at the Commission level, for instance, in the framework of "Community for European Research and Innovation for Security" (CERIS) activities. Defining expectations realistically and providing a safe space and method for organizations to share their vulnerabilities would prove beneficial in maintaining a nuanced and granular approach to findings.

The results of this final deliverable will feed into T2.2. by providing topics for the 5th year articles and for Work Package 3 (D3.10), "Final Report on Innovation and Research Monitoring", as an input to scan and monitor potential research and innovations that can cover the gaps, needs and requirements.

3.1.1 DEFINITION OF TARGET AREAS FOR IMPROVEMENT AND INNOVATIONS

Final Report on Innovation and Research Monitoring

EU-HYBNET's Task (T) 3.3 "Ongoing Research Projects Initiatives Watch" deliverable "Final Report on Innovation and Research project Monitoring" (D3.10) is focused on reflecting the work done during the three previous cycles of T3.3, reflecting on the practical application of used method, and consolidating final recommendations relevant beyond the end of the project (April 2025).

In the same ways as the whole EU-HYBNET project, Deliverable D3.10 is structured around Core Themes:

• Resilient Civilians, Local Level and Administration

• Cyber and Future Technologies • Information and Strategic Communications

• Future Trends of Hybrid Threats

Analysing the Core Themes, all 3 deliverables (of three cycles) and D2.8 "Final evaluation of Gaps and Needs" were reviewed in a consolidating manner. Within this deliverable, we avoid chronological review but rather take all three iterations' material as a consolidated body of knowledge. Still, observations about how similar topics are iterated over cycles may be important to emphasize.

There was a notable difference in the research scanning process used in D3.7, the first iteration of the task T3.3 "Ongoing Research Projects Initiatives Watch", and the subsequent two deliverables D3.8 and D3.9. Every deliverable in detail describes the process used, here, we aim to highlight key differences.

As an initial step, all iterations started their work from analysis of T2.1, "Needs and Gaps Analysis in Knowledge and Performance" and its relevant Deliverable iteration. In this task practitioners of hybrid threats identified relevant hybrid threat areas, defined the gaps which expose countries to the threats, and pointed to needs which must be filled to mitigate risks.

EU-HYBNET was structured through the 4 core themes, so T3.3 deliverables consistently stuck to this structure. In all three iterations, T3.3 operationalized these findings. Gaps and Needs were redefined from broadly framed phenomena to rather more focused areas with a strong hybrid threats dimension.

In D3.7 the team targeted their scanning to the overall research arena. The deliverable aimed to define and discuss selected topics from the point of view of hybrid threats. The scanning team analyzed the scientific research landscape for the gaps and needs identified by practitioners in the field of hybrid threats. The deliverable contributed to deeper understanding of the hybrid threats community of the state of play of the research on the phenomena of interest, and what outcomes could be expected from the scientific research field. Not less importantly, document identified areas, which apparently lack research of the phenomena, which is deeply important for mitigation of hybrid threats.

D3.8 and D3.9 focused on EU-funded research projects. The team was reviewing EU-funded projects that are relevant to topics identified by practitioners. In the deliverables, projects were analysed from the perspective of hybrid threats, what specific aspects of the project may be of interest to community and what can be expected as an outcome of this project.

In three iterations T3.3 reviewed over 70 EU funded projects. Some of the projects were reviewed from different angles, as the same project might have been relevant in several core themes. The evolution of the method of research scanning allowed better respond to the needs of the hybrid threats community, improve understanding of the EU-funded projects which are relevant and to facilitate communication and collaboration between projects.

D3.10 concluded the work done in the EU-HYBNET project T3.3 "Ongoing Research Projects Initiatives Watch". We believe that the work of T3.3 extends the understanding of the hybrid community about

the investments the EU is making in the research of phenomena, which has direct practical value for deeper understanding and mitigation of hybrid threats. At the same time, such knowledge sharing facilitates the leverage of EU research project results for wider purposes than they were intended to.

3.1.2 EU-HYBNET T4.2 STRATEGY FOR INNOVATION UPTAKE AND INDUSTRIALIZATION

The WP4 *"Recommendations for Innovations Uptake and Standardization"*/ T4.2 "*Strategy for Innovation Uptake and Industrialization*" (lead by RISE) contributes in its D4.7 "Final Report on Strategy for Innovation uptake, Industrialization and research.

The "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) project Description of Action (DoA) describes this deliverable (D4.7) as the fourth and final report on "Defining a concrete strategic approach for innovation uptake, industrialisation and research". It is part of the overall objective to find common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities in research, innovation, and training concerning hybrid threats. This work is focused on four core themes: Future Trends of Hybrid Threats, Cyber and Future Technologies, Resilient Civilians, Local Level and National Administration, and Information and Strategic Communication.

The main objective for this final deliverable of Task 4.2 is to produce a comprehensive review of the work performed in the earlier full project cycles. The focus of the review is on the coverage of the developed solutions concerning the hybrid threat arena and a review of the methodology developed and used for the creation of uptake, industrialization, and research strategies. Building on the results of WP2 and WP3, a final solution with concrete strategic approaches for uptake and industrialisation was created. This final innovation is about developing a framework that can help build trust in AI-based tools. There is a need to adopt the view that even if you trust a solution, it should be verified that the trust is warranted.

The deliverable (D4.7) is the final report of Task 4.2, focusing on strategies for innovation uptake, industrialization, and research. It builds on the results of WP2 and WP3, refining methodologies and assessing key innovations aimed at strengthening resilience against hybrid threats. The final innovation selected in this project cycle addresses AI-Model Verification and Validation, a critical area ensuring trustworthy, safe, and robust AI models. This solution provides a framework for validation and verification, evaluating AI systems based on fairness, bias detection, robustness against adversarial attacks, explainability, and aiming for compliance with ethical and legal standards. The Innovation Uptake Canvas was developed to outline a clear vision, mission, strategy, and roadmap for adoption and industrialization. Additionally, key recommendations have been made regarding essential research, standardization, and organisational initiatives necessary for implementation.

A comprehensive review of the thirteen proposed solutions confirms their role in a multi-layered strategy against hybrid threats, addressing governance, civic, and service sectors. These solutions integrate technological innovation, structured governance, and community engagement, forming parts of a resilient ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats. Many solutions functions as enablers, including the AI-Model Verification and Validation Platform and A Common Information and Analysis Environment, which facilitate secure information sharing for real time situational awareness. The findings highlight that hybrid threats evolve faster than regulatory

frameworks, emphasizing the urgency of EU-wide standardization to ensure resilience. AI and Big Data play critical roles in real-time threat analysis, media verification, and crisis response, while early end-user involvement is essential to ensure security tools are practical and effective. Expanding media literacy training and education is also crucial for long-term resilience against misinformation.

To strengthen resilience, cross-sector collaboration between governments, academia, and industry must be enhanced through public-private partnerships and increased citizen engagement. Procurement strategies should focus on leveraging existing solutions, refining innovation descriptions, and incorporating best practices to streamline adoption.

The Methodology for Creation of Uptake, Industrialization and Research has been reviewed and updated, integrating insights from strategy development, innovation uptake, and roadmap creation. The updated Innovation Uptake Canvas incorporates additional components, ensuring better alignment between innovation descriptions and implementation strategies. Moving forward, Proof of Concept development and simulated environments will be crucial for validating solutions before full-scale deployment. Adherence to existing standards should be prioritized, with extensions or new standards developed as needed.

By prioritizing standardization, collaboration, and AI-driven innovation, the EU can build a resilient ecosystem capable of countering evolving hybrid threats in a proactive manner. The updated methodologies and frameworks developed through this project will serve as a foundation for future research and innovation uptake strategies.

The WP4 *"Recommendations for Innovations Uptake and Standardization"*/ T4.3 "Recommendations for Innovation Uptake and Standardization" (lead by PPHS) contributes in its D4.11 "Final Report on standardization recommendations.

The main goal of Task 4.3 (T4.3) within Work Package 4 (WP4) "Recommendations for Innovation Uptake and Standardization" is to map the current status and identify needs and possibilities for standardisation in the context of innovations that are seen most promising to fulfil the practitioners' gaps and needs to counter hybrid threats – as it is described in "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) Grant Agreement.

The main objective of this deliverable is to present how T4.3 partners have mapped the current status and developed recommendations in the areas of standardization, legal harmonization and best practices during the final EU-HYBNET cycle, with reference to:

a) gaps and needs identified in Work Package 2 (Definition of Needs and Gaps of Practitioners' against Hybrid Threats) especially in "Final Gaps and Need Evaluation" (Deliverable 2.8);

b) the most promising innovations identified in the Work Package 3 (Surveys to Technology, Research and Innovations);

c) selected feasible innovation areas and projects that counter hybrid threats and foster hybrid threat situational awareness described in Work Package 4 (Recommendations for Innovations Uptake and Standardization).

The EU-HYBNET T4.3 "Recommendations for Standardization" has a central role in delivering results to the third of the Three lines of Actions "Priorities as Regards Increasing Knowledge and performance Requiring Standardization" focusing on areas and innovations that recommend the scope of countering hybrid threats for standardization. A note to T4.3 research is that T4.3 does not focus on developing standards (e.g. ISO) but on making the best recommendations for standards and finding standardized ways to proceed with relevant innovations. In this context, it has been important for T4.3 to also solve key existing features that support recommending the identified, most promising EU-HYBNET innovations for standardization.

In every EU-HYBNET working cycle (M1-M17/ cycle I, M18-34/ cycle II, M35-51/ cycle III, M52-M60/ cycle IV), T4.3 is the final project Task that will highlight the key selected project innovations that are seen as a sound solution for the identified working cycle gaps and needs and answering to the pan-European security practitioners and other relevant actors' needs. Therefore, during the reporting period in T4.3/D4.11 "Final report for standardization recommendations", it is highlighted what the best practices and key regulations, and even standards are that eventually support the EU-HYBNET's recommended innovation uptake for pan-European security practitioners and other relevant actors use.

The purpose of this deliverable is to present a final analysis based on the findings of all Reports on Standardization Recommendations prepared throughout the entire five-year project cycle, including:

* D4.8 First Report on Standardisation Recommendations
* D4.9 Second Report on Standardisation Recommendations
* D4.10 Third Report on Standardisation Recommendations

3.1.3 EU-HYBNET T5.3 PROJECT ANNUAL WORKSHOPS FOR STAKEHOLDERS

During the reporting period EU-HYBNET in WP5 "*Communication, Dissemination and Exploitation Activities*"/ T5.3 "*Project Annual Workshops for Stakeholders*" (Lead by Laurea) 5th Annual Workshop (AW) was arranged by Laurea together with EC Joint Research Centre (JRC) in Brussels 12th of February 2025 (AW Agenda in Annex).

In general, the main goal of T5.3 is to arrange the EU-HYBNET Annual Workshop (AW) every year. The 5th AW was arranged in Brussels (12th of February 2025) in person and online. According to DoA, AW is arranged to disseminate project findings for large-scale stakeholders and to ensure vivid interaction with industry, academia, and other providers of innovative solutions outside of the consortium to assess the feasibility of the project findings and possible recommendations for innovation uptake and standardization. AW will foster network activities, raise awareness of the project, and bring together relevant practitioners and stakeholders who may join the EU-HYBNET network and its activities. Eventually, the goal of AW is to bring sustainability of the project activities and increase relevant members in the network.

AW brought together c. 55 participants on-site and c. 25 participants online (Reported in D5.14: 5th annual workshop report). Partners, network members, industry representatives, European Commission participated in the workshop where we looked results from the past 5 years. We presented the main findings of the past 5 years in innovation mapping, uptake, and standardization

(WP3, WP4). Industry session presentations shared the latest insights by industry network members Logically AI and Maltego and Frédéric Guyomard from EDF and PREATORIAN project, who presented different industrial views of HYBRID threats.

3.2 COMMON REQUIREMENTS AS REGARDS INNOVATIONS THAT COULD FILL IN GAPS AND NEEDS

The Deliverable D3.6 titled 'Final Report on Improvement And Innovations' summarises the work completed as part of Work Package 3 (WP3) titled 'Surveys to Technology, Research and Innovations' and specifically Task 3.2 'Technology and Innovations Watch'

In more detail, the present Deliverable provides a list of Innovations and Ideas proposed to counter specific dimensions of Hybrid Threats for specific focus areas. The latter are primarily defined in the Description of Action (DoA) as 'Core Themes', which are studied in detail by WP2 of EU-Hybnet. The Core themes represent the leading multidisciplinary methodological principles of the project, together with the Conceptual Model approach developed by the Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). The EU-HYBNET project has four core themes, which are as follows: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication.

The work also serves to present the most important innovations that have been presented in the previous cycles.

The selection of the innovations presented in the current Deliverable was based on continuous monitoring of technology advances and a thorough search in various fields. The different scientific backgrounds and complementarity of the T3.2 partners allowed for a deeper understanding of possible applications of various technologies.

Additionally, during the EU-HYBNET 5th Annual Workshop and 5th Future Trends workshop (T3.4) that took place in Brussels, February 13th-14th 2025, the T3.2 partners had the opportunity to discuss with innovation providers and consortia that were invited to participate and present their solutions in these events.

It should be highlighted that, as detailed in the Grant Agreement, the technological innovations presented aim to help European Practitioners counter hybrid threats. This Deliverable also lists societal interventions, that could help European practitioners protect European citizens from offensive populist influences

For the **first Core Theme, Future Trends of Hybrid Threats**, and more specifically the *primary context relevant to destabilization due to the instrumentalization of migration*, the idea presented is a video plugin to debunk fake videos on social media that spread conspiracy theories, aiming to help respond quickly and effectively to the spread of misinformation. Additionally, the Media Pluralism Monitor developed by EUI is proposed, to assess the potential weaknesses in national media systems that may hinder media pluralism.

For the primary context of *Foreign Interference in domestic politics, including election processes*, the new idea presented is the Establishment of a fully functional intelligence cooperation service at the EU

level, complemented by an online collaboration platform for Foreign Interference. The Information network that will be created will ensure the information flow for all EU member states' administration, enhancing their ability for policy planning and programming future strategic actions, also on a political level.

For the primary context of *Leveraging Lags in Foresight and anticipation,* the Smart message routing and notification service is proposed for sharing the operational picture to every agency involved in the response at every level of coordination. This tool can be utilized for cross-border and cross-organizational operations and has been tested in various cases to enable the sharing of information among involved actors at every level of coordination, thus enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. Additionally, considering the European Integrated Border Management concept and the EU Customs Action Plan, the tools developed in EU-funded projects like CONNECTOR can be considered. The proposed CE-CISE is a fully interoperable technical framework, which expands the scope and capabilities of CISE to the Customs domain, ensuring effective management of EU external borders at operational, tactical & strategic levels, facilitating the information exchange at interagency and transnational levels. This can help improve the common operational picture and enhance situational awareness, enable the EU cross-border joint operations and support, and complement the different agencies' work.

With respect to the **second Core Theme, Cyber and Future Technologies,** for the primary context of *Targeting European critical infrastructure and the psychological reliability of digital infrastructures*, *Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience are* proposed. Thus, stress testing a supply chain with 'what if' scenarios can reinforce any mitigation strategy and strengthen the resiliency of a critical entity.

For the primary context of *Weaponization of Mass Data - massive availability of societal data aggregates & algorithmic computation,* the Nordlayer (only named for exemplary purposes) or other similar solutions are proposed that can be used to prevent the leak of hospital patient data.

Regarding the primary context of *leveraging the autonomy and power of digital actors*, tools for the protection of personal data are proposed to be used. Additionally, a legislation initiative is proposed on an EU level for the selling of mass data, which has been a crucial question since the emergence of social media. Such legislation can help reduce the growth of the power of companies owning social platforms.

With respect to the **third Core Theme, Resilient Civilians, Local level and administration**, and the first primary context *Mainstreaming violence -The growing broadcasting and becoming accustomed to violence weaken democratic politics,* it is proposed that existing directives are expanded, and new legislation initiatives are put forward, for the protection of the phycological health of the citizens, both minors and seniors, as well as the minimization of violence spread

Regarding the second primary context *Intimidation of civil society and political engagement,* the BREACH GUARD or any other similar available solution is proposed against doxing, which involves publicly exposing someone's real name, address, job, or other identifying info without a victim's consent, aiming to humiliate, bully, harass, or otherwise harm a victim. Commercially available software can help protect personal information against data loss, leaks, breaches and collection by third parties. Furthermore, the software automatically scans the dark web for personal information

that may have been part of a data leak or data breach and helps protect the user's personal information and avoid identity theft. Besides individuals, these solutions can help fact checkers and activists of Civil Society Organizations that are often victims of such attacks.

For online political harassment and SLAPP, a network of financial and legal support is proposed, as in the case of the Foreign Policy Centre, the Justice for Journalists Foundation and the International Bar Association's Human Rights Institute, that jointly organized the European Anti-SLAPP conference. Such a network can be used to stop the intimidation of journalists which forces them to spend an enormous number of resources and energy and prevents them from offering their service to democracy, which has a profound impact on media freedom.

For the third primary context of *Boosting Demand and Spread of Conspiracy Theories, Exploiting Emotions & Promoting Victimhood In Social Relations*, the Hypster project initiative is proposed, that aims to develop a Hybrid Information Psychological Societal Threats Handling System that applies recent developments in OSINT, SocMINT, NLP, and AI to automatically detect, attribute, and counter or prevent prioritized threats. Additionally, the use of common frameworks and outcomes of FIMI-related EU-funded projects is proposed to be studied, to fight the continuous effort to create a different perception of the environment, and to ultimately help maintain our European Values.

The first primary context of the **fourth core theme, Information and Strategic Communications**, named *Reversing priorities from what needs to be broadcasted to what people want to be broadcasted*, is also relevant to creating a different perception of reality.

The Media Pluralism Monitor (MPM), developed by the European University Institute, can also be utilized in this case, but it is also important to recall the Journalism Trust Initiative (JTI) that was presented in the 1st cycle. JTI is a collaborative standard-setting process according to the guidelines of CEN, the European Committee for Standardization. More than 120 experts have contributed to this process-focused tool that evaluates how information is produced and disseminated.

For the second *primary context, Advanced Forms of AI enhanced Disinformation,* blockchain-based verification is proposed, to help establish a robust system to verify the authenticity of images and videos. It should be noted that blockchain should be used in conjunction with other strategies, such as media literacy and fact-checking, to create a comprehensive approach to combating visual misinformation.

Finally, for the third primary context *Understanding the Systemic Impacts of Disinformation, Misinformation, Propaganda, And Other Manipulative Activities in the Information Domain*, the bad news Prebunking Game platform is proposed, which was created by DROG and the University of Cambridge. This game can help users learn about six common misinformation techniques. This gamified inoculation treatment incorporates an active and experiential component to resistance-building.

4. THREE LINES OF ACTION REPORTING

This chapter describes EU-HYBNET's activities, especially in Work Packages (WPs) and Tasks (T) relevant to the Three Lines of Action during the project's past six months, namely the period November 2024 – April 2025. According to the EC's request, EU-HYBNET should report according to the following Three Lines of Action:

1) Monitoring of research and innovation projects to recommend the uptake or the industrialization of results

2) Common requirements as regards innovations that could fill in gaps and needs

3) Priorities as regards of increasing knowledge and performance requiring standardization

The subchapters below describe one by one, EU-HYBNET's contribution to each of the Three Lines of Action.

4.1 MONITORING OF RESEARCH AND INNOVATION PROJECTS WITH A VIEW TO RECOMMENDING THE UPTAKE OR THE INDUSTRIALISATION OF RESULTS

In the final cycle of the EU-HYBNET project, the development of standardization recommendations included an in-depth analysis of the contributions of research and innovation projects to practitioners. The recommendations and best practices identified in this process stem from both European and international research and innovation activities. This approach ensures that the EU-HYBNET project remains aligned with emerging trends and technological advancements in countering hybrid threats. The analysis conducted within D4.11 serves as a crucial input to EU-HYBNET's Objective 4, goal 4.3, by contributing to the development of a mapping matrix that links identified gaps and needs of European actors to the most promising innovations across various domains. Additionally, D4.11 supports EU-HYBNET's Objective 4, goal 4.1, by addressing industrialization and public procurement aspects. These recommendations play a vital role in appraising best innovations—both technical and non-technical—thereby facilitating their potential industrial uptake.

Observations and discussion

MATURATION OF HYBRID THREATS KNOWLEDGE IS NEEDED. Hybrid threats knowledge areas are still in the maturation stage, and EU-HYBNET no doubt is a very impactful initiative of EC in this maturation path. It helps to expand the hybrid threat community, deepen and spread the knowledge of hybrid threats, as well as build a common vocabulary and understanding. This maturation path is not easy. Hybrid threats is a very complex and interrelated research area, where management, regulation, and technical aspects of social media and their algorithms, cybersecurity, etc. are very important. But the hybrid threats community still must find its distinct and very clear voice to show what is hybrid in cybersecurity? What is hybrid in space technology? Task T3.3 "Ongoing Research Projects Initiatives Watch" had its mission to look for the hybrid angle in the social and technical phenomena selected as research areas. This work is ongoing and by no means completed, thus must be continuously done to shape the efforts of hybrid threat community in a most productive manner. We strongly believe that the efforts like EU-HUBNET is important for consolidating awareness on hybrid threats, developing community and integrating this knowledge area in all aspects of the functioning of society.

NECESSITY OF EVIDENCE-BASED REGULATION. One of the frequently proposed solutions in various research areas is regulatory at the international, EU, or member state level, for some aspects of the phenomenon (be it space or social media). While regulations are an extremely important instrument of risk mitigation and encouragement of positive outcomes, two aspects should be stressed in this regard. First of all, it is important to engage in education of policymakers on hybrid threats, as well as the hybrid community to actively participate in shaping such regulation, bringing depth of understanding of the phenomena. Secondly, hybrid threats related phenomena (e.g. social media) are based on human thought process, motivation, and behaviour, and in a broader perspective, politics. So, further extensive research is needed to understand fake news-related phenomena – how much people are susceptible to propaganda? Are they immune to known false information when it supports their beliefs? How much does it influence their actual behaviour? It is obvious that even in the very short time the EU-HYBNET project lasted, the fact-checking necessities were researched in several iterations and highlighted the importance of tools and mechanisms there, while after the US President D. J. Trump election, there was high profile questioning of the concept and cancellation of several initiatives in this area. Thus, recognizing the necessity of regulation, it is important to highlight that extensive research of the human sciences is needed on how information shapes human behaviour.

STRONG EFFORT TO INTEGRATE HYBRID THREATS TO VARIOUS RESEARCH DOMAINS AND MULTIFACETED FUNCTIONING OF SOCIETY. Research and efforts in areas relevant to countering hybrid threats are usually fragmented and lack coordination. We consider it a widespread issue. The ongoing Research Projects Initiatives Watch task revealed that even EU-funded research that works in the areas directly related to the hybrid threats (e.g. chemical and radioactive incidents), hybrid threats are not recognized and consequently defined as the relevant areas in their projects. D3.10 Final Report on Innovation and Research Monitoring Grant Agreement : 883054 Dissemination level: PUBLIC p. 27 EU-HYBNET demonstrated the necessity to integrate hybrid threats understanding across the board, as this is a cross-disciplinary area. Insufficient understanding and awareness of hybrid threats will result in omitted signals, delays in reaction, and failure to act, which can have huge cascading effects on countries. Thus, it seems of high importance that hybrid threats become an integral part of disciplines.

HYBRID THREATS MITIGATION NEEDS TO EMBRACE MORE SOCIETAL MECHANISMS, NOT TO RELY SOLELY ON TECHNICAL CAPABILITIES. Both in the discussion of Gaps & Needs and the scanning of research on solutions mitigating hybrid threats, there is a visible tendency to erode the capacity of traditional strategic communication to deliver impactful messages to the population. At the same time, social media with popularized alternative views further challenge institutional information. There are two directions of research. The prevailing line of thought sees the strengthening of resilience against hybrid threats in new regulations, technologies, institutional capacities, etc. Not so expressed but also visible tendency is to look for up-to-date concepts, methods, and tools, with clear guidance for constructive social dialogue between government and the public. Societal resilience, built on social trust, legitimate governance, and effective institutions, is key to preventing governance breakdown and violent conflict and must be constantly reinvented.

HYBRID THREATS SHOULD BECOME A PAN-EUROPEAN DISCIPLINE. In the research, there is an expressed need for better data sharing at the strategic and tactical level, as well as common action in the European level. This stems from the essential feature of hybrid threats – adversaries try to act under the radar, without triggering warning signals in the attacked country. So, there is a very clear case for better cooperation and coordination among the EU members. Common strategies, sharing

signals and information about incidents, sharing competence, can significantly improve situational awareness, identify planned hybrid attacks beyond separate incidents, and improve attribution as well as reaction capacities.

HYBRID THREATS RESEARCH AND PRACTICAL IMPLEMENTATION EFFORTS SHOULD BE SUSTAINED, ESPECIALLY IN THE TURBULENT TIMES OF GLOBAL POLITICS. The overarching common denominator of many observed trends we can identify as "commercialization", increasingly private ownership of critical Infrastructures, communication platforms, etc. connected with complex and hidden ownership. Their regulation becomes increasingly complex, as one usually must deal with the very large companies with the complex corporate structure across geographies, significant technological complexities, and extremely wide supply chains. At the beginning of the EU-HYBNET project, Russia's full-fledged war against Ukraine started, which significantly changed the landscape of the hybrid threats. The hybrid threat subject does not lose its dynamism further. With the re-election of D.J. Trump, his somewhat unpredictable and very active second term will bring significant changes in global politics, as well as reshape transatlantic partnerships. There is still a very clear case to follow the situation and continue research from the point of view of the Hybrid Threats in ever ever-changing global political landscape.

4.2 COMMON REQUIREMENTS AS REGARDS INNOVATIONS THAT COULD FILL IN GAPS AND NEEDS

Many of the recommendations described above are related to technological and non-technological innovations. It should be underlined that even best practices from one country can be innovative in many others. D4.11 also contributes to the EU-HYBNET's Objective 2, goal 2.4. enabling to definition of common requirements for new research and innovation possibilities that can fill knowledge gaps and enhance capabilities, endeavors concerning hybrid threats. The above recommendations suggested key focus research, innovation areas, and actions for the future in the field of countering hybrid threats.

Lessons learned

We have found that the framework methodology developed in the first project cycle, with the road mapping and the innovation uptake canvas, still represents a valid procedure to base the Task 4.2 work on. The process of the review of the methodology evaluated whether the objectives and activities carried out were clearly defined, which they were found to be. However, some clarifications of who the end-users, recipients, or practitioners are and who could benefit from the methodology were needed. Simplification of the methodology steps was also carried out, and the relevant input and desired output were better depicted. Moreover, the review of the methodology verified that an alignment of the content in the innovation description with the required content in the uptake canvas would simplify the work to fill in the canvas. The innovation descriptions should better cover the State-of-the-Art, including EU initiatives related to the innovation's scope. Furthermore, more specificity is needed to distinguish new functionality from existing solutions.

A better project timeline would also have been helpful. The following timeline has allowed for a more structured and well-defined procedure to select innovations on which to base solutions. It would also allow for a better integration of tests, providing complementary standards considerations and experts' review: 1. WP3 proposes and evaluates innovations and relevant research activities and selects the innovations for which solutions with uptake and research strategies are to be developed. 2. Task 4.2

scopes the innovations into proposed solutions. 3. WP2 performs an assessment of the solutions in DTAG exercises, as such training events and practical trials help assess a solution's fit-for-purpose rating. 4. Task 4.3 reviews the solutions from a standardization perspective. 5. Task 4.1 reviews the solutions from a procurement point of view. 6. Task 4.2 develops the uptake strategies.

When solutions have high TRLs, such as TRL 8 or 9, efforts should focus on developing proof-of-concept implementations for test-before-invest trials and market studies. Bringing innovations closer to the market at an early stage can significantly benefit innovators by enhancing competitiveness, creating niche opportunities, and improving innovation capability, outreach, and excellence.

To obtain reliable results in evaluating and synthesizing solutions, as well as in developing adoption strategies, the involvement of domain experts is crucial. Overall, our experience suggests that engaging end-users and stakeholders earlier in the process leads to more refined innovations and effective adoption strategies. To have a more efficient review and evaluation process, it would today be possible to automate parts of the processes and leverage AI tools to pre-screen innovation descriptions for completeness and relevance.

For future work in the area of finding and defining solutions that can be of service in detecting and mitigating hybrid threats and operations we propose

• Define new innovations by starting from Gaps and Needs and following the Double Diamond steps.

• Use the updated MCUIR and align the ID with the IUC (or use the updated IUC as ID) D4.7 Final report on strategy for innovation uptake, industrialisation and research

• To “sell” the solutions to practitioners and end-users, provide for developing POCs (Proof of Concept) and simulated environments.

• Build on existing standards or extend/develop new ones when required.

4.3 PRIORITIES AS REGARDS OF INCREASING OF KNOWLEDGE AND PERFORMANCE REQUIRING STANDARDISATION

Many of the recommendations presented contribute directly to the dissemination of knowledge and the enhancement of performance in standardization efforts. These recommendations not only focus on technological advancements but also encompass non-technological innovations that contribute to capacity-building and skill development in addressing hybrid threats. Given that D4.11 builds upon previous deliverables (D4.8, D4.9, D4.10), it integrates prior findings while updating and refining insights to ensure continued relevance. The focus remains on advancing the standardization landscape by identifying and advocating for best practices, fostering harmonization, and supporting the evolution of counter-hybrid threat capabilities.

Conclusions

In the final, fourth project cycle, the state of play was revised and adapted based on the outcomes of EU-HYBNET reports from the previous three cycles. These revisions were conducted within various tasks relevant to the recommendations for standardisation.

The "Final Report on Standardization Recommendations" presents recommendations across the four EU-HYBNET Core Themes, building upon the work completed in all project cycles. Section 2 outlines the most significant aspects related to the selected areas—the four Core Themes—highlighting current state of play, main issues, and needs. This section also links the identified issues to innovation recommendations for standardization. Section 3 elaborates on the Three Lines of Action.

The authors emphasize that T4.3 of EE-HYBNET not only focused on recommendations for standards per se, but also addressed legal harmonization and the identification of best practices. The project encourages the adoption of these best practices, as they often serve as the foundation for the development of official standards (e.g., ISO, CEN, or national standards). Given that the standardization process typically takes at least 2-3 years, it is challenging to ensure that standards remain aligned with the rapidly evolving landscape of hybrid threats. While relevant standards exist in areas such as safety, physical security, and cybersecurity, they are generally not specifically tailored to hybrid threats as described in this deliverable.

As this is the final report under Task 4.3 within EU-HYBNET, the recommendations presented serve as a foundation for future discussions and developments in the field of hybrid threat mitigation. These recommendations aim to provide strategic guidance on standardization efforts, legal harmonization, and best practices that can enhance the resilience of European and international actors against hybrid threats. Given the dynamic and evolving nature of hybrid threats, continuous adaptation and proactive engagement from stakeholders will be necessary to ensure that standardization efforts remain relevant and effective. To advance these efforts, collaboration among multiple stakeholders is essential. This includes engagement between public authorities, private sector actors, industry representatives, research institutions, and policymakers at both the national and EU levels. The European Commission plays a pivotal role in facilitating this coordination by aligning research and innovation funding, regulatory frameworks, and policy guidelines to support the implementation of the proposed recommendations. Strengthening synergies between different standardization bodies, such as CEN, CENELEC, and ISO technical committees, will be crucial to developing comprehensive and widely accepted standards that address the unique challenges posed by hybrid threats.

Moreover, fostering cross-sectoral cooperation between security agencies, technology providers, and academia will help bridge gaps in knowledge, accelerate the uptake of innovative solutions, and promote a harmonized approach to standardization across Europe. Future efforts should also include continuous monitoring and evaluation of existing standards to ensure their applicability in addressing emerging hybrid threats. Ultimately, the success of these standardization recommendations depends on sustained commitment, resource allocation, and policy support from all relevant actors.

The T4.3/D4.11 work on recommendations for standardization is built on the most promising innovation analysis and innovation uptake strategy created in T4.2, and hence in T4.3 the innovations under focus are:

- **Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo)**
- **Starlight Disinformation-Misinformation Toolset (STARLIGHT)**
- **AI Enhanced Disaster Emergency Communications (CRP)**
- **Media Pluralism Monitor (LMHTT)**

Within the above-mentioned innovations, T4.3 created recommendations and priorities for innovation uptake because they are seen to increase knowledge and performance with the view of requiring standardizations. Next to "Recommendations" also a type of recommendation (legal, standard, best practice) has been defined in T4.3. Moreover, a relevant institution is also identified as the primary institution that should receive a given recommendation for their information and possible future actions regarding this area. Additionally, each recommendation is marked with information on whether it is most feasible for implementation in the short, medium, or long term. The recommendations are mentioned below according to each of the selected innovations (CiReTo, STARLIGHT, CRP, LMHTT).

The Task 4.3 team will share insights from Deliverable D4.10 with relevant stakeholders, including CEN, CENELEC, and ISO technical committees. Additionally, through Work Package 5 (Communication and Dissemination), this information will be shared with other organizations, agencies, institutions, and projects working in the field of countering hybrid threats.

3.2.2 EU-HYBNET T3.4 INNOVATION AND KNOWLEDGE EXCHANGE EVENTS

During the reporting period, EU-HYBNET T3.4 "Innovation and Knowledge Exchange Events" (lead by EOS) delivered also insights into the second Three Lines of Action in the 5th Future Trends Workshop (FTW) arranged by JRC, EOS and LAUREA in Brussels on February 13th, 2025. The comprehensive description on FTW is delivered in D.3.18 "5th Future Trends Workshop Report". 5th Future Trends Workshop gathered diverse participants, enabling transdisciplinary interactions, delivering high-quality analyses, and involving high-level representatives. Feedback confirmed the event's value, highlighting its impact on understanding and countering hybrid threats through innovative solutions, hence replied to the second Three lines of action "Common requirements as regards innovations that could fill in gaps and needs".

The 3rd Innovation Standardisation Workshop (ISW) (T4.3), organized by PPHS and Laurea, took place in Brussels on October 22nd, 2024. The event brought together over 40 participants, including consortium members, representatives of the EU-HYBNET network, industry stakeholders, practitioners, and policymakers. Attendees from external organizations (practitioners, industry, academia) and consortium partners engaged in discussions on standardisation recommendations for innovations to counter hybrid threats across EU-HYBNET 4 core themes. This final ISW successfully facilitated the exchange of opinions and methods among the audience, consortium, and speakers, focusing on innovation implementation, standardisation needs, and procurement processes, and it responded to all three lines of action. 3rd Innovation Standardisation Workshop report is available on EU-HYBNET webpages: EU-HYBNET-3rd-ISW-Report.pdf.

5. CONCLUSION

SUMMARY

In the chapters above it is described how the EU-HYBNET project activities from the past six project months (November 2024 – April 2025) . In addition, chapters have described how the work in the project Tasks has been conducted now when the 4rd project cycle is finalizing to deliver its' results.

The aim and value of the Six-Month Action report is to track the results and to highlight their importance for the project proceeding and in the final Six-Month Action Report, also hand-over for key stakeholders in order to empower the pan-European measures and extension of the pan-European network to counter hybrid threats.

Furthermore, final analysis on EU-HYBNET Dissemination, Communication and Exploitation activities will support the project to consider new ways to tell about the project's results for the pan-European stakeholders. In addtion, Policy Briefs highlight the main findings from EU-HYBNET to policy makers and other pan-European stakeholders to be take into further actions in order to strengthen European response to hybrid threats.

All the above elements are to be reported thoroughly in the final report.

ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
EU-HYBNET	A Pan-European Network to Counter Hybrid Threats
EU	European Union
EC	European Commission
EU MS	European Union Member States
H2020	Horizon 2020
GA	Grant Agreement
DoA	Description of Action
WP	Work Package
T	Task
OB	Objective
KPI	Key Performance Indicator
IA	Innovation Arena
D	Deliverable
MS	Milestone
L3CE	Lithuanian Cybercrime Center of Excellence for Training Research & Education
URJC	University Rey Juan Carlos
UiT	Arctic University of Tromsa
RISE	RISE – Research Institutes of Sweden
PPHS	Polish Platform for Homeland Security

LAUREA	Laurea University of Applied Sciences Ltd
HYBRID CoE	European Centre of Excellence for Countering Hybrid Threats
JRC	Joint Research Centre-European Commission
MPM	Media Pluralism Monitor
SLAPP	Strategic lawsuit against public participation
OSINT	Open Source Intelligence
TRL	Technical readiness level
POC	Proof of concept
CiReTo	Mobile application to pinpoint acts of harassment/violence on the street and online
STARLIGHT	Starlight Disinformation-Misinformation Toolset
CRP	AI Enhanced Disaster Emergency Communications
LMHTT	Media Pluralism Monitor

Table 2: Glossary and Acronyms

ANNEX II. EVENTS' AGENDA

5th Annual Wokshop Agenda

Time CET	Topic	Speakers
	Welcome and registration	
11:00-11:30	Registration	
11:30-11:45	Welcome & Practical information	**Julien Theron**, *Researcher in Hybrid Threats, European Commission Joint Research Council* **Isto Mattila**, *EU-HYBNET Coordinator, Laurea University of Applied Sciences*
	EU-HYBNET and the Big Picture	
11:45-12:30	Linking Hybrid Threats Needs and Gaps with the Defense and Security Domain	**Antonios Platias**, *Executive Director; Brig. General (ret.)* *Foreign Affairs Institute*
	Network-based Approach to Counter Disinformation: Political and Research Perspectives	**Todor Tagarev**, *Institute of ICT, Bulgarian Academy of Sciences.*
12:30-13:00	Audience Q&A	**Host: Isto Mattila**, *EU-HYBNET Coordinator, Laurea University of Applied Sciences*
13:00-14:00	LUNCH	
	EU-HYBNET's latest findings and results	
14:00-14:30	Gaps & Needs	**Maxime Lebrun**, *Deputy Director R&A, Hybrid CoE*
14:30-15:00	Technology and Innovation Mapping	**Souzanna Sofou**, *Senior Research Engineer & Innovation Manager, SATWAYS*
15:00-15:30	Recommendations for Innovation Uptake and Standardization	**Afroditi Gagara Kozonaki,** *Research associate, KEMEA*
15:30-15:45	Insights from Network Building	**Maxime Lebrun**, *Deputy Director R&A, Hybrid CoE*
15:45-16:00	Q&A	**Host**: **Isto Mattila**, *Laurea University of Applied Sciences*
16:00-16:15	Coffee break	
16:15-16:45	Session for Policy	**Julien Theron**, *Researcher in Hybrid Threats, JRC*

		Giannis Skiadaresis, *DG HOME* **Rolf Blom,** *RISE*
16:45-17:15	Session for Practitioners	**Sabina Magalini**, *UCSC* **Hans van Leeuwe**, *NLD Ministry of Defence*
17:15-17:45	Session for Industry	**Beth Lambert**, *Logically AI* **Frédéric Guyomard**, *EDF* **Jean Backhus,** *Maltego*
17:45-18:15	Session for Academia – Articles written during the course of the project; avenues for further research.	**Souzanna Sofou**, *SATWAYS* **Gunhild Hoogensen Gjørv**, *UIT*
	Q/A	Host: Julien Theron, JRC
18:15-18:30	*Closing remarks* Mr. Isto Mattila, EU-HYBNET Coordinator Dr. Julien Theron, JRC	

5th Future Trends Workshop Agenda

Time CET	Topic	Speaker
09.00-09.30	Registration	
09.30-09.45	**Official Introductory Speeches**	**Georgios Giannopoulos,** Deputy Director, EC DG Joint Research Centre
09.45-10.00	Welcome & Practical Information	**Julien Théron**, Researcher, EC DG Joint Research Centre **Isto Mattila**, EU-HYBNET Coordinator, Laurea University of Applied Sciences
10:00-10:30	**Keynote Speeches**	**Jacob Tamm**, Deputy Head of Division, European External Action Service
10:00-10:30	Audience Q&A	**Moderator: Julien Théron**, Researcher, EC DG Joint Research Centre
10:30-10:45	Coffee Break	
10:45-12:15	**How foresight can increase preparedness and disaster resilience –** Presentation of the European Strategy and Policy Analysis System's (ESPAS) horizon scanning process and the Risks on the Horizon foresight report with the Polycrisis exploration workshop toolkit.	**Maija Knutti,** Policy Analyst, EC DG Joint Research Centre **Tommi Asikainen,** Policy Officer, EC DG Joint Research Centre
12:15-13:15	Lunch Break	

13:15-15:15	**Session #1: Cyber & Future Technologies & Resilient Civilians, Local Level and National Administration** **Topic:** Future Trends in Cyber and Future Technologies	**Co-Chair: Evaldas Bružė,** Lithuanian Cybercrime Center of Excellence for Training, Research, and Education **Co-Chair: Gunhild Hoogensen Gjørv,** UiT The Arctic University of Norway
15:15-15:30	Coffee Break	
15:30-16:30	**Session #2: Information & Strategic Communication Topic:** Trends and emerging issues in disinformation/FIMI: anticipatory analysis and identity-based disinformation/FIMI	**Chair: Rubén Arcos Martín**, Rey Juan Carlos University **Beatriz Marin**, Data analyst, European External Action Service
16:30-17:00	**Session #3: Wrap-up session - Future Trends of Hybrid Threats**	**Chair: Maxime Lebrun**, European Centre of Excellence for Countering Hybrid Threats
17:00-17:30	**Ending keynote** **Closing Remarks**	**Nicolas Bessot**, EC DG HOME **Tomasz Tokarski**, Polish presidency

3rd Innovation Standardisation Workshop

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	LAUREA, Polish Platform for Homeland Security, Helsinki EU Office
09:15-09:30	**Keynote Speech #1** Hybrid Threats innovation uptake in the future, **Giannis Skiadaresis, DG Home**	
09:30-09:40	Audience Q&A	*Moderator:* LAUREA, EU-HYBNET Coordinator Prof. Isto Mattila
9:40 – 10:40	**Session 1 – Innovation: Citizen – Responder Platform for Information Sharing in a case of an Emergency and Crises (CRP),** - Presentation of the innovation: Citizen – Responder Platform (CRP), **Isto Mattila, LAUREA** (9:40 – 9:45) - Standards in European and international level in the field of security, **Pertti Woitsch, Woitsch Consulting** (9:45 – 10:05) - Live Long and Collaborate: Crowdsourcing for Strategic Decision-Making in a complex galaxy, **Jorge Gomes, VOST Europe** (10:05 – 10:25) - Discussion (10:25 – 10:40)	*Moderator:* LAUREA, EU-HYBNET Coordinator, Prof. Isto Mattila
10:40-11:00	Coffee Break	
11:00 – 12:00	**Session 2 – Innovation: Local Media Hybrid Threats Tracker (LMHTT)** - Presentation of the innovation: Local Media Hybrid Threats Tracker (LMHTT), **Rashel Talukder, Polish Platform for Homeland Security** (11:00 – 11:05) - FIMI Trends Landscape, **Chiara Pacenti, European External Action Service** (11:05 – 11:25) - Disinformation in the context of media and media literacy, **Karina Stasiuk-Krajewska, SWPS University / CEDMO** (11:25 – 11:45) - Discussion (11:45 – 12:00)	*Moderator:* Polish Platform for Homeland Security, Rashel Talukder
12:00 – 13:00	**Session 3 – Innovation: Citizens Reporting Tool on Suspicious Signs (CiReTo)** - Presentation of the innovation: Citizens Reporting Tool (CiReTo), **Rolf Blom, RISE** (12:00 – 12:05)	*Moderator:* RISE, Rolf Blom

	- National Security Threat Map – interactive tool of the Polish Police for communication with local communities, **Łukasz Niezabitowski, National Police HQ Poland** (12:05- 12:25) - Police's view to tools used by citizens to announce suspicious actions – room for AI to support data analysis and to pin point critical cases, **Tomas Divis, Police of the Czech Republic** (12:25 – 12:45) - Discussion (12:45 – 13:00)	
13:00 – 14:00	Lunch Break	
14:00 – 15:00	**Session 4 – Innovation: STARLIGHT and Innovation testing best practices** - Presentation of the innovation: STARLIGHT and Innovation testing best practices, **Edmundas Piesarskas, L3CE** (14:00 – 14:05) - Starlight CODEV model, **Nikolaos Gkalelis, EUROPOL Innovation Lab** (14:05 – 14:25) - Insights from the STARLIGHT Project**, Pierre Vanbeveren, Brussels Police and Edmundas Piesarskas, L3CE** (14:25 – 14:45) - Discussion (14:45 – 15:00)	*Moderator:* L3CE, Edmundas Piesarskas
15:00 – 15:30	iProcureNet Project. Procurement at the heart of security innovation **Jorge Garzon, French Ministry of Interior** Audience Q&A	*Moderator:* LAUREA, EU-HYBNET Coordinator, Prof. Isto Mattila
15:30 – 16:00	Workshop outcomes & Closing Remarks	LAUREA, EU-HYBNET Coordinator, Prof. Isto Mattila;