



EU-HYBNET

FOURTH SIX MONTH ACTION REPORT

DELIVERABLE 1.5

Lead Author: Laurea

Contributors: All consortium 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

D1.5 FOURTH SIX MONTH ACTION REPORT

Deliverable number	1.5	
Version:	1.0	
Delivery date:	10/5/2022	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status	Ready	
Nature:	Report	
Main authors:	Päivi Mattila, Tiina Haapanen	Laurea
Contributors:	Review: Petri Häkkinen, Satu Laukkanen	Espoo
	Input to the report from all consortium partners due to their project work	MTES, URJC, Hybrid CoE, PPHS, UiT, RISE, KEMEA, L3CE, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, Maldita, ZITIS, COMTESSA

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	20/4/2022	Päivi Mattila/ Laurea	First draft.
0.2	23/4/2022	Tiina Haapanen/ Laurea	Description of activities conducted during the reporting period.
0.3	25/4/2022	Päivi Mattila/ Laurea	Description of activities conducted during the reporting period. Text editing.
0.4	27/4/2022	Tiina Haapanen/ Laurea	Text editing and content delivery
0.5	28/4/2022	Päivi Mattila/ Laurea	Description of activities conducted during the reporting period. Text editing.
0.6	30/4/2022	Päivi Mattila/ Laurea	Text delivery and editing. Delivery of the document for the review.
0.7	2/5/2022	Petri Häkkinen, Satu Laukkanen/ Espoo	Review
0.8		Tiina Haapanen/ Laurea	Review and text editing
0.9		Päivi Mattila/ Laurea	Final text editing
1.0		Päivi Mattila/ LAurea	Document to be submitted for the EC

DISCLAIMER

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

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

© Copyright in this document remains vested in the Project Partners

TABLE OF CONTENT

1. Introduction.....	3
1.1 Overview.....	3
1.2 Structure of the deliverable	3
2. Six Month Action Report and impact to the project.....	4
2.1 Contribution to the project	4
2.2 Six Month Action Report contributors	5
3. Three Lines of Action reporting.....	6
3.1 Monitoring of Research and Innovation Projects with a View to Recommending the Uptake or the Industrialisation of Results	6
3.1.1 EU-HYBNET WP2 Gaps and Needs of European Actors against Hybrid Threats	7
3.1.2 EU-HYBNET WP3 Surveys to Technology, Research and Innovations.....	9
3.1.3 EU-HYBNET WP5 Communication, Dissemination and Exploitation Activities	11
3.2 Common Requirements as Regards Innovations that Could Fill in Gaps and Needs.....	16
3.2.1 EU-HYBNET WP2 Gaps and Needs of European Actors against Hybrid Threats	16
3.2.2 EU-HYBNET WP4 Recommendations for Innovations Uptake and Standardization.....	19
3.3 Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation.....	22
3.3.1 EU-HYBNET T4.3 Recommendations for Standardization	22
3.3.2 EU-HYBNET T4.2 Strategy for Innovation Uptake and Industrialization.....	26
3.3.4 EU-HYBNET T4.4 Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge.....	28
3.3.3 EU-HYBNET WP2 Gaps and Needs of European Actors against Hybrid Threats	31
4. CONCLUSION	33
4.1 Summary.....	33
4.2 Future Work	33
ANNEX I. GLOSSARY AND ACRONYMS	36
ANNEX II. REFERENCES.....	39
ANNEX III. The 2 nd Future trends Workshop	40
ANNEX IV. The 2 nd ANNUAL WORKSHOP	43

TABLES

Table 2 Glossary and Acronyms	36
-------------------------------------	----

FIGURES

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities.....	4
--	---

1. INTRODUCTION

1.1 OVERVIEW

The goal of the *Empowering a Pan-European Network to Counter Hybrid Threats* (EU-HYBNET) project deliverable (D) 1.5 “*Fourth Six Month Action Report*” in project month (M24) (April 2021) is to describe how the project has proceeded from M19 until end of M24 of the project (Nov 2021 – April 2022) 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 of research and innovation projects with a view to recommending the uptake or the industrialisation of results;
- 2) common requirements as regards innovations that could fill in gaps and needs
- 3) priorities as regards of increasing knowledge and performance requiring standardization

Furthermore, D1.5 also highlights what actions and results are expected from EU-HYBNET during the next six-month period (May 2022 - October 2022).

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 D1.5 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 19-24 (November 2021 - April 2022) 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 (May 2022 – October 2022).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.5 “*Fourth 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 D1.5, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.5 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 flow chart 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.

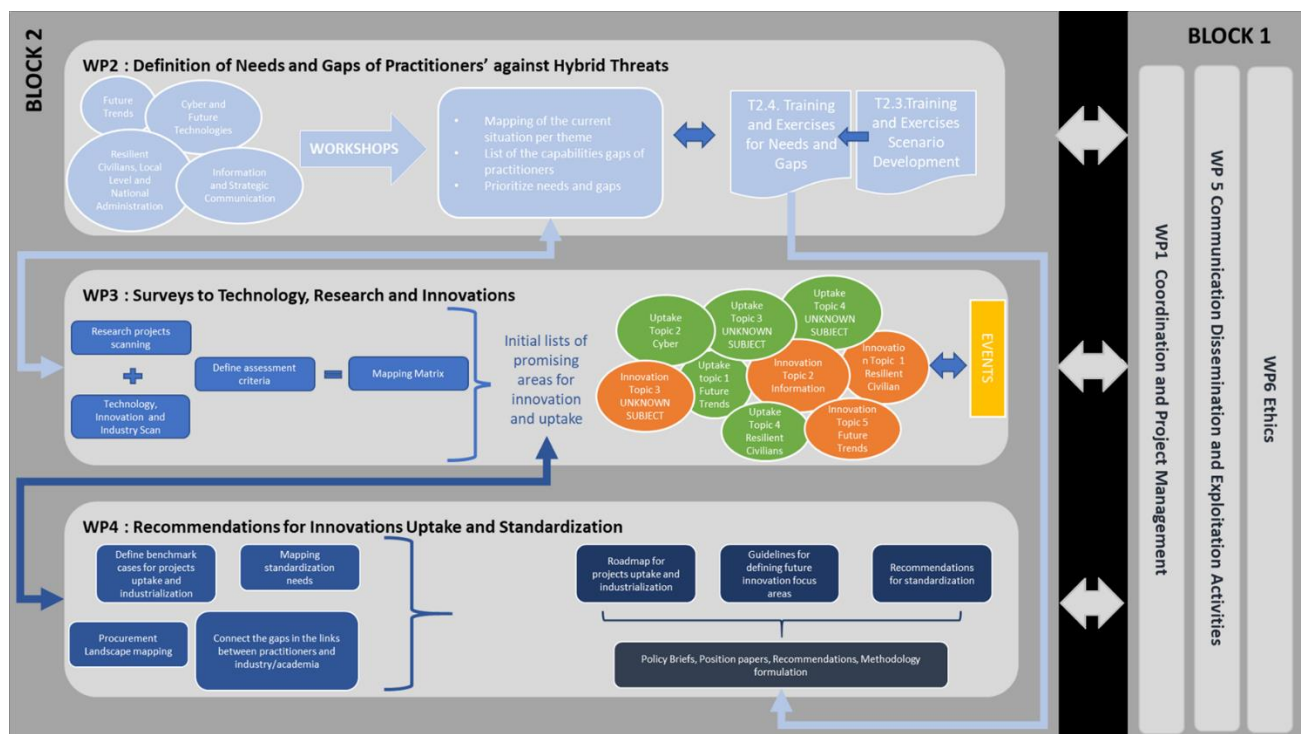


Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in D1.5 are linked to the project milestones (MS) achieved during the last six month period. The milestones relevant to D1.4 are following:

Milestone No.	Milestone (MS) name	MS related Task	Due project month
26	1 st Policy Briefs, Position Papers or Recommendation Document are Published	All	19
6	2 nd EU-HYBNET Project Management Board Meeting	All	24
35	2 nd Annual workshop	All	24

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The fourth Six-Month Action Report (D1.5) main author is Laurea, the organization responsible for the delivery of D1.5. 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 fourth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager have contributed to D1.5 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's third six months (May - October 2021). 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 second project cycle (M18-M34/ October 2021 – February 2023) practitioners'¹ and other 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) 2.10 "Deeper analysis, delivery of short list of gaps and needs" (M22/ February 2022) where the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats were listed. Therefore, the D2.10 signified in the second project cycle (M18 – M34/ October 2021 – February 2023) 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) to cover the identified gaps and needs and with a goal of recommending the uptake or the industrialization of results.

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

During this reporting period the innovation analysis work relevant to the first Three Lines of Action reporting has mainly been conducted in Work Package (WP) 3 “Surveys to Technology, Research and Innovations”/ T3.2 “*Technology and Innovations Watch*” (lead by Satways) and T3.3 “*Ongoing Research Projects Initiatives Watch*” (lead by L3CE). However, activities in WP5 “Communication, Dissemination and Exploitation Activities”/ T5.3 “*Project Annual Workshops for Stakeholders*” (lead by Laurea) and in T5.1 “*Dissemination and Communication Strategy and Plan*” (lead by EOS) have also provided significant input to the results and further proceeding.

The results achieved in the named WPs according to the three lines of actions topic **monitoring of research and innovation projects with a view to recommending the uptake or the industrialization of results** are described in the following subchapters.

3.1.1 EU-HYBNET WP2 GAPS AND NEEDS OF EUROPEAN ACTORS AGAINST HYBRID THREATS

EU-HYBNET’s 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) have delivered deliverables (D) D2.6 “Long list of defined gaps and needs” (M19/ November 2021) and D2.10 “Deeper analysis, delivery of short list of gaps and needs” (M23/ February 2022) that included analysis of the most important pan-European security practitioners’ and other relevant actors’ gaps and needs (G&Ns) to counter Hybrid Threats for the second project working cycle (M18-M34/ October 2021 - February 2023) to focus on.

The following tables describe the identified key gaps and needs in the form of threats from the project four core themes. The domains mentioned in the tables highlight the relevant domain of the threat according to the research approach used in EU-HYBNET, namely the “A Landscape of Hybrid Threats: The Conceptual Model”. The threats mentioned in the table provide the starting point for the analysis of **research and innovation projects with a view to recommending the uptake or the industrialisation of results** to the most critical pan-European security practitioners’ and other relevant actors’ gaps and needs to counter Hybrid Threats. The gaps and needs and threats to focus on are following according to the project four core themes:

Core theme - Information and Strategic Communication:

<u>Threats</u>		<u>Domains</u>
Information manipulation with the aim of destabilization		Information, Cyber
Foreign interference in key information institutions		Political, Culture

Promoted ideological extremism and violence			Information, Intelligence, Legal
---	--	--	-------------------------------------

Core theme - Future Trends of Hybrid Threats:

<u>Threats</u>		<u>Domains</u>
Geopolitical heavyweight of domestic policy		Political, Economy, Infrastructure
Digital escalation and AI-based exploitation		Cyber, Military/defence, Political
Rise of populism		Political, Social/societal, Information

Core theme - Cyber and future Technologies:

<u>Threats</u>		<u>Domains</u>
Space interference and counterspace weapons		Space, Cyber, Military/defence
Offensive cyber capabilities		Cyber, Infrastructure
Disruptive innovations		Political, Social/societal, Military/defence

Core theme - Resilient Civilians, Local Level and National Administration:

Threats		Domains
Exploitation of existing political cleavages		Political, Public administration, Social/societal
Exploitation of critical infrastructure weaknesses and economic dependencies		Infrastructure, Economy, Cyber
Exploitation or investment in companies by foreign actors		Political, Economy

According to the EU-HYBNET project proceeding plan what follows after the definition of the most critical gaps and needs, vulnerabilities and threats of the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats is that Tasks in WP3 will start to identify promising technological and non-technological/human-science based innovations and solutions from existing research and innovation projects and other possible sources or providers (e.g. industry, academia) to the gaps and needs. The status of the work in WP3 is described in the next subchapter.

3.1.2 EU-HYBNET WP3 SURVEYS TO TECHNOLOGY, RESEARCH AND INNOVATIONS

Work Package (WP) 3 "Surveys to Technology, Research and Innovations" includes Tasks T3.2 "*Technology and Innovations Watch*" (lead by Satways) and T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) that are delivering the key results to **research and innovation projects with a view to recommending the uptake or the industrialisation of results**. The work in T3.2 and T3.3 is ongoing at present and hence only preliminary results and insights on their forthcoming results are described in the chapters below.

T3.3 Ongoing Research Projects Initiatives Watch

EU-HYBNET T3.3 monitors research and innovation (R&I) projects that may deliver sound innovations and solutions to present most critical gaps and needs, threats to counter Hybrid Threats. The 3.3 contributing partners have selected the main threats to focus on, and to map EU MSs' and especially European Commission (EC) funded relevant security projects that to deliver sound innovation(s) and

solution(s) to the threats. In the work, especially the EC CORDIS platform is much used to find primary information on the most promising projects. This is followed more detailed investigation of the project content and results. It has been observed, that there is an abundance of research and innovation (R&I) projects and other research material (e.g. articles, journals, studies, research publications) which needs to be scanned for the most relevant solutions to satisfy the identified gaps and needs, and which can be recommend for further analysis and possibly innovation uptake or industrialization into further analysis in T3.1 *“Definition of Target Areas for Improvements and Innovations”* (lead by TNO) and in WP4 *“Recommendations for Innovations Uptake and Standardization”* (lead by KEMEA). What has supported T3.3 to proceed in the analysis is that the each threat has been described in a format of a concrete case that highlights more thoroughly the expectations and needs for a projects that may deliver sound technological or non-technological innovation and solution to the threat.

T3.3 assessment has also focused on the EC funded projects that were invited to present their innovations and solutions in the 2nd EU-HYBNET Annual Workshop (AW) in Rome and on-line during 6th of April 2022. The AW was arranged by T5.3 *“Project Annual Workshops for Stakeholders”* together with Laurea and UCSC. The projects who were invited to present their results were following:

- ALIGNER/ Artificial Intelligence Roadmap for Policing and Law Enforcement <https://cordis.europa.eu/project/id/101020574>
- 7SHIELD/ Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats <https://cordis.europa.eu/project/id/883284>
- PRECINCT/ Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection <https://cordis.europa.eu/project/id/101021668>
- MEDEA/ Mediterranean practitioners’ network capacity building for effective response to emerging security challenges <https://cordis.europa.eu/project/id/787111>

The named projects are seen to focus on innovations and solutions that are important to analyse in T3.3 as possible innovation projects that may deliver wanted solutions to the EU-HYBNET’s identified most critical present gaps and needs, threats to counter Hybrid Threats. The cooperation is to support possible recommendations of the uptake or the industrialisation of the project’s innovations and results.

Due to the abundance of material related R&I projects, the information scanning is now under final work. T3.3 will deliver it’s findings in D3.8 *“First Mid-Term report on Innovation and Research Project monitoring”*, (L3CE) in M24 (April 2022) that is still under work. Therefore, the next six month action report in M30 (October 2022) will describe D3.8 results with more details.

T3.2 Technology and Innovations Watch

Similar to T3.3, T3.2 is at present conducting research to find innovations which to provide solutions to the identified gaps and needs, threats and that could be recommended for innovation uptake or industrialization. The focus of T3.2, however, is not only for R&I projects as in T3.3, but also and mainly to assess the technological innovations developed initially by the European private sector and

secondly, to investigate related innovative products from countries outside Europe to identify possibly related innovative approaches. The assessment will be based initially on the information done in desk studies but also provided by contacted companies. Furthermore, T3.2 will also arrange from face to face discussions with companies that will be invited to present their solutions in the framework of EU-HYBNET events, such WP5 Annual Workshop (AW).

The T3.2 did make interviews of innovation and solution providers that were selected to provide a pitch in the 2nd EU-HYBNET Annual Workshop (AW) in Rome and on-line on 6th of April 2022. However, more detailed description of the pitching providers and their solutions in the next subchapter dedicated to EU-HYBNET AW.

While T3.2 may also focus on research and innovation project's this has supported T3.2 to focus on the EC funded project 7SHIELD's innovations, especially because the project's solutions are very relevant to the identified threat "Space interference and counter space weapons" under EU-HYBNET core the "Cyber and Future Technologies". Another reason for the interest is that during the first project cycle (M1-M17/ May 2020 – September 2021) T3.1 *"Definition of Target Areas for Improvements and Innovations"* (lead by TNO) identified 7SHIELD as a key project that may deliver unique capability to initiate efficient response actions, right after or even before the occurrence of catastrophic events. Due to this finding, and also importance of cooperation in the context of innovations between the 7SHIELD and EU-HYBNET project, T3.2 has continued the interaction with 7SHIELD in order to learn more on their promising innovations and solutions for uptake and recommendations also in the content of countering Hybrid Threats.

At the moment T3.2 is finalizing its scanning of technological innovations and the results will be presented in D3.4 *"First Mid-Term Report on Improvement and innovations"* (Satways) in M24 (April 2022). The results and key findings of T3.2 will be reported in the next Six Month Action Report D1.10 in M30 (October 2022).

3.1.3 EU-HYBNET WP5 COMMUNICATION, DISSEMINATION AND EXPLOITATION ACTIVITIES

Even though the main contribution of the EU-HYBNET project is to deliver results to the Three Lines of Action **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** is conducted especially in WP3 and WP4, also WP5 *"Communication, Dissemination and Exploitation Activities"* (lead by EOS) contribute to the results too due to project event arrangements and hence engagement with relevant projects. In WP5 this activity is especially done in T5.3 *"Project Annual Workshops for Stakeholders"* (lead by Laurea) and T5.1 *"Dissemination and Communication Strategy and Plan"* (lead by EOS), and the next subchapters describes their key activities from the reporting period.

T5.3 "Project Annual Workshop for Stakeholders"

T5.3 is dedicated to arrange the EU-HYBNET Annual Workshop on a yearly basis. The 2nd Annual Workshop (AW) was arranged in M24 (April 2022) in hybrid format (on-line and in person in Rome) in the premises of the EU-HYBNET partner UCSC/Università Cattolica del Sacro Cuore. Program of the event is attached in ANNEX IV. According to DoA Annual Workshop 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 with a view to assessing the feasibility of the project findings and possible recommendations to innovations uptake and standardization. Annual Workshops will foster network activities, raise awareness of the project and bring together relevant practitioners and stakeholders who may join to the EU-HYBNET network and its activities. Eventually the goal of Annual workshops is to bring sustainability of the project activities and increase relevant members in network.

As one of the EU-HYBNET Annual Workshop (AW) goal is to focus on innovation uptake and recommendations, in the 2nd Annual workshop a session was dedicated to pitches of innovations and innovative solutions. Few months before the AW, the EU-HYBNET announced possibility for innovative solutions 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 2nd cycle gaps and needs, threats to counter Hybrid Threats. This call resulted to seven (7) pitches that were presented in the 2nd Annual Workshop. The pitches were given by following organization on following innovations or innovative solutions, and some of the innovations had EC project funding background:

1. **Provider:** Research Driven Solutions Limited
Innovation: *Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes*
2. **Provider:** HENSOLDT Analytics GmbH
Innovation: *HENSOLDT Analytics OSINT System*
3. **Provider:** European Risk & Resilience Institute
Innovation: *Resilience Tool incl. Risk Radar*
4. **Provider:** HybridCore
Innovation: *Smart Navigator*
5. **Provider:** NORD University
Innovation: *NORDLAB Concept*
6. **Provider:** Austrian Institute of Technology GmbH
Innovation: *Defalsif-AI Forensics Platform*
7. **Provider:** European External Action Service, Strategic Communication division.
Innovation: *Disinformation Data Space*

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

- critical infrastructure protection
- disinformation; information manipulation and interference
- crises management

The Innovative solution "*Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes*" presented by Research Driven Solutions Limited is part of the PRECINCT project, and hence also highlighted the importance for cooperation between PRECINCT and EU-HYBNET. The PRECINCT project was also invited next to other three EC funded security projects to present the innovations from their projects because they all may deliver sound solutions to the present pan-European gaps and needs, threats to counter Hybrid Threats.

The projects who were invited to the 2nd EU-HYBNET AW are listed below. Next to the project(s), it is highlighted which EU-HYBNET's identified critical gaps and needs and threats the project may deliver important solutions and research.

- **ALIGNER/** Artificial Intelligence Roadmap for Policing and Law Enforcement
 - Connection to EU-HYBNET's identified Hybrid Threat area: *Digital escalation and AI-based exploitation*
- **7SHIELD/** Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats
 - Connection to EU-HYBNET's identified Hybrid Threat area: *Space interference and counterspace weapons*
- **PRECINCT/** Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection
 - Connection to EU-HYBNET's identified Hybrid Threat area: *Exploitation of critical infrastructure weaknesses and economic dependencies*
- **MEDEA/** Mediterranean practitioners' network capacity building for effective response to emerging security challenges
 - Connection to EU-HYBNET's identified Hybrid Threat area: *migration and e.g. in the context of information manipulation with the aim of destabilization*

These named four project presentations on their focus and solutions were especially important to EU-HYBNET T3.2 and T3.3 to proceed with their analysis and **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results**. As mentioned in the earlier chapters the final results of T3.2 and T3.3 analysis will presented in the next EU-HYBNET Six Months Action Report D1.10 (October 2022). Further findings on 2nd Annual workshop will be reported in D5.11 "Annual Workshop report 2" (M25/ May 2022).

T5.1 “Dissemination and Communication Strategy and Plan”

The EU-HYBNET T5.1 is to deliver EU-HYBNET “Dissemination, Communication and Exploitation” (DCE) Plan for internal and external communication in order to ensure efficient dissemination and communication activities in the project as well as the project internal information sharing, and the preparation of a clear and sustainable exploitation plan. The task is to promote EU-HYBNET objectives, progress and results to a wide range of stakeholders. Furthermore, T5.1 is to support that project yearly results are taken into use and seen beneficial by the EU-HYBNET stakeholders. Therefore, the T5.1 is much involved to the cooperation done with other EC funded projects with whom EU-HYBNET shares the interests for measures relevant also to counter Hybrid Threats. For this reason the cooperation and connections established in T5.1 also delivers material and insights especially for the T3.3 and T3.2 for their further analysis what comes to **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** relevant also to the EU-HYBNET’s identified gaps and needs, threats in the Hybrid Threats landscape.

During this Six Month Action Report Period EU-HYBNET has established cooperation with following EC funded security projects due to following EU-HYBNET’s focus areas and interests:

- **ILEANET/** Innovation by law Enforcement Agencies Networking <https://cordis.europa.eu/project/id/740714>
- **Cooperation with EU-HYBNET:**
 - *The learn on innovative solutions that may also deliver answer to the EU-HYBNET’s identified gaps and needs, threats to counter hybrid threats. In addition, gain feedback from the ILEANET LEAs network on the feasibility of EU-HYBNET findings and suggested solutions.*
 - *EU-HYBNET provided a presentation on the project’s activities in the ILEANET’s final conference on 6th of April 2022*
- **ECHO/** European network of cybersecurity centres and competence hub for innovation and operations <https://cordis.europa.eu/project/id/830943>
- **Cooperation with EU-HYBNET:**
 - *The learn on innovative solutions that may also deliver answer to the EU-HYBNET’s identified gaps and needs, threats to counter hybrid threats in the field of cyber security. In addition, gain feedback from the cyber security practitioners and other experts on the feasibility of EU-HYBNET findings and suggested solutions.*
 - *EU-HYBNET provided a presentation on the project’s activities in the ECHO’s Cyber Morning on 27th of April 2022*
- **MIRROR/** Migration-Related Risks Caused by Misconception of Opportunities and Requirement <https://cordis.europa.eu/project/id/832921>
- **Cooperation with EU-HYBNET:**
 - *The learn on innovative solutions that may also deliver answer to the EU-HYBNET’s identified gaps and needs, threats to counter hybrid threats in the field of border and*

maritime security. In addition, gain feedback from the security practitioners on the feasibility of EU-HYBNET findings and suggested solutions.

- *EU-HYBNET is requested to provide a presentation on the project's activities in the MIRROR's Conference on 5th of May 2022*

- **PRECINCT/ Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection**
<https://cordis.europa.eu/project/id/101021668>
 - **Cooperation with EU-HYBNET:**
 - *The learn on innovative solutions that may also deliver answer to the EU-HYBNET's identified gaps and needs, threats to counter hybrid threats in the field of critical infrastructure (CI) protection. In addition, gain feedback from the CI practitioners and other experts on the feasibility of EU-HYBNET findings and suggested solutions.*
 - *EU-HYBNET is requested to provide a presentation on the project's activities in the PRECINCT's Workshop and to be a representative in Workshop panel on 5th of May 2022*

- **ECSCI cluster/ European Cluster for Securing Critical Infrastructures** <https://www.finsec-project.eu/ecsci>
 - **Cooperation with EU-HYBNET:**
 - *The learn from cluster's various projects' on innovative solutions that may also deliver answer to the EU-HYBNET's identified gaps and needs, threats to counter hybrid threats in the field of critical infrastructure (CI) protection. In addition, gain feedback from the CI practitioners and other experts on the feasibility of EU-HYBNET findings and suggested solutions.*
 - *EU-HYBNET has provided a presentations on the project's activities and key findings relevant to CI protection in the ECSCI's Workshop during 27-29th of April 2022*

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'² 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 D2.9 *"Deeper analysis, delivery of short list of gaps and needs"* (M5/ September 2020), and now during the second project cycle (M18-M34/ October 2021-February 2023) to D2.10 *"Deeper analysis, delivery of short list of gaps and needs"* (M23/ February 2022) 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 2nd project cycle for the project to focus on.

The identified gaps and needs, threats in D2.10 provide the basis for other EU-HYBNET Tasks to proceed in their work related to innovation mapping to gaps and needs, finding 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 jointly by T4.3 *"Recommendations for Standardization"* (lead by PPHS), T4.2 *"Strategy for Innovation uptake and industrialization"* (lead by RISE). More detailed description from the named EU-HYBNET WPs and Tasks in the following subchapters.

3.2.1 EU-HYBNET WP2 GAPS AND NEEDS OF EUROPEAN ACTORS AGAINST HYBRID THREATS

As mentioned above T2.1 *"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) have delivered during the 2nd project cycle research on the most important pan-European practitioners' and other relevant actors' (industry, SMEs, academia, NGOs) gaps and needs to counter Hybrid Threats in D2.6 *"Long list of defined gaps and needs"* (M19/ November 2021) and in D2.10 *"Deeper analysis, delivery of short list of gaps and needs"* (M23/ February 2022). Because both D2.6 and D2.10 are labelled as "Consortium Only" Deliverables the key findings cannot be reported as such. However, the key gaps and needs are formulated as threats. The Threats are already presented under chapter 3.1

² 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) *ministry level* (administration), II) *local level* (cities and regions), III) *support functions to ministry and local levels* (incl. Europe's third sector).

but because of the importance of the findings and results to the second three lines of action “**Common requirements as regards innovations that could fill in gaps and needs**” the information is repeated. In short, the latest gaps and needs and threats for the project to focus on during the 2nd project cycle are following according to the project four core themes. The domains mentioned in the tables highlight the relevant domain of the threat according to the research approach used in EU-HYBNET, namely the “A Landscape of Hybrid Threats: The Conceptual Model”.

Core theme - Information and Strategic Communication:

<u>Threats</u>		<u>Domains</u>
Information manipulation with the aim of destabilization		Information, Cyber
Foreign interference in key information institutions		Political, Culture
Promoted ideological extremism and violence		Information, Intelligence, Legal

Core theme - Future Trends of Hybrid Threats:

<u>Threats</u>		<u>Domains</u>
Geopolitical heavyweight of domestic policy		Political, Economy, Infrastructure
Digital escalation and AI-based exploitation		Cyber, Military/defence, Political
Rise of populism		Political, Social/societal, Information

Core theme - Cyber and future Technologies:

<u>Threats</u>		<u>Domains</u>
Space interference and counterspace weapons		Space, Cyber, Military/defence
Offensive cyber capabilities		Cyber, Infrastructure
Disruptive innovations		Political, Social/societal, Military/defence

Core theme - Resilient Civilians, Local Level and National Administration:

<u>Threats</u>		<u>Domains</u>
Exploitation of existing political cleavages		Political, Public administration, Social/societal
Exploitation of critical infrastructure weaknesses and economic dependencies		Infrastructure, Economy, Cyber
Exploitation or investment in companies by foreign actors		Political, Economy

In the next six month period the project innovation mapping to the identified most critical gaps and needs, threats have proceeded in EU-HYBNET WP3 and WP2. Therefore the next Six Month Action report (October 2022) may describe more about **common requirements as regards innovations that could fill in** the EU-HYBNET 2nd project cycle (M18-M34/ October 2021-February 2023) **gaps and needs**. However, according to the identified domains of the gaps and needs, threats it is obvious that the innovations in the interest of EU-HYBNET would deliver innovations and focus on common requirements of security practitioners especially in following fields of the gaps and needs, threats:

- Cyber,
- Information,
- Intelligence,
- Legal,
- Political,
- Economy,
- Infrastructure,
- Space,
- Military/defence,
- Public administration,
- Social/societal,
- Culture

Furthermore, additional information gained to gaps and needs focusing especially to threats relate to populism, social networks and international groups from the EU-HYBNET “Future Trends Workshop” (FTW) that was arranged by T3.4 (EOS and UCSC) on 5th of April will be reported in the next Six Month Action Report (October 2022). The T3.4 “Innovation and Knowledge Exchange Events” will describe the FTW findings in the deliverable 3.15 “2nd Future Trends analysis Workshop Report” (May 2022) with more details, however, program of the FTW in Annex III.

3.2.2 EU-HYBNET WP4 RECOMMENDATIONS FOR INNOVATIONS UPTAKE AND STANDARDIZATION

In EU-HYBNET WP4 “Recommendations for Innovations Uptake and Standardization” activities to deliver **common requirements as regards innovations that could fill in gaps and needs** has been taken place in T4.2 “*Strategy for Innovation uptake and industrialization*” (lead by RISE) and T4.3 “Recommendations for Standardization” (lead by PPHS) which has lead to identify in the context of the first project cycle (M1 – M17/ May 2020 –September 2021) an innovation that well seems to deliver a needed solution to some of the first cycle’s identified gaps and needs. However, the discovery of the innovations is results of the whole workflow between EU-HYBNET WP2 “*Gaps and Needs of European Actors against Hybrid Threats*”, WP3 “*Surveys to Technology, Research and Innovations*” and WP4 “*Recommendations for Innovations Uptake and Standardization*” ending up to the T4.2 Innovation uptake strategy compilation for the most four promising innovation to the gaps and needs. The innovation in question is “**Public-Private info sharing groups for collaborative investigations/ Common Information Sharing and Analysis Environment (CISAE)**” that has lead in the discussions together with EEAS/ Strat Comm. to discover their interest to very similar innovation but in the field of disinformation, namely “*The FIMI Data Space (A common framework and methodology for collecting systematic evidence on disinformation (FIMI) – Open CTI tool*”. Due to the noticed need of “CISAE” innovation and “*FIMI Data Space-Open CTI tool*”, EU-HYBNET has continued cooperation with EEAS to promote and to solve requirements for uptake in the case of *FIMI Data Space-Open CTI tool*. Therefore, EEAS was invited to present a pitch on the “*FIMI Data Space-Open CTI tool*” innovation in EU-HYBNET T5.3’ 2nd Annual Workshop on 6th of April 2022. In the pitch more details on *FIMI Data Space-Open CTI*

tool's common requirements as regards innovations that could fill in gaps and needs were provided alike in the EU-HYBNET's T4.4 3rd Policy Brief on the innovation. The key elements and common requirements for the *FIMI Data Space-Open CTI tool* are:

Requirement 1. Large number stakeholders on domestic, EU and international level needed for information sharing, incl. private sector

- *Rationale:* Information Manipulation Interference (IMI) activities and campaigns and the mitigation of their effects, affect and involve a large number of stakeholders on domestic, EU and international level which all need to exchange information. Therefore, joint efforts are needed in order to learn on the activities and share the findings of the activities.
- The solution will serve the governmental and security sector which requires in-time and complete information on the security situation to enable fast reaction. Private sector companies (particularly online platforms) will benefit from a systematic inflow of threats observed and flagged to them for interventions. Academia may be the biggest benefactor as for the first time structured data on IMI and hybrid threats will be made available for research.

Requirement 2. Need to counter limitations in effective information sharing between key stakeholders

- *Rationale:* There are currently no available solutions addressing the challenge of making up-to-date, complete and machine-readable data on IMI activities available to all stakeholders to inform products and countermeasures. According to the brief, effective sharing of relevant threat-related information between key stakeholders is limited by three factors that needs to be overcome:
 - 1) the lack of a commonly accepted and jointly used taxonomy for IMI and TTPs (Tactics, Techniques and Procedures),
 - 2) the confidentiality of some of the information and
 - 3) the inaccessibility and non-machine-readable format information is currently shared.
- Solution is to replace a multitude of incompatible and incomplete bilateral, text-based information exchange means with a common approach accessible and usable for all stakeholders

Requirement 3. Need for mutually reinforcing elements from standards to tools, e.g. DDS-alpha

- *Rationale:* To achieve common situational awareness within reasonable delays we propose a set of mutually reinforcing elements from standards to tools which will overcome this information exchange problem and pave the way for an evidence based development and application of solutions as well as facilitating new innovation
- DDS-alpha is the Disinformation Data Space, a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan. Introduction is an inclusive set of open tools, frameworks and standards, adapted from the cybersecurity sector and best case practices on information manipulation and interference (IMI) analysis to provide the most comprehensive database on informational threats. DDS-alpha allows all stakeholders with information on IMI activities in government, international organisations, civil society, the private sector and academia to pool,

extract and recombine those insights to enable a wide range of countermeasures and products, depending on the stakeholders' needs and capabilities. It will also offer new insights on the threat, enabling new and faster means to achieve situational awareness or build new products.

EU-HYBNET will continue to solve the common requirements for the *FIMI Data Space-Open CTI tool* uptake. This work will be part of the EU-HYBNET forthcoming two events "Innovation Knowledge Exchange Workshop" arranged by T3.4 (by EOS and TNO) and "Innovation Standardization Workshop" arranged by T4.3 (by PPHS) to which EEAS/Strat.Comm. will be invited to present the tool and have further discussion on its' uptake possibilities and requirements for standardization. The results from the events will be reported in the next Six Moth Action Report (October 2022).

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

In EU-HYBNET the main tasks which contributed during the reporting period to the Three Lines of Action **“Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation”** were 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) and T4.4 *“Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge”* (lead by Hybrid CoE). However, also other EU-HYBNET Tasks delivered results important for the topic, esp. in Work Package (WP) 2 *“Gaps and Needs of European Actors against Hybrid Threats”* T2.1 *“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 following subchapters describe the contribution from each of the named tasks.

3.3.1 EU-HYBNET T4.3 RECOMMENDATIONS FOR STANDARDIZATION

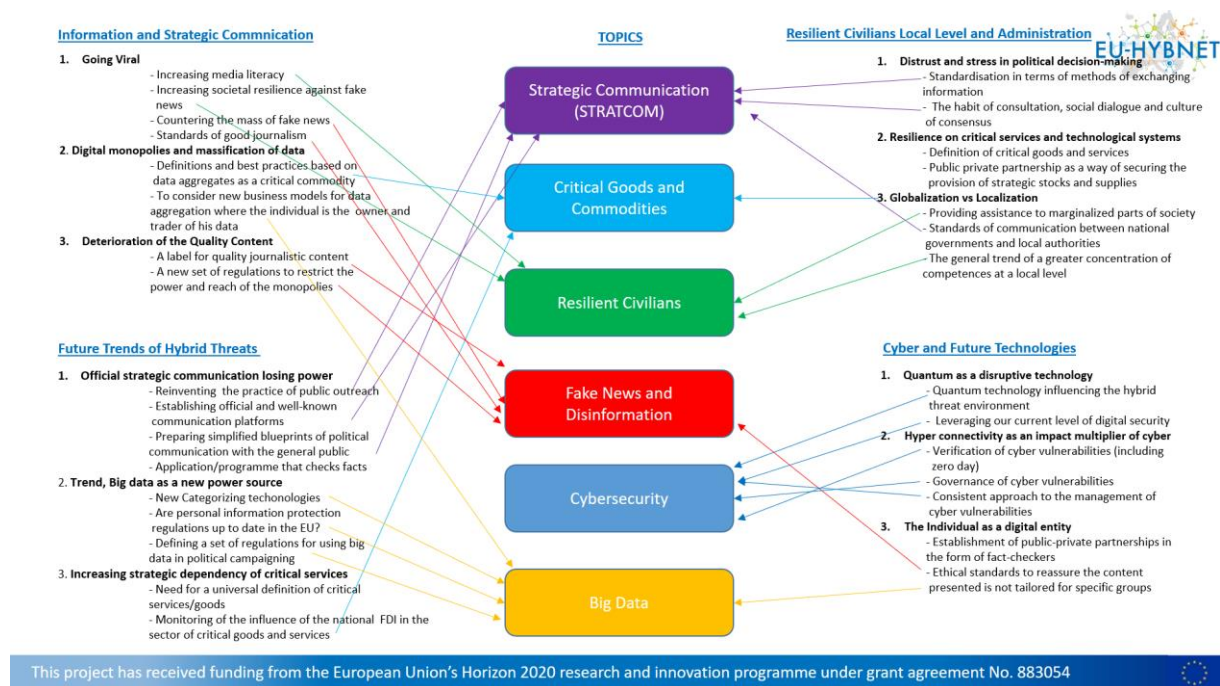
The EU-HYBNET T4.3 *“Recommendations for Standardization”* has a central role in delivering results to the third of the Three lines of Actions **“Priorities as Regards of Increasing Knowledge and performance Requiring Standardization”** focusing on areas and innovations that recommend the scope of countering 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 (incl. EU policies) that support recommending the identified, most promising EU-HYBNET areas and innovations for standardization.

On the basis of EU-HYBNET Task 3.1 *“Definition of Target Areas for Improvements and Innovations”* identified 27 most promising innovations and EU-HYBNET T2.2 *“Research to Support Increase of Knowledge and Performance”* D2.9 *“Deeper analysis, delivery of short list of gaps and needs”*, T4.3 discovered six (6) priority areas of increasing knowledge, performance and innovations requiring standardization.

The six priority focus areas are in line with the EU-HYBNET project four project core themes (Future Trends of Hybrid Threats; Information and Strategic Communication; Cyber and future Technologies; Resilient Civilians, Local Level and National Administration) and they are following:

1. Strategic Communication
2. Critical Goods and Commodities
3. Resilient Civilians
4. Fake News and Disinformation
5. Cybersecurity
6. Big data

The picture below highlights the EU-HYBNET four core themes and the prioritized innovation focus areas under each of the core themes, and how they are linked to the T4.3 selected six focus areas.



As described in the picture above, the EU-HYBNET's priorities for increasing knowledge and performance requiring standardization under each of the EU-HYBNET four core themes are following:

Core theme - Information and Strategic Communication:

1. Going Viral

- Increasing media literacy
- Increasing societal resilience against fake news
- Countering the mass of fake news
- Standards of good journalism

2. Digital monopolies and massification of data

- Definitions and best practices based on data aggregates as a critical commodity
- To consider new business models for data aggregation where the individual is the owner and trader of his data

3. Deterioration of the Quality Content

- A label for quality journalistic content
- A new set of regulations to restrict the power and reach of the monopolies

Core theme - Future Trends of Hybrid Threats:

1. Official strategic communication losing power

- Reinventing the practice of public outreach
- Establishing official and well-known communication platforms
- Preparing simplified blueprints of political communication with the general public
- Application/programme that checks facts

2. Trend, Big data as a new power source

- New Categorizing technologies
- Are personal information protection regulations up to date in the EU?
- Defining a set of regulations for using big data in political campaigning

3. Increasing strategic dependency of critical services

- Need for a universal definition of critical services/goods
- Monitoring of the influence of the national FDI in the sector of critical goods and services

Core theme - Cyber and future Technologies:

1. Quantum as a disruptive technology

- Quantum technology influencing the hybrid threat environment
- Leveraging our current level of digital security

2. Hyper connectivity as an impact multiplier of cyber

- Verification of cyber vulnerabilities (including zero day)
- Governance of cyber vulnerabilities
- Consistent approach to the management of cyber vulnerabilities

3. The Individual as a digital entity

- Establishment of public-private partnerships in the form of fact-checkers
- Ethical standards to reassure the content presented is not tailored for specific groups

Core theme - Resilient Civilians, Local Level and National Administration:

1. Distrust and stress in political decision-making

- Standardisation in terms of methods of exchanging information
- The habit of consultation, social dialogue and culture of consensus

2. Resilience on critical services and technological systems

- Definition of critical goods and services

- Public private partnership as a way of securing the provision of strategic stocks and supplies

3. Globalization vs Localization

- Providing assistance to marginalized parts of society
- Standards of communication between national governments and local authorities
- The general trend of a greater concentration of competences at a local level

With reference to the identified focus areas, according to the T4.3 further analysis presented in the T4.3 Deliverables (D) 4.8 “1st Report for standardisation recommendations” (Nov 2021), the key finding is that at the moment **priorities as regards of increasing of knowledge and performance requiring standardization** are in the domains of *disinformation* and *cyber security* in order to enhance European resilience and measures to counter hybrid threats. In addition, an important area is critical infrastructure protection while this was also highlighted in EU-HYBNET T4.2 identified most promising four innovations for pan-European security practitioners and other relevant actors to counter hybrid treats. The T4.2 four most promising innovations requiring standardization are:

1. Public-private information-sharing groups developing collaborative investigations and collective action
2. Debunking of fake news
3. Training application for media literacy
4. Guides to identify fakes

In order to proceed in the analysis of measure that are required to the named four innovations standardization and to learn more about the innovations standardization environment of the named innovations, T4.3 will arrange an innovation standardization workshop on 15th of June 2022 in Hague, the Netherlands. Due to the fact that the nature of the four most promising innovations is either reflecting the area of disinformation and fake news or critical infrastructure protection, the Innovation Standardization Workshop will focus on these areas or environments in the innovation standardization analysis of needed measures. The results of the Innovation Standardization Workshop are described in the next six month Action report D1.10 in project month (M) 30 (October 2022).

Furthermore, T4.3 has recognized the need to engage with the European policy actors in order to highlight the **priorities as regards of increasing of knowledge and performance requiring standardization** to counter hybrid threats. For this reason, T4.3 formulated on the basis of its' results in D4.8 short reports to highlighted specific recommendations for actions to be taken in the context of EU polices in the European Union (EU), EU Member States (EU MS) and in relevant European institutions so as to increase the knowledge and performance in the identified area. The reports were sent to selected EU and EU MS institutions by EU-HYBNET coordinator/ Laurea and T4.3 leader/ PPHS. Feedback to the reports was welcomed and e.g. the Prime Minister's Office in Finland was interested in learning more about the EU-HYBNET activities in the field. The reports were seen well to reflect the existing EU policy and recommendations environment and hence to deliver good basis for T4.3 to solve for the EU-HYBNET's most promising four innovations the needed actions in the innovation standardization in the context of disinformation and fake news (innovations: Debunking of fake news;

Training application for media literacy; Guides to identify fakes) and critical infrastructure protection (innovation: Public-private information-sharing groups developing collaborative investigations and collective action).

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

Because in EU-HYBNET Task (T) 4.2 “*Strategy for Innovation uptake and industrialization*” (lead by RISE) most promising innovations analyzed were focusing in three cases out of four to disinformation and fake news, European External Action Service (EEAS)/ Strategic Communication Division (Strat.Comm.) was contacted in order to tell about the EU-HYBNET findings. In addition, EU-HYBNET was interested in having a discussion, if there would be a possibility to proceed in the innovation uptake and recommendation process with the named innovations with the EEAS. The following two innovations were presented from T4.2 side to the EEAS/ Strat.Comm. because they were considered to support possible development of EEAS’s Rapid Alert System (RAS):

- Information sharing environment among practitioners in the scope of hybrid threats in a so-called EU Communication Awareness Environment (EUCAE) or “**Public-Private info sharing groups for collaborative investigations / Common Information Sharing and Analysis Environment (CISAE)**”
- Support to Media Literacy plans and uptake in EU Member States

The discussion between EU-HYBNET and EEAS supported EU-HYBNET to describe in more depth the innovations and the main advantages that they can bring to the practitioners as well as the challenges that can be faced during the innovations implementation. These issues are described in details in T4.2 D4.4 “1st Innovation uptake, industrialisation and research strategy”. Furthermore, the discussions between EU-HYBNET and EEAS/ Strat.Comm highlighted that not only innovations that support identification of disinformation and fake news are much needed but also creation of clear definitions of disinformation and fake news is a **priority as regards of increasing knowledge and performance requiring standardization**. Therefore, EU-HYBNET has continue the development work of the named innovations, especially EUCAE type of innovations, with EEAS so that EU-HYBNET work may benefit pan-European practitioners on a large scale in measures to counter hybrid threats especially in the information domain. However, the discussion between EU-HYBNET and EEAS/Strat.Comm on the EUCAE type of innovation and the EEAS’s needs on new innovations next to the RAS lead to notice joint interest to develop EEAS/Strat.Comm. innovation called “*The FIMI Data Space (A common framework and methodology for collecting systematic evidence on disinformation (FIMI))*” because it seems to answer all the development needs.

The EEAS/Strat.Comm has been developing the *FIMI Data Space* lately and it is established by using OpenCTI. The OpenCTI is a comprehensive tool allowing users to capitalize technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of analysed information to its primary source (a report, new article, etc.) when

solving the traits of disinformation. The key features of the OpenCTI is highlighted by the EEAS/Strat.Comm. in the picture below:

Bringing it all together: OpenCTI



Because the *FIMI Data Space-Open CTI tool* is an innovation answering to the noticed development needs of practitioner in the field of disinformation, EEAS/Strat. Comm. was invited to present the innovation in the EU-HYBNET 2nd Annual Workshop (in Rome & on-line 6th of April 2022) for pan-European Stakeholders and security practitioners to counter Hybrid Threats in order to gain feedback on the innovation's further development needs and usability. The EU-HYBNET's and EEAS/Strat.Comm.'s joint efforts to solve pan-European security practitioners' views on the *FIMI Data Space-Open CTI tool* will continue in the forthcoming EU-HYBNET events.

In short, the EEAS/Strat.Comm. has been invited to present the *FIMI Data Space-Open CTI tool* in the EU-HYBNET "Innovation and Knowledge Exchange Workshop" (IKEW on 14th of June in Hague) where more feedback on pan-European security practitioners is gained on the innovation's usability and possibilities for uptake. Furthermore, the EEAS/Strat.Comm. is planned to join to the EU-HYBNET's "Innovation Standardization Workshop" (on 15th of June 2022 in Hague) in order to analyse the landscape of standardization of the *FIMI Data Space-Open CTI tool* and to learn more on the features needed for the standardization and innovation uptake.

Moreover, at present the *FIMI Data Space-Open CTI tool* innovation is under the analysis of EU-HYBNET T3.2 "Technology and Innovations Watch" (lead by Satways) in order to solve the key features and needs for the tool's uptake and how it serves pan-European security practitioners' and other relevant actors (industry, SMEs, academia, NGOs) measures to counter Hybrid Threats.

Furthermore, EU-HYBNET T2.3 "Training and Exercises Scenario Development" (lead by KEMEA) is to imbed the *FIMI Data Space-Open CTI tool* to forthcoming EU-HYBNET training and exercise scenarios so that the tool will be tested in the forthcoming EU-HYBNET training event in September 2022. The EU-HYBNET training is arranged by the EU-HYBNET T2.4 "Training and Exercises for Needs and Gaps" (Lead by L3CE). During the training pan-European security practitioners and other relevant actors will test EU-HYBNET's selected most promising innovations as promising solution to the EU-HYBNET's

identified most important pan-European security practitioners' and other relevant actors present gaps and needs, vulnerabilities to counter hybrid threats. The *FIMI Data Space-Open CTI tool* testing in the EU-HYBNET training and exercises will have an important role to solve priorities as regards of increasing knowledge and performance in the use of the tool and also the possible features affecting to the tools standardization.

Proceeding in the *FIMI Data Space-Open CTI tool* analysis and measures requested to the standardization will be reported in the next EU-HYBNET D1.10 "Six Month Actions report" (October 2022).

3.3.4 EU-HYBNET T4.4 POLICY BRIEFS, POSITION PAPER, RECOMMENDATIONS ON UPTAKE OF INNOVATIONS AND KNOWLEDGE

EU-HYBNET has delivered two Policy Briefs during this six month action report reporting period (November 2021 - April 2022) and both of the policy briefs present **priorities as regards of increasing knowledge and performance requiring standardization**. The policy briefs are written by EU-HYBNET consortium partners TNO and RISE, and the Policy Briefs are published in the EU-HYBNET webpage <https://euhybnet.eu/policy-briefs/>. The topics of the Policy Briefs are following:

- "Countering Hybrid Threats: Areas for Improvement and Developing Innovations" by TNO on December 2021
- "Build Societal Resilience – Share IMI (Information Manipulation and Interference) Information" by RISE on February 2022

In the next subchapter key messages from the EU-HYBNET policy briefs to **priorities as regards of increasing knowledge and performance requiring standardization** in countering hybrid threats are highlighted.

"Countering Hybrid Threats: Areas for Improvement and Developing Innovations" Policy Brief

The key six observations in the Policy brief to **priorities as regards of increasing knowledge and performance requiring standardization** in the context of countering hybrid threats are following:

Observation 1. All solutions are directed to increasing resilience and defence against hybrid threats

Western ethical and legal restrictions are a limiting factor to the identification of offensive solutions and innovations to counter Hybrid Threats. Policymakers should evaluate such limitations and consider the pro's and cons of such limitations in light of increased tensions and hybrid threats proliferation.

Observation 2. Information collection and information sharing opportunities

Information is collected by many different entities, including governments, NGO's, private business, and citizens. Yet the willingness to share information cross sectors remains inadequate. It is seen essential that information sharing is enhanced. This ranges from establishing and expanding specialized cross-sector cyber threat information sharing platforms, early damage assessment platforms, public-private information sharing groups civilian emotional detection tools, and foreign direct investment monitoring platforms, to a more holistic society-wide resilience-improving network in the form of resilient democracy infrastructure platforms.

Observation 3. There are structural challenges to the upscaling of national initiatives to EU level

All EU member states work on various hybrid threats and appropriate tools to counteract these challenges. Still it remains a challenge to share best practices and to scale-up effective solutions from a national level to the EU level. Such challenges include diverging conceptualisations of hybrid threats, different prioritizations of hybrid threats, and a lack of awareness of clear benefits from such sharing. In short, information sharing between EU MS is a priority as regards of increasing knowledge and performance to counter hybrid threats also pan-European wide.

Observation 4. Blowback risk due to low societal acceptance

Innovations related to improving civilian resilience and enhancing governmental strategic communications to citizens are highly dependent on citizens' acceptance of tooling that interacts with, informs, and influences the citizens. Therefore, societal acceptance of this type of innovations is a priority for proceeding while policymakers have an essential role in understanding the constraints of citizen-focused solutions, and should consider roadmaps of implementation for such solutions.

Observation 5. Lacklustre addressing of legal and ethical challenges

A lacklustre anticipatory approach towards legal and ethical challenges is not surprising, but nonetheless a hindrance to developing and implementing solutions. Legal and ethical challenges should be addressed throughout the entire process of identifying, developing, and implementing solutions. Policymakers have a vital role in setting up and monitoring adherence to legal and ethical for possible solutions. Without these structures that dictate how innovations would fit within the legal and ethical frameworks of practitioners, innovations might remain unusable upon development.

Observation 6. Improve post-quantum cyber security position

It is essential to invest in cyber security against future quantum computing-enhanced cyber-attacks. The quantum key distribution testbed could help improve societal resilience against such quantum computing-enhanced cyber-attacks for Business-to-Business and Business-to-Consumer collaborations, as well as for crisis-time emergency communications. Research into quantum technology and its implications is not well regulated yet. Such regulations could help ensure that critical applications that are being built today, are quantum-safe or quantum-upgrade-ready.

“Build Societal Resilience – Share IMI (Information Manipulation and Interference) Information” Policy Brief

The Policy Brief focused on the challenges in handling foreign or domestic Information Manipulation and Interference (IMI) activities and campaigns together with actions that would help to build increased societal resilience against such threats. The policy brief is also linked to the development of the EEAS/Strat.Comm. innovation “*FIMI Data Space-Open CTI tool*” that EU-HYBNET has identified as an important innovation for uptake in order to enhance pan-European security practitioners’ and other relevant actors’ response to Hybrid Threats.

According to the Policy brief following key aspect are **priorities as regards of increasing knowledge and performance** in in handling foreign or domestic Information Manipulation and Interference (IMI) activities and campaigns. The same elements holds for the EEAS/Strat.Comm.’s innovation “*FIMI Data Space-Open CTI tool*” to which uptake EU-HYBNET is contributing. The priorities are:

- sharing, analysis and aggregation of IMI information between stakeholders is of outmost importance, especially for early/immediate and successful mitigation of the effects of IMI activities and campaigns.
- Having the means to produce joint near real-time situational awareness and a comprehensive overview of the threats in the mid and long term that are common to stakeholders within and between member states are key
- A solution for efficient cooperation between stakeholders would allow access to IMI information coming from concerned sources and would constitute a basis for early detection and joint actions to counter IMI activities
- Cooperation must be based on trust between involved stakeholders and joint actions must rely on a common view of the situation at hand
- Cooperation should include and involve a large number of stakeholders
- To achieve rapid and near real-time joint situation awareness more low-level IMI information must be shared and distributed analysis solutions employed. The sharing and analysis must be supported by automatic and/or semi-automatic functions and services to allow handling of the very large amount of IMI data involved and especially being capable of handling multi-lingual settings.
- The need for efficient tools supporting distribution and analysis of IMI information is of particular importance when immediate/early successful detection and mitigation of IMI activities is required

Furthermore, according to the Policy Brief following actions are recommended so as to proceed in handling foreign or domestic Information Manipulation and Interference (IMI) activities and campaigns in the way needed:

- **Develop an IMI taxonomy**, which comprises common definitions and required terminology to adequately and precisely describe the IMI threats and approaches.
- **Develop standards for IMI information exchange**. Such as standard could take the STIX standard (Standard Threat Information Expression) as a starting point and extend it to cover

relevant but missing IMI aspects. STIX allows sharing of information about incidents including actors, vulnerabilities, TTPs etc., in a machine-readable format.

- **Develop a distributed networking solution for IMI information sharing and analysis.** The networking solution could take e.g., the European Maritime Security Authority (EMSA) Maritime CISE (Common Information Sharing Environment) networking solution format as a starting point and extend it with capabilities for joint automatic or semi-automatic analysis of IMI data. The networking solution must include functionality which gives the information owner control of which information that is shared with whom. It should also ensure that systems currently in use by different stakeholder for IMI situational awareness and analysis can be accommodated.
- **Initiate research and development in the area of automatic and / or semi-automatic IMI analysis tools.** Such tools will be required to cope with the increasing amount of information that has to be monitored, scanned and analysed for IMI activities and/or attacks. As sharing of information related to IMI may be sensitive and block sharing of IMI information, a remedy would be to base joint analysis efforts on federated machine learning methods. Furthermore, it should be considered to develop AI tools based on behaviour-based AI techniques as they may provide a more reliable solution which also is privacy and freedom-of-speech protecting.
- **Initiate an EU task force investigating how to build trust between private and public sector stakeholders** with the aim to make IMI information sharing available, i.e., analyse and propose solution for how to enable participation of private sector stakeholders in IMI information sharing and analysis networks. Issues at hand are how private ownership/control of assets should influence possibilities to participate, trust issues in general and barriers against sharing of secret or sensitive information, etc.

3.3.3 EU-HYBNET WP2 GAPS AND NEEDS OF EUROPEAN ACTORS AGAINST HYBRID THREATS

EU-HYBNET's 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) have delivered deliverables (D) D2.6 "Long list of defined gaps and needs" (M19/ November 2021) and D2.10 "Deeper analysis, delivery of short list of gaps and needs" (M23/ February 2022) that included analysis of the most important pan-European security practitioners' and other relevant actors' gaps and needs to counter Hybrid Threats for the second project working cycle (M18-M34/ October 2021 - February 2023) to focus on. Naturally the most critical gaps and needs frame the **priorities as regards of increasing knowledge and performance requiring standardization** to counter Hybrid Threats. However, the T2.1 and T2.2 results are described both in chapter 3.1 and chapter 3.2, and hence the most critical gaps and needs, in a form of threats is not repeated here.

However, in the next EU-HYBNET "Six Month Actions report" D1.10 (October 2022) results from the second EU-HYBNET project cycle (M18-M34/ October 2021 – February 2023) on identified promising

innovations to the second cycle critical gaps and needs, threats to counter Hybrid Threats will be described.

4. CONCLUSION

4.1 SUMMARY

In the chapter above it is described how the EU-HYBNET project activities from the past six project months (November 2021 - April 2022) 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 2nd project cycle has started to deliver results from this cycle as well and how some results still serve and continue the project work conducted during the first project cycle (M1-M17/ May 2020 – September 2021). Furthermore, the goal of the document has been also partly 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 addition, we gave a short description of the contributors to the Six Month Action Report.

In Section 3. we showed how the EU-HYBNET project tasks and project actors have contributed and 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 beginning of the second project cycle (2nd cycle duration: M18-M34/ October 2021 – February 2023) have been now explained to the EC. However, the next Six Month Action Report (in October 2022) will describe more the second cycle results and findings to the Three Lines of Actions and also provide iteration to the 1st cycle findings and improvements and how to project has been able to implement the findings event 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 further work in the second cycle and Three Lines of Action related work in different EU-HYBNET project work packages and Tasks. During the next project period, the following eight (8) deliverables and one (1) milestone will be delivered:

Deliverables (D):

T5.3 Project Annual Workshops for Stakeholders

- D5.11 Annual Workshop Report 2 (UCSC), M25

T3.4 Innovation and Knowledge Exchange Events

- D3.15 Future Trends analysis Workshop Report (UCSC), M25

T2.3 Training and Exercises Scenario Development

- D2.18 Training and Exercise, Scenario Delivery (KEMEA), M27

T3.4 Innovation and Knowledge Exchange Events

- D3.12 2nd Innovation and Knowledge Exchange Events Report (EOS), M27

T2.4 Training and Exercises for Needs and Gaps

- D2.21 Training and exercises delivery on up-to-date topics (LEC3), M29

T1.1 Administrative and Financial Planning and Coordination

- D1.10 Fifth Six Month Action Report (Laurea), M30

T.1.2 Project Management, Quality Control, Ethics and Risk Management

- D1.17 Societal Impact mid-term report (Laurea), M30

T1.3 EU-HYBNET Community Extension

- D1.24 EU-HYBNET Network Sustainability Initial Report (Hybrid CoE), M30

Milestones (MS):

- MS17/ 2nd cycle of mapping gaps and needs on the innovations and research completed and shortlist of solutions handed over to WP4. Due by project month (M) M28 (August 2022).

As the deliverables and milestones highlight, 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 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 from EU-HYBNET Tasks (T) T3.2 and T3.3 will be ready. The deliverables will describe on identified innovations as promising solutions to the project's second working cycle (October 2021 – February 2023) deriving the EC and EU MS funded research and innovation projects and from European industry and SMEs. In addition, analysis of the innovations presented during the EU-HYBNET's 2nd Annual Workshop by pitching providers and relevant EC projects to EU-HYBNET will be more thoroughly analysed and goal is to describe how the proposed innovations may deliver promising solution to the identified critical pan-European security practitioners gaps and needs, threats to counter Hybrid Threats. Moreover, an important part of the next Six Month Action report will be results from the forthcoming two EU-HYBNET events, namely "Innovation and Knowledge Exchange Workshop" (IKEW) and "Innovation Standardization Workshop" (ISW) during 14th – 15th of June 2022 in Hague.

IKEW will deliver insights of some selected and during IKEW proposed, new innovative solutions soundness to present, 2nd project cycle gaps and needs, threats to counter Hybrid Threats. Next to IKEW, ISW will deepened the knowledge to measure that are requested in order to proceed in the uptake and standardization of the EU-HYBNET's selected, most promising innovations to the EU-

HYBNET 1st project cycle gaps and needs, threats in field of “critical infrastructure protection” and “disinformation and information manipulation and interference”.

Lastly, EU-HYBNET will continue to share the key findings with DG HOME and other relevant DGs via emails, invitations to the project events (e.g. IKEW and ISW) and of course to contribute to EC’s possible requests for information. In addition, cooperation with EEAS/Strat.Comm in the context of “Open CTI tool” development will continue alike the first concrete measure to establish the cooperation with the EUROPOL Innovation Lab will be taken. This all is to benefit the pan-European stakeholders from the EU-HYBNET results and to enhance joint measures to counter Hybrid Threats.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threat –project, No. 883054
EC	European Commission
GA	Grant Agreement
DoA	Description of Action Part A and B
H2020	Horizon2020, EC funding Program for EU projects' funding
FP7	The EC's 7 th 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
ISO	ISO Standard is a formula that describes the best way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials – standards cover a huge range of activities. Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators
FDI	Foreign Direct Investment
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
Open CTI	OpenCTI is a comprehensive tool allowing users to capitalize technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of analysed information to its primary source (a report, new article, etc.) when solving the traits of disinformation
PRECINCT	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges
7Shield	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats –project


ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement
ILEANET	Innovation by law Enforcement Agencies Networking -project
ECHO	European network of cybersecurity centres and competence hub for innovation and operations –project
MIRROR	Migration-Related Risks Caused by Misconception of Opportunities and Requirement –project
ECSCI	European Cluster for Securing Critical Infrastructures
DDS-alpha	DDS-alpha is the Disinformation Data Space
STIX	STIX standard: Standard Threat Information Expression
CISAE	Common Information Sharing and Analysis Environment. Similar innovation as CISE while focusing to other domain than maritime CISE.
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
RAS	Rapid Alert System in EEAS
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsø
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibernetiniu 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	Nederlandse Organisatie voor Toegepast Natuureenschappelijk 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 Viazul / The Romanian National Intelligence Academy
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 Infosüsteemi Amet / Estonian Information System Authority

MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
UniBW	Universitaet der Bundeswehr München


.

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. THE 2ND FUTURE TRENDS WORKSHOP


EU-HYBNET 2nd Future Trend Workshop, Hybrid #FTW



**In Rome and
online**



09.00- 16.00 CEST

The purpose of the Future Trends workshop is to support the practitioners' and stakeholders' everyday work by providing a future outlook for strategic planning and consider consequences of today's policy choices in long-term.

This workshop builds on the EU-HYBNET project findings and provides a platform of interaction for various stakeholders. Since the landscape of hybrid threats is continuously evolving, foresight and creative thinking is central for understanding, detecting and responding to emerging threats. It focuses on a more anticipatory and prospective outlook, highlighting the weak signals and outliers of disruptive and paradigmatic change to the European security environment. The title for this event will be **"Democracies on the edge?"**

To who? EU-HYBNET Partners, stakeholders, EAB members, network members, and interested innovation providers, industry, SMEs and NGOs, according to registration check.


When? 5th of April 2022 at 09.00-16.00 CEST

Registration Link: <https://forms.office.com/r/xhQccFHs41>

The instructions on how to join the meeting (both in presence and online) will be sent once you registration will be approved.

More information: Event organizer at Università Cattolica del Sacro Cuore, MS Monica Bernassola monica.bernassola@unicatt.it

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054.



EU-HYBNET

Agenda

2nd EU-HYBNET Future Trends Workshop: democracies on the edge?

Tuesday 05 April 2022 | 09.00 a.m. – 04.00 p.m. CEST

In presence at UCSC (Meeting room 5: plenary – Meeting rooms 3,4 and 5: breakout sessions)
On line via Zoom call

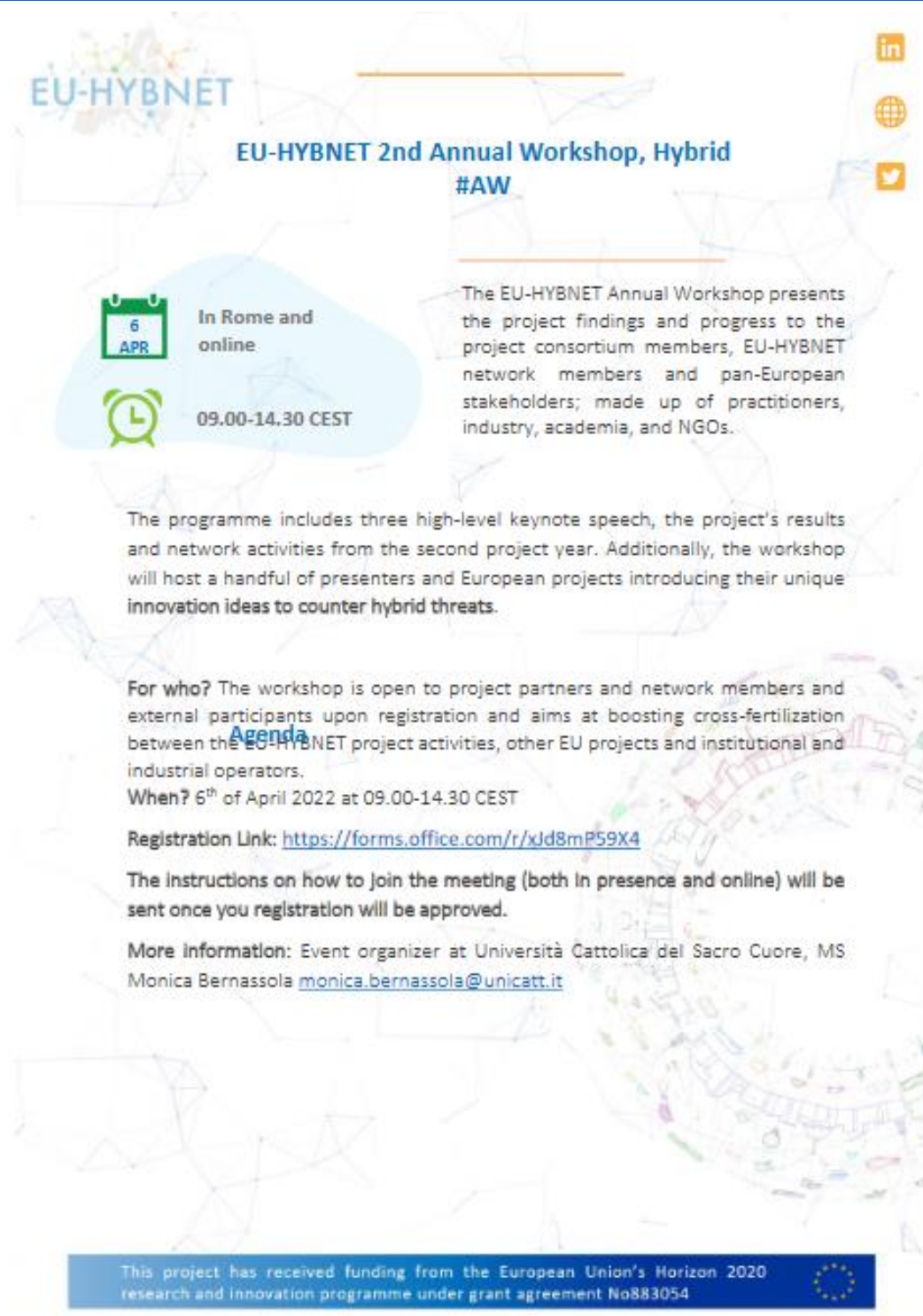
Time	Topic	Speaker(s)
08.30-09.00	Welcome and Registration	
09.00-09.10	Welcome words	Hanna Smith, European Centre of Excellence for Countering Hybrid Threats
09.10-09.15	Practical information	Sabina Magalini, Università Cattolica del Sacro Cuore
09.15-09.30	Keynote Speech: "Are democracies on the edge?"	Jonas Cederlöf, DG DEFS
09.30-09.45	Q&A from the audience	
09.45-10.00	Leg stretch break	
10.00-11.20	Panel discussion	Chair: Hanna Smith, HOOE Discussants: <ul style="list-style-type: none"> • Lauri Tiersia, European Digital Media Observatory • Georgios Kolliarakis, German Council on Foreign Relations
11.20-11.40	Break	
11.40-12.50	Breakout sessions: Meeting Room 5 - Populism Meeting Room 4 - Social Network Meeting Room 3 - International Groups	Chairs: <ul style="list-style-type: none"> • Evaldas Bružė, Lithuanian Cybercrime Center of Excellence for Training, Research & Education • Gunhild Hoggensen Gjølrv, The Arctic University of Norway

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054





		<ul style="list-style-type: none"> • Rubén Arcos, Universidad Rey Juan Carlos
12.50-13.50	Lunch break	
	Breakout sessions:	
	Meeting Room 5 - Populism	
13.50-14.50	Meeting Room 4 - Social Network	
	Meeting Room 3 - International Groups	
14.50-15.10	Leg stretch break	
		Chair: Maxime Lebrun, HCOE
		Rapporteurs:
15.10-15.50	Closing panel	<ul style="list-style-type: none"> • Evaldas Bružė, LCOE • Gunhild Hoogensen Gjølrv, UiT • Rubén Arcos, URJC
15.50-16.00	Closing remarks	HCoE and UCSC

ANNEX IV. THE 2ND ANNUAL WORKSHOP


EU-HYBNET

EU-HYBNET 2nd Annual Workshop, Hybrid #AW

6 APR
In Rome and online

09.00-14.30 CEST

The EU-HYBNET Annual Workshop presents the project findings and progress to the project consortium members, EU-HYBNET network members and pan-European stakeholders; made up of practitioners, industry, academia, and NGOs.

The programme includes three high-level keynote speech, the project's results and network activities from the second project year. Additionally, the workshop will host a handful of presenters and European projects introducing their unique innovation ideas to counter hybrid threats.

Agenda

For who? The workshop is open to project partners and network members and external participants upon registration and aims at boosting cross-fertilization between the EU-HYBNET project activities, other EU projects and institutional and industrial operators.

When? 6th of April 2022 at 09.00-14.30 CEST

Registration Link: <https://forms.office.com/r/xjd8mP59X4>

The instructions on how to join the meeting (both in presence and online) will be sent once your registration will be approved.

More information: Event organizer at Università Cattolica del Sacro Cuore, MS Monica Bernassola monica.bernassola@unicatt.it

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

2nd EU-HYBNET Annual Workshop:

Wednesday 06 April 2022 | 09.00 a.m. – 02.30 p.m. CEST

In presence at UCSC (Meeting room 5)

On line via Zoom call

Time CEST	Topic	Speakers
Welcome and registration		
8.30-9.00	Registration and Welcome	Senior Surgeon, Dr. Sabina Magalini/ Università Cattolica Sacra Cuore
9.00-9.10	Keynote Speech "The role of Research and Innovation in responding to hybrid threats"	Policy Officer, Mr. Giannis Skladarexis/ DG HOME
9.10-9.20	Keynote Speech "Innovations to foster pan-European security practitioners' response to hybrid threats"	Head of Team, Mr. Gregory Mounier/ EUROPOL, Innovation Lab
9.20-9.30	Keynote Speech "Hybrid threats and critical infrastructure protection"	Head of International relations, Mr. Rasmus Hindrién/ The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)
9.30-9.50	Questions and discussion	
EU-HYBNET's latest findings and results		
9.50-10.00	EU-HYBNET presents pan-European gaps and needs to counter hybrid threats	Senior Analyst, Mr. Maxime Lebrun/ Hybrid CoE
10.00-10.15	Innovations to counter hybrid threats	Senior Research & Innovation Manager, Dr. Souzanna Sofou/ Setways, Scientist, Mr. Okke Geurt Lucassen/ TNO
10.15-10.25	Innovation uptake and standardization activities	Research Associate, Alexios Koniaris/ KEMEA
10.25-10.40	Questions and discussion	
10.40-11.00	Leg stretch break	
Pitches - Innovation and ideas to counter hybrid threats by organizations and projects		
11.00-11.10	Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes	Mr. Lorcan Connolly/ Research Driven Solutions Limited
11.10-11.20	HENSOLDT Analytics OSINT System	Ms Victoria Toriser/ HENSOLDT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054



EU-HYBNET

11.20-11.30	Resilience Tool incl. Risk Radar	Dr Somik Chakravarty/ European Risk & Resilience Institute
11.30-11.40	Smart Navigator	Mr. Hasan Suzen/HybridCore
11.40-11.50	NORDLAB Concept	Prof. Odd-Jari Borch/ NORD University
11.50-12.00	Defalsify-AI Forensics Platform	Mr. Martin Boyer/ Austrian Institute of Technology GMBH
12.00-12.10	Disinformation Data Space	Mr. Daniel Fritz/ European External Action Service, Strategic Communication division
12.10-12.15	Questions and discussion Moderator: EU-HYBNET Innovation Manager Isto Mattila/ Laurea	
12.15-13.00	Lunch Break	
EU-HYBNET Network activities and innovations from other projects		
13.00-13.10	Artificial Intelligence Roadmap for Policing and Law Enforcement (ALIGNER) -project	Mr. Kai Pervöiz/ Fraunhofer-IAIS
13.10-13.20	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats (7SHIELDS) -project	The Coordinator Gabriele Giunta/ Engineering
13.20-13.30	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection (PRECINCT) -project	Mr. Stefan Schauer/ Austrian Institute of Technology GMBH
13.30-13.40	Mediterranean practitioners' network capacity building for effective response to emerging security challenges (MEDEA) -project	The Coordinator George Kokkinis/ Centre for Security Studies KEMEA
13.40-13.50	EU-HYBNET Network today and core activities	EU-HYBNET Network Manager Jari Räsänen/ Laurea
13.50-14.10	Questions and discussion Moderator: Senior Surgeon, Dr. Sabina Magalini/ Università Cattolica Sacro Cuore	
14.10-14.30	Closing remarks and wrap-up	Senior Surgeon, Dr. Sabina Magalini/ Università Cattolica Sacro Cuore EU-HYBNET Coordinator Päivi Mattila/ Laurea

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054



.

.