9TH SIX MONTH ACTION REPORT

DELIVERABLE 1.13

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

D1.13 9TH SIX MONTH ACTION REPORT

Deliverable number:	**1.13**	
Version:	**1.0**	
Delivery date:	**25/11/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	Isto Mattila, Tiina Haapanen	**Laurea**
Contributors:	Petri Häkkinen, Satu Laukkanen	**Espoo**
	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
0.10	1/10/2024	Isto Mattila/ Laurea	1st draft of text
0.11	2/10/2024	Isto Mattila/ Laurea	Text editing
0.20	7/10/2024	Isto Mattila/ Laurea	Text editing
0.21	8/10/2024	Isto Mattila/ Laurea	Text editing
0.22	9/10/2024	Isto Mattila/ Laurea	Text editing
0.23	10/10/2024	Isto Mattila/ Laurea	Text editing
0.3	14/10/2024	Isto Mattila/ Laurea	Text editing
0.4	28/10/2024	Isto Mattila/ Laurea	Text editing
0.5	31/10/2024	Isto Mattila/ Laurea	Text editing
0.60	02/11/2024	Isto Mattila/ Laurea	Text editing
0.61	03/11/2024	Isto Mattila/ Laurea	Text editing
0.62	04/11/2024	Isto Mattila/ Laurea	Text editing
0.7	08/11/2024	Isto Mattila/ Laurea	Text editing, document ready for review
0.80	18/11/2024	Jari Räsänen, Petteri Partanen/ Laurea	Review
0.81	../11/2024	Petri Häkkinen, Satu Laukkanen, Jenni Laukkonen / Espoo	Review
0.90	25/11/2024	Tiina Haapanen, Jari Räsänen/ Laurea	Text editing
1.0	2/12/2024	Tiina Haapanen/ Laurea	Final editing and document submission to the EC

DISCLAIMER

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) 1.13 "*Ninth Six Month Action Report*" in project month (M) 54/Oct 2024 is to describe how the project has proceeded from M49 until end of M54 of the project (May – October 2024) according to the European Commission (EC) defined, *"three lines of action*" which 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) are:

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

2) Common requirements regarding innovations that could fill gaps and needs.

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

Furthermore, D1.13 also highlights what actions and results are expected from EU-HYBNET during the next and last six-month period (November 2024 - April 2025).

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1. Provides an overview to the document content.
- Section 2. Describes the importance of deliverable D1.13 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 49 - 54 (May – October 2024) have contributed to the EC's requested "three lines of action" activities.

- Section 4. Conclusion and next steps for the upcoming 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)1.13 "*Ninth 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 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 the D1.13, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.13 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.

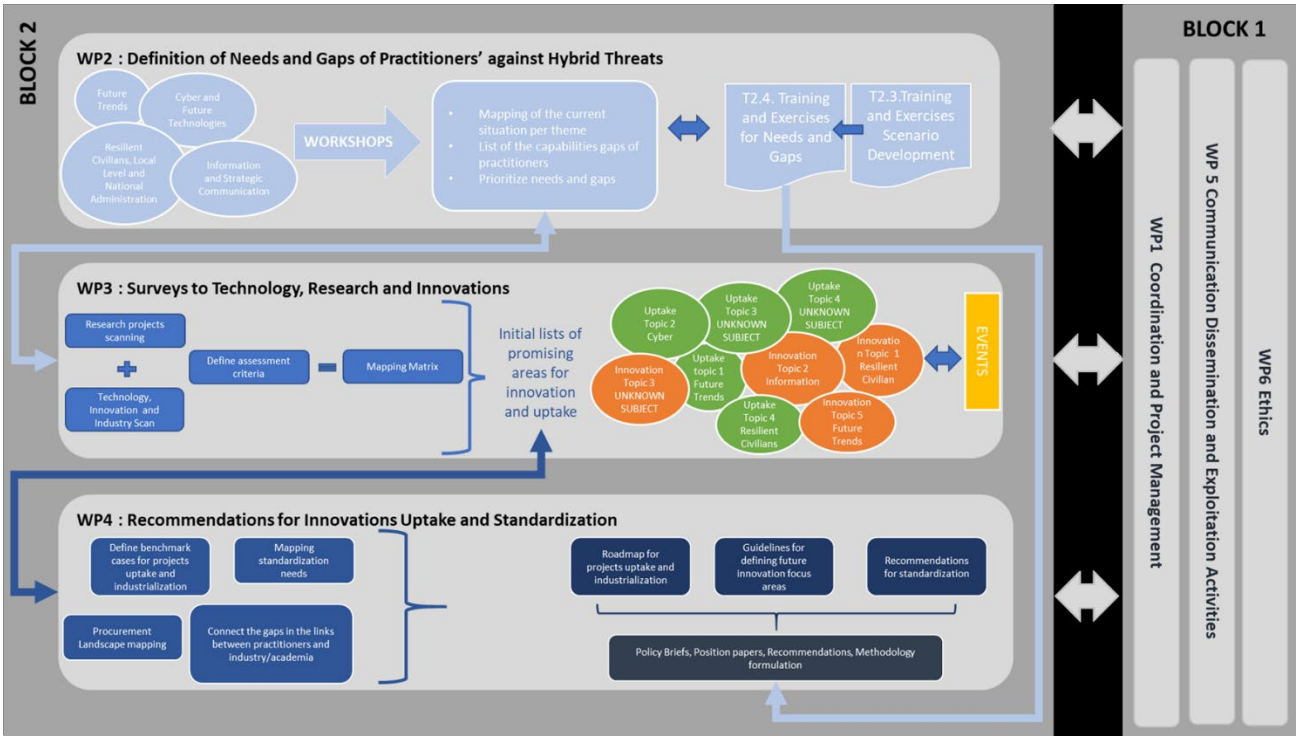

Figure 1: EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in EU-HYBNET Six Moth Action Reports are often linked to the project milestones (MS) achieved during the last six-month period. During D1.13 reporting period project Milestone set to the project was following while the milestone has been only partly

achieved in T4.4 Lead by Hybrid CoE. In short T4.4/ deliverables (D) 4.14 is under final review but not published yet that should however happen in few weeks. The milestone in question is MS28:

MS number.	MS action description
28	3rd Policy briefs, Position Papers, or Recommendations documents are published

Table 1: Milestone 28

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The Ninth Six-Month Action Report (D1.13) main author is Laurea, the organization responsible for the delivery of D1.13. 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 D1.13 by providing general remarks on the project's general progress and innovation uptake.

3. 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 past six months, namely period May - October 2024. 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 with a view to recommending 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 of knowledge and performance requiring standardization

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

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

The starting point for the first "Three Lines of Action" reporting is coming from the EU-HYBNET Task (T)2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" (lead by Hybrid CoE) and T2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC) who identified during the beginning of the third project cycle (M35-M52/ March 2023 – August 2024) practitioners'[1] and other

[1] A practitioner is defined in EU-HYBNET as the following (DoA Part B, Chapter 3.3): *A practitioner is someone who is qualified or registered to practice a particular occupation or profession in the field of security or civil protection*." In addition, practitioners in the context of hybrid threats are expected to have a legal mandate to plan and take security measures, or to provide support to authorities countering hybrid threats. Accordingly, EU-HYBNET practitioners are categorized as follows: I)

relevant actors' (industry, SMEs, academia, NGOS) gaps and needs, vulnerabilities to counter hybrid threats. The work conducted in T2.1 and T2.2 contributed to deliverable (D) 2.11 "Deeper analysis, delivery of short list of gaps and needs" (M39/ July 2023) where the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats were listed. Therefore, the D2.11 signified in the third project cycle (M35 – M52/ March 2023 – August 2024) the starting point for the EU-HYBNET project to start monitoring and mapping technological and non-technological/human-science based innovations, solutions from existing research and innovation (R&I) projects and other possible sources or providers (e.g. industry, academia, NGOs) to cover the identified gaps and needs and with a goal of recommending the uptake or the industrialization of results.

During the previous reporting period many promising innovations to the most critical gaps and needs as identified in D2.11 were reported in T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) and T3.2 "*Technology and Innovations Watch*" (Lead by Satways). The information on the promising innovations was then going through during this reporting period thorough analyses of T3.1 "*Definition of Target Areas for Improvements and Innovations*" (Lead by TNO). Because T3.1 delivers final analysis of the most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats, the results from T3.1/ D3.19 "*Final report with overview mapped on gaps and needs*" (M50/June 2024) are reported below in sub-chapter 3.1.1.

Next to T3.1 important innovation analysis relevant to the first Three Lines of Action reporting has been conducted in WP4 "*Recommendations for Innovations Uptake and Standardization*" T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE)/ D4.5 "*2nd Innovation uptake, industrialization and research strategy"* (M34 / Feb 2023, RISE). The results achieved in T4.2 according to the three lines of actions topic **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** are described in the following sub-chapter 3.1.2.

Lastly, also in WP5 "*Communication, Dissemination and Exploitation Activities*"/ T5.3 "*Project Annual Workshops for Stakeholders*" (Lead by Laurea) important innovation mapping relevant to the first Three Lines of Action reporting has been conducted. In T5.3 EU-HYBNET 4th Annual Workshop (AW) was arranged on 24th of April 2024 in Valencia where sound projects to D2.11 identified pan-European security practitioners' gaps and needs were provided pitching opportunities. More on the selected projects in the subchapter 3.1.3. below.

3.1.1 EU-HYBNET T3.1. DEFINITION OF TARGET AREAS FOR IMPROVEMENT AND INNOVATIONS

Task (T) 3.1 "*Definition of Target Areas for Improvement and Innovations*" (lead by TNO) Deliverable (D) 3.19 "*Final report with overview mapped on gaps and needs*" (M50/June 2024) is the third and final report of Task 3.1. The objective of Task 3.1 as defined in the DoA, is to identify target areas (that are linked to existing projects) in which improvements and innovations for countering hybrid threats need

ministry level (administration), II) *local level* (cities and regions), III) *support functions to ministry and local levels* (incl. Europe's third sector).

to be taken up. In addition, it is T3.1's role to review, complement and assess the innovations that have been identified in T3.2 "*Technology and Innovations Watch*"/ D3.5 and T3.3 "*Ongoing Research Projects Initiatives Watch*"/D3.9. Finally, the formulation of target areas and the assessment of innovations from T3.1/D3.19 are used to prioritise innovations and feed these 'selected' innovations into WP4 "*Recommendations for Innovations Uptake and Standardization*" for further processing and uptake. The figure below shows the T3.1 process and workflow.

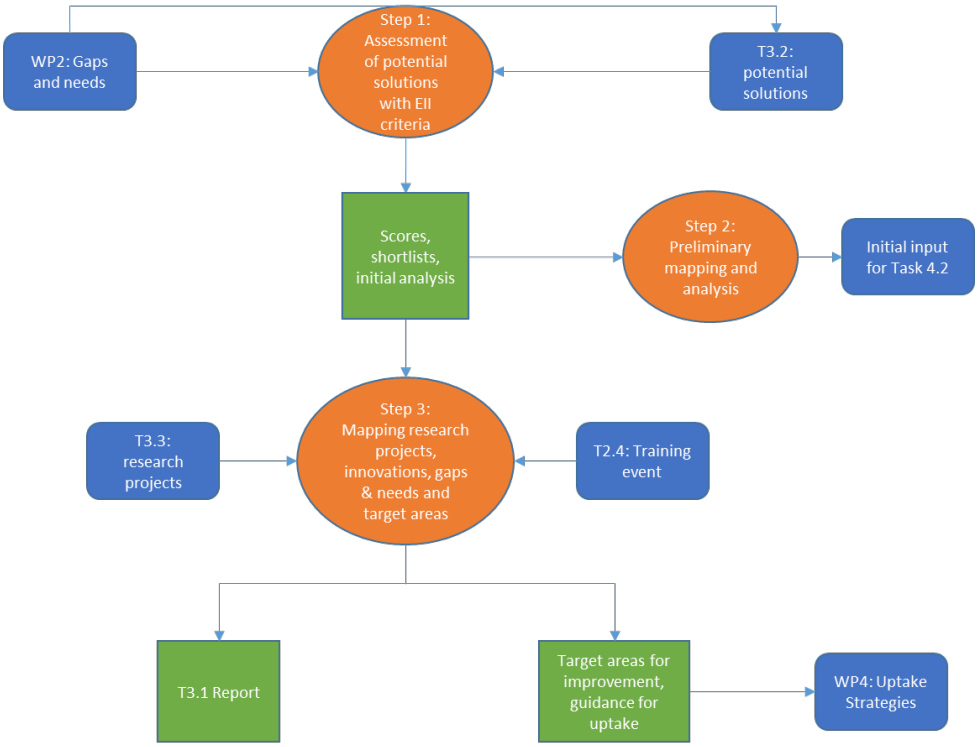

Figure 2: Task 3.1. process and workflow

The main criteria and drivers of assessment are: Excellence, Impact and Implementation. Excellence refers to how well the innovations are described as well the credibility and soundness of the innovations. Impact relates to how well-suited innovations are in countering hybrid threats, and more specifically against which threats and what (societal) vulnerabilities are protected by those innovations. Finally, implementation covers the difficulty to get innovations implemented and working. The criterium of implementation also considers the required efforts in resources, restrictions for use, and cost drivers like development, acquisition and exploitation. In addition to these criteria, a scoring system including thresholds has been defined

A total of 22 innovations have been processed and assessed in the 3nd cycle of Task 3.1. These 22 innovations have been divided into 3 categories: 10 innovations that are less favored and that for the time being will not be followed up on, but will be kept in the Innovation Arena for further discussion with the consortium's network; 4 innovations that are potentially promising but require some additional effort to leverage their potential; and 8 innovations that get high assessments and that are recommended for integration into WP4 that deals with the uptake of those innovations. The figure below provides an overview of all 22 innovations and their categorization.

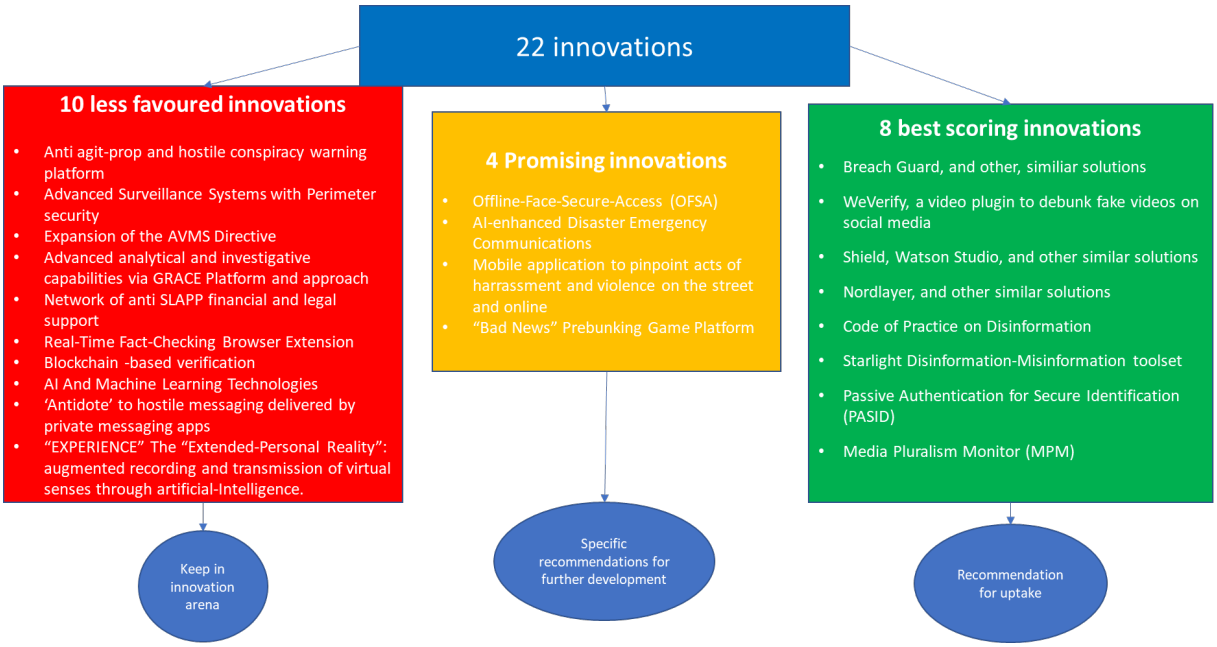

Figure 3: Prioritization of the 22 assessed innovations, divided into the 3 categories

The innovations have also been categorized according to 3 target areas. A target area is considered to be a cluster of comparable and coherent innovative solutions for a specific, shared domain, vulnerability, or purpose. The 7 identified target areas are: (1) Integration of cyber solutions, (dis)information detection tools, and (fake) news platforms; (2) Preparation, analysis and management of complex hybrid threats; (3) Improving and expanding information sharing capabilities; (4) Improving Societal Resilience; (5) Safeguarding democratic processes and institutions; (6) Strengthening physical security; and (7) fundamental research and low TRL innovations.

According to the T3.1 analysis, supported by the scoring system, the most promising or **"best assessed" 8 innovations** in EU-HYBNET to the pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats are presented in the table 2.

Innovation number	Innovation name	Scores		
		Excellence	Impact	Implementation
5	Breach Guard or Any Other Similar Available Solution	5	5	5
		4	4	4
		5	4	5
	13,7	4,7	4,3	4,7
3	WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories	4	4	4
		5	5	4
		5	5	4
	13,3	4,7	4,7	4,0
7	Shield, Watson Studio, Or Any Other Similar Available Solution	4	4	3
		3	4	5
		5	5	5
	12,7	4,0	4,3	4,3
6	NordLayer Or Other Similar Solution	5	4	5
		4	4	3
	12,5	4,5	4,0	4,0
8	Code of Practice on Disinformation	3	3	4
		5	4	3
		5	4	4
	11,7	4,3	3,7	3,7
9	Starlight Disinformation-Misinformation toolset	4	4	4
		4	4	4
		3	3	3
	11,0	3,7	3,7	3,7
15	Passive Authentication for Secure Identification (PASID)	4	4	4
		4	3	3
		4	4	3
	11,0	4,0	3,7	3,3
19	Media Pluralism Monitor (MPM)	4	4	4
		4	4	4
		3	3	3
	11,0	3,7	3,7	3,7

Table 2: Most promising innovation according to T3.1 analysis

In the analysis work, T3.1 also benefited from innovation analysis conducted in T2.4 "*Training and Exercises for Needs and Gaps*". The results of the training event innovation testing, T3.1 could further validate the most promising innovations. **The following EC and EU MS-funded projects that T3.1 identified to include innovations or elements that support the eight best-assed innovations uptake are the following:**

- **#1: Breach Guard (or Any Other Similar Available Solution) (e.g.** Data Breach Monitoring Software | Avast BreachGuard)
  Commentary and recommendations for development: Good solution for a very narrow and specific challenges. Mostly relates to data and information protection of individuals. Helps protect people

preventively, for example against microtargeting by hostile actors. This innovation could be further aligned with other solutions and innovations that pertain to the prevention of data theft, and analysis of such networks. N.B. No relevant research projects.

- **#2: WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories (**Home - WeVerify)
  This is a known and proven solution. Open source; questionable longevity/life cycle maintenance. The solution could benefit from more integration with other tools and toolsets that work on identifying, tracking and fighting disinformation/misinformation.

  Relevant research projects:
  - IMMUNE 2 INFODEMIC aims to immunise EU citizens against the disinformation and misinformation on selected themes by empowering and equipping them with several methods using eye-catching material and easy-to-use tools. IMMUNE 2 INFODEMIC | Beyond the Horizon ISSG
  - vera.ai / VERification Assisted by Artificial Intelligence: The main goal is to fighting online disinformation with trustworthy AI solutions. Home – vera.ai VERification Assisted by Artificial Intelligence
  - FERMI: Fake nEws Risk Mitigator: FERMI develops a framework to detect and monitor the way that disinformation spreads, both in terms of locations and within different segments of the society, and to put in place relevant security countermeasures. FERMI Project - Fake News Risk Mitigator

- **#3: Shield, Watson Studio (or Any Other Similar Available Solution) (e.g.** Shield Advanced Solutions Ltd)
  Application, that contribute to preventing the theft of data and information online.

  Relevant research projects:
  - HARPOCRATES Data analytics and cryptography for privacy preservation: HARPOCRATES will design and demonstrate several practical cryptographic schemes (functional encryption and hybrid homomorphic encryption) for analysing data in a way that preserves privacy and enables a comprehensive approach where data analytics and cryptography are associated with increased privacy. Homepage - Harpocrates project
  - ENCRYPT, A Scalable and Practical Privacy-Preserving Framework: ENCRYPT will, based on different use cases, evaluate and validate Differential Privacy, Multi-Party Computation, Full Homomorphic Encryption (FHE) and Local Differential Privacy. Home - Encrypt
  - SPATIAL: Security and Privacy Accountable Technology Innovations, Algorithms, and machine Learning: SPATIAL will address the challenges of black box AI and data management in cybersecurity. SPATIAL H2020 – Achieving trustworthy, transparent and explainable AI for cybersecurity solution

- **#4: NordLayer (Or Other Similar Solution)** Network Access & Security Solutions | NordLayer
  Clear solution to a clear problem. Rather basic cyber security standards to protect patient data and information. Healthcare sector is a vital sector, and needs to be better protected and monitored. This solution can contribute to that.

Relevant research projects:

- FLUTE, Federate Learning and mUlti-party computation Techniques for prostatE cancer: Flute will provide an example of a novel federated AI toolset to provide privacy protection, pushing the performance envelope of secure multi-party computation, used for diagnosis of clinically significant prostate cancer. Flute Project: Federate Learning and mUlti-party computation Techniques for prostatE cancer
- SECURED, Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation: SECURED demonstrate technologies developed in health-related use cases like real-time tumour classification, telemonitoring for children and access to genomic data. Home - SECURED EU project
- HARPOCRATES Data analytics and cryptography for privacy preservation: HARPOCRATES will design and demonstrate several practical cryptographic schemes (functional encryption and hybrid homomorphic encryption) for analysing data in a way that preserves privacy and enables a comprehensive approach where data analytics and cryptography are associated with increased privacy. Homepage - Harpocrates project
- PAROMA-MED, Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications: PAROMA-MED aims to develop novel technologies, tools, services and architectures for patients, health professionals, data scientists and health domain businesses so that they will be able to interact in the context of data and machine learning federations according to legal constraints and with complete respect to data owners' rights to privacy protection to fine grained governance, without performance and functionality penalties of ML/AI workflows and applications. PAROMA-MED
- ENCRYPT, A Scalable and Practical Privacy-Preserving Framework: ENCRYPT will, based on different use cases, evaluate and validate Differential Privacy, Multi-Party Computation, Full Homomorphic Encryption (FHE) and Local Differential Privacy. Home - Encrypt
- SPATIAL: Security and Privacy Accountable Technology Innovations, Algorithms, and machine Learning: SPATIAL will address the challenges of black box AI and data management in cybersecurity. SPATIAL H2020 – Achieving trustworthy, transparent and explainable AI for cybersecurity solution

- **#5: Implementation guidance on the code of Practice on Disinformation**

  There are differences between MS on what qualifies as disinformation. 27 EU MS, 27 different approaches and definitions. This can lead to a differentiation of implementation across the EU. VOST Europe is helping EU MS to implement the code of Practice on Disinformation to improve the level and efficacy of their implementation.

  Basically no relevant research projects were identified while D3.9 has analyzed a myriad of research projects that are relevant to fighting disinformation and making civilians more resilient to disinformation. However, this identified solution is a specific implementation guidance of a unique code of practice. Therefore, the identified research projects relevant to disinformation may help the general landscape of fighting disinformation and empowering civilians to become more resilient, but they cannot contribute to this unique initiative.

- **#6: Starlight Disinformation-Misinformation toolset (**Leveraging Continuous Learning for Fighting Misinformation | Starlight)
    - The project contains clear technical information. It describes a clear, wide range of tools for specific, narrow problems. This is a project-in-development, with close consultation with LEA's, which improves its further R&D process and ultimate feasibility into implementation.

      Relevant research projects:
    - PaCE – Populism And Civic Engagement: a fine-grained, dynamic, context-sensitive and forward-looking response to negative populist tendencies. The project developed an open source tool relying on machine learning algorithms for identifying and tracking populist narratives. Populism And Civic Engagement – a fine-grained, dynamic, context-sensitive and forward-looking response to negative populist tendencies | PaCE | Project | News & Multimedia | H2020 | CORDIS | European Commission
    - ViEWS – a political Violence Early Warning System: ViEWS is a political violence early warning system. Predicting political violence is useful for first responders and policymakers and ViEWS is a tool for research on high-quality forecasts of political violence. ViEWS: A political Violence Early-Warning System – Peace Research Institute Oslo (PRIO)
    - FERMI: Fake nEws Risk Mitigator: FERMI develops a framework to detect and monitor the way that disinformation spreads, both in terms of locations and within different segments of the society, and to put in place relevant security countermeasures. The main goal is to analyse and assess direct risks posed by disinformation to the offline environment and minimise the impact. FERMI Project - Fake News Risk Mitigator
    - ODYCCEUS – Opinion Dynamics and Cultural Conflict in European Spaces: ODYCCEUS sought conceptual breakthroughs in Global Systems Science, including a fine-grained representation of cultural conflicts based on conceptual spaces and sophisticated text analysis, extensions of game theory to handle games with both divergent interests and divergent mindsets, and new models of alignment and polarization dynamics. odycceus.eu
    - vera.ai / VERification Assisted by Artificial Intelligence: The main goal is to fight online disinformation with trustworthy AI solutions. Vera.ai aims to build professional, trustworthy AI solutions against high-level disinformation techniques, to be co-created with and for media experts and researchers, and to lay the groundwork for future research in AI counter disinformation. Home – vera.ai VERification Assisted by Artificial Intelligence

- **#7: Passive Authentication for Secure Identification (PASID)**

  This application promises a novel way of continuously tracking and identifying individuals in high-security environments. It pertains to a very narrow group of users. This is more related to physical site security, rather than protecting social structures. N.B. Relevant research projects: None.

- **#8: Media Pluralism Monitor (MPM)** Media Pluralism Monitor 2024 - CMPF

  MPM seems like a useful tool to showcase and analyze the generic media landscape and its vulnerabilities/strengths regarding pluralism.

  Relevant research projects:

- RECLAIM: Reclaiming Liberal Democracy in Europe: New tools to address post-truth politics in Europe. RECLAIM project will address the implications of post-truth phenomena in three distinct phases by generating a conceptual definition, operationalisation and empirical indicators to analyse post-truth/post-factual politics. About us | RECLAIM
- MeDeMAP: Mapping Media for Future Democracies: Project aims to establish forward-looking pathways to strengthen democracy by improving accountability, transparency and efficiency in media production and expanding active and inclusive citizenship. Home - MEDEMAP - Mapping Media for Future Democracies
- ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE: Resilient Media for Democracy in the Digital Age (ReMeD) responds to the European Commission's call HORIZON-CL2-2022-DEMOCRACY-01-06: "Media for democracy – democratic media" and will tackle existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. About ReMeD – ReMed

Conclusions

The results of 3rd cycle innovations and projects above summarize key findings that come to the First Three Lines of Action "Monitoring of research and innovation projects to recommend the uptake or the industrialization of results". The reporting highlights especially EC-funded projects that seem to deliver solutions important to uptake and industrialization to empower pan-European actors' measures to counter hybrid threats. **However, there were 3 innovations, and we didn't find any relevant projects. Therefore, these three: Passive Authentication for Secure Identification (PASID), Implementation guidance on the code of Practice on Disinformation, and Breach Guard are recommended to look for new Horizon projects.**

This 3rd cycle was the final full working cycle (17 months) of the EU-HYBNET project. Whilst there will be still a fourth mini working cycle (8 months), it does not include a deliverable dedicated to innovation mapping and research projects mapping to the 4th cycle gaps and needs as done during the other 3 main project cycles. Therefore, to give a holistic and final appraisal of the work across the EU-HYBNET project from the T3.1 point of view, we will give in final reporting.

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 D4.6 "*Third innovation Uptake Industrialization and Research Strategy*" to the first of the Three Lines of Action "***Monitoring of research and innovation projects with a views to recommending the uptake or the industrialisation of results***" from innovations' uptake recommendations perspective. In short, in T4.2/D4.6 four most promising innovations to cover the 3rd EU-HYBNET project cycle's identified pan-European security practitioners' gaps and needs to counter Hybrid threats have been described next to sound projects' where the innovations may originate or may benefit in further development.

In T4.2/D4.6 the main focus has been to select feasible analyzed innovations and projects from the T3.1/D3.19 "*Final Report, Mapping of Solutions on Gaps and Needs*" that counter hybrid threats and

foster hybrid threat situational awareness. In addition, in T4.2 goal has been to build concrete roadmaps on strategies for innovation uptake. The activities in T4.2 during the third project cycle (M35 – M52/ March 2023 – August 2024) have been to apply the methodology developed in the first and second project cycles (M1-M17/ May 2020 – September 2021; M18-M34/ October 2021 – February 2023). The major difference compared to the earlier work done in EU-HYBNET project cycles is that the innovations in the third project cycle were based on innovations and projects with high TRLs.

In the OECD Oslo Manual the collection of non-technological innovation data[2], an innovation is defined in the following way:

1. An Innovation is defined as the implementation of a new or significantly improved product (good or service) or process, a new marketing method, or a new organizational method in business practices, workplace organization or external relations.

The categorization of technical and non-technical innovations is given as follows (in our wording):

2. **A technical innovation** relates to the introduction of a technologically new or substantially changed good or service or to the use of a technologically new or substantially changed process.
3. **A non-technical Innovation** is, expressed in its simplest form, an innovation that is not a technological innovation. The major types of non-technological innovation are likely to be organizational and managerial innovations, such as
    a. the implementation of advanced management techniques, e.g., Total Quality Management (TQM), Total Quality Service (TQS).
    b. the introduction of significantly changed organisational structures; and
    c. the implementation of new or substantially changed corporate strategic orientations.

In EU-HYBNET T3.1/D3.19[3] identified a set of 12 promising innovations, i.e., they fulfil the basic assessment criteria defined by Task 3.1, i.e., having a score greater or equal to 10 (out of 15 possible). Out of these promising innovations, a subset of 8 was identified as "best assessed" while they fulfilled additional evaluation criteria. Out of the best-assessed innovations five belong to EU-HYBNET project Core theme Cyber and Future Technology and for the other three to EU-HYBNET project Core themes there was one innovation belonging to each.

The T4.2 rationale behind the choice of the four **innovations** and related research initiatives/solutions listed below are:

1. **AI Enhanced Disaster Emergency Communications (CRP)** belongs a) to the D3.19 group of promising innovations with a score of 10 and was one of the innovations which received the highest priority ranking in the EU-HYBNET 3rd Training and Exercise event[4] in Vilnius, Lithuania. It is about citizens contacting the first and second responders during large scale emergencies and crises in order to via a mobile app announce/report their situation and their need for help. E.G. AI Disaster Emergency Com' – SecurIT
2. **Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo)** belongs a) to the D3.19 group of promising innovations with a score of 10 and was judged by

[2] OECD, Oslo Manual, https://www.oecd.org/science/inno/2367614.pdf.

[3] EU-HYBNET D3.19 Final Report Mapping of Solutions on Gaps and Needs. To be published

[4] EU-HYBNET 3rd Training and Exercise event in Vilnius, Lithuania, January 2024. The outcome of the event is reported in D2.22 Training and Exercises Delivery on Up-to-Date Topics.

T4.2 as a very straightforward solution that could involve citizens to help in the early detection of hybrid threats. The aim of the innovation "Mobile application to pinpoint acts of harassment/violence on the street and online" (or Citizens Reporting Tool – CiReTo for short) is to use readily and widely available technology – i.e. smartphones – to record and geolocate acts of harassment and violence (or calls for violence) in physical space as well as online.

AI tools like Spot, AI2HR, and SaferSpace leverage advanced algorithms to analyze data from incident reports, employee surveys, and workplace communications. These tools aim to identify patterns and potential risks, allowing organizations to address issues before they escalate.

3. **Media Pluralism Monitor (LMHTT)** belongs a) to the D3.19 group of the eight "best assessed" innovations with a score of 11 and b) is the only innovation in the group representing core theme Information and Strategic Communication. Innovation offers a specialized solution for hybrid threat security practitioners, enhancing their capability to monitor (F)IMI campaigns across local and regional media in European countries. This diagnostic tool conducts comprehensive analyses of the local and regional media landscape, enabling experts (responsible for producing report) to identify and map potential risks related to (F)IMI campaigns and other threats to media pluralism.
   E.g. Media Pluralism Monitor 2024 - CMPF

4. **Starlight Disinformation-Misinformation Toolset (STARLIGHT)** belongs a) to the D3.19 group of the eight "best assessed" innovations according to Task 3.1 with a score of 11 and was one of the innovations that received the highest priority ranking in the EU-HYBNET 3rd Training and Exercise event[4] in Vilnius, Lithuania. This project is one of the flagship projects dedicated to deliver easily deployable AI-enabled toolsets addressing various needs of LEAs (Law Enforcement Agencies) and other security practitioners. There are various innovative developments within the project. Some of them are dedicated to countering disinformation and misinformation on social platforms. rise-sd-proceedings-book-compressed.pdf

Table 4 describes the Relation between selected projects/innovations and EU-HYBNET core themes according to original innovation descriptions.

Innovations	**Core Themes**			
	Resilient civilians, local level and administration	Cyber and Future Technologies	Information and Strategic Communi-cation	Future Trends and Hybrid Threats.
AI Enhanced Disaster Emergency Communications (CRP)	X			
Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo)		(X)		X
Media Pluralism Monitor (LMHTT)			X	

Starlight Disinformation-Misinformation Toolset (STARLIGHT)	(X)	X	(X)	(X)

Table 3: Relation between selected projects/innovations and EU-HYBNET core themes according to original innovation descriptions.

CRP and CiReTo innovations are mainly technical innovations while STARLIGHT has a technical and a non-technical component. LMHTT innovation is a purely a non-technical solution. CRP and CiReTo are strongly related in that CRP focuses on information handling of citizens' reports in an information sharing environment while CiReTo focuses on the means for citizens to report emergencies and hybrid threat related events to first- and second-line responders. Some of the tools developed in the EC funded STARLIGHT project would be useful in CRP and, as its non-technical component relates to the technical development process of applications, it may/should be applied in the development of the CRP and CiReTo solutions.

In general, the four most promising uptake of innovative solutions (CRP, CiReTo, LMHTT, STARLIGHT) that T4.2 recommends for innovation uptake and industrialization are strongly or at least some parts linked to other EC funded projects' and their results and innovations/ innovative solutions. The link to other EC funded project's results is especially important in the STARLIGHT innovation and CRP. In short, EU-HYBNET STARLIGHT innovation builds directly on the results gained in the EC-funded project STARLIGHT https://www.starlight-h2020.eu/ , and in CRP an innovation called "AI Enhanced Disaster Emergency Communications" from company Highwind is part of EC-funded project SECURE-IT. However, LMHTT and CiReTo innovations have no direct link to any EU projects but benefit and link with some existing relevant research results and non-technological or technological solutions available already. The strategy for innovation uptake and industrialization that EU-HYBNET supports is described in Table 4.

Innovation	Project	Uptake and industrialization
CRP In an EC funded project SECURE-IT Highwind company has delivered solutions called "AI Enhanced Disaster Emergency Communications" that CRP sees as a critical building block in order to deliver communications system between citizens and first responders	SECURE-IT https://securit-project.eu/	The road mapping indicates that it needs to be an EU initiative behind the realization and development of the proposed CRP. The development of CRP will probably never take place without such an initiative and allocation of the required funding also inside each EU MSs to take the CRP in its own use. However, we note that the EU already has many actions in the area, and this would only be an add-on to the already ongoing efforts e.g. BroadEU.Net https://broadeu.net/ Thus in EU-HYBNET deliverable D4.3 "3rd Report on Procurement Landscape" 32 it has been analysed that CRP type of solution would qualify for public procurement and hence this would support the platforms uptake.
STARLIGHT The Starlight project is one of the flagship projects dedicated to deliver easy deployable AI-enabled toolset to address various	https://www.starlight-h2020.eu/	The difference with this practice is that it is to be applied in the security sector, where organisations tend to be very couscous, and operate in very sensitive environments. The gap between understanding of AI-supported technologies among developers and end users in the sector to be mentioned. Uptake

need of LEA and other security practitioners driven by constantly changing tech-driven crimes modus operandi. It is to be mentioned that there are different solutions available to analyse content in social platforms, detect bots, identify deepfakes etc. But they are not LEA specific and are known for the general public, including adversaries. Focus is on new developments, that are specifically tailored for LEA's and not available for wider audience, thus leaving details of functionalities undisclosed. Such is the primary focus of the Starlight project. On the other hand, such specifics limit our possibilities to wider present the solutions under development.		in this case is not only the adjustment of solutions to end-user needs, this is also learning, common language development, identification of relevant peculiarities, and many other aspects that allow to move developers closer to end users. The Starlight project demonstrates that this practice can work in the LEA environment so far. This allows us to say that it is somewhat specific and unique. There are no specific thresholds for the application of this practice, as a proposition is about the methodological approach connecting to very different universes. No additional funding is required. The uptake of this practice by organizations is more dependent on awareness of it, willingness to apply it, and resources that can be dedicated.
CIRETO The aim of the innovation "Mobile application to pinpoint acts of harassment/violence on the street and online" (or Citizens Reporting Tool - CiReTo for short) is to use readily and widely available technology – i.e. smartphones – to record and geolocate acts of harassment and violence (or calls for violence) in physical space and acts of harassment and calls for violence online	AI tools like Spot,	Success will depend on offering innovative features, ensuring data security, building partnerships, and effectively engaging with the community. By addressing these factors, the CiReTo app can make a significant impact on personal safety and community well-being. To successfully fund and organize the uptake and industrialization of the CiReTo a comprehensive approach strategy should be followed that encompasses strategic planning, effective funding acquisition, deliberate partnership building, user-centric design, robust technological development, proactive marketing, and user engagement. The success of the CiReTo will depend on a holistic approach that combines these elements. By following these steps, a powerful tool to combat harassment and violence, fostering safer communities both online and offline can be created.

Media Pluralism Monitor (LMHTT) The proposed solution addresses the effective tracking and combating of hybrid threats that arise in the media sphere, specifically the manipulation of the information space, FIMI campaigns aimed at spreading disinformation and causing negative impacts among the society. The solution is extremely necessary to implement as it relates to the social domain and how media influence social life, causing cleavages in societies, spreading disinformation and manipulating the public	Media Pluralism Monitor 2024 - CMPF	The recommended roadmap indicates that it must be an EU-initiative behind the realisation and development of LMHTT solution. There is also a need that MSs embrace the idea and that national security stakeholders are prepared to join in using LMHTT. In addition, the EU already conducts a number of initiatives in the area of dealing with FIMI campaigns, and the LMHTT solution would be new but highly relevant addition to the already existing activities.

Table 4: The strategy for innovation uptake and industrialization

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) 4th Annual Workshop (AW) was arranged by Laurea together with Valencia Local Police (PLV) in Valencia during 24th of April 2024 (AW Agenda in Annex). Because the AW also provided a floor for relevant European Commission (EC) funded projects and innovative solutions that are seen relevant to the pan-European security practitioners and other relevant actors to counter hybrid threats, a more thorough analysis on their soundness for uptake and industrialization is provided below. In addition, in the AW the Keynote Speeches were related to the first Three Lines Actions focus area: "*Monitoring of research and innovation projects with a view to recommending the uptake or the industrialization of results"* and hence they are also described below according to T5.3/D5.13 "*Annual Workshop report 4*" (M49/ May 2024) results.

In general, the main goal of T5.3 is to arrange the EU-HYBNET Annual Workshop (AW) every year. The 4th AW was arranged in Valencia (24th of April 2024) in person in the premises of the EU-HYBNET partner PLV/ Valencia Local Police. According to DoA AW is arranged to disseminate project findings for large-scale of 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 to innovations 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.

As one of the EU-HYBNET AWs goal is to focus on innovation uptake and recommendations, in the 4th AW a session was dedicated to pitches of innovations and innovative solutions. A few months before the AW, the EU-HYBNET announced the possibility for innovative solution providers to suggest their innovation as a sound solutions to counter hybrid threats. In the EU-HYBNET announcement "Call for Pitches" the areas where innovation pitches were wished to have, were reflecting the EU-HYBNET project's 3rd cycle gaps and needs to counter Hybrid Threats. This call resulted to pitches that were presented in the 4th AW by the following organization on the innovations:

1. **Provider:** Marios Thoma, Director, CyberEcoCul Global Services
   Innovation: Denial-of-service/DDOS / attack on infrastructures critical to population livelihood

2. **Provider:** Marina Galiano Botella, CSIRT-CV Spain
   Innovation: Smart city

3. **Provider:** Vazha Sopromadze, The University of Georgia Security, Policy and Nationalism Center
   Innovation: Resilience Assessment Tool (R/VAT)

4. **Provider:** David Arroyo, The Spanish National Research Council
   Innovation: Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats

All the presented innovative solutions were providing tangible solutions to the EU-HYBNET's present, identified pan-European security practitioners' and other relevant actors' gaps and needs to counter Hybrid Threats and especially in the following areas:

- cyber security
- resilience in society
- disinformation and its links to business

The above-mentioned pitches and their solutions were especially important to EU-HYBNET T3.1 in order to proceed with the analysis and monitoring of research and innovation projects to recommend the uptake or the industrialization of results. In addition, T3.1 were also gaining information from some selected EC funded projects, that EU-HYBNET invited to pitch their project's innovative solutions because they were seen to deliver promising solutions for pan-European security practitioners' needs to counter hybrid threats in the following areas:

- foresight
- crime prevention. esp. recruitment of youngster to criminal actions
- critical infrastructure protection

The projects who were invited to the 4th EU-HYBNET AW to present their innovative solution are listed below. Next to the project(s), it is highlighted which EU-HYBNET's identified critical gaps and needs and threats the projects are seen to contribute with their solutions.

"Toward Sustainable Foresight Capabilities for Increased Civil Security" (AHEAD) project https://he-ahead-project.eu/

- Connection to EU-HYBNET's identified Hybrid Threat area: *Detection of the weak signals and vulnerabilities to improve foresight capability.* According to EU-HYBNET AHEAD delivers methodology for foresight analysis that can be adopted by wide range of security practitioners to conduct their gaps and need analysis. AHEAD's foresight analysis also supports future technological or non-technological solutions need mapping and hence supports organizations' needed solutions analysis and procurement. AHEAD methodology is to support security practitioners' to pay attention on future possible hybrid threats campaigns and how they might establish themselves in various forms of harming democratic states stability and decision making.

"Gaming Ecosystem as a Multi-Layered Security Threat" (GEMS) project https://www.projectgems.eu/

- Connection to EU-HYBNET's identified Hybrid Threat area: *Spreading violence.* According to EU-HYBNET GEMS delivers new methods and technological solutions for law enforcement authorities to prevent youngsters recruitment in gaming environment (physical and on-line) to criminal actions. GEMS is to deliver counter measures for adversaries recruitment processes of citizens to malicious actions or priming and espionage.

"European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection" (EU-CIP) Project https://www.eucip.eu/

- Connection to EU-HYBNET's identified Hybrid Threat area: *Undermining institutions' internal organisation.* According to EU-HYBNET EU-CIP provides welcomed network to pan-European critical infrastructure operators and other relevant actors (industry, SMEs, Academia, NGOs) to share information on research results and innovative solutions that may enhance the security of critical infrastructure operators.

In general, the invitation of EU-HYBNET to these projects highlights the importance of cooperation between them and EU-HYBNET especially in the efforts of promoting EC-funded projects' solutions to areas and activities that the solutions might not be tailored in the first place but may still deliver sounds solution for the new area(s) and groups of security practitioners as well.

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

As mentioned in chapter 3.1, EU-HYBNET project activities were launched by identification of practitioners' and other relevant actors' (industry, SMEs, academia, NGOS) gaps and needs and vulnerabilities to counter hybrid threats, in EU-HYBNET Tasks (T) 2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" (lead by Hybrid CoE) and T2.2 "*Research to Support Increase of*

Knowledge and Performance" (lead by JRC). The work conducted in T2.1 and T2.2 resulted in T2.2/D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (M39/ July 2023) where the most important pan-European practitioners' and other relevant actors' (industry, SMEs, academia, NGOs) gaps and needs to counter hybrid threats were listed for the 3rd project cycle for the project to focus on.

The identified gaps and needs, threats in D2.11 provide the basis for other EU-HYBNET Tasks to proceed in their work related to innovation mapping to gaps and needs, finding the most promising innovations and to compile recommendations for innovation uptake and standardization.

What comes to the second Three Lines of Actions focus area "**common requirements as regards innovations that could fill in gaps and needs",** the research activities and results in this Six Month Action Report reporting period are delivered by various Tasks especially from WP3 "Surveys to Technology, Research and Innovations" and WP4 "*Recommendations for Innovations Uptake and Standardization*.

In short, work in T3.1 "*Definition of Target Areas for Improvements and Innovations*"/ (Lead by TNO) focuses on delivering a final analysis of the most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs to counter hybrid threats in its' D3.19 "*Final report with overview mapped on gaps and needs*" (M50/June 2024) also lists **common requirements as regards innovations that could fill in gaps and needs**. In addition, in WP3/T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) where the latest, 4th Future Trends Workshop was arranged, provides insights on possible future, needed solutions and their requirements. The key results from T3.1 and T3.4 to the second Three Lines of Actions is reported in the sub-chapters 3.2.1. and 3.2.2 below.

Next to WP3 important innovation analysis relevant to the second Three Lines of Action has been conducted in WP4 "*Recommendations for Innovations Uptake and Standardization*"/ T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE) in D4.2 "3rd *Innovation uptake, industrialization and research strategy"* (M51/July 2024) and in T4.3 "*Recommendations for Standardization*" (lead by PPHS) in D4.10 "*3rd Report for standardization recommendations*" (M53/ Sept 2024). Both Tasks focused on the EU-HYBNET's 3rd project working cycle four most promising innovations (CRP, CiReTo, LMHTT, STARLIGHT) uptake analysis esp. what requirements the innovations need to meet that their uptake strategy may be successful, and they may face industrialization and be in-line with relevant standardization. The results achieved in T4.2 and T4.3 according to the second three lines of actions topic area "**common requirements as regards innovations that could fill in gaps and needs"** are described in the following sub-chapter 3.2.3 and 3.2.4.

3.2.1 EU-HYBNET T3.1 DEFINITION OF TARGET AREAS OF IMPROVEMENTS AND INNOVATIONS

T3.1 "*Definition of Target Areas for Improvements and Innovations*"/ (Lead by TNO) focuses on delivering a final analysis of the most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs to counter hybrid threats in its' D3.19 "*Final report with overview mapped on gaps and needs*" (M50/June 2024) also lists **common requirements as regards innovations that could fill in gaps and needs**. The key findings from D3.19 are listed below.

Target areas serve as guidance for standards and best practices in order to foster the development and implementation of like-wise innovations. The 7 identified target areas are: (1) Integration of cyber solutions, (dis)information detection tools, and (fake) news platforms; (2) Preparation, analysis and management of complex hybrid threats; (3) Improving and expanding information sharing capabilities; (4) Improving Societal Resilience; (5) Safeguarding democratic processes and institutions; (6) Strengthening physical security; and (7) fundamental research and low TRL innovations. In each target area, the assessment of innovations in terms of requirements that could fill in gaps and needs follows a path similar to the way that Horizon 2020 project applications are evaluated. There are three dimensions to be assessed: Excellence, Impact, and Implementation.

EXCELLENCE

In the Excellence dimension, there are 3 main aspects to consider in the assessment. This dimension has to do with how clear and pertinent the description of the innovation and its intended use is. All relevant aspects should be clearly described to enable a fair assessment. In particular, the scoring should be based on:

1. Clear definition of intended scope/applicability. Is the claimed coverage of EU-HYBNET Gaps and Needs, JRC domains, and core themes convincing? Is it clear which groups of practitioners and end-users (NGO's, private citizens, private companies, media outlets, police, firefighting departments) will benefit and how? Who will provide the service?

2. Clarity and pertinence of the solution description. Are the main components or elements of the innovation and their interactions (relations) described? Are the involved technologies, procedures and human/social aspects clearly pronounced? Are the required environmental prerequisites like operating environment given?

3. Credibility and soundness of the concept. Is the proposed innovation viable? Is the solution, based on the innovation, realistic?

IMPACT

In the Impact dimension, there are 4 main aspects to consider in the assessment. This dimension has to do with how big impact the innovation will have in detecting and/or countering threats and/or attacks and its coverage of use cases. In particular, the scoring should be based on:

1. The coverage. Is the solution useful in many domains versus only in a single or a small number of domains? In the covered domains, is this a dearly needed solution or is it a nice-to-have solution?

2. The scope. Is the solution applicable to a narrow and specific problem space or does it apply to a broad set of problems? Is the solution scalable to the extent required to cope with the claimed scope? Does it rely on cooperation between MS and/or different practitioner groups and end users? If so, is there a need for standardization for interoperability?

3. Acceptance: How high is the level of resistance from practitioners and end-users to the use and implementation of the solutions due to possible changes of processes or needed introduction of new processes? Will an implementation of the innovation lead to major immediate changes in current ways of working or will it be a gradual change? Will society accept the consequences of the innovation being implemented? Is there a need for changes in regulatory frameworks? Are there side

effects to consider? How strong are the influences on the economy, society and politics? What is the SRL (Societal Readiness Level 5) for this type of solution?

4. Effectiveness and robustness: How effective is the solution in handling the problem at hand? How robust is the solution against attack and/or threat variations? Are there restrictions (legal or ethical) that limit the use of the solution? If so, do they differ between MS and practitioner groups? Which is the expected longevity of a solution based on the innovation?

IMPLEMENTATION

In the Implementation dimension, there are 5 main aspects to consider in the assessment. This dimension has to do with the size of the effort required for bringing the innovation to life, its operational and maintenance cost as well as the time when it can be taken into practical use. In particular, the scoring should be based on:

1. Preconditions: Are all conditions met, which are required to bring the innovation to life? Are there any important tasks, developments or decisions that remain to be made? Are there any specific barriers identified, which could hinder an implementation? Is there a reliance on external partners or functionalities?

2. Implementation effort: How big are the expected costs (development cost, capital expenditure and operational expenditure) for bringing the innovation into a practically usable technical and operational solution? If relevant, which is the TRL level of the key technologies used. What are the difficulties/cost of integration in current organization and/or processes for the set-up of an operational environment?

3. Implementation resources: Would finding the required funding for development be a problem? Would finding development and/or implementation resources be a problem? Are there scarce key competencies required for a successful implementation? Are there any willing early adopters?

4. Life-cycle maintenance: Who will operate, maintain, update and upgrade the solution? Does this require a lot of effort? Is specific (critical, scarce, costly) manpower required for the maintenance? Can it be done by internal manpower or does maintenance needs to be outsourced?

5. Time aspects: What is the expected time to market: relatively short (0-3 years) or is it foreseen to take longer than 5 years from now? Is the implementation of this innovation time-dependent on the introduction of other innovations?

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 4th Future Trends Workshop (FTW) arranged by EOS and PLV in Valencia on April 24th, 2024. The comprehensive description on FTW is delivered in D.3.17 "4th *Future Trends Workshop Report*" (by PLV on M49/May 2024). The sub-chapters below summarize the key FTW findings on "**Common requirements as regards innovations that could fill in gaps and needs**" according to the FTW Agenda starting from Keynote speeches and ending to the panel discussion on the days' key findings (Agenda in Annex III).

EU-HYBNET 4th Future Trends Workshop (FTW) provided a platform of interaction on emerging hybrid threats in the EU's neighbourhood, their implications for the future of EU security and potential innovations to counter them. Discussions between academics, researchers, institutional stakeholders at national and EU level, civil society representatives and practitioners were extremely useful as they allowed enhancing of awareness, shaping of new perspectives, better understanding of the interdisciplinary character of the challenges addressed while, at the same time, facilitated transfer of knowledge.

While FTW key note speeches and panel presentations aimed to give participants insight from reputed pan-European security practitioners and industry representatives national and EU level on key aspects of hybrid threats detection and understanding, the other part of the workshop gave participants the chance to interact and debate in break-out sessions (BOS) existing and future trends in the EU-HYBNET core themes: (1) Cyber & Future Technologies, (2) Resilience of civilians, local and national level administration, (3) Information & Strategic Communication, (4) Future Trends of Hybrid threats. In addition, the discussions in the BOSs aimed at understanding the contexts of hybrid threats and trends, drawing a broad picture of the environment in which potential innovations could be imagined. The participants' task was to define, what they think are the most relevant trends affecting the future of hybrid threats and what kind of common requirements are needed form innovations answering the future challenges. The key take aways form keynote speeches, panel discussions alike topics of each BOS session are summarised below alike their feedback to the needed innovations and common requirements.

Keynote Speeches

The first FTW Keynote speech on "*Models for Conflict Analysis & Some Critical Remarks on Dealing with Hybrid Threats*" was given by Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience from Belgian General Intelligence and Security Service, Belgian Armed Forces. The speech focused on various methodological approaches to discover hybrid threats and hence highlighted the importance of non-technological solutions to answer security practitioners' gaps and needs to counter hybrid threat. Common requirements as regards innovations/ innovative approaches that could fill in gaps and needs were highlighted to be following:

1. *Multi faceted taxonomies and standardization models to remove blind spots*
   It became apparent that there are various different conceptual models that can be used to analyse conflicts, events and threats and they all built in biases or different levels. This makes it then challenging to skew understanding in a way that renders a common situational awareness. The question then arises, how to formulate the past of various identified issues in a complex and multi-level environment, such as border management where multiple actors

are involved, into a prompt and generally shared common situational awareness. A suggestion was to use multi-faceted taxonomies and standardization models in order to remove blind spots and to have wide and generally shared situational awareness among practitioners on hybrid threats.

2. *Foresight and use of scenarios and creation of strategies to improve preparedness and response*
   Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don't pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to understand how technology can be used in new ways to undermine border security or slow down border management processes.

The second Key note speech on "*Future of Hybrid Threats in Relation to Border Management*" was given by Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX. Mr. Rempling highlighted that FRONTEX has been actively assessing and addressing the challenges posed by hybrid threats. The starting point is that Hybrid threats encompass a wide range of tactics that blend conventional and unconventional methods to achieve strategic objectives. The threats can include cyberattacks, disinformation campaigns, irregular migration, smuggling, terrorism, and more. Hybrid threats are particularly complex because they often exploit vulnerabilities in multiple domains simultaneously, making them difficult to detect and counter. In the context of this complexity, hybrid threats pose significant challenges for FRONTEX and in general border security agencies. Therefore innovative approaches and technological innovations are required to fill in following gaps and needs:

1. **Cyberattacks**. Hybrid threats may involve cyberattacks targeting critical border management systems, such as databases, surveillance networks, and communication infrastructure. These attacks can disrupt border operations, compromise sensitive information, and undermine the effectiveness of security measures.

2. **Disinformation**. Hybrid actors may spread disinformation to manipulate public opinion, create confusion, and undermine trust in border management authorities. False narratives about migration, border security, and EU policies can exacerbate tensions and complicate efforts to address security challenges.

3. **Irregular Migration and Smuggling**. Hybrid threats often exploit vulnerabilities in migration routes and border controls to facilitate irregular migration and smuggling activities. Criminal networks may use sophisticated tactics to evade detection, exploit legal loopholes, and circumvent border security measures.

4. **Terrorism and Extremism**. Hybrid threats may involve the infiltration of terrorist or extremist elements among migrant flows, posing a security risk to border management authorities and the wider community. Identifying and intercepting individuals with links to terrorist organizations or radical ideologies requires robust intelligence-gathering capabilities and effective cooperation with law enforcement agencies.

As an answer to address these challenges, FRONTEX supports a multi-layered and integrated approach to border management, combining technological innovation, intelligence-led operations, cooperation with EU member states and third countries, and strategic partnerships with international organizations. By enhancing situational awareness, improving information sharing, and strengthening border controls, FRONTEX aims to mitigate the risks posed by hybrid threats and safeguard the integrity of the EU's external borders.

Panel

The Panel discussion focused on "*Border Management to counter future hybrid threats*" and the panel representatives were coming from the Finnish Ministry of Interior/ Mr. Jarmo Puustinen, Laurea University of Applied Sciences/ Mr. Isto Mattila, Europol Innovation Lab and Satways/ Dr. Souzanna Sofou.

The starting point for the panel discussion was the fact that in border management to counter future hybrid threats there is need for clear strategies and tactics. The strategies and tactics aim at protecting a nation's borders from a wide range of threats that may involve both conventional and unconventional elements. Hybrid threats typically combine conventional military force with non-military means such as cyberattacks, propaganda, and economic pressure to achieve their objectives. The key components and considerations for border management in countering hybrid threats were considered to be following innovative approaches and technological innovations:

1. *Integrated Approach*. Effective border management requires an integrated approach that combines military, law enforcement, intelligence, diplomatic, and other relevant agencies. Coordination and cooperation among these entities are essential to address the diverse nature of hybrid threats.

2. *Intelligence Gathering and Analysis*. Border security efforts rely heavily on intelligence gathering and analysis to identify potential threats before they materialize. This includes monitoring activities such as illicit trafficking, cyber intrusions, and hostile propaganda aimed at destabilizing the country.

3. *Technology and Surveillance*. Advanced technology, including drones, sensors, radar systems, and surveillance cameras, plays a crucial role in monitoring and securing borders. These technologies help in detecting and intercepting threats, including unauthorized border crossings and smuggling activities.

4. *Cyber Defense*. In the modern era, cyber threats are a significant component of hybrid warfare. Robust cybersecurity measures are essential to protect critical infrastructure, communication networks, and government systems from cyberattacks aimed at undermining national security.

5. *Border Infrastructure.* Investing in physical infrastructure such as border fences, checkpoints, and surveillance towers can enhance border security and deter unauthorized activities. Additionally, improving transportation infrastructure can facilitate the movement of security forces and enable rapid response to emerging threats.

6. *International Cooperation*. Hybrid threats often transcend national borders, requiring cooperation with other countries and international organizations. Information sharing, joint

exercises, and collaborative initiatives can strengthen border security and counter hybrid threats more effectively.

7. *Public Awareness and Resilience.* Educating the public about potential threats and promoting resilience can enhance a nation's ability to withstand hybrid attacks. This includes raising awareness about cybersecurity best practices, emergency preparedness, and the role of citizens in reporting suspicious activities.

8. Adaptability and Flexibility: Border management strategies must be adaptable and flexible to respond to evolving threats. Continuous assessment of risks and vulnerabilities is essential to adjust tactics and allocate resources effectively

Break Out Session Outcomes

The breakout sessions facilitated by the EU-HYBNET project's four core theme leaders: L3CE, JRC, URJC and Hybrid CoE. These sessions explored Cyber & Future Technologies, Resilient Civilians, Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats and esp. on topic: *"Securing the EU's borders to 2040 – Thinking about the security landscape*".

Every breakout session was customized to address recognized deficiencies and requirements within its corresponding core theme. Participants actively engaged in conversations surrounding emerging trends, advancements, and hurdles associated with hybrid threats, with chances for hands-on demonstrations and dialogue focused on finding solutions. These sessions served as a forum for thorough exploration and the exchange of ideas, enhancing comprehension of hybrid threats and guiding the development of future strategies and innovations for their effective mitigation. Eventually the key takeaways to "Common requirements as regards innovations that could fill in gaps and needs" were mainly focusing on topic "Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats" and were following:

- **Sharing Intelligence and Best Practices**. Countries need to collaborate closely in sharing intelligence about emerging disinformation campaigns and the tactics used. Pooling resources and expertise can lead to more effective identification and mitigation strategies.
- **Unified Regulatory Frameworks**. Establishing common regulatory standards and cooperative frameworks can help govern the digital landscape where much of this disinformation proliferates.
- **Cross-Border Collaborative Initiatives**. Initiatives like joint educational programs, public awareness campaigns, and cross-border fact-checking teams can significantly enhance the resilience of societies against disinformation.
- **International Research and Dialogue.** Encouraging research, dialogue, and exchange programs focused on understanding and addressing the global dynamics of disinformation can foster a unified approach.

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

During the reporting period EU-HYBNET T4.2 identified four most promising innovations to innovation uptake strategy creation on the basis of T3.1/D19 most promising innovations analysis and priority ranking. In T4.2 the selected four most promising innovations were following:

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

Because T4.2 inherited form T3.1 analysis how well the suggested innovations could answer to the pan-European security practitioners' and other relevant actors gaps and needs to counter hybrid threats, the innovation uptake strategies created in T4.2 to the four most promising innovations does describe key elements that are seen as **common requirements as regards innovations that could fill in gaps and needs.** Uptake strategies to each of the four most promisng innovations are described below.

AI Enhanced Disaster Emergency Communications (CRP) - innovation

- Study existing solutions and researched approaches for how and what citizens can report in the platform. Define a taxonomy; a starting point could possibly be found in: A Taxonomy of Crisis Management Functions[5]
- Study how anonymization / pseudonymization may be integrated in the solution to protect citizens when reporting incidents.
- Develop a standardized solution for how to report.
- Develop an extensible standard for what can be reported.
- Develop and/or extend existing encodings and protocols (e.g., STIX /TAXI as used in CTI reporting and hybrid threats related information transfer.
- Design a generic language interface for language adaptations to allow use in all EU MSs.
- Develop AI based analytical tools for authentication of data (fake or real)
- Develop a proof-of-concept implementation.
- **Summa summarum:** it is recommended that an R&D action is initiated to define standards for interfacing existing tools that would be useful in the CRP context and also develop missing tools.
    - Standardise and define principles for how AI analysis results can be shared to the first and second responders, and in case of indicated false, fake alarms as part of a possible hybrid threats campaign should be shared with relevant intelligence services. The work should cover the needs for situational awareness in EU crises response and for monitoring and analysis of disinformation from large amount of data.
    - Initiate an innovation action to implement a proof of concept and use it to evaluate/demonstrate the solutions benefits for first- and second-line responders.

[5] A Taxonomy of Crisis Management Functions

Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo) - innovation

- User-Centric Design: Prioritize user experience by designing an intuitive and easy-to-use interface that encourages reporting while also considering the sensitive nature of the subject matter.
- Multi-Platform Accessibility: Develop the application for iOS & Android mobile environments, but perhaps also for web platforms, to ensure accessibility for a wider range of users.
- Community Engagement: Implement features that promote community engagement, such as forums, support groups, or educational resources, to foster a sense of solidarity and support among users.
- Partnerships and Collaborations: Forge partnerships with law enforcement agencies, advocacy groups, and other stakeholders to enhance the effectiveness of incident response and support services.
- Data Security and Privacy: Prioritize data security and privacy by implementing robust encryption protocols and obtaining explicit consent from users before collecting any personal information. Investigate the possibility to use anonymization of the reporting user/device and still allow use of reported data as evidence.
- Awareness and Education: Launch awareness campaigns and educational initiatives to inform users about the importance of reporting and preventing harassment and violence, as well as providing resources for self-defence and conflict resolution.
- Continuous Improvement: Regularly solicit feedback from users and iterate on the application based on their suggestions and evolving needs. Stay updated on emerging trends and technologies to enhance the app's effectiveness in addressing harassment and violence.
- **Summa summarum**: It is recommended that an R&D action is initiated to
  - Develop and standardize an architecture for how current and future tools for citizens reporting of emergencies and hybrid threat related events can be integrated in an efficient central service.
  - Develop guidelines on how to ensure a user-centric design, providing multi-platform accessibility of a citizens mobile reporting app and at the same time ensure that security and adequate privacy can be maintained.
  - Study how users' (citizens') consent for the use of a reporting app can be obtained and registered.
  - Use standardized taxonomy, encoding formats and transport protocols defined.
  - Initiate an innovation action to implement a proof of concept for evaluation/demonstration of the CiReTo concept.
  - Foster community engagement and forge partnerships and collaborations with law enforcement agencies, advocacy groups, and other stakeholders to enhance the effectiveness of incident reporting, response and support services.

Media Pluralism Monitor (LMHTT) - innovation

- Establish an institution who will take responsibility for the methodology of the LMHTT solution or delegate this task to e.g., EDMO (European Digital Media Observatory) and its

14 Hubs covering all 27 EU MSs as well as Norway. The selected institution should be tasked to ensure that assessments are performed regularly.

- Build a comprehensive methodology and evaluation questionnaire.
- Division of each country into regional/local areas, taking into account internal circumstances and observable needs/signals.
- Collect data according to the questionnaire (prepare several regional/local reports).
- Analysis of the gathered data.
- Presentation and visualisation of results and recommendations on a LMHTT platform. Another European institution could be responsible for maintaining, updating and managing the solution.
- Notification and alerting of security agencies and government institutions responsible for internal security in European countries.
- **Summa summarum**: It is recommended the following to ensure the implementation of LMHTT:
  - Initiate a research and innovation action to investigate the situation of local and regional media in the MSs. Involve end-users (security practitioners) to understand their exact needs.
  - Design a comprehensive LMHTT diagnostic tool by defining standardized procedures for data collection and reporting in a questionnaire.
  - Develop comprehensive data analytics tools and an interactive dashboard for data visualisation.
  - Delegate the maintenance of the LMHTT tools to a competent body, possibly ENISA.

Starlight Disinformation-Misinformation Toolset (STARLIGHT) - innovation

- Finalise development of tools with clear involvement of end users.
- Test tools in real environment, using real data and based on real cases.
- Complete supporting components of developed tools.
- Make tools available for LEAs through dedicated channels (Europol, EACTDA, own Starlight repository).
- Encourage end-users in security sector to get involved in the early stage of solution development.
- **Summa summarum:** To initiate and increase use of co-development of tools in the field of hybrid threats it is recommended to:
  - Promote use of an agile co-development methodology as demonstrated in the STARLIGHT project. Development of solutions together with end-users is considered a good practice, facilitating end-users' interest and involvement.

As a conclusion to the innovations mentioned above, it is relevant to know that the innovations reviewed and scoped from T3.1 into T4.2 recommended four most promising solutions, were categorized by high TRLs. This means that the time from adoption of the ideas till working solutions should be relatively short. Together, the four innovations will benefit the resilience of the society as a whole. The innovations CRP and CiReTo are strongly related in that CRP focuses on information handling of citizens' reports in an information sharing environment while CiReTo focuses on the means for citizens to report emergencies and hybrid threat related events to first- and second-line responders. Some of the tools developed in STARLIGHT would be useful in CRP and the use of

STARLIGHT's technical development process should result in solutions (for CRP and CiReTo) that are end-user friendly and easy to integrate into existing operating environments. of applications. LMHTT would also contribute to building resilience in the society as a whole by detecting and tracking worrying signs of decreased media pluralism which eventually may lead to hybrid threats related (F)IMI.

3.2.4 EU-HYBNET T4.3 RECOMMENDATIONS FOR STANDARDIZATION

In T4.3 "*Recommendations for Standardization*" (lead by PPHS)/ D4.10 "*3rd Report for standardisation recommendations*" (M53/ Sept 2024) focus during the EU-HYBNET's 3rd project working cycle has been in EU-HYBNET's four most promising innovations (CRP, CiReTo, LMHTT, STARLIGHT) uptake analysis esp. what requirements the innovations need to meet that their uptake strategy may be successful and they may face industrialization and be in-line with relevant standardization. The results achieved in T4.3/D4.10 according to the second three lines of actions topic area "**common requirements as regards innovations that could fill in gaps and needs"** are described below according to each of the EU-HYBNET's four most promoted innovations.

Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo)

Attacks on societal structures and cohesion, both in the form of online harassment, as well as in the form of the spread of violence, present current but also future trends in hybrid threats that need to be challenged. To be challenged successfully, the first signs of such occurrences should be noted in order to provide situational awareness of the threat, if not to provide an early warning. In such a case, the responsible law enforcement agencies could react in a timely manner in both the virtual, but also in physical space and use their resources intelligently according to the situation. Should the situation continue to escalate, a response from rescue services may be needed as a precaution or to assist possible victims.

Involving the public in detecting signs of harassment or hybrid threats serves multiple purposes. Firstly, it allows for saving on valuable resources, such as on expensive online monitoring systems or CCTV, or patrolling of the streets. Secondly, it significantly diminishes the required time for discovering and locating occurrences of the above-mentioned threats. Thirdly, it facilitates in society resilience building by providing everybody – especially the youth – with the opportunity and the option of participating in the creation of more security.

Smartphones integrate three important technologies to conduct such activities: the clock to have a timestamp on the occurrence; the camera to record the action or written text as video or audio; the geolocation to pinpoint the occurrence on the virtual map. Adding an option to report occurrences online gives the users – law enforcement agencies and other stakeholders – the opportunity to monitor evolving situations in real time and note the correlations in physical space and online. The application would be especially useful in crisis situations like riots if used by a large number of users.

Integration with other platforms, such as social media, public transportation systems and other platforms to enhance its functionality and reach, in addition to AI and machine learning can be used to predict high-risk areas and times, offering proactive safety suggestions to users

Starlight Disinformation-Misinformation Toolset (STARLIGHT)

The Starlight project is still in progress and technological solutions are still under development and will be made available at the end of the project. However, at this stage, STARLIGHT methodological approach can be already adopted by many other institutions beyond LEA. During the implementation of the STARLIGHT project, the co-development methodology gained a lot of end-users' interest and involvement and hence it is also seen as valuable by EU-HYBNET to deliver tangible common requirements as regards innovations that could fill in gaps and needs. On the whole, STARLIGHT's activities are end-user focused and they are involved in the evaluation and testing of innovative solutions at different stages. The concept of "test before invest" is also gaining popularity in many sectors. In the given circumstances this approach is rather novel for the security sector, especially LEA's, as they traditionally tend to be rather closed ecosystems. Uptake of innovative solutions and co-development is not a common practice in those institutions. There is no final evaluation of the efficiency and impact of the practice in scope, but current developments indicate good results. This is also the reason why already on the basis of the preliminary results EU-HYBNET considers STARLIGHTS approach to test innovations and develop them further as a solid common requirement as regards innovations that could fill in gaps and needs.

AI Enhanced Disaster Emergency Communications (CRP)

Citizen Responder Platform (CRP) is an innovative technological solution designed to facilitate the trusted exchange of information between citizens and first and second responders in emergencies and crises. This platform is unique in its use of AI-powered analysis and the ability to integrate new services, apps, and tools. While similar systems, such as "Common information Sharing Environment" (CISE https://www.emsa.europa.eu/cise.html) in the maritime sector, already exist, CRP stands out due to its broad applicability and inclusion of both citizens and authorities.

The successful launch and development of CRP require an EU initiative that provides the necessary funding and facilitates integration into the existing systems of EU member states. Existing EU projects could support this effort and enhance the platform's acceptance, particularly through public procurement.

However, the implementation of CRP faces several challenges. Technologically, standardized integration processes for apps and services need to be developed, and a robust AI analysis must be ensured to minimize false alarms. Interoperability issues may arise when integrating the platform into the existing systems of first and second responders.

User acceptance is another critical factor. It will take time for new approaches to become popular and widely adopted. Intelligence agencies could develop additional interest in CRP if the platform effectively provides information on hybrid threat campaigns.

Regulation and ethical acceptance are also important. The platform must comply with data protection regulations and be secure against hacking. Citizens could share videos and information that raise privacy concerns, which could impact societal acceptance.

Economic barriers could arise if the costs of building and implementing the platform are too high. Operational barriers exist in implementing the necessary structures and cooperation between various stakeholders.

Ultimately, it is crucial to involve and convince relevant practitioners, citizens, SMEs, and the industry in all EU member states of the benefits of CRP to ensure its broad acceptance and use.

Media Pluralism Monitor (LMHTT)

Media at the regional and local levels are particularly important for democracy, and their relationship with local citizens tends to be closer if compared to national media. However, local and regional media are receiving less attention in the public discussion and the situation shows that they are increasingly struggling to survive.

The main issues and concerns relating to media pluralism, with a particular focus on the challenges facing local and regional media in the EU and candidate countries, are presented in the latest Media Pluralism Monitor 2024 Report (MPM)6. The report provided a comprehensive overview of the media pluralism situation in the European Union (EU) and candidate countries for 2023. The average risk level for media pluralism has generally increased across the EU and candidate countries, indicating a growing concern for media diversity and freedom. The report highlights a significant increase in risk concerning local and regional media. This is mainly due to the existence of the threat called "news deserts" - defined as "geographic or administrative area, or a social community, where it is difficult or impossible to access sufficient, reliable, diverse information from independent local, regional and community media" - in many countries, where local media outlets have diminished or disappeared altogether. Moreover, local and regional media are particularly vulnerable to economic pressures. The report notes a deepening crisis in the economic sustainability of local media, with traditional revenue models continuing to decline. Innovative practices and new models have not yet fully countered these challenges. This situation can also have a major impact on pluralism and media freedom.

As the report showed, many countries lack specific legal safeguards for local and regional media, which contributes to the overall increase in risk. The absence of dedicated support mechanisms and policies to sustain these media outlets makes them particularly vulnerable. Moreover, the indicator on media viability, which includes local and regional media, showed that economic situation has affected media revenue, with local media being the hardest hit. Employment within these outlets also remains precarious. When it comes to market plurality, the report showed that no country is at low risk. The Market Plurality area scores at high risk at 69%, the same level registered in the MPM2023. The main risks in this area have the source in the concentration of media ownership and the concentration in the digital markets, which are threatening the media pluralism.

The MPM2024 also found average risk of spreading disinformation high (71% for all countries studied). It has been found that there is a lack of comprehensive strategy that defines the role of different stakeholders involved and only six countries have taken significant steps to develop comprehensive strategies against disinformation.

Another point, which is not a new issue, is gender equality in media. It is an integral part of human rights that everyone shall care about and respect. It is a part of media social inclusiveness that is a key element of media pluralism. According to the report, there is an average medium or high risk when it comes to gender equality in media landscape.

[6] https://cadmus.eui.eu/handle/1814/77028

The above findings highlight the crucial role of local and regional media in maintaining media pluralism and ensuring that diverse voices are heard in all regions. The decline of these media outlets poses a serious threat to the democratic process, and therefore encourages emerging FIMI campaigns and the spread of disinformation.

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

In EU-HYBNET the WP4 *"Recommendations for Innovations Uptake and Standardization*" two of its' Tasks have delivered main contribution during the reporting period to the Three Lines of Action "**Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation**" – the WP4 contribution has been delivered by Task (T) 4.3 "*Recommendations for Standardization*" (lead by the Polish Platform for Homeland Security/ PPHS) and T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE). Afterall, both of the Task, T4.2 and T4.3, have been focusing on the promoting the four most promising EU-HYBNET's identified innovations for uptake that is then providing a prioritization on knowledge and skills/performance that needs to be focused on and, if possible, also to address to standardization. Valuable findings from T4.2 and T4.3 concerning the third three Lines of Action goals are described in in the sub-chapters below.

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

The T4.2 "*Strategy for Innovation Uptake and Industrialization*" (lead RISE) contribution to the third Three Lines of Action "**Priorities as regards of increasing of knowledge and performance requiring standardization**" is well highlighted in T4.2/ D4.6 "*Third Innovation uptake, industrialisation and research strategy"* in M51 (July 2024) because the main goal in D4.6 is to describe four most promising innovations (acronyms: CRP, CiReTo, LMHTT, STARLIGHT) for innovation uptake, and in the analysis also insights to existing standards or standardized actions are highlighted to support the uptake.

Each of the T4.2/D4.6 identified and promoted innovation with relevant standards or standardizations needs under EU-HYBNET Core themes to which they contribute are described below in their own subchapters.

Core Theme: Future Trends of Hybrid Threats/ Innovation: "*Mobile application to pinpoint acts of harassment/violence on the street and online" (CiReTo)*

According to T4.2, the rationale behind the choice of the innovation "**Mobile application to pinpoint acts of harassment/violence on the street and online**" (or Citizens Reporting Tool – CiReTo for short) as one of the most promising innovation to focus on was two-fold. First, in T3.1 "*Definition of Target Areas for Improvements and Innovations*" analysis, CiReTo was rated high and belong to the group of ten most promising innovations that may support security practitioners to overcome challenges related to hybrid threats detection and response esp. among civilians daily life. In addition, in T4.2 analysis CiReTo was also rated high and seen as a very straightforward solution which could especially involve citizens to work with law enforcement authorities and to enhance law enforcement authorities' performance to detect hybrid threats campaign(s).

In short, attacks on societal structures and cohesion, both in the form of online harassment, as well as in the form of the spread of violence, present current but also future trends in hybrid threats that need to be challenged. To be challenged successfully, the first signs of such occurrences should be noted in order to provide situational awareness of the threat, if not to provide an early warning. In such a case, the responsible law enforcement agencies could react in a timely manner in both the virtual, but also in physical space and use their resources intelligently according to the situation. Should the situation continue to escalate, the response from rescue services may be needed as a precaution or to assist possible victims. Involving the public in detecting signs of harassment or hybrid threats serves multiple purposes. Firstly, it allows for saving on valuable resources, such as on expensive online monitoring systems or CCTV, or patrolling of the streets. Secondly, it significantly diminishes the required time for discovering and locating occurrences of the above-mentioned threats. Thirdly, it facilitates in society resilience building by providing everybody – especially the youth – with the opportunity and the option of participating in the creation of more security.

The aim of the innovation CiReTo is to use readily and widely available technology (i.e. smartphones) to record and geolocate acts of harassment and violence (or calls for violence) in physical space and acts of harassment and calls for violence online (geolocation can be achieved via Geotagging, or GeoTagging, which is the process of adding geographical identification metadata to various media such as a geotagged photograph or video). Such acts may occur in the form of physical action on the street, but also in the form of graffiti and/or leaflets in physical space and/or online. Smartphones integrate three important technologies to conduct such activities: the clock to have a timestamp on the occurrence; the camera to record the action or written text as video or audio; the geolocation to pinpoint the occurrence on the virtual map. Adding an option to report occurrences online gives the users – law enforcement agencies and other stakeholders – the opportunity to monitor evolving situations in real time and note the correlations in physical space and online. Therefore, the CiReTo aims both to increase knowledge among law enforcement authorities on possible on-going hybrid threat campaigns (e.g. graffiti that aim to affect mindset and to increase polarization) but also to provide source of information that should support law enforcement authorities' performance to reveal hybrid threat campaigns and track the actors.

Because CiReTo is mainly technical innovation, an important part of its' uptake focuses on IT issues. The standardization considerations from technical perspective are following:

- Integration with other platforms, such as social media and public transportation systems, to enhance its functionality and reach. In addition to AI and machine learning can be used for analysis.
- Basic examples of existing apps used for reporting emergencies are the 112 apps available in many MSs. Some even have special accessible versions for e.g., persons with hearing disabilities. Another example which could be implemented as an app is that of the solution "Right To Be"7, which is a platform for reporting street harassment.
- The proposed mobile application aims to provide users with a platform to report and document acts of harassment or violence both on the street and online, including real-time reporting, mapping, community support, and resource access to empower individuals and promote safer environments. A brief recapitulation of the key functional features the solution

[7] https://righttobe.org/

might entail are: User Registration / Authentication and Profile Management; Incident Reporting using media uploads with an anonymity option; Real-Time Geolocation and Mapping with heat maps of high-density areas of reported incidents to identify hotspots, as well as suggested safe routes based on reported incidents; Community Engagement via community alerts, discussion forums and upvoting/downvoting reports that will allow users to validate or question the authenticity of reports; Verification Tools and Moderation Badges to indicate users have been reviewed by a moderator or verified by multiple users; Safety Resources; Data Analytics and Reporting; Privacy and Security, guaranteeing data encryption, GDPR compliance and two-factor authentication (2FA) which provides an extra layer of security for user accounts; a User Interface with intuitive design, accessibility features, notifications and custom alerts; Multi-Language Support; Cross-Platform Availability; Community Partnerships with local organizations and authorities to enhance the app's effectiveness and credibility. By incorporating these features, the mobile application can effectively support individuals in documenting and addressing incidents of harassment or violence, fostering a safer and more aware community.

Core Theme: Cyber and Future Technologies/ Innovation: "*Starlight Disinformation-Misinformation Toolset" (STARLIGHT)*

According to T4.2, the rationale behind the choice of the **Starlight Disinformation-Misinformation Toolset** (**STARLIGHT,** coming from STARLIGHT project https://www.starlight-h2020.eu/) as one of the most promising innovations is two-fold. First, in T3.1 *"Definition of Target Areas for Improvements and Innovations*" analysis, STARLIGHT was rated high, belonging to the group of eight most promising innovations that may support security practitioners to overcome challenges related to hybrid threats esp. in the information and cyber domain. In addition, in the last EU-HYBNET training event in Vilnus (Jan 2024) STRALIGHT was among the highest priority ranked tested innovations. STARLIGHT was seen to deliver important support for law enforcement authorities' performance to detect and analyse foreign information manipulation and interference (FIMI) with the support of a set of AI-powered tools.

On the whole, identifying content in social platform media that has been manipulated to attack democracies is a complex task which has becomes relevant for different stakeholders such as media outlets, factcheckers, professionals of strategic communication alike for law enforcement organizations (LEA's). Their scope primarily focused on illegal content that can be MS specific, but includes hate speech, use of forbidden symbols, direct threatening, but might include wider subjects.

In EU-HYBNET's STARLIGHT innovation's focus is on development of a wide range of AI-supported tools, esp. advanced LEA tools for social platform content analysis to detect illegal and inappropriate content by providing specifically tailored solutions and improvement of up-take capabilities/understanding by end-users in the security sector. The disinformation and misinformation co-development (named CODEV in Starlight project) is composed of several organisations developing different tooling, enabling deep access of information in social platforms and tools to detect different misleading aspects of the information. The goal is to increase performance of LEAs to counter hybrid threats.

In addition, in EU-HYBNET also STRALIGHT's innovation testing approaches are promoted and highlighted as priority to increase knowledge among LEAs, how the selected tools may support their

work. In short, Agile co-development methodology, applied in the STARLIGHT project implementation is promoted as testing approach when there is need to cover wide variety of different tools developments. According to the Agile methodology tools are grouped together according to their functionalities and intended use, and there are co-development cycles in each of the groups in scope. Co-development means that each group has potential end-users of the solutions under development. Development is done based on aligned expectations, end-users provide use cases and are involved in the overall development process. Each co-development cycle ends up with the Tool Fest, where all solutions are presented to end-users. Such approach provides benefits for both, developers and end-users. Developers getting to understand the realistic needs of end-users during the development, so they can adjust functionalities, interface or other aspects during the early stage. At the same time end-users can understand the solution better, get to know how they can use it and what results they can expect. Early involvement and co-development are essential for the uptake process. This approach can also be applied in other projects or uptake processes in different organizations in general.

Because the STARLIGHT tool testing methodology (Agile) can be applied wider for the security sector, and the methodology will eventually support LEAs to have the most fitting tools empowering their performance, in EU-HYBNET we promote the testing methodology standardization. The key elements in the methodology are:

- To divide experts into few co-development groups where different type of solutions is developed uniting end-users and developers.
- Tool development is made in various (e.g. three) cycles, during each some milestones are to be reached. In this good practices are:
  - Development is guided towards the realistic needs of end-users and resources are directed to the expected functionalities instead of "blind" development;
  - End-users understand the intended solution at the early stage and during the co-development process and can understand how it can help in their daily activities, fit process and up-take challenges.

What also speaks on behalf of Agile testing methodology standardization is that similar approach with some modifications is also applied in other initiatives, e.g. in EACTDA (European Anti-Cybercrime Technology Development). In short, EACTDA activities are end-user focused and they are involved in the evaluation and testing of innovative solutions at different stages. EACTDA's concept of "test before invest" is also gaining popularity in many sectors while this approach is rather novel for security sector. Still there seems to be increasing interest for co-development of innovative solutions before their uptake.

Core Theme: Resilient Civilians, Local Level and Administration/ Innovation: *"AI Enhanced Disaster Emergency Communications" (CRP)*

According to T4.2 the rationale behind the choice of the innovation **"AI Enhanced Disaster Emergency Communications" (CRP)** as one of the most promising innovations to focus on was two-fold. First, in T3.1 "*Definition of Target Areas for Improvements and Innovations*" analysis, CRP was rated high, belonging to the group of ten most promising innovations to counter hybrid threats esp. when preventing adversaries to harm communication between citizens and emergency first responders during crises. In addition, in the last EU-HYBNET training event in Vilnus (Jan 2024) CRP received the highest priority ranking among tested innovations to counter hybrid threats especially

when focusing on solutions that supports fast and exact information sharing and communication between citizens and emergency first responders during crises.

In general, tools to solve "attack on social structures" such as hospitals and hospitals' capabilities to conduct their work under crisis and large-scale emergencies amplified by malicious actors' in hybrid threat campaigns e.g. in a form of false emergency calls to hospitals are seen highly important. Civil protection authorities also play an important role in the handling of crises and emergencies and esp. patient afflux next to hospitals. Therefore, company HighWind's "*AI Enhanced Disaster Emergency Communications*" (AI-EDEC) solution and "*Disaster Mode*" app, tools such as the company WeSolve's "*Resilience Bridge Net"* (ReBriNett) were seen very relevant building blocks to EU-HYBNET's CRP innovation.[8] On the whole, ReBriNett is a solution for first- and second-line responders to support them in information sharing and learning during preparation for and during recovery from an emergency. ReBriNett is able to deliver the following services for the first- and second-line responders:

> *"Resilience Bridge Net" (ReBriNett) is a cutting-edge technology designed to help the coordination and decision-making of first- and second-line responders by providing during all the operation real-time information directly from local communities affected by the disaster. Local communities will be able to report crucial information through a digital web module that can be integrated in existing web/mobile emergency solutions that enhances cross-communication capabilities with inclusive and effective communication. Content auto-translated from more than 90 languages.*

Both of the above-mentioned solutions (AI-EDEC with the "Disaster Mode" app and ReBriNett) are to support the first- and second-line responders (hospitals and emergency services) to gain trusted information on an emergency and/or crises situation and to support decision making and to act promptly for the real need. Furthermore, in case phone calls would be jammed by adversaries generating thousands of false emergency calls, the "Disaster Mode" App would still allow citizens in distress to report their situation. Therefore, the solution supports the firs- and second-line responders to more effectively carry out their work according to their normal routines and thereby ensure the society's trust in them. This then leaves less room for adversaries to amplify crisis and emergencies with hybrid threat campaigns targeting to diminish citizens trust in authorities' capabilities to conduct their basic services.

Even though the above-mentioned tools (AI-EDEC with "Disaster Mode" app and ReBriNett) are valuable, what would benefit even more the first- and second-line responders (hospitals and emergency services) would be an **Information sharing environment (ISE)** that can host all the needed tools and even analyse the information gained from them with AI-based tools and thereby ensure that the information from the tools could be trustworthy and real, not fake. After all, adversaries could also use e.g. "Disaster Mode app" by uploading thousands of false, fake videos and emergency requests via the tool for the first- and second-line responders to go through and in this way jam their analysis capabilities and harm fast decision making.

On the whole, the following key elements are seen necessary in an information sharing environment, to ensure that its information for first- and second-line responders (hospitals and emergency services) can be verified and trusted:

[8] ReBriNett solution from WeSolve, see : https://wesolve.app/solutions/emergency-management/

- the ISE needs to have capability to analyse large amount of data, including meta data provided by the tools that feed the data to the ISE in order to validate the trustworthiness of the given information incl. videos, geolocation etc. Thus, the ISE needs to include tools for the data verification where artificial intelligence (AI) may have crucial role. In short there needs to be AI based analysis tools to verify authenticity of the data and hybrid threats related information.
- the ISE needs to have a standardized approach for how the variety of tools (e.g. *AI-EDEC* with "*Disaster Mode*" app and *ReBriNett*) can be connected to it and for the data analysis. Thus, creation of the standard use of standardized forms plays important role.
- For easy integration in an ISE the tools need to have standardized interfaces / APIs, so that new tools, solutions and services can be easily added (compare e.g., with the taxonomy and coding with STIX / TAXI for CTI)
- The ISE formats should to the largest extent possible be language independent. This will support EU MSs to with minimum effort create their own language specific modules.
- CRP is first and foremost a tools framework for local/regional /national level information sharing. The information may also be shared to the national intelligence via other channels, whenever the platform identifies fake, false information. However, the platform as such should be usable in all MSs independently.

The really new thing in the proposed platform is that it will allow citizens' reports on crises and emergencies to reach first- and second-line responders (hospitals and emergency services) i.e., we **extend needed information collection/sharing so it can handle information submitted from mobile phones owned by private citizens** and at the same time **reduce adversaries means to provide false data and amplify a crisis with a hybrid threat campaign**. The ISE will also **deliver information to intelligence services on adversaries** false and fake alarms which will support early discovery of adversaries' hybrid threat campaigns in crises and emergency situations. Moreover, the data on adversaries' false alarms will support intelligence services in learning adversaries' methods and means to create and use hybrid threat campaigns and how they escalate situation during crises and emergencies. In other words, the collected and shared data will eventually support whole-of-society to be more prepared for hybrid threat attacks and campaigns. The lessons learned (LL) on adversaries is to support authorities and whole society for preparedness and prevention in the future in similar crises and emergency context. We may call the ISE a "**Citizen – Responder Platform**" (**CRP**). An example of the CRP's use is described below:

> *During early spring a tightly populated mountainous region with many rivers is hit by severe thunder storms, cutting electricity and followed by lasting extreme heavy rains for many days causing severe landslides. Flooded rivers have cut roads and destroyed bridges, many houses are washed away due to floods and landslides. People are severely injured when escaping the floods and having hypothermia due to cut off electricity and cold climate. Water is infected and causes sickness among the population. Thousands of people are calling to 112 and hospitals via mobile phones as landlines have been cut, this in order to get help but this jams the phone lines and the first- and second-line responders do not have clear awareness where help is especially and most severely needed.*
>
> *The region is located in a country that is targeted by adversaries in order to cause demand for new elections that would most likely bring new parties into power and hence destabilize the country's decision-making capabilities and bring it more politically close to the adversaries' ideas. Adversaries plan hybrid threat campaigns that underline that present government and regime and authorities*

under their lead are unable to conduct actions to the best for their citizens. Therefore, during the natural emergency/disaster that the mountainous region now faces, adversaries jam lines for emergency calls at their best. However, population has learned to use services available in the "Citizen – Responder Platform" (CRP) where they can easily select a solution to report the first- and second-line responders about their status promptly and the first- and second-line responders may in this way get faster awareness where the most critical need for help is. Adversaries are also using the CRP by sending fake videos to it but CRPs' AI analysis reveals the fake videos and fake geolocation and hence prevents these alarms to get through to first- and second-line jbut instead they are sent to the intelligence service. National intelligence receives huge amount of this data and may clearly state that the country and the region is under hybrid threat campaign. This can then be communicated via CRP-service to the population in the exposed region and the information calms them as they know that authorities are doing their best to solve the situation.

On the whole, CRP innovation is seen as a priority tool to support emergency first responders', civil protection authorities' and intelligence's knowledge and performance to act during crises in a manner that will reduce adversaries goals to escalate the crises with false information. The approaches linked to the CRP innovation are hence seen in EU-HYBNET to require standardization.

Core Theme: Information and Strategic Communication/ Innovation: "Media Pluralism Monitor" (LMHTT)

According to T4.2, the rationale behind the choice of the innovation **"Media Pluralism Monitor" (LMHTT)** as one of the most promising innovation to focus was two-fold. First, in T3.1 "*Definition of Target Areas for Improvements and Innovations*" analysis, LMHTT was rated high, belonging to the group of eight most promising innovations to counter hybrid threats esp. in focus of foreign information manipulation and interference. In addition, LMHTT was the only innovation in the group representing EU-HYBNET project Core Theme "Information and Strategic Communication" that was rated high.

The importance of the LMTHH solution is that it will enable observation and information on potential risks to local and regional media pluralism and alert authorities and governments to potential existing cleavages, foreign interference, disinformation and manipulation that may affect the society in a negative way. Furthermore, LMHTT is to deliver a methodological approach and tool to analysing and map the existence of risks to media pluralism and FIMI campaigns in a regional and local perspective. The solution will support national security agencies and government institutions responsible for internal security in European countries in tracking FIMI campaigns.

The solution is extremely necessary to implement as it relates to the social domain and how media influence social life, causing cleavages in societies, spreading disinformation and manipulating the public. The currently available diagnostic tool (MPM) only provides a general overview of the problem of media pluralism in EU and candidate countries, and the situation may vary within a single country, where often local media conditions and the general political situation in the region/local territory are of great concern. The proposed solution will allow this risk to be mapped. In this way, it will be possible to alert security practitioners and tackling FIMI campaigns, improve the situation through support, agree new policies and spread best practices.

LMHTT is seen to require standardization efforts because, the solution addresses the effective tracking and combating of hybrid threats that arise in the media sphere, specifically the manipulation of the

information space, FIMI campaigns aimed at spreading disinformation and causing negative impacts among the society. The proposed data providers are researchers who assess media on a local and regional basis, while the end-users of these reports and analyses are government institutions and national agencies responsible for internal security in European countries, e.g. ABW (The Internal Security Agency). An interactive platform with the results from researchers would alert end users to hybrid threats at both local and regional levels, which could also be significant for the entire country or indicate connections and foreign influences that are part of coordinated hybrid attacks (by countries like China or Russia). This would also impact the international cooperation of national security agencies in tracking FIMI activities in local and regional media owned or used by adversaries and identifying individuals involved in the revealed FIMI campaigns. Based on the available analyses, the agencies would be able to interpret certain anomalies and unusual situations in the local and regional media markets that are linked to the manipulation of the information space.

3.3.2 EU-HYBNET T4.3 RECOMMENDATIONS FOR 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 of 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 to develop standards (e.g. ISO) but to solve best recommendations for standards and to find standardized ways to proceed with relevant innovations. In this context, it has been important for T4.3 to solve also 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/D4.10 "3rd *report on standardization recommendations*" it is highlighted what are the best practices and key regulations and even standards that eventually support the EU-HYBNET's recommended innovation uptake for pan-European security practitioners' and other relevant actors use.

The T4.3/D4.10 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 which 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).

Mobile application to pinpoint acts of harassment/violence on the street and online (CiReTo)

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Legal Recommendations (Medium Term) • **Privacy Laws and Data Protection** • **Reporting and Liability** • **Security Regulations** • **Intellectual Property**	Privacy Laws and Data Protection recommendations refer to ensuring GDPR (General Data Protection Regulation) compliance for users in the European Union, CCPA (California Consumer Privacy Act) for users in California, USA, HIPAA (Health Insurance Portability and Accountability Act) if handling health-related data in the USA. These recommendations also refer to data minimization in terms of only collecting necessary data and ensuring anonymization where possible, as well as obtaining explicit consent from users before collecting, storing, or sharing their data. Reporting and liability recommendations refer to mandatory reporting laws for understanding and complying with laws related to mandatory reporting of violence or harassment in one's jurisdiction, as well as content moderation, in terms of developing clear guidelines for content moderation to avoid liability issues. Security Regulation recommendations refer to data encryption, both in transit and at rest, as well as to access controls, by implementing robust authentication and authorization mechanisms. Intellectual Property recommendations refer to copyright and trademarks, which are required to ensure non infringement on third-party intellectual property.	**European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online harassment/violence, as well as tech companies developing tools to combat such activities** **EU Member States stakeholders (social care workers, police, teachers, NGOs)** **Providers of online services (social media, private messaging applications, search engines)** **Legislative authority in EU Member States** **Local and Regional Authorities in EU Member States** **Research institutions** **NGOs**

Standardization Recommendations (Medium Term) • **Data Standards** • **Accessibility Standards** • **Security Standards**	Data Standards recommendations refer to interoperability, through the use of standard data formats (e.g. JSON, XML) for data exchange, as well as designing APIs following REST or GraphQL standards for consistency and one again interoperability. Accessibility Standards recommendations refer to following WCAG (Web Content Accessibility Guidelines) to ensure the app is accessible to users with disabilities. Security Standards recommendations refer to implementing an Information Security Management System (ISMS), to be compliant with ISO/IEC 27001, as well as following best practices to address top mobile security threats (i.e. OWASP Mobile Security Project[9]).	**European Commission** **Ministry Level** **National and Local Authorities** **Providers of online services (social media, private messaging applications, search engines)** **Legislative authority in EU Member States** **Research institutions** **NGOs** **Local and Regional Authorities in EU Member States** **EMSA:** The Common Information Sharing Environment (CISE) is an EU initiative which aims to make European and EU/EEA Member States surveillance systems interoperable to give all concerned authorities from different sectors access to additional classified and unclassified information they need to conduct missions at sea.

[9] https://mas.owasp.org/

Best Practice Recommendations (Medium Term) • **User Interface and Experience** • **Reporting Mechanisms** • **Community Guidelines** • **Collaboration with Authorities** • **Ethical Considerations** • **Regular Audits and Updates** • **User Education**	User Interface and Experience best practices refer to usability and localization, by designing a user-friendly interface with clear navigation and easy reporting mechanisms, in addition to offering multilingual support to cater to a global audience. Reporting Mechanisms best practices refer to allowing users to report incidents anonymously, as well as implementing a system to verify the authenticity of reports without compromising user privacy. Community Guidelines best practices refer to establishing and enforcing a code of conduct for users, in addition to employing both automated and human moderation to handle reports of harassment and violence. Collaboration with Authorities best practices refer to partnerships with law enforcement and local authorities for effective response and support and the development of clear protocols for escalating serious incidents to the relevant authorities. Ethical Considerations best practices refer to ensuring that algorithms and moderation practices are fair and free from bias and that transparency is guaranteed in how data is used, as well as in the criteria selection for content moderation. Regular Audits and Updates refer to conducting regular security audits to identify and fix vulnerabilities and to the regular update of the app to include new features, security patches, and improvements. User Education refers to ensuring and promoting awareness, by providing resources and tips on recognizing and reporting harassment and violence and to offering links to support services and hotlines for victims.	**European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online harassment/violence, as well as tech companies developing tools to combat such activities** **EU Member States stakeholders (social care workers, police, teachers, NGOs)** **Europol** **The Radicalisation Awareness Network (RAN Practitioners)** **The VOX-Pol Network of Excellence (NoE)** **Providers of online services (social media, private** **messaging applications, search engines)** **Legislative authority in EU Member States** **Research institutions**

		Local and Regional Authorities in EU Member States **NGOs** **EMSA:** The Common Information Sharing Environment (CISE) is an EU initiative which aims to make European and EU/EEA Member States surveillance systems interoperable to give all concerned authorities from different sectors access to additional classified and unclassified information they need to conduct missions at sea.

Table 5: Recommendations and priorities for innovation uptake (CiReTo)

Starlight Disinformation-Misinformation Toolset (STARLIGHT)

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation
Recommendations from the Starlight project at this stage can be considered as best practice. **(short/medium/long term)**	Long term (2-5 years) co-development, involving solution developers and end-users in security sector could influence the innovation up-take process in the domain heavily. Co-development can be described in more details, as joint efforts can be challenging to implement. The main reason is difference of relevant components – solution developers are focused on technological aspects (Solution internal components), while users are concerned with results (external components of the solution). Following the practice in Starlight project a few success factors can be highlighted: - Technical development preferable to be separated from the co-development process. There are separate meetings organised for technical development of tools. Data formats, pipelining, integration and other technical details are discussed. While other meetings, where end-users are involved are focused on inputs (e.g. data sources) and outputs (e.g. interface, accuracy, interface, etc.) aiming to understand the results and how they can be used (e.g. used as evidence, etc.). - Pace of work should be also rather intense. As co-development might take more than a year, sometimes few years, there should be some milestones for assessing the progress, relocation of resources, reprioritisation of functionalities and other changes. In Starlight project one co-development cycle is one year. Each cycle ends with ToolFest where solutions are presented and evaluated by wider group of end-users. Working meetings are organised on weekly – biweekly bases. One of the questions is how to include such practice into daily routine of security related organizations. This can be facilitated by dedicated financial instruments aiming to involve organisations in earlier stages of solution development. One of such instruments can be considered pre-commercial procurement or GovTech Lab in Lithuania. Such practice could also be facilitated by recommendations from policy makers or stakeholders to include innovation co-development related strategic measures and KPIs.

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation
Recommendations from the Starlight project at this stage can be considered as <u>best practice.</u> **(short/medium/long term)**	Long term (2-5 years) co-development, involving solution developers and end-users in security sector could influence the innovation up-take process in the domain heavily. Co-development can be described in more details, as joint efforts can be challenging to implement. The main reason is difference of relevant components – solution developers are focused on technological aspects (Solution internal components), while users are concerned with results (external components of the solution). Following the practice in Starlight project a few success factors can be highlighted: - Technical development preferable to be separated from the co-development process. There are separate meetings organised for technical development of tools. Data formats, pipelining, integration and other technical details are discussed. While other meetings, where end-users are involved are focused on inputs (e.g. data sources) and outputs (e.g. interface, accuracy, interface, etc.) aiming to understand the results and how they can be used (e.g. used as evidence, etc.). - Pace of work should be also rather intense. As co-development might take more than a year, sometimes few years, there should be some milestones for assessing the progress, relocation of resources, reprioritisation of functionalities and other changes. In Starlight project one co-development cycle is one year. Each cycle ends with ToolFest where solutions are presented and evaluated by wider group of end-users. Working meetings are organised on weekly – biweekly bases. One of the questions is how to include such practice into daily routine of security related organizations. This can be facilitated by dedicated financial instruments aiming to involve organisations in earlier stages of solution development. One of such instruments can be considered pre-commercial procurement or <u>GovTech Lab</u> in Lithuania. Such practice could also be facilitated by recommendations from policy makers or stakeholders to include innovation co-development related strategic measures and KPIs.

Table 6: Recommendations and priorities for innovation uptake (STARLIGHT)

AI Enhanced Disaster Emergency Communications (CRP)

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Standardization (Medium Term) • **Data standards** • **Interfaces (API, communication)** • **Security** • **Availability** **Best Practices (Short Term)** • **Reporting processes** • **Cyclic testing and practical exercises**	To integrate apps, services, and tools with the CRP platform, a standardized approach is necessary. The platform's AI analysis must be robust to distinguish genuine emergencies from false alarms. Interoperability issues may arise with responders' existing systems. Additionally, intelligence services may need support to identify whether false alarms are part of hybrid threats or actions by uninformed citizens.	**The European Commission** **Ministry Level** **National and Local Authorities** **EU Member States stakeholders (social care workers, police, emergency services, NGOs)**
Legal (Medium Term) • **Privacy Laws** • **Data Protection** • **Liability** • **Security Regulations** **Standardization (Medium Term)** • **Security** • **Availability** **Best Practices (Short Term)** • **Ethical Considerations**	CRP requires advanced AI to ensure accurate and reliable data analysis while complying with existing regulations and laws. The platform must be highly secure to prevent hacking and data leaks. Ethical concerns arise from the potential for citizens to share videos and information without adhering to privacy regulations, which could hinder societal acceptance and the positive impact of CRP.	**The European Commission** **Ministry Level** **National and Local Authorities** **Legislative authority** **Research institutes**

Standardization (Medium Term) • **Data standards** • **Interfaces (API, communication)** • **Security** • **Availability** **Best Practices (Medium Term)** • **Interfaces (API, communication)** • **Reporting processes** • **Cyclic testing and practical exercises** **Legal (Medium Term)** • **Privacy Laws** • **Data Protection** • **Liability** **Security Regulations**	CRP aims to facilitate information sharing between citizens and first- and second-line responders through various apps, tools, and solutions during large-scale crises and emergencies. This goal is likely to be well-received by end-users. Providers of these apps, tools, and services may view CRP as a valuable platform to offer their solutions. However, as with any new approach, it may take time for CRP to gain popularity and widespread adoption. If intelligence services recognize CRP's potential to identify signs of hybrid threat campaigns, it could further boost interest in the platform.	**National and Local Authorities** **Ministry Level** **The European Commission** **Legislative authority** **Providers of online services (social media, messenger applications, search engines)** **EU Member States stakeholders (social care workers, police, emergency services, NGOs)** **NGOs**
Best Practices (Medium Term) • **Planning of Invest** • **Sharing the costs** • **Cyclic testing and practical exercises** **Legal (Long Term)** • **budgetary law (EU member states, national)**	The development and implementation of the CRP across EU member states could face significant economic barriers due to high costs. These include expenses for advanced technologies, integration with existing systems, and training for responders. Financial constraints may lead to uneven adoption, and ongoing costs for updates and maintenance could create long-term economic challenges. Careful financial planning and potential cost-sharing will be necessary to overcome these barriers and ensure the platform's sustainability.	**National and Local Authorities** **The European Commission** **EU Member States stakeholders (social care workers, police, emergency services, NGOs)** **NGOs**

Best Practices (Medium Term) • **Interfaces (API and User)** • **Reporting processes** • **HowTo Guidelines** • **Ethical Considerations** • **Cyclic testing and practical exercises** **Legal (Medium Term)** • **Privacy Laws** • **Data Protection** • **Liability** • **Security Regulations**	Implementing the necessary operational structures and cooperation for the CRP is achievable, despite current gaps, due to the success of similar services like CISE and the 112 app. These platforms provide a strong foundation and positive user experiences that can be leveraged to ensure smooth integration and widespread adoption of the CRP across the EU. Utilizing existing frameworks reduces risks and fosters quicker acceptance, making it easier to achieve the desired level of information sharing and operational efficiency.	**The European Commission** **National and Local Authorities** **Legislative authority** **NGOs**

Table 7: Recommendations and priorities for innovation uptake (CRP)

Media Pluralism Monitor (LMHTT)

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation
Standardisation (implementation and maintenance) **(Medium Term)**	**For implementation of LMHTT:** Design a comprehensive LMHTT diagnostic tool by defining standardized procedures for data collection and reporting in a questionnaire. Develop comprehensive data analytics tools and an interactive dashboard for data visualisation. Delegate the maintenance of the LMHTT tools to a competent body, possibly ENISA. To integrate local/regional services, and tools with the LMHTT platform.
Legal (general recommendation) **(Long Term)**	**Establish clear, comprehensive gender equality policy as a social policy to all EU Member States and candidate countries** Social policies have the most prominent role in promoting gender equality. Since not all EU countries have gender equality policy, all EU states should implement some kinds of gender equality policy. Clear and comprehensive gender equality policy would strengthen the rights of women in media. Gender equality policies have a major impact on the equity in the labour market, access to employment, protection of groups and special vulnerability situations and thus significantly promote gender equality.
Legal (market plurality) **(Long Term)**	**Establish common rules for the proper functioning of the internal market for media services with the strong focus on safeguarding independence and pluralism** (European Media Freedom Act). Establish harmonized law for media pluralism. The rules would promote independence of media and would protect journalists from external and internal influences.

	Legal framework to ensure independence of the media and safeguard media pluralism - Freedom of Expression (coe.int) European Media Freedom Act - European Commission (europa.eu)
Best practice (market plurality) **(Short Term)**	**Create media ownership monitoring system that displays state-based ownership information database.** It contributes to transparency of media ownership. European Media Freedom Act - European Commission (europa.eu)
Best practice (disinformation) **(Medium Term)**	**The need to define and establish a comprehensive strategy or action plan that focuses on the role of various stakeholders in protecting the EU against disinformation** (Ireland - a National Counter-Disinformation Strategy Group created in 2023, Estonia- having strategy combating disinformation focusing on 5 core elements, Lithuania- National Crisis Management Centre).
Best practice (disinformation, FIMI) / Legal **(Medium/Long Term)**	**Create/develop initiatives promoting digital literacy among the public**. This is to increase media literacy in the EU states, raise public awareness of disinformation in media and what impact it has on the civil society. Education of the public about the dangers of disinformation is crucial. There are multiple initiatives focused on promoting media literacy, for example EDMO, but there are also systemic solutions necessary on national and EU level.
Standardisation **(Short Term)**	The ultimate goal of the "Journalism Trust Initiative" is to support the universal, individual freedom of opinion through access to information and independent, pluralistic media. The application of JTI means safeguarding professional standards, a more healthy digital media landscape should emerge, from which each citizen and media worker, but also societies at large, could benefit. CEN/WS JTI - Journalism Trust Indicators

Table 8: Recommendations and priorities for innovation uptake (LMHTT)

4. CONCLUSION

4.1 SUMMARY

In the chapters above it is described how the EU-HYBNET project activities from the past six project months (May – October 2024) have contributed to the Three Lines of Action. In addition, chapters have described how the work in the project Tasks has been conducted now when the 3rd project cycle is finalizing to deliver its' results and the final, 4th mini working cycle (October 2024 - April 2025) has kicked-off. Furthermore, the goal of the document has partly also been to highlight what kind of results EU-HYBNET is expected to achieve in the Three Lines of Action during the next six months reporting period.

Furthermore, in section 2. we explained the importance of the Six Month Action Report to the project proceeding and quality control.

In Section 3. we showed how the EU-HYBNET project tasks and project actors have contributed or will contribute in the next six months to the Three Lines of Action to reach the set project goals.

In Section 4. we provided a summary of the deliverables and explained their importance to the project's proceeding and what are the next actions to follow.

4.2 FUTURE WORK

The EU-HYBNET project results to the Three Lines of Actions from the 3rd project cycle (duration: M35-M52/ March 2023 – September 2024) have been now explained to the EC from the reporting period of this deliverables. The next Six Month Action Report (in April 2025) will describe 4th project cycle results and findings to the Three Lines of Actions, and how the project has been able to implement the findings even more to the benefit of pan-European practitioners to counter hybrid threats. Definitely, best practices and lessons learned and key findings will be taken into extensive hand-over from EU-HYBNET to stakeholders now until April 2025 when the project ends. The following deliverables will be delivered during next six-month period, and there are also milestones to take place during the reporting period.

Deliverables (D):

T1.1 Administrative and Financial Planning and Coordination

- D1.10 10th Six month action report (Laurea), M60/ Apr 2025
- D1.18 Societal Impact final Report (Laurea), M60/Apr 2025

T1.3 EU-HYBNET Community Extension

- D1.23 List of actors to the extended EU-HYBNET network (Hybrid CoE), M60/Apr 2025
- D1.25 EU-HYBNET Network Sustainability Final Report (Hybrid CoE), M60/Apr 2025

T2.1 Needs and Gaps Analysis in Knowledge and Performance

- D2.8 Final Gaps and Needs Evaluation (Hybrid CoE), M55/Nov 2024

T2.2 Research to Support Increase of Knowledge and Performance

- D2.16 Articles and publications on themes and measures (UIT), M60/Apr 2025

T3.2 "Technology and Innovations Watch" (Satways)

- D3.6 Final report for Improvement and Innovations (SATWAYS), M58/ Feb 2025

T3.3 "Ongoing Research Projects Initiatives Watch

- D3.10 Final report on Innovation and Research Project monitoring (L3CE), M58/ Feb 2025

T3.4 Innovation and Knowledge Exchange Events

- D3.18 5th Future Trends analysis Workshop (JRC), M58/ Feb 2025

T4.2 Strategy for Innovation uptake and industrialization

- D4.7 Final report for innovation uptake, industrialisation research (RISE), M58/Feb 2025

T4.3 Recommendations for Standardization

- D4.11 Final report for standardisation recommendations (PPHS), M59/Mar 2025

T4.4 Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge

- D4.15 4th Policy Briefs, Positions Papers, Recommendations report (Hybrid CoE), M55/Nov 2025
- D4.16 5th Policy Briefs, Positions Papers, Recommendations report (Hybrid CoE), M60/Apr 2025

T5.1 Dissemination and Communication Strategy and Plan

- D5.5 Updated dissemination, communication and exploitation plan 3. (EOS), M54/ Oct 2024

T5.3 Project Annual Workshops for Stakeholders

- D5.14 Annual Workshop report 5 (JRC), M58/ Feb 2025

Milestones (MS):

- MS29 "4th Policy briefs, position papers, or recommendations documents are published" in M55 (November 2024)
- MS15 "Final Gaps and Needs Evaluation is delivered for the Network to proceed" in M55 (November 2024)
- MS24 "Strategy ready for innovation uptake and industrialisation" in M58 (February 2025)
- MS38 "5th Annual workshop is organised" in M58 (February 2025)
- MS25 "Standardization Recommendation ready" in M59 (March 2025)
- MS30 "Policy briefs, Position Papers, or Recommendations documents are published" in M60 (April 2025)
- MS10 "EU HYBNET Network Sustainability Final Report" in M60 (April 2025)

As the deliverables, the EU-HYBNET project will deliver many more results to the Three Lines of Action in the forthcoming months. The aim and value of the Six Months Action report is to track the results and to highlight their importance for the project proceeding and in the next 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, new project results to the Three Lines of Action will be reported especially because deliverables focusing on the last identified pan-European security practitioners' gaps and needs are ready following analysis of the most promising innovations to present pan-European security practitioners gaps and needs to counter hybrid threats (by T4.2). 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 will highlight the main findings from EU-HYBNET to policy makers and other pan-European stakeholders to be take into further actions in order to stregthen European repsonse to hybrid threats.

Lastly, EU-HYBNET will continue to share the key findings with DG HOME and other relevant DGs, EU Agencies and Offices via emails, invitations to the project events, and of course to contribute to EC's possible requests for information. In addition, cooperation with EEAS/Strat.Comm in the context of Foreign Information Manipulation and Interference/FIMI tool and fruitful information exchange with EUROPOL Innovation Lab is in the EU-HYBNET's plans. This all is to benefit the pan-European stakeholders from the EU-HYBNET results and to enhance joint measures to counter Hybrid Threats. In addition, EU MSs' needs to learn and to implement EU-HYBNET's results will be focused on in order to ensure the maximum input from the project to EU and EU MSs.

ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threat –project, No. 883054
EC	European Commission
EU	European Union
GA	Grant Agreement
DoA	Description of Action Part A and B
H2020	Horizon2020, EC funding Program for EU projects' funding
FP7	The EC's 7th Framework Program to EU project funding
D	Deliverable
CO	Consortium only deliverable
WP	Work Package
T	Task
M	Month
MS	Milestone
OB	Objective
KPI	Key Performance Indicator
NoP	Network of Practitioners project
R&I	Research and innovations
EU MS	European Union Member State
G&N	gaps and needs
IKEW	Innovation and Knowledge Exchange Event
BOS	Break Out Session
ISW	Innovation Standardization Workshop
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
AI	Artificial Intelligence
VR	Virtual Reality
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos

MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
EOS	European Organisation for Security Scrl
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
SATWAYS	SATWAYS
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
UCSC (UNICAT)	Universita Cattolica del Sacro Cuore
JRC	JRC - Joint Research Centre - European Commission
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
HCoE/ Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NLD MoD	Ministry of Defence/NL
ICDS	International Centre for Defence and Security, Estonia
PLV	Ayuntamiento de Valencia / Valencia Local Police
ABW	Polish Internal Security Agency
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
UniBW	Universitaet der Bundeswehr München

Table 9: Glossary and Acronyms

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. EVENTS' AGENDA(S)

4th Annual Wokshop Agenda

Time CET	Topic	Speakers
	Welcome and registration	
8:30-9:00	Registration	

9:00-9:10	Welcome & Practical information	José L. Diego, Inspector, Head of Innovation & Project Management Division, PLV Päivi Mattila, EU-HYBNET Coordinator, Laurea
9:10-9:20	Keynote Speech "From analysis to (re)action – a framework for networked defence"	Chiara Pacenti Information Systems Officer European External Action Service (EEAS)/ Strategic Communications and Information Analysis
9:20-9:30	Keynote Speech "The EU approach to countering hybrid threats"	Torben Fell, Policy Officer EEAS/SECDEFPOL.2, Hybrid Threats and Cyber, Hybrid Threats Sector
9:30-9:40	Keynote Speech "European elections 2024 and hybrid threats"	Manuel Rodríguez Vico Director for Technologies and Information, DG SAFE – European Parliament
9:40-10:10	Audience Q&A	**Host**: José L. Diego, PLV
EU-HYBNET's latest findings and results		
10:10-11:10	Round Table Discussion on "EU-HYBNET 4th year findings and results to counter hybrid threats" – topics: • "Findings on present pan-European security practitioners' gaps&needs/ threats to counter hybrid threats" • "Identified promising innovations to counter hybrid threats" • "Innovation uptake recommendations" • "EU-HYBNET Network activities and sustainability"	**EU-HYBNET Consortium:** - Hanne Dumur-Laanila, Analyst, Reseach & Analyses, European Center of Excellence for Countering Hybrid Threats - Evaldas Bruze, L3CE - Souzanna Sofou, Senior Research and Innovation Manager, Satways - Julien Theron, Researcher in Hybrid Threats, Joint Research Centre (JRC) - Päivi Mattila, EU-HYBNET Coordinator, Laurea
11.10-11:20	Audience Q&A	**Hosts:** Tiina Haapanen, EU-HYBNET Project Manager, Laurea Iván Luis Martínez Villanueva, Project Manager at the

		Innovation & Project Management Division, PLV
11:20-11:50	Coffee break	
Pitches Innovations and solutions to counter hybrid threats by organizations and projects		
11:50-12:00	Denial-of-service/DDOS / attack on infrastructures critical to population livelihood - Pitch	Marios Thoma, Director, CyberEcoCul Global Services
12:00-12:10	Smart City -Pitch	Marina Galiano Botella, CSIRT-CV
12:10-12:20	Resilience Assessment Tool (R/VAT) -Pitch	Vazha Sopromadze, The University of Georgia Security, Policy and Nationalism Center
12:20-12:30	Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats - Pitch	David Arroyo, The Spanish National Research Council
12:30-12:40	"European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection" (EU-CIP), Horizon project	EU-CIP coordinator Emilia Gugliandolo, Senior Researcher, ENGINEERING
12:40-12:50	"TOWARD SUSTAINABLE FORESIGHT CAPABILITIES FOR INCREASED CIVIL SECURITY" (AHEAD), HORIZON PROJECT	Laure Brévignon-Dodin, Head of Office, Directorate for International Security Cooperation, Ministry of the Interior in France
12:50-13:00	"Gaming Ecosystem as a Multi-Layered Security Threat" (GEMS), Horizon project	Bledar Feta, Hellenic Foundation for European and Foreign Policy
13:00-13:10	"Protecting our strategic Assets, Values and Economy against harmful Disinformation" (PAVED) project, initiative of France	Frederic Tatout, Anatase; Anne-Marie Duval, Ministry of Ecological Transition in France
13:10-13:40	Audience Q&A	**Host:** Isto Mattila, EU-HYBNET Innovation Manager, Laurea
13:40-13.50	Closing remarks	José L. Diego, PLV

4th Future Trends Workshop Agenda

Time EEST	Topic	Speaker
09.00-09.30	Registration	
Plenary session		
09.30-09.45	Welcome & Practical Information	Mr Jesús Carbonell Aguilar, City Councillor, representative of the Valencia Local Police

		Mr José Vicente Herrera Arrando, Chief Constable of the Valencia Local Police
09.45-10.00	**"Models for Conflict Analysis & Some Critical Remarks on Dealing with Hybrid Threats"**	Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces
10:00-10:30	Audience Q&A	***Moderator:*** *Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police*
10:30-10:45	Coffee Break	
10:45 – 12:15	**Border Management to Counter Future Hybrid Threats**	***Chair:*** *Isto Mattila, EU-HYBNET Innovation Manager* *Panel speakers:* • *Dr. Souzanna Sofou, Satways* • *Dr. Jarmo Puustinen, Finnish MoI* • *Europol Innovation Lab Representative*
12:15 – 13:15	Lunch Break	
Parallel Breakout Sessions		
13:15-14:15	**Breakout Session #1:** Cyber & Future Technologies	Evaldas Bružė, Analyst and Consultant in Commercial Development at L3CE.
	Breakout Session #2: Resilient Civilians, Local Level and National Administration	Dr. Julien Theron, Researcher in Hybrid Threats at the JRC
14:15-14:30	Coffee Break	
14:30-15:30	**Breakout Session #3: Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats** Core Theme: Information & Strategic Communication	Rubén Arcos Martín (URJC) and Irena Chiru (MVNIA)
	Breakout Session #4: Securing the EU's borders to 2040 – Thinking about the security landscape Core Theme: Future Trends of Hybrid Threats	Maxime Lebrun, Deputy Director R&A at The European Centre of Excellence for Countering Hybrid Threats

		Hanne Dumur-Laanila, Analyst at the The European Centre of Excellence for Countering Hybrid Threats
15:30-15:45	Conclusions of the BOS & Audience Q&A	
15:45 – 16:00	"FRONTEX's View on the Future of Hybrid Threats in Relation to Border Management"	Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX
16:00 – 16:10	Closing remarks & Practical Information for Annual Workshop	Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police
16:10 – 17:10	EU-HYBNET Societal Impacts Workshop	Tuomas Tammilehto, EU-HYBNET Ethics Manager

.