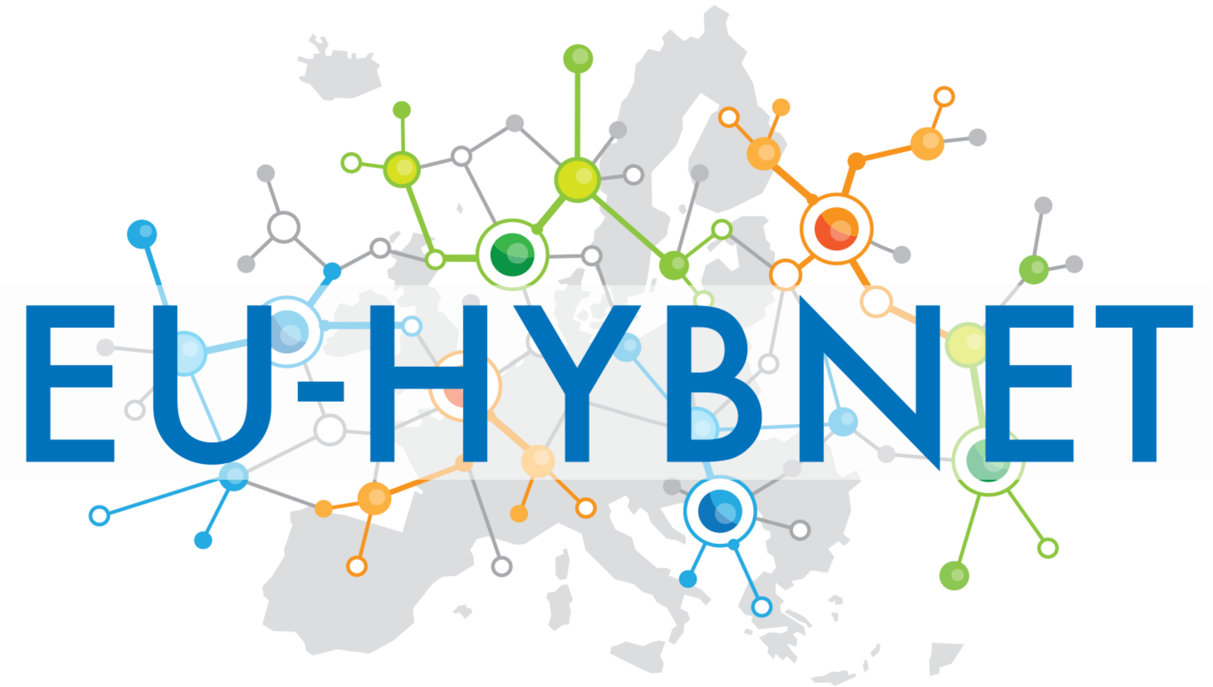


THIRD SIX MONTH ACTION REPORT

DELIVERABLE 1.4

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

D1.4 THIRD SIX MONTH ACTION REPORT

Deliverable number	**1.4**	
Version:	**1.0**	
Delivery date:	**19/11/2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	Päivi Mattila, Isto Mattila	**Laurea**
Contributors:	**Review:** Pablo Fernandez/ Maldita **Input to the report from all consortium partners :** Laurea, MTES, URJC, Hybrid CoE, PPHS, UiT, RISE, KEMEA, L3CE, TNO, Satways, Espoo, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, Maldita, ZITiS, COMTESSA	

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	08/10/2021	Päivi Mattila/ Laurea	First draft
0.2	01/11/2021	Päivi Mattila/ Laurea	Update text according to the projects' results from October
0.3	5/11/2021	Päivi Mattila/ Laurea	Text editing
0.4	12/11/2021	Päivi Mattila/ Laurea	Text editing
0.5	18/11/2021	Pablo Fernandez/ Maldita	Review
0.6	18/11/2015	Isto Mattila/ Laurea	Review
0.7	19/11/2021	Päivi Mattila/ Laurea	Final editing according to comments
1.0	19/11/2021	Päivi Mattila/ Laurea	Document for submission

DISCLAIMER

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

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

TABLE OF CONTENT

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The goal of the *Empowering a Pan-European Network to Counter Hybrid Threats* (EU-HYBNET) project deliverable (D) 1.4 "*Third Six Month Action Report*" in project month (M18) (October 2021) is to describe how the project has proceeded from M13 until end of M18 of the project (May 2020 – October 2021) 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*" are:

1) Monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results

2) Common requirements regarding innovations that could satisfy gaps and needs

3) Priorities regarding the increase of knowledge and performance requiring standardisation

Furthermore, D1.4 also highlights what actions and results are expected from EU-HYBNET during the next six month period (November 2021 - April 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 D1.4 to the whole project and it'sproceeding will be explained.
- Section 3. Describes how the project activities from months 13-18 have contributed to the EC's requested "three lines of action" activities.
- Section 4. Conclusion and next steps for the upcoming 6-month period of the project (November 2021 – April 2022).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.4 "*Third 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 D1.4, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.4 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.

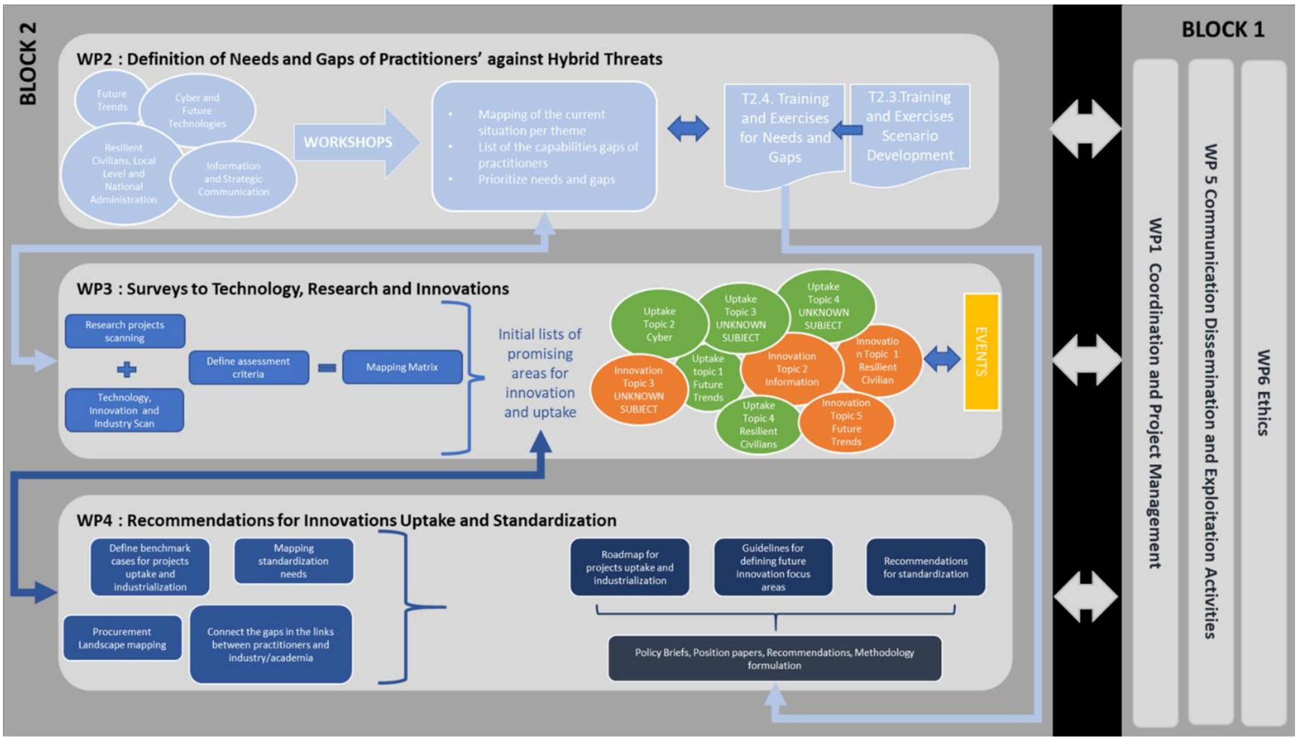

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

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

In addition, the project results and findings described in D1.4 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
23	Strategy started for innovation uptake and industrialisation	T4.1, T4.3	17
13	Cycle II has started	All	18

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The Third Six-Month Action Report (D1.4) main author is Laurea, the organization responsible for the delivery of D1.4. 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 second six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager have contributed to D1.4 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 second 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 industrialisation 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 standardisation

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 T2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" and T2.2 "*Research to Support Increase of Knowledge and Performance*" who identified during the first five project months 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 D2.9 "Deeper analysis, delivery of short list of gaps and needs" (M5/ September 2020) where the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats were listed. Therefore, the D2.9 signified 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.

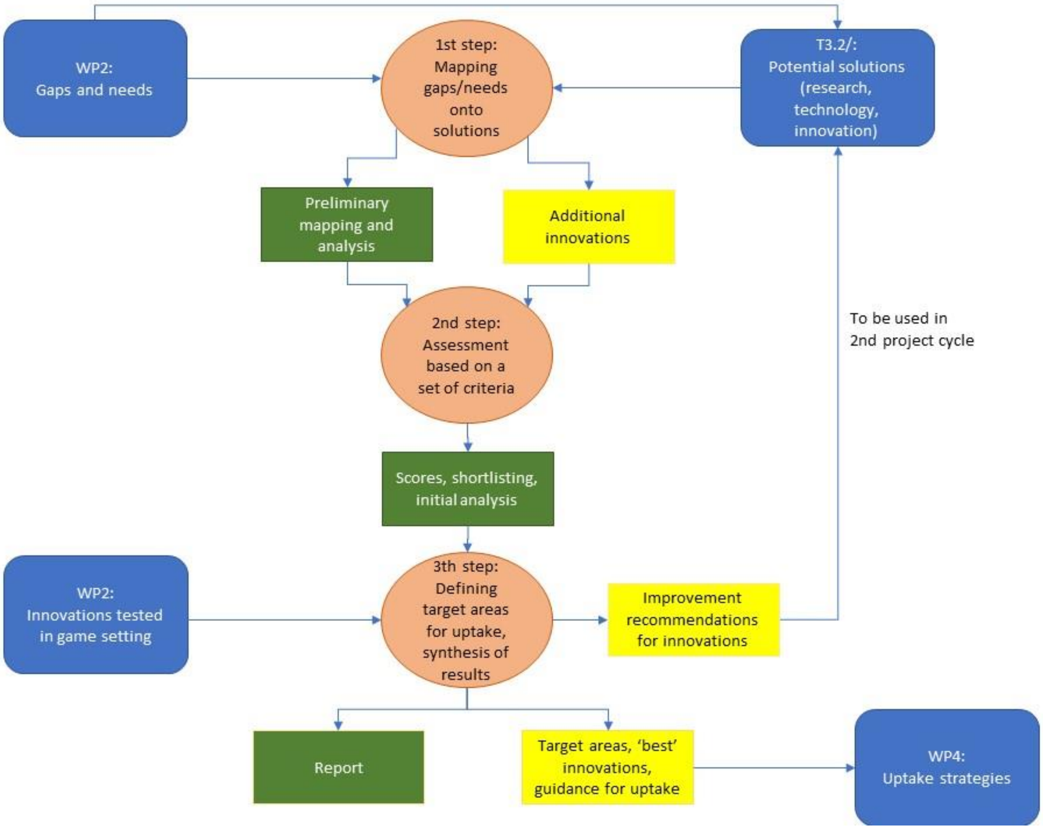
During this reporting period the innovation analysis work relevant to the first Three Lines of Action reporting has mainly been conducted in Work Package (WP) 3 "Surveys to Technology, Research and

[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).

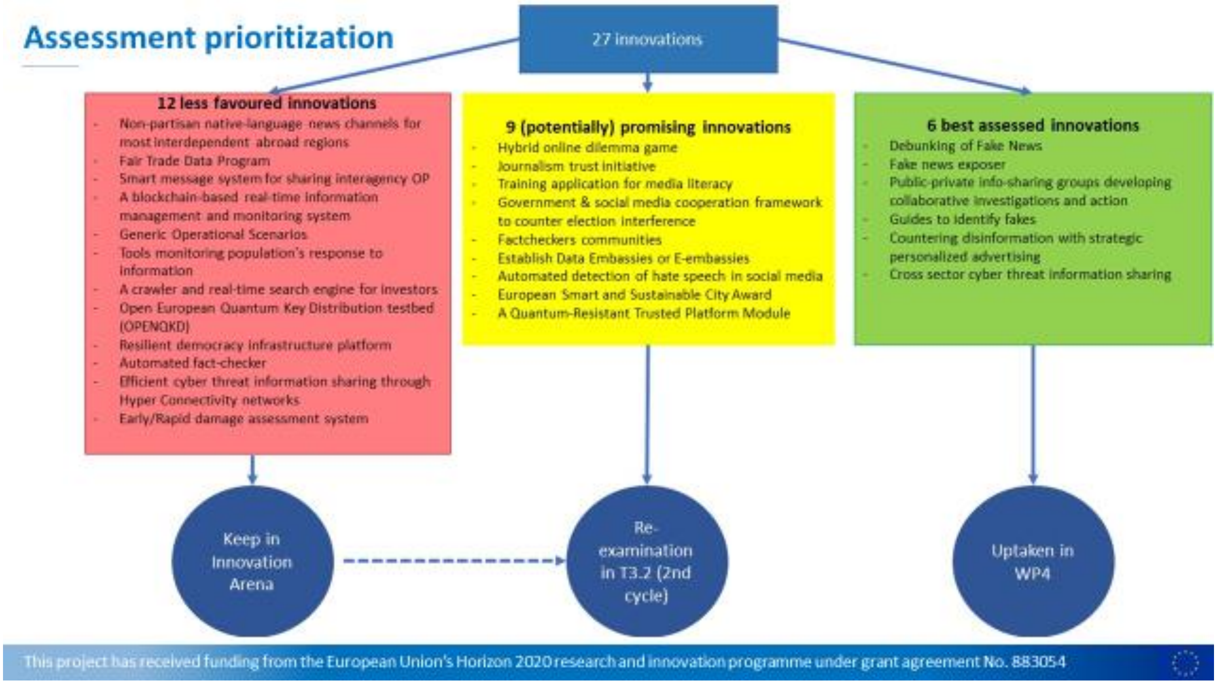
Innovations"/ T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead TNO) and WP4 "Recommendations for Innovations Uptake and Standardization"/ T4.2 "*Strategy for Innovation uptake and industrialization*" (lead RISE). However, activities in WP5 "Communication, Dissemination and Exploitation Activities"/ T5.3 "*Project Annual Workshops for Stakeholders*" (lead Laurea) has also provided input to the results and reporting. The results achieved from all 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 industrialisation of results"* are described in the following subchapters.

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

Task (T) 3.1 "*Definition of Target Areas for Improvements and Innovations*" has delivered final analysis of the most promising innovations to identified gaps and needs. In the analysis a three step approach was used in order to ensure that all relevant project information is imbedded to analysis and research work. This has ensured T3.1's important and central contribution to the Three Lines of Action "*Monitoring of research and innovation projects regarding the uptake of recommendations or the industrialisation of results"*. The three step approach has been explained in details in the Second Six Month Action Report (D1.3, M6), however the picture below highlights the main features and steps is the analysis work and connection to EU-HYBNET relevant tasks:



The three step approach focused to analyse 27 identified most promising innovations coming from T3.2 “*Technology and Innovations Watch*” (lead Satways) and T3.3 “*Ongoing Research Projects Initiatives Watch*” (lead L3CE) in large scale. Thorough analysis conducted in T3.1 led to identify out of the 27 innovations 12 less favoured innovations, 9 potential and promising innovations and 6 best assessed innovations. The process and thorough analysis of the innovation analysis is described in details in T3.1 D3.1 “First interim-report mapped on gaps and needs” (by TNO, M16/ August 2021). In addition, the picture below describes the innovation assessment and prioritization results – the picture is from D3.1 by TNO:



Assessment prioritization

27 innovations

12 less favoured innovations
- Non-partisan native-language news channels for most interdependent abroad regions
- Fair Trade Data Program
- Smart message system for sharing interagency OP
- A blockchain-based real-time information management and monitoring system
- Generic Operational Scenarios
- Tools monitoring population's response to information
- A crawler and real-time search engine for investors
- Open European Quantum Key Distribution testbed (OPENQKD)
- Resilient democracy infrastructure platform
- Automated fact-checker
- Efficient cyber threat information sharing through Hyper Connectivity networks
- Early/Rapid damage assessment system

9 (potentially) promising innovations
- Hybrid online dilemma game
- Journalism trust initiative
- Training application for media literacy
- Government & social media cooperation framework to counter election interference
- Factcheckers communities
- Establish Data Embassies or E-embassies
- Automated detection of hate speech in social media
- European Smart and Sustainable City Award
- A Quantum-Resistant Trusted Platform Module

6 best assessed innovations
- Debunking of Fake News
- Fake news exposer
- Public-private info-sharing groups developing collaborative investigations and action
- Guides to identify fakes
- Countering disinformation with strategic personalized advertising
- Cross sector cyber threat information sharing

Keep in Innovation Arena

Re-examination in T3.2 (2nd cycle)

Uptaken in WP4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Furthermore, according to the T3.1 analysis, supported by the scoring system used in T3.1 innovation analysis, the most promising or “best assessed” 6 innovations in EU-HYBNET to the pan-European practitioners’ and other relevant actors’ gaps and needs to counter hybrid threats are following:

‘Best assessed’ innovations	Total score	Excellence score	Impact score	Implem-entation score
Debunking of Fake News	13,0	4,5	4,0	4,5
Fake news exposer	12,1	3,7	3,7	4,7
Public-private info-sharing groups developing collaborative investigations and action	11,4	3,7	4,0	3,7
Guides to identify fakes	11,3	3,8	3,5	4,0
Countering disinformation with strategic personalized advertising	11,0	4,0	3,3	3,7
Cross sector cyber threat information sharing	11,0	4,3	3,7	3,0

In the analysis work, T3.1 also benefited from innovation analysis conducted in T2.4 "*Training and Exercises for Needs and Gaps*". In short, during the training event arranged by T2.4 the selected 27 innovations were shortly introduced to the training event participants who then selected the most interesting ones to innovation testing and further analysis during the training execution and play. The results of the training event and tested innovations are described in details in D2.20 "Training and exercises delivery on up-to-date topics" (L3CE, M12) and in D1.3 "Second Six Month Action Report". However, after the training event innovation testing in T3.1 it was seen fruitful to find possible European Commission (EC) or European Member States' (EU MS) funded research and innovation projects that could further highlight possible promising innovations in the same context as the tested innovations with a view to recommending the uptake or the industrialisation of results.

The EC and EU MS funded projects that T3.1 identified to include innovations or elements that support the innovations identified promising in the EU-HYBNET are following:

Context – EU-HYBNET Project Core Theme: Future Trends of Hybrid Threats

Finding 1.

Topic: Cross sector cyber threat info sharing platform

Relevant Action point: Sharing information among services and agencies

Project: CONCORDIA ("Cyber Security Competence Network for Research and Innovation") https://www.concordia-h2020.eu/

Issue: The innovation is expected to find synergies and complementarity as well as continuity / deepening of the CERT-EU (Computer Emergency Response Team) model in order to integrate disinformation. **H2020 Concordia** project has for instance resulted in "Threat Intelligence Platforms for Europe" enabling cross sector collaboration. It is based on a mutual cyber intelligence sharing agreement among partners. Such arrangement would be a way to join up disparate sources of information, based on open source information and partners' information

Finding 2.

Topic: Cross sector cyber threat info sharing platform

Relevant Action point: Sharing information among services and agencies

Project: INFRASTRESS ("Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system") https://www.infrastress.eu/ ; 7Shied ("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://www.7shield.eu/project/ ; EU-Circle ("A pan-European Framework for Strengthening Critical Infrastructure Resilience to Climate Change") https://www.eu-circle.eu/

Issue: Algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event. This would take the form of a Critical Infrastructure

Resilience Platform (CIRP) when fed with real time nowcasting or forecasting data instead of a scenario hazard, can be turned into an early or rapid damage assessment system respectively, thus providing the unique capability to initiate efficient response actions, right after (in case of now-cast data) or even before (in case of forecast data) the occurrence of catastrophic events. Long term investment supporting and enabling other IoSs (Internetwork Operating System). Metadata analysis is essential in this loop. The idea is in use within **INFRASTRESS H2020** project as well as **7Shield Project** and **EU-Circle H2020.**

Context – EU-HYBNET Project Core Theme: Cyber and Future Technologies

Finding 1.

Topic: Quantum key distribution testbed

Relevant Action point: NIST response / digital rescue package

Project: QKD ("Open European Quantum Key Distribution Testbed") https://openqkd.eu/

Issue: Scalable solutions in different infrastructure for protection against quantum computing enhanced attacks. The **QKD project** consortium should be leveraged in order to have updates on the most relevant advances in terms of quantum secure communications. This could apply in terms of B2C (Business to Consumer) and B2B (Business to Business) communication as well as emergency communications in times of crisis. Quantum communication engagement would enhance the security of institutional communications.

Context – EU-HYBNET Project Core Theme: Resilient Civilians, Local Level and National Administration

Finding 1.

Topic: Emotional detection tool on SOME and automated detection of hate speech in social media

Relevant Action point: Social media scans

Project: Several Github projects

Issue: Semantic analysis and machine learning are a usual part of the work with big data. By training the used algorithm to map a group of words to the most likely meaning, a detection of a particular topic can be performed. For example, several **Github projects** provide tools to detect hate speech. Such concepts are already used on Twitter to detect and censor discriminatory contents. Detection and analysis of emojis. Tools subject to spoofing, fake accounts, artificially generated content, large group of bystanders on social media

Finding 2.

Topic: Smart messaging routing and notification service

Relevant Action point: Fact checking

Project: INFRASTRESS ("Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system") https://www.infrastress.eu/ ; SATIE ("Security of Air Transport Infrastructure in Europe") https://satie-h2020.eu/

Issue: The service enables the sharing of the information among involved actors at every level of coordination enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. This way relevant information will reach the appropriate persons at every level of coordination in a timely manner. It can be evolved and integrated to share the operational picture to every agency involved in the response at every level of coordination. This idea is implemented in **InfraStress H2020** and **SATIE H2020 project**.

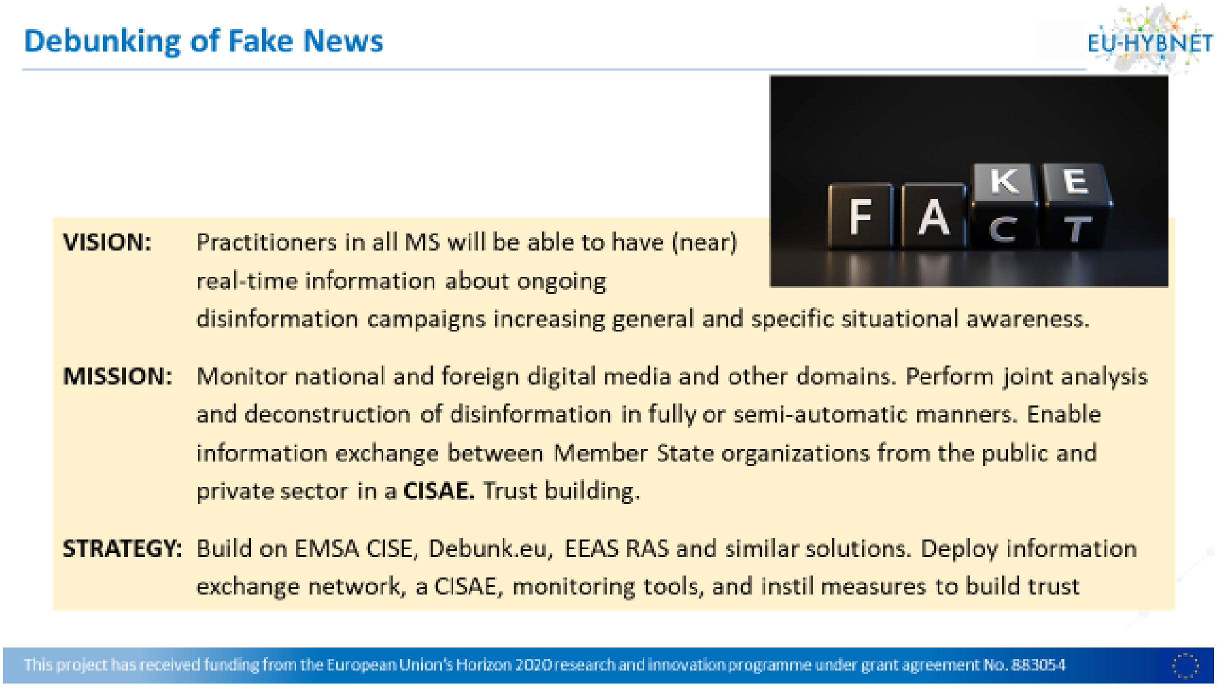
The identified projects in T3.1 highlight that EC and EU MS funded security projects have solutions that are also seen relevant to practitioners countering hybrid threat especially in the domains of critical infrastructure protection (incl. space), cyber security and information sharing in relation to crises between authorities. This finding will support to recommend EC funded projects (esp. CONCORDIA, INFRASTRESS, 7Shield, EU-Circle, SATIE) innovation uptake for practitioners. The finding also underlines the importance of cooperation in the context of innovations between these named projects and EU-HYBNET.

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 RISE) contribute 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***" while T4.2 provides also input to the second Three Lines of Action "Common Requirements as Regards Innovations that Could Fill in Gaps and Needs". The T4.2 contribution to the first Three Lines of Action is described below.

T4.2 delivered D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in M17 (August 2021) and the document described four most promising innovations identified by EU-HYBNET tot eh innovation uptake recommendations. In addition, T4.3 had prepared a thorough strategy for each of the four innovation in order to support its uptake process. the four most promising innovations described in the D4.4 are:

Innovation No.1./ Debunking of fake news



Debunking of Fake News

EU-HYBNET
FAKE
FACT

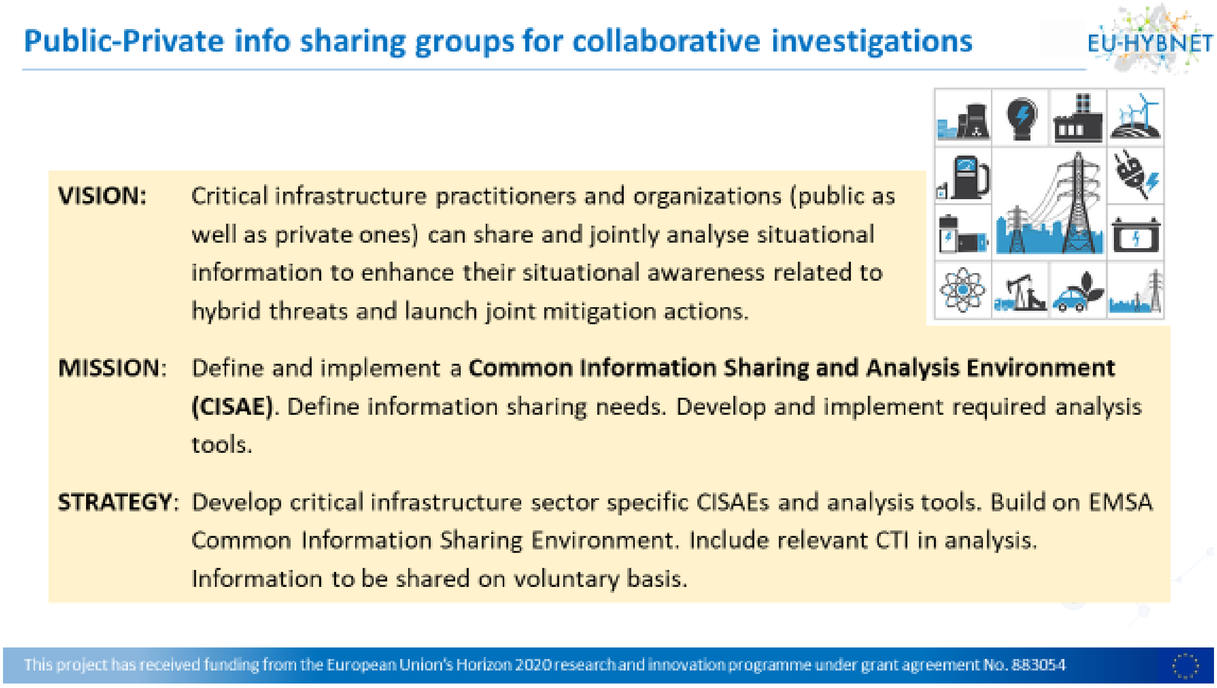
VISION: Practitioners in all MS will be able to have (near) real-time information about ongoing disinformation campaigns increasing general and specific situational awareness.

MISSION: Monitor national and foreign digital media and other domains. Perform joint analysis and deconstruction of disinformation in fully or semi-automatic manners. Enable information exchange between Member State organizations from the public and private sector in a **CISAE.** Trust building.

STRATEGY: Build on EMSA CISE, Debunk.eu, EEAS RAS and similar solutions. Deploy information exchange network, a CISAE, monitoring tools, and instil measures to build trust

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Innovation No.2./ Public-Private info sharing groups for collaborative investigations



Public-Private info sharing groups for collaborative investigations

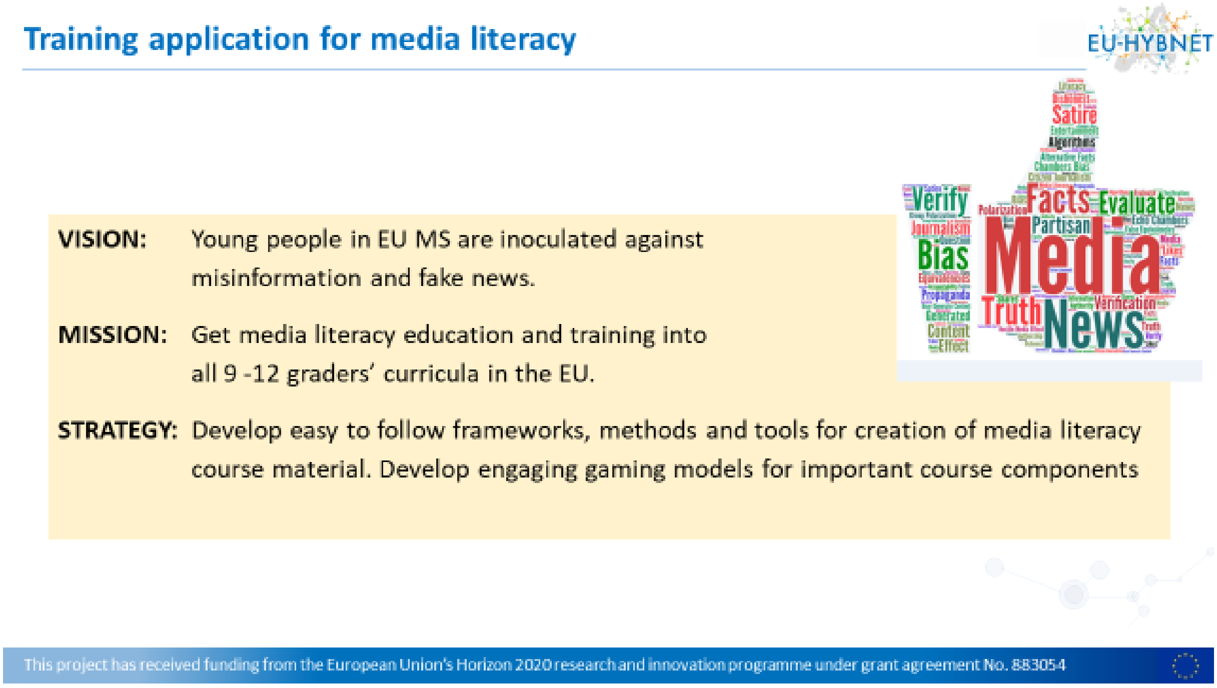
VISION: Critical infrastructure practitioners and organizations (public as well as private ones) can share and jointly analyse situational information to enhance their situational awareness related to hybrid threats and launch joint mitigation actions.

MISSION: Define and implement a **Common Information Sharing and Analysis Environment (CISAE)**. Define information sharing needs. Develop and implement required analysis tools.

STRATEGY: Develop critical infrastructure sector specific CISAEs and analysis tools. Build on EMSA Common Information Sharing Environment. Include relevant CTI in analysis. Information to be shared on voluntary basis.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Innovation No.3./ Training application for media literacy



Training application for media literacy

EU-HYBNET
Satire
Verify
Facts
Evaluate
Journalism
Partisan
Bias
Media
Propaganda
Truth
News
Verification
Content

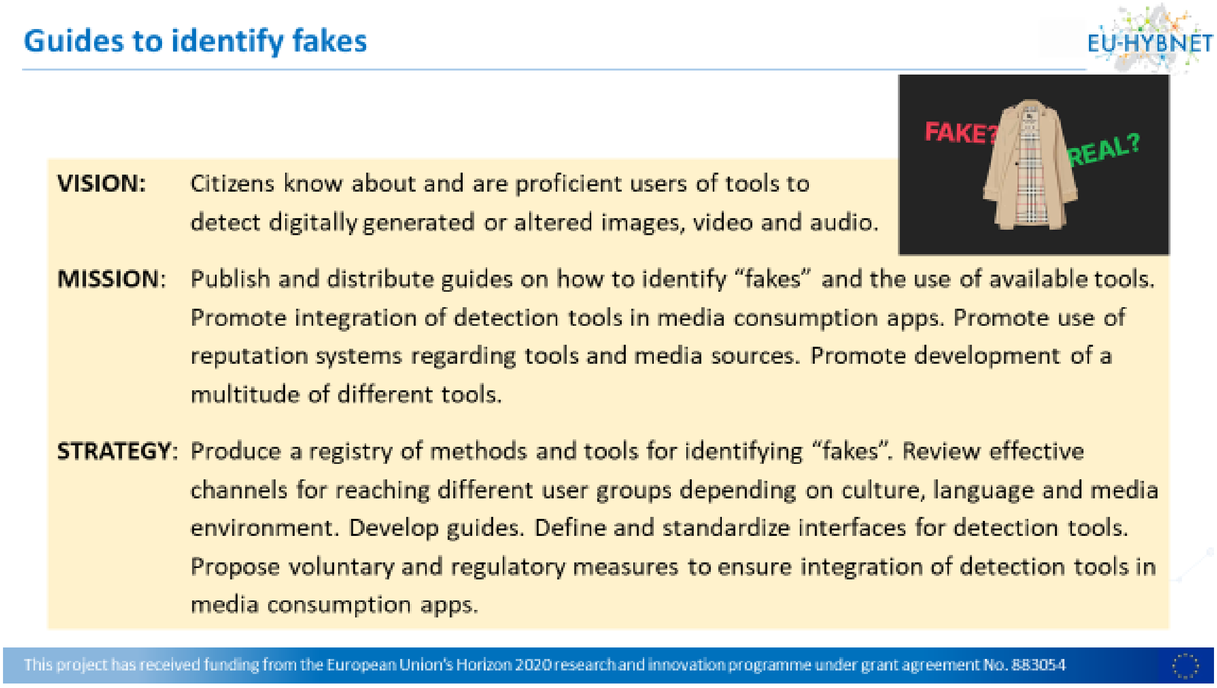
VISION: Young people in EU MS are inoculated against misinformation and fake news.

MISSION: Get media literacy education and training into all 9 -12 graders' curricula in the EU.

STRATEGY: Develop easy to follow frameworks, methods and tools for creation of media literacy course material. Develop engaging gaming models for important course components

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Innovation No.4./ Guides to identify Fakes



Guides to identify fakes

EU-HYBNET
FAKE?
REAL?

VISION: Citizens know about and are proficient users of tools to detect digitally generated or altered images, video and audio.

MISSION: Publish and distribute guides on how to identify "fakes" and the use of available tools. Promote integration of detection tools in media consumption apps. Promote use of reputation systems regarding tools and media sources. Promote development of a multitude of different tools.

STRATEGY: Produce a registry of methods and tools for identifying "fakes". Review effective channels for reaching different user groups depending on culture, language and media environment. Develop guides. Define and standardize interfaces for detection tools. Propose voluntary and regulatory measures to ensure integration of detection tools in media consumption apps.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

In the case of Innovation No.1. "Debunking of fake news and Innovation" and No.2. "Public-Private info sharing groups for collaborative investigations" EC FP7 funded project EUCISE2020 (European Union Common Information Sharing Environment 2020) https://cordis.europa.eu/project/id/608385 was highlighted as an innovation where to build on the named two innovations as well. In short, the CISE model was seen as a key innovation that can be recommended to build and to take into use also in the domains of information sharing and critical infrastructure protection. In short, EU-HYBNET discovery and recommendation is that CISE model supports to create needed “Debunking of fake news and Innovation” and “Public-Private info sharing groups for collaborative investigations” innovations.

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” contribute to the results too due to support given to project event arrangements.

An important event supported by WP5 (EOS) was “Defined Innovations to Hybrid threats” Event (see ANNEX III) on 4/10/2021, was arranged jointly by T3.1 “Definition of Target Areas for Improvements and Innovations” (TNO), T3.2 “Technology and Innovations Watch” (Satways), T4.2 “Strategy for Innovation Uptake and Industrialization” (RISE) and T1.2 “Project Management, Quality Control, Ethics and Risk Management” (Laurea). The event was arranged in order to tell about the EU-HYBNET ways to identify promising innovations to pan-European practitioners’ and other relevant actors’ (industry, SMEs, academia, NGOs) gaps and needs to counter hybrid threats, and what kind of methodology and analysis methods were used in order to define the most promising innovations. Furthermore, during the event the four most promising innovations identified in EU-HYBNET Task4.2 were presented to the audience. The audience consisted of EU-HYBNET consortium partners and Stakeholder group and network members and invited EC policy actors.

Because two of the four most promising innovations identified in the EU-HYBNET highlight the importance of the EUCISE2020 project, CISE (Common Information Sharing Environment) model as a basis for innovation uptake recommendations, it was an important message, especially for the practitioners and EC policy actors to hear, so that possible next steps in the innovation uptake could be taken.

The participants background in the 4/10 event is presented in the table below:

Background of participants	Amount of persons	Amount of organizations
Consortium partners	31	16
Stakeholder Group	1	1
Network Members	25	18
Israel Aerospace Industries	3	-
EC/ EUROPOL	3	-
EC/ DG HOME	3	-
In Total 66 participants out of 73 registered		

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) where the most important pan-European practitioners' and other relevant actors' (industry, academia, NGOs) gaps and needs to counter hybrid threats were listed.

The identified gaps and needs in D2.9 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.

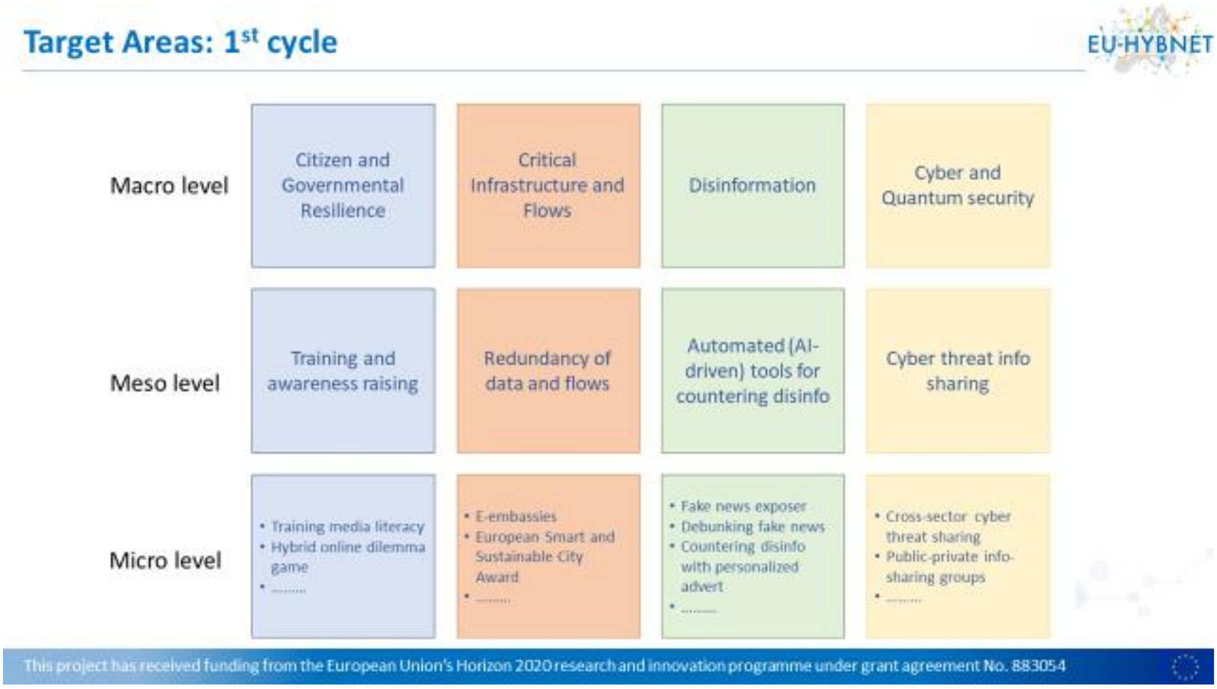
What comes to the second Three Lines of Actions focus area, namely "**Common requirements as regards innovations that could fill in gaps and needs**" the research activities and results are delivered from a common requirements point of view in T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) and in T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE). However, during this document reporting period, project months (M) 13 – 18 (May – October 2021) the second cycle of the project (M17-M34) has started and hence also new practitioners gaps and needs to counter hybrid threats have been identified in T2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" (lead by Hybrid CoE) during the M17 (September 2021). Therefore, also some insights from the 2nd cycle gaps and needs will be highlighted. The results from each of the named EU-HYBNET Tasks are described in the forthcoming sub-chapters.

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

Next to the analysis and identification of the most promising innovations, T3.1 is also to define **target areas** that are clusters of comparable and coherent innovative solutions for a specific hybrid threat domain and/or vulnerability seen as a key areas to focus on in EU-HYBNET during each project cycle. Generally speaking, the target areas serve as a guidance for EU-HYBNET WP4 to look for standards and best practices in order to foster the development and implementation of like-wise innovations.

[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).

Furthermore, target areas can be defined at different aggregation levels. In T3.1 following target areas, with three level approach (Macro, Meso and Micro Level) for innovations to gaps and needs were identified during the 1st project cycle under four different topics that are linked to the project four core themes:



Target Areas: 1st cycle

EU-HYBNET

Macro level	Citizen and Governmental Resilience	Critical Infrastructure and Flows	Disinformation	Cyber and Quantum security
Meso level	Training and awareness raising	Redundancy of data and flows	Automated (AI-driven) tools for countering disinfo	Cyber threat info sharing
Micro level	• Training media literacy • Hybrid online dilemma game • ………	• E-embassies • European Smart and Sustainable City Award • ………	• Fake news exposer • Debunking fake news • Countering disinfo with personalized advert • ………	• Cross-sector cyber threat sharing • Public-private info-sharing groups • ………

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

According to the identified target areas and three levels (Macro, Meso and Micro level), following observations of innovations were delivered in T3.1 what comes to the challenges, recommendations and common requirements as regards innovations to identified gaps and needs.

Topic: Citizen and governmental resilience

- Concerns about privacy, centralization and influencing temper value/expectations of innovations
- Education and training are elementary elements, probably already started at primary schools
- Citizen-involvement is a prerequisite
- The citizen-government relationship needs further research and focus (trust building, societal dialogue, social cohesion, consensus building etc.)

Topic: Critical Infrastructure and flows

- More attention for back-up and graceful degradation solutions
- Demand for risk assessment, chain analysis solutions will grow due to higher connectivity (IoT)

Topic: Disinformation

- Privacy, integrity, transparency of algorithms might hamper the public acceptance of related innovations; do more experimentation, validation and testing in approved laboratories.

- Potential added value of public-private partnerships for co-creation of tools
- To enhance wide use of tools (e.g. within the EU) the linguistic challenge should be addressed

Topic: Cyber and Quantum security

- Threat sharing requires willingness to share; high level of trust needed, start at small scale
- Public-private cooperation requires new (innovative) models of cooperation (addressing privacy , security, 'business model')
- Cyber vulnerabilities, plan ahead towards post-quantum security solutions
- Improvement of cyber security throughout our whole society requires more than just technology. The human and organizational dimension is just as important.

The thorough analysis of innovations and identified target areas in Task3.1 supports the need to look for standards and best practices in order to foster the development and implementation of like-wise innovations. These activities are conducted especially in WP4 Task4.2 and more about the findings in the next sub-chapters.

3.2.2 EU-HYBNET T4.2 STRATEGY FOR INNOVATION UPTAKE AND STANDARDIZATION

The key activity in Task (T) 4.2 is to define a concrete strategic approach for innovation uptake and industrialization and to the innovations seen as most promising ones in WP3 to the identified present pan-European actors' gaps and needs to counter hybrid threats identified in WP2. In addition, T4.2 is to formulate new approaches and procedures for innovation uptake, and during each of the project cycle an innovation uptake strategy for the most promising areas is developed. Furthermore, T4.2 is to state at least four innovations, an innovation to each of the project's four core themes, that EU-HYBNET recommends for pan-European stakeholders, especially security practitioners for innovation uptake process. Therefore, T4.2 activities have major input to the second of the Three Lines of Action: "**Common requirements as regards innovations that could fill in gaps and needs**".

The starting point for T4.2 work has been to select at least one promising innovation to each of the project's core themes for the innovation uptake and standardization strategy development. The selection was based on especially T3.1 analysis on most promising innovations, and hence in T4.2 following four innovations were selected to further analysis and strategy development:

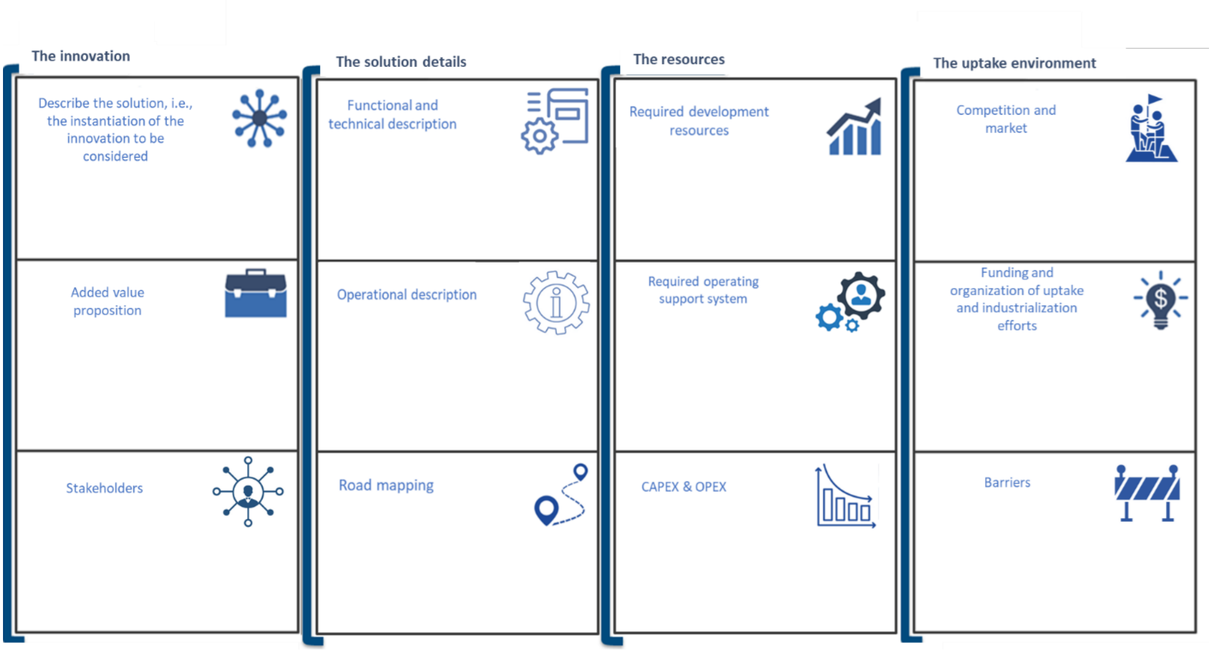
Innovations	**Project four core themes**			
	Resilient civilians, local level and administration	Cyber and Future Technologies	Information and Strategic Communication	Future Trends and Hybrid Threats.
1. Public-private information-sharing groups developing collaborative investigations and collective action		X	X	

2. Debunking of fake news	X		X	
3. Training application for media literacy	X		X	X
4. Guides to identify fakes	X		X	X

The selection of these four innovations based not only on the fact that they were among the T3.1 most promising innovations or the six "best assessed" innovations but they were also thoroughly analyzed in T4.2 internal consortium workshops. Furthermore, "*Public-private information-sharing groups developing collaborative investigations and collective action", "Debunking of fake news"* and *"Guides to identify fake news***"** were also selected in the EU-HYBNET training event by stakeholders as most promising innovations to be tested during the training (April 2021). Moreover, an important feature in "*Training application for media literacy"* innovation is that it exhibits both technical and non-technical features.

After the selection of the most promising innovations, T4.2 could proceed in its key activity: creation of strategy for innovation uptake and industrialization.

The starting point in this work has been to develop an Innovations Canvas for EU-HYBNET innovations uptake and common requirements analysis. The canvas has eventually been supported to create an uptake strategy for each of the selected four innovations in T4.2. The canvas is based on large scale research on many different existing innovation uptake canvases and tailored to the EU-HYBNET's needs while the innovation uptake in the hybrid threats domain is seen to ask very through innovation analysis so that the soundness of the innovation and the innovation uptake can be ensured. The research work related to the canvas development is described in detail in T4.2 D4.4 (M17/ September 2021 by RISE). The T4.2 Innovation Canvas created in T4.2 is following:


The innovation
Describe the solution, i.e., the instantiation of the innovation to be considered
Added value proposition
Stakeholders
The solution details
Functional and technical description
Operational description
Road mapping
The resources
Required development resources
Required operating support system
CAPEX & OPEX
The uptake environment
Competition and market
Funding and organization of uptake and industrialization efforts
Barriers

The Innovation Uptake Canvas consists of four main pillars dedicated to the four main topics (1) *the innovation*, (2) *solution details*, (3) *resources*, (4) *uptake environment* which all include three critical elements to consider in the innovation uptake strategy. The subtopics under each of the four main topics are following and their rationale is explained in more details in T4.2 D4.4 (M17/ September 2021):

The innovation

- Description of the solution, i.e., the instantiation of the innovation to be considered*
- Added value proposition
- Stakeholders and domains

Solution details

- Functional description
- Operational description
- Roadmapping

Resources

- Required development resources*
- Required operating support system*
- CAPEX & OPEX*

Uptake environment

- Competition and market*
- Funding and organization of uptake and industrialization efforts*
- Barriers*

Each of the four selected innovations were analyzed in details in T4.2 according to the canvas as described in D4.4. However, in the context of the second Three Lines of Action "**Common requirements as regards innovations that could fill in gaps and needs"** the canvas results "Resources" and "Uptake Environment" and in some parts of "Innovation" (esp. definition) are highlighted in the chapters below.

Public-private information-sharing groups developing collaborative investigations and collective action - Innovation

THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered**

  The **Public-private information-sharing groups developing collaborative investigations and collective action** innovation have been transformed into a solution for a critical infrastructure (near) real-time sharing and ***analysis*** of hybrid and related threat information (a Common

Information Sharing and Analysis Environment, CISAE). Situational awareness is key in detecting hybrid threats and mitigate attacks. The more information available, if analysed correctly, the better the situational awareness. We note that the skills, data and capabilities to detect threats and disrupt attacks often reside within the private sector.

In the presented solution, the CISAE users are practitioners affiliated with relevant public and private organizations in one critical infrastructure sector. Each critical infrastructure domain(/vertical/sector) can/will implement its own CISAE.

SCOPE: Practitioners in public and private organizations

VISION: All Member State critical infrastructure practitioners and organizations (public as well as private ones) can on a voluntary basis and in a controlled manner share and jointly analyse situational information to enhance their situational awareness related to hybrid threats and launch joint mitigation actions.

MISSION: Define and implement a CISAE. Define information sharing needs. Develop and implement required analysis tools.

STRATEGY: Develop critical infrastructure sector specific CISAEs and analysis tools. In The EC Green paper, 11 infrastructure sectors are listed with a total of 29 subsectors. Build on EMSA CISE (or other existing information-sharing solutions). Include relevant CTI in analysis. Information to be shared on a voluntary basis.

LIMITATIONS: The solution has no major limitations compared to the reviewed innovation.

RATIONALE: Security and resilience of critical infrastructure need to be a shared responsibility among multiple stakeholders because neither governmental nor the private sector alone has the knowledge, authority or resources to handle it alone. Public-private partnerships have been considered the foundation for effective critical infrastructure security and resilience strategies, and timely, trusted information sharing among stakeholders is essential for the security of EU critical infrastructures. Stakeholders involved in such a network should be from EU Member States. Access rights should be assigned according to needs, confidentiality/access level and trust relations.

RESOURCES

- **Required development resources**

The development of the information sharing part of a (sector specific) CISAE, building on the EMSA CISE, will in essence be a straightforward engineering activity. Some resources with sector expertise will be needed to define which information to share and the standardization of exchange formats.

The design and development of the intelligent analysis tools will require sector specific expertise as well as expertise in machine learning and AI and would require the set-up of EU research projects supported by the European Commission. It should be an ongoing activity to be able to cope with new threats and attacks. Competition for resources may be an issue in this area.

- **Required operating support system**

  A governance body, possibly a part of the European Reference Network for Critical Infrastructure Protection (ERNCIP) or ENISA, which controls the specifications and oversees the operational procedures of the CISAE, including maintenance, updates and upgrades. It should also provide a forum for the CISAE stakeholders to discuss and share experiences and agree on CISAE improvements and extensions. Furthermore, the governance body should initiate activities and research for development of new analysis tools.

- **CAPEX & OPEX**

  Based on the descriptions of the requirements for development and operational resources it is estimated that the CAPEX for the set-up of the organization and the initial development work would be in the order of 7 – 10 MEURO. The required resources for the research in analysis tools would most likely require 2 to 3 research projects with a budget of 3 - 5 MEURO each.

  Maintenance, updates and upgrades of the specifications of the system would be relatively low effort activities which would require no more than 1 to 2 man-years per year. After the initial research work to develop analysis tools, a budget of 1 MEURO per year seems reasonable.

  The total cost to launch the solution as proposed here with the suggested research activities would then be in the order of 20 – 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be in the order, that is 1 – 2 MEURO, after the CISAE has been developed and the initial launch of the solution.

  The cost estimates above reflect our experiences and knowledge about the development efforts and costs for EMSA CISE.

UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives to increase the security in critical infrastructures, an overview of work in progress presented by the European Commission Migration and Home Affair is well explained in DG HOME website. An existing information sharing network is the Critical Infrastructure Warning Information Network (CIWIN) offering recognised members of the EU’s CIP community the opportunity to exchange and discuss CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity. The CIWIN portal, following its prototype and pilot phases, has been up and running since mid-January 2013. However, it does not cover real-time sharing, and as far as we understand, there is no ongoing initiative with the vision and scope of the solution proposed here.

- **Funding and organization of uptake and industrialization efforts**

  The roadmapping indicates that it needs to be an EU initiative behind the realization and development of the proposed CISAE. The development of a (sector) specific CISAE will probably never take place without such an initiative and allocation of the required funding. However, we note that the EU already has many actions in the area and this would only be a minor add-on to the already ongoing efforts.

- **Barriers**

  Required actions that may become barriers in the work to realize the solution are:

  - To implement the required operational structures as a concrete and institutional and legal framework is missing.
  - To engage the relevant practitioners, end-users and organizations in all Member States and convince them all that this is the right way to proceed. This should in general not be too hard as it already has been decided that protection of the European Critical Infrastructure must be improved and that sharing of threat and attack information for situational awareness and coordinated responses is key.
  - To develop trust both at EU and Member States level in the context of information-sharing. Trust in other parties' security and operational practices may be missing. Regulations and laws have to be reviewed to find the cases when information cannot be shared.
  - To agree on which information to share with whom and how.
  - To organize the funding of the required development and research work.
  - Availability of sector specific competence and machine learning may be scarce.

Debunking of fake news

THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**

  The **Debunking of fake news** innovation has been narrowed down into a solution for near real-time situational awareness regarding disinformation campaigns in the public space by monitoring, sharing and analysis of related domestic as well as foreign activities and events in a CISAE. This excludes topics like media literacy campaigns and issues around use of human fact checkers.

  Situational awareness is key in detecting campaigns and threats and to be able to mitigate attacks. The more information available, if analysed correctly, the better the situational awareness. We note that the skills, data and capabilities to detect and disrupt what is happening on the Internet often reside within the private sector. In the Action Plan against Disinformation, it is stated that "The first hours after disinformation is released, are critical for detecting, analysing and responding to it".

  The CISAE users would be practitioners and relevant public and private users and organizations involved in following and trying to control and mitigate disinformation campaigns.

SCOPE: Authorities, practitioners (in public and private sector)

VISION: Practitioners in all MS will be able to have (near real-time information about ongoing disinformation campaigns increasing general and specific situational awareness.

MISSION: Monitor national and foreign digital media and other domains. Perform joint analysis and deconstruction of disinformation in fully and / or semi-automatic manners. Enable information exchange between Member State organizations from the public and private sector in a CISAE. Trust building.

STRATEGY: Build on EMSA CISE, Debunk.eu, EEAS RAS and similar solutions.

- Deploy information exchange network
- Deploy monitoring tool
- Develop and deploy analysis tools
- Instil measures to build trust

LIMITATIONS: Compared to the original innovation, this solution is limited in that it only considers monitoring, sharing and analysis of disinformation campaigns. It does not integrate identification of disinformation and responses from civilians and / or society in a more broad sense.

RATIONALE: Sharing of information from many sources about activities and events related to or indicating disinformation campaigns will increase the possibilities for immediate or at least very early detection of such campaigns. It will in also make it possible to base individual and / or joint counter actions on a collective situational awareness. Identification, sharing and analysis is a pre-condition to debunking and note that early identification may increase chances for pre-bunking.

RESOURCES

- **Required development resources**

The set-up of the governance body in itself and the work to define the detailed scope of work should not require any major resources.

The development of the information sharing part of the CISAE, building on the EMSA CISE, will in essence be a straightforward engineering activity. Some resources with specific expertise in the disinformation area and threat intelligence will be needed to define which information to share and for the standardization of the corresponding exchange formats.

The development of needed and required fully or semi-automatic analysis tools will require resources for their design and implementation. The monitoring of media will have to rely on available interfaces unless new ones can be agreed and their implementation enforced.

The roadmap proposes several EU funded projects to establish the required knowledge base and the development of the monitoring and analysis tools. The required resources for this part of the work will be researchers with expertise in hybrid threats, disinformation procedures and targets, federated machine learning and AI. We find it reasonable to start two to three three-year 3 MEURO projects for these tasks.

- **Required operating support system**

  A governance body, possibly a part of EEAS Strategic Communications or EDMO, should be established, which controls the specifications, the development and oversees the operational procedures of the CISAE, including maintenance, updates and upgrades. It should organize a forum for the stakeholders to serve as a reference group for the CISAE development and to discuss and share experiences and agree on CISAE improvements and extensions. Furthermore, the governance body should initiate activities and research for development of new analysis tools.

- **CAPEX & OPEX**

  The CAPEX and OPEX estimates in this section follow the same considerations as for the CIP CISAE and it is estimated that the required effort to implement a disinformation CISAE is of the same order:

  - The CAPEX for the set-up of the organization and the initial development work would be in the order of 7 - 10 MEURO.
  - Two to three research projects with a budget of 3 -5 MEURO each.
  - Maintenance, updates and upgrades of the specifications of the system would be relatively low effort activities which would require no more than 1 to 2 man-years per year. After the initial research work to develop analysis tools, a budget of 1 MEURO per year seems reasonable.
  - The total cost to launch the solution as proposed here with the suggested research activities would then be in the order of 20 - 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be in the order, that is 1 – 2 MEURO, after the CISAE has been developed and the initial launch of the solution.

UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives in the field of understanding and deconstructing disinformation. One could first mention the DebunkEu.org project which inspired the proposed solution. Furthermore, EU has launched a number of activities like the EDMO and the EEAS Rapid Alert System (RAS) on disinformation. RAS has as target to provide rapid alerts and enable individual or joint counter actions, but has as far as we understand, not been used for such purposes. Furthermore, the EU Hybrid Fusion Cell mentioned in**Error! Reference source not found.**, the EDMO,the EEAS StratCom task forces, e.g. the East StratCom Task Force and the EUvsDiSiNFO flagship project**Error! Reference source not found.**, all perform analysis and debunking activities. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the proposed solution.

- **Funding and organization of uptake and industrialization efforts**

  The roadmap points at that it must be an EU initiative behind the realization and development of the proposed solution. This solution would most likely never happen without such an initiative and the required corresponding funding. In particular, we note that the EU already has a number of activities in the area of handling and understanding disinformation and that the proposal just would be a relatively small extension of the already ongoing activities.

- **Barriers**

  Required actions that may become barriers in the work to realize the solution are:

  - To engage the relevant practitioners, end-users and organizations in all Member States and convince them all that this is the right way to proceed. This should in general not be too hard as it already has been decided that the awareness and handling of disinformation campaigns must be improved. However, as has been shown in a special report on disinformation **Error! Reference source not found.**, the activity level varies greatly between Member States.
  - To develop trust both at EU and Member States level in the context of information-sharing about disinformation campaigns. This will be especially so, if also Member State internal disinformation campaigns are in scope. Then trust in other parties' security and operational practices may be missing.
  - To agree on which information to share with whom and how.
  - To organize the funding of the required development and research work.
  - Availability if sector specific competence and in machine learning may be scarce.

Guides to identify fake news

THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered**

  The **Training application for media literacy** innovation has been transformed into a solution which in one way is more generic but in another sense is narrower, as its target audience is smaller. The solutions are concerned with the required foundations for bringing media literacy competence to students. This to increase their and the society's resilience against disinformation campaigns.

  SCOPE: Students, 9 -12 graders.

  VISION: Young people in EU MS are inoculated against misinformation and fake news.

  MISSION: Get media literacy education and training into all 9 -12 graders' curricula in the EU.

STRATEGY: Develop easy to follow frameworks, methods and tools for creation of media literacy course material. Develop engaging gaming models for important course components.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern direct development of course material and/or training apps.

RATIONALE: Media literacy is a wide area and concerns many aspects, but at the core it is about having the competence to control one's own interpretation of presented media and not uncritically accept any overt message. Media literacy refers to skills, knowledge and understanding that allow citizens to use media effectively and safely and equip them with the critical thinking skills needed to exercise judgment, analyse complex realities and distinguish between opinion and fact. However, the way to express ideas and information varies between cultures, languages and communities, so to reach all citizens with media literacy training it is necessary to have trainings adapted for the respective audiences. Furthermore, it is important to have multiple providers of media literacy training programs to exclude claims that the training is a centralized program for indoctrination about correct opinions and thinking. Thus, we propose to build a profound basis for the production of media literacy training programs on which involved companies and organizations can base their developments.

RESOURCES

- **Required development resources**

  The roadmap proposes one or more EU finance projects to establish the required knowledge base and to develop the framework, tools and training app skeletons. The required development resources for this part of the work will be researchers in media literacy and app/game developers. We find it reasonable to start two three-year 3 MEURO projects for these tasks. This estimate takes into account the possibilities to cooperate with EDMO and the just launched setup of the eight EDMO local nodes (cost 11 MEURO). Coordination of research activities should of course be encouraged/enforced.

  The set-up of the governance body and to define the detailed, evidence based, research program for media literacy following the proposed solution should not require any major resources. The work with local adaptations will require involvement of local media literacy experts and admin personnel. It is hard to estimate the total efforts required before knowing what the framework, tools and apps will look like. But each adaptation task will most likely require efforts in the order of man-years.

- **Required operating support system**

  The governance body should ensure that a body is assigned which is responsible for required updates and upgrades of the solution to have it keep up with threat developments and to provide expected performance. This task would require close cooperation between central and local media literacy experts and possibly companies involved in developing the teaching material and the training apps. It is hard to estimate the total efforts required before knowing what the framework, tools, apps and local adaptations will look like. But the update and upgrade work will most likely only require efforts in the order of man-years.

- **CAPEX & OPEX**

  Based on the descriptions of the requirements for development and operational resources we estimate that the CAPEX for the set-up of the organization and the initial research work would be in the order of 6 – 8 MEURO.

  The initial local adaptations would, if they require 1 - 3 man years per Member State and end up to about in the same order.

  The total cost to launch such a comprehensive action as proposed here would then be in the order of 10 – 15 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be of the same order, that is 2 – 3 MEURO per year but financed by each Member State.

UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives in the field of media literacy and there are tools and educational material available. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the proposed solution.

  Examples on ongoing initiatives in the area are:

  - The EU Media literacy expert group (MLEG).
  - The Center for media literacy.
  - A course developed by the Erasmus+ project Crescent in which KEMEA is active. The course is on Strategic Communication to Counter Security Threats in the Disinformation Era.
  - A web page with the best apps for teaching media literacy**Error! Reference source not found.**.
  - The CommonSenseEducation web page with parental guidance on media literacy training.
  - The International Society for Technology in Education (ISTE) web page presenting 10 resources to boost student media literacy**Error! Reference source not found.**.
  - ERASMUS Student Network (ESN) has launched a training program on media literacy**Error! Reference source not found.**.
  - YLE (Finnish broadcasting company) troll factory training app

- **Funding and organization of uptake and industrialization efforts**

  The roadmap points that it must be an EU initiative behind the realization and development of the proposed framework, tools and app skeletons and the required local adaptations. This would most likely never take place without that initiative and the required corresponding funding. In particular, we note that the EU already has expressed interest and has tried to initiate work as Member States are asked to rapidly implement the media literacy provisions of the Audio-Visual Media Services Directive.

- **Barriers**

  Required actions that may become barriers in the work to realize the solution are:

  - To convince the EU that this is the right way to proceed. This should in general not be a barrier as it already has been decided that media literacy is an essential competence for EU citizens.
  - To engage the MSs in the work and get them involved. As has been shown in the special report on Disinformation, the activity level varies greatly between Member States.
  - To organize the funding of the research activities and the related local adaptations.

Training application for media literacy

THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**

  The **Guides to identify fakes** innovation has been transformed into a solution for bringing competence to Member State citizens on how they can detect that media is "fake", i.e., digitally generated or that images, video and audio have been altered. The main objective is to increase citizens' and thereby society's resilience against disinformation.

SCOPE: Member State citizens.

VISION: EU Member State citizens know about and are proficient users of tools to detect digitally generated or altered images, video and audio.

MISSION: Publish and distribute guides on how to identify "fakes" and the use of available tools Promote integration of detection tools in media consumption apps. Promote use of reputation systems regarding tools and media sources. Promote development of a multitude of different tools.

STRATEGY: Produce a registry of existing and upcoming methods and tools for identifying "fakes". Review which media channels to use with respect to their effectiveness in reaching different user groups depending on culture, language and media environment. Develop appropriate guides and promotion material for the different channels and user groups. Define and standardize interfaces of detection tools. Propose voluntary and regulatory measures to ensure integration of detection tools in media consumption apps.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern the development of detection tools or apps, only promotion of their use.

RATIONALE: Being able to detect "fake" media in the form of digitally generated or altered images, video and audio is a first basic step in learning how to reveal and counter disinformation. By making all EU citizens aware of the available tools and methods for detection, it will be much harder for different actors to launch successful disinformation campaigns. Furthermore, it is important to have multiple providers of methods and tools to exclude claims that their use is part of a centralized program for enforcing politically correct opinions and thinking. Integration of tools in media consumption apps should be according to a concept of add-ons so that users can choose a solution which they trust.

RESOURCES

- **Required development resources**

  The set-up of the governance body and the work to define the final scope of work should not require any major resources, especially if this task can be assigned to an already existing organization like EDMO**Error! Reference source not found.**. The inventory work and the production of guides should be handled by national/local organizations and would also constitute a relatively small task.

  It is hard to estimate the total efforts required to develop locally and group specific promotion material before knowing what the recommendations by market experts /local organizations will be.

  The standardisation of media formats and interfaces should be left to the media app companies. The reputation system should preferably be integrated in already existing solutions.

- **Required operating support system**

  The governance body should ensure that there is a responsible organization for required updates and upgrades of the database and its content. The set-up of regular review meetings must also be supported.

  Test and rating of the detection tools will require some resources. Required resource will likely decrease over time as testing will be most needed when the system is launched,

- **CAPEX & OPEX**

  Based on the descriptions of the requirements for development and operational resources we estimate that the CAPEX for the set-up of the organization and the initial work would be in the order of 1 – 2 MEURO.

  Operating expenses are expected to be 0,5 – 1 MEURO per year

UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives to develop tools and guides to identify fakes. However, this solution does not compete with those as this is an effort to improve citizens competence in using these tools. As far as we understand, there is no ongoing initiative with the vision and scope of the proposed solution.

  Some examples for already existing guides/web tools are:

  - FotoForensics for the analysis of images.
  - Amnesty International's Citizens Evidence Lab**Error! Reference source not found.**, which offers several guides on digital verification.

  Most existing guides provided by governmental organizations do not include recommendation of tools as can be seen in the following guides:

  - How to spot, avoid, and report fake check scams, by the US Federal Trade Commission Consumer Information.
  - The SHAREChecklist by the British HM Government
  - Wie Sie Falschmeldungen erkennen, by the German Bundesregierung.

- **Funding and organization of uptake and industrialization efforts**

  The roadmap points out that it must be an EU initiative to support the actions described in the roadmap and implement the solution. This work would most likely never take place without such an EU funded initiative.

- **Barriers**

  Required actions that may become barriers in the work to realize the solution are:

  - To convince the EU that this is the right way to proceed. This should in general not be a barrier as it already has been decided that media literacy is an essential competence for EU citizens.
  - To engage the Member States in the work and get them involved. As has been shown in the special report on Disinformation**Error! Reference source not found.**. The activity level varies greatly between Member States.
  - To get media app providers interested in integrating the checking tools interfaces and allow such add-ons.

According to T4.2 D4.4 findings presented above the focus in the most relevant innovations that EU-HYBNET sees to fill in identified pan-European gaps and needs to counter hybrid threats, lies on the areas of increasing resilience in critical infrastructures and building resilience against disinformation campaigns. Furthermore, it is seen in D4.4 that following important actions or requirements needs to be considered in order to provide an answer to the identified gaps and needs.

First of all, in both areas (critical infrastructure protection and disinformation) there is seen a need for *improving (near) real-time situational awareness to enable timely responses and mitigating actions*. To be effective, such responses and actions *require cooperation between different stakeholders*; stakeholders in one or different member states, stakeholders in the public and private sectors and that the stakeholders have a common view of the situation at hand. Moreover, **new fully or semi-automatic analysis tools** will be required to *cope with the increasing amount of information* that has to be monitored, scanned and analysed for suspicious activities and/or attacks. As sharing of information may be sensitive, **federated machine learning may be one avenue to implement efficient analysis tools without compromising required secrecy of monitored data and events**.

In addition, in the area of disinformation, there is a *crucial need to increase media literacy in the population* in order to enhance society's resilience against disinformation. Part of media literacy *is to learn how to detect and use tools to detect that digital media has been manipulated*. Another more generic media literacy skill is to *learn about drivers behind disinformation campaigns* and *how they are instigated and spread*. An important condition is that the **media literacy and guide to identify fakes innovations need to work in tandem to be fully effective**, as they (potentially) target different parts of the population that, in turn, affect each other (i.e., students impacting families and vice versa). As well, it is important to **see the role and influence of civilians/citizens as a stakeholder in many of these innovations** (including "Debunking fake news", for example) **even if they are not the primary actors implementing the innovation**. In short, a key recommendation and requirement is that both technological and non-technological (human science based, social) features are imbedded to the solution/innovation development and its' use, and only then the innovation may deliver coherent and requested support to identified gaps and needs to counter hybrid threats especially in the field of disinformation.

3.2.3 EU-HYBNET T2.1 NEEDS AND GAPS ANALYSIS IN KNOWLEDGE AND PERFORMANCE

During reporting period of D1.4 also the project 2nd working cycle has started (project months 18 – 34/ October 2021 – February 2022) and each of the project cycle (1st cycle M1-M17, 2nd cycle M18 – M34, 3rd cycle M35 – M51, 4th cycle M52 – M60) starts with EU-HYBNET gaps and needs event where most critical, present pan-European gaps and needs to counter hybrid threats are identified. Therefore, in this report it is also possible to share the views of the second round of results of identified gaps and needs that partly indicates forthcoming actions that will take place in EU-HYBNET in order to deliver results to the Second Three Lines of Action "**Common requirements as regards innovations that could fill in gaps and needs**".

The 2nd cycle Gaps and Needs of pan-European practitioners and other relevant actors (industry, SMEs, academia, NGOs) event took place on 7th and on 28th-29th September. The event arrangements, used methodology and event preliminary findings are described in detail in D2.5 (M18/ October 2021 by Hybrid CoE; consortium only (CO) deliverable). However, more detailed analysis of the most critical gaps and needs that EU-HYBNET will focus on during the second cycle will be reported in EU-HYBNET deliverables D2.6 "Long list of defined gaps and needs" (M19/ November 2021, by Hybrid CoE, CO deliverable) and D2.10 "Deeper analysis, delivery of short list of gaps and needs" (M22/ February 2022, by JRC, CO deliverable). Still, some general features on identified gaps and needs for the future innovation mapping and analysis work at EU-HYBNET can already be mentioned.

Critical gaps were still seen to exist in the information domain, especially because the activities in this domain are strongly linked with other hybrid threats domains and hence may easily cause critical cascading effects.

Also the critical needs were noticed in the information domain, especially the need for education and increase of awareness of citizens and practitioners on measures to identify disinformation. Furthermore, the communication between different levels and actors in society, especially between practitioners and industry and business actors should be enhanced in order to have large scale situational awareness of hybrid attacks and influencing. Next to the disinformation domain, also space and economical and infrastructure domains are identified to phase critical needs to have solutions to counter hybrid threats.

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

In EU-HYBNET the main tasks which contribute to the third of the Three Lines of Action "**Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation**" are 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). However, also discussion in WP1 "*Coordination and Project Management*" in T1.1 "*Administrative and Financial Planning and Coordination*" (lead by Laurea) to DG HOME's request to provide input to ISF forthcoming funding instrument topics deliver input to the issue. 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 on standards development or standards creation. Therefore, T4.3 has solved the key existing features, including EU policies that support recommending the identified, most promising EU-HYBNET areas and innovations for standardization.

On the basis of T3.1s' 27 most promising innovations identified and T2.2 D2.9 "Deeper analysis, delivery of short list of gaps and needs", T4.3 has conducted research and 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. Still, some additional and more detailed focus areas have been raised into analysis because they are seen to highlight present needs to prioritize knowledge and performance in standardization. The six *focus areas* in prioritizing knowledge and performance that require standardization are:

1. Big data
2. Critical Goods and Commodities
3. Cyber Security
4. Fake News and Disinformation
5. Resilient civilians
6. Strategic Communication

Next to the focus areas, T4.3 has started research for deeper analysis on standardization environment and needs. The template includes four themes where collected research information is analyzed in seven sub-fields (i-vii). The four research themes are (1) definition of regulation; (2) new business models; (3) new categorizing technologies, (4) information protection. The use of this approach is described below in the context of "Big Data" case study:

Theme 1. "Defining a set of regulation for using *big data* in political campaigning"

i. Relevant document initiative,
ii. Description,
iii. Links,
iv. State of Pay,
v. Recommendation: Legal/ Standardization,
vi. Explanation on recommendation,
vii. Relevant Institutions

Theme2. "To consider new business models for data aggregation where the individual is the owner and trader of his data"

i-vii sub-fields to analyze

Theme3. "New Categorizing Technologies"

i-vii sub-fields to analyze

Theme4. "Are personal information protection regulation up to date in the EU"

i-vii sub-fields to analyze

The research of the seven knowledge, performance and innovation area context is conducted according to the four research themes and seven sub-fields, of which the final results of the research will be reported in D4.8 "1st Report for standardisation recommendations" M19 (November 2021). However, T4.3 has already recognized the importance of connecting the recommendations for standardization to the existing and the latest EU policies. The focus is to ensure that the knowledge, performance and innovation areas prioritized and recommended for standardization in the context of hybrid threats, has acknowledged the existing EU policies. Therefore, EU policies will support measures to proceed in standardization priority recommendations to increase knowledge and performance to counter hybrid threats.

The preliminary results from T4.3 and D4.8 under each of the six main focus areas are explained in the subchapter below and in the context prioritized topics of Increasing Knowledge and performance Requiring Standardization. The "topic" identified to standardization is highlighted in ***italics and bold*** and the "measure" linked to the standardization highlighted in **bold**

1. Big data

- Defining a **set of regulation for using big data** in ***political campaigning***
- To consider **new business models for data aggregation** where the ***individual is the owner and trader of his data***
- **Formation of a unified or all-encompassing strategy** on ***new categorising technologies***
- **Updates** to ***personal information protection*** **regulations** in the EU
- **Ethical standards** to the ***use of big data*** and use of material collected and analysed

2. Critical Goods and Commodities

- **Monitoring** of the ***influence of the national FDI in the sector of critical goods and services***
- **Public-private partnerships as a way of securing** the provision of ***strategic stocks and supplies***
- **Definitions and best practices** based on ***data aggregates as a critical commodity***

3. Cyber Security

- **Unified cyber strategy** for ***technological development*** taking place in the field ***of cyber and future technologies***
- EU **vision and approach** to reach coherent ***cyber security measures*** in the context of rapidly developing ***technological environment***
- EU **vision and approach** on interoperability across platforms in the context of ***Hyper-connectivity***
- **Standards** to ***quantum computing*** engaging in a **symbiotic relationship** with classical and legacy systems
- **Standards** to ***deepfakes*** in the ***context of 'synthetic media'***

4. Fake News and Disinformation

- **Support** to ***media pluralism***
- **Standards** for ***good journalism***
- **Countering** the ***mass of fake news***
- **Increasing awareness** of ***fact checkers and their findings*** pan-European wide in EU MSs by citizens, media actors and governments

5. Resilient civilians

- **Increasing** ***media literacy***
- **increasing** ***societal resilience against fake news***
- **Increasing knowledge of competences and measure** at a local level to counter ***disinformation***
- Providing **assistance** to ***marginalized parts of society***

6. Strategic Communication

- **Reinventing** the **practice** of ***public outreach***
- **Standards** of ***communication between national governments and local authorities***
- **Establishing** official and well-known ***communication platforms***
- Preparing simplified **blueprints** of ***political communication with the general public***

With reference to the preliminary results from T4.3 D4.8 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. However, because the T4.3 has conducted very profound EU strategy and regulation analysis on its six (6) thematic areas, together with the EU-HYBNET coordinator/ Laurea, T4.3/ PPHS have decided to share the reports to EC policy actors. After all, in each of the six thematic area reports, specific recommendations were developed for actions to be taken at the level of the European Union and Member States (EU MS). Furthermore, the purpose of developing the recommendation is to indicate particularly important aspects in each of the topics, which will be affected by the reports. Moreover, each recommendation was addressed to one or more of the institutions operating at the EU and EU MS level. The selection of institutions to which the recommendations are addressed was made using two basic criteria

- The first criterion is the substantive area to which the recommendation relates. In this case, it was necessary to identify in T4.3 the content related area of the institution's operation, so as to match the recommendation to the area of the institution's activities. Furthermore, it was important to identify the addressee of the recommendation as concretely and precisely as possible. Hence, within the framework of large institutions such as the European Commission or the European Parliament, the idea behind was to identify a particular unit or committee, so that the reports reach people who deal with a given topic on a daily basis. This approach was aimed at avoiding a situation in which reports would be sent to people dealing with other meteoric areas or sent to general addresses, from where it would have to be redirected to the persons responsible for the substance.
- The second criterion taken into account in the process of identifying groups of recipients of substantive reports was the criterion of diversity of entities. It was seen important in T4.3 that the reports reached the institutions from different sectors. First of all, to representatives of public authorities, both legislative and executive powers. However, T4.3 also wanted to reach out to the entities of the broadly understood civil society, opinion leaders and all kinds of expert bodies, networks and representations of the sectorial interests. In short, the purpose of such addressing the recommendation was to contribute to the discussion on the substantive issues tackled in the reports in the public debate. At the same time, it was wanted to reach out to experts and representatives of various lobbies and groups of interests. Apart of this, by submitting the reports, T4.3 wanted to define entities from different sectors that could be interested in the EU-Hybnet project, as well as be interested in joining as affiliates of the project.

As mentioned T4.3 six different thematic reports have been sent to the identified EU and EU MS institutions by EU-HYBNET coordinator/ Laurea and T4.3 leader/ PPHS. Both institutions will monitor feedback from institutions that have received reports with recommendations. Feedback will be consulted among the partners of Task 4.3 and its content will be taken into account, as far as possible, in further project work.

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

Because in Task (T) 4.2 most promising innovations analyzed were related in many cases 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 and to see, if there is a possibility to proceed in the innovation uptake and recommendation process with the named innovations and 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)
- 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. 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 p**riority as regards of increasing knowledge and performance requiring standardization**. Therefore, EU-HYBNET will 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.

3.3.3 EU-HYBNET T1.1 ADMINISTRATIVE AND FINANCIAL PLANNING AND COORDINATION

EU-HYBNET was requested to deliver comments from the project's and hybrid threats perspective to the Workshop on "*Synergies between EU security research and innovation and the Internal Security Fund (ISF) and the Border Management and Visa Policy (BMVI)*" arranged by DG HOME on 14th of October. Therefore, T1.1 "*Administrative and Financial Planning and Coordination*" arranged an internal EU-HYBNET meeting before the DG HOME workshop so that all consortium partners could share their views to the ISF workshop and especially from the point of view of **priorities as regards of increasing knowledge and performance requiring standardization**. As a result of the discussion EU-HYBNET addresses the following issues as key elements to enhance European response to hybrid threats.

First of all, there is a clear need to raise general awareness and identification of hybrid threats in each European security practitioner domains (police, border and coast guard, intelligence, civil protection) in order to realize the hybrid threats in their domain. This supports the capability development and also understanding of technological and non-technological innovations needed to counter hybrid threats in each of the domain. Without raising awareness and understanding and mapping of target areas where innovations are needed, European security practitioners' capability development cannot take place. Second, in the context of hybrid threats, non-technological innovations (e.g SoPs, training, media literacy skills etc) are seen as very important for the capability development and hence funding for them should not be overlooked. Of course, many times technological and non-technological innovations do meet each other and hence they can be developed simultaneously. Still the emphasis on non-technological innovations in the case of hybrid threats should not be overlooked. Lastly, non-technological innovations procurement and uptake does not have the straight forward proceeding format or funding opportunities in EU as in the case of technical innovations, and hence this leaves rooms for adversaries to benefit on this weakness in Europe, and the soft skills needed to counter hybrid threats will not face the required development activities.

The above mentioned comments were shared in the DG HOME workshop and they were also delivered to DG HOME policy officers Mr. Giannis Skiadaresis and David Rios-Morentin via email and after an tri-lateral telco on the EU-HYBNET innovation findings. This all is to support EU-HYBNET contribution to

priorities as regards of increasing knowledge and performance requiring standardization in the context of hybrid threats and pan-European response to hybrid attacks.

4. CONCLUSION

4.1 SUMMARY

In the chapter above it is described how the EU-HYBNET project activities from the third six project months (May - October 2021) contributed to the Three Lines of Action. In addition, chapters have described how the work in the Tasks has been finalized during the 1st project cycle and will also continue or contribute to the 2nd project cycle. Furthemore, 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 first project cycle (M1-M17/ May 2020 – September 2021) have been now explained in this alike previous two "Six Month Action Reports" deliverables (D1.2, D1.3) to the EC. However, in this document, D1.4, also first findings from the second project cycle (M18-M34) to the Three Lines of Actions have been able to describe in some, though very limited one month period, level. Therefore, the next Six Month Action Report (in April 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 nine (9) deliverables and two (3) milestones will be delivered:

Deliverables (D):

Task (T) 4.4 Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge

- ➢ Deliverable (D) 4.12 “1st Policy Briefs, Positions Papers, Recommendations report” (Hybrid CoE), project month (M) 19

T4.3 Recommendations for Standardization

- ➢ D4.8 “1st Report for standardisation recommendations” (PPHS), M13

T2.1 Needs and Gaps Analysis in Knowledge and Performance

- ➢ D2.6 “Long list of defined gaps and needs” (Hybrid CoE), M19

T2.2 Research to Support Increase of Knowledge and Performance

- ➢ D2.10 “Deeper analysis, delivery of short list of gaps and needs” (JRC), M22
- ➢ D2.13 “Articles and publications on themes and measures” (UiT), M24

T1.3 EU-HYBNET Community Extension

- ➢ D1.20 “List of actors to the extended EU-HYBNET Network” (Hybrid CoE), M23

T3.3 Ongoing Research Projects Initiatives Watch

- ➢ D3.8 “First mid-term report innovation and research monitoring” (L3CE) M24

T3.2 Technology and Innovations Watch

- ➢ D3.4 “First mid-term report Improvement and innovations” (Satways) M24

T1.1 Administrative and Financial Planning and Coordination

- ➢ D1.5 “4th Six Month action Report” (Laurea), M24

Milestones (MS):

- MS26/ 1st Policy Briefs, Positions Papers or Recommendation Document are published, Project Month (M) 19 (November 2021)
- MS6/ 2nd EU-HYBNET Project Management Board Meeting, M24 (April 2022)
- MS35/ 2nd Annual Workshop, M24 (April 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, some new openings in the project results sharing will be taken into use, and one of those is the T4.3 activity to share thematic results reports to the identified EU and EU MS institutions and to monitor their feedback from the received reports with recommendations. It is obvious that the possible feedback will be consulted among the partners and its content will be taken into account, as far as possible, in further project work.

Furthermore, in the next reporting period more policy briefs and position papers are expected to be published from the key EU-HYBNET findings, and at the moment two policy briefs are under preparations – one is from T3.1 “Definition of Target Areas for Improvements and Innovations” and another from T4.2 “Strategy for Innovation uptake and industrialization”. In both of the policy brief cases, the goal is to describe the results to EU Policy actors in order to enhance the implementation of the EU-HYBNET findings, especially in the context of Three Lines of Actions.

In addition EU-HYBNET excellent feedback and experience to arrange additional project events/ telcos where to share key findings and results to pan-European stakeholders, like it was done 4/10 “Innovations to Hybrid Threats” event case, will be continued. Naturally, the key findings will also be part of official and planned EU-HYBNET project events such as Annual Workshop and Future Trends Workshop in April 2022.

Lastly, EU-HYBNET will continue to share the key findings with DG HOME and other relevant DGs via emails and of course contribute to the DG HOME INFRA CERIS workshops by sharing the key findings to enhance the 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 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
RI	Research and innovations
EU MS	European Union Member State
EUROPOL	The European Union Agency for Law Enforcement Cooperation
DG HOME	EC Directorate General for Migration and Home Affairs
CERT-EU	Computer Emergency Response Team
QKD	Open European Quantum Key Distribution Testbed
CONCORDIA	Cyber Security Competence Network for Research and Innovation –project
INFRASTRESS	Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system –project
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
EU-Circle	A pan-European Framework for Strengthening Critical Infrastructure Resilience to Climate Change –project
SATIE	Security of Air Transport Infrastructure in Europe –project

CISE	Common Information Sharing Environment –innovation, deriving from EUCISE2020 project
EUCISE2020	European Union Common Information Sharing Environment 2020 -project
CISAE	Common Information Sharing and Analysis Environment. Similar innovation as CISE while focusing to other domain than maritime CISE.
EMSA	European Maritime Security Agency
ENISA	European Union Agency for Cyber Security
EDMO	European digital Media Observatory
EEAS	European External Action Service
RAS	Rapid Alert System in EEAS
CTI	Computer Technology Integration
CIRP	Critical Infrastructure Resilience Platform
CIP	Competiveness and Innovation Framework Program
IoS	Internetwork Operating System
B2C	Business to Consumer
B2B	Business to Business
Git, Github	Git is a version control system. When developers create something (an app, for example), they make constant changes to the code, releasing new versions up to and after the first official (non-beta) release.
ERNCIP	European Reference Network for Critical Infrastructure Protection
CAPEX	Capital expenditures
OPEX	Operating Expenses
CIWIN	Critical Infrastructure Warning Information Network
ISTE	The International Society for Technology in Education
ERASMUS	EuRopean Community Action Scheme for the Mobility of University Students
YLE	Finnish broadcasting company
MLEG	EU Media literacy expert group
ISF	Security Fund, EC
BMVI	Border Management and Visa Policy (BMVI), part of EC ISF funding instrument
ESDC	European Security and Defence College
SoP	Standard Operating Procedure
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	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

.

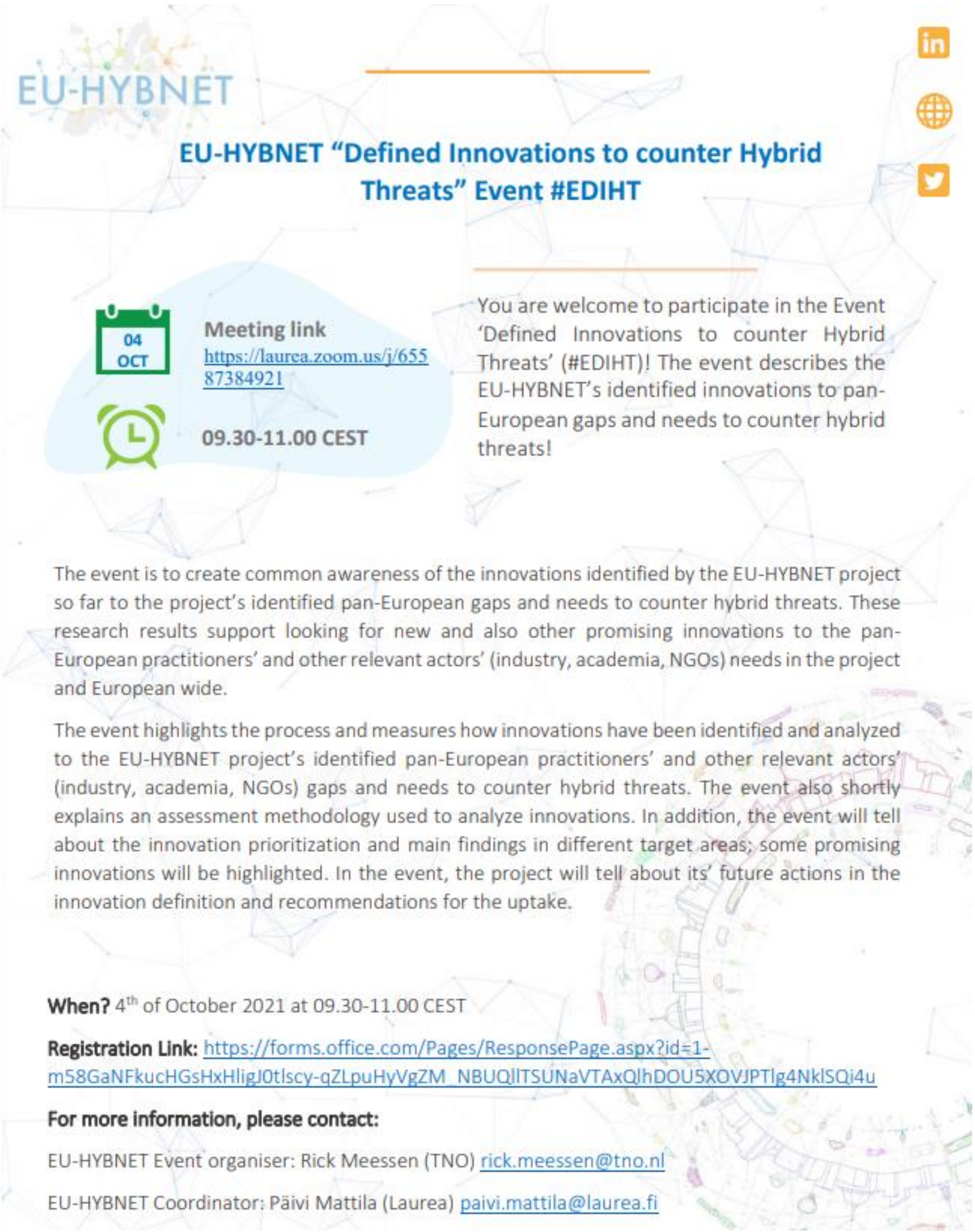
ANNEX II. REFERENCES

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

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

ANNEX III. EU-HYBNET INNOVATIONS TO HYBRID THREATS -EVENT PROGRAM

.



EU-HYBNET

EU-HYBNET "Defined Innovations to counter Hybrid Threats" Event #EDIHT

04 OCT

Meeting link
https://laurea.zoom.us/j/65587384921

09.30-11.00 CEST

You are welcome to participate in the Event 'Defined Innovations to counter Hybrid Threats' (#EDIHT)! The event describes the EU-HYBNET's identified innovations to pan-European gaps and needs to counter hybrid threats!

The event is to create common awareness of the innovations identified by the EU-HYBNET project so far to the project's identified pan-European gaps and needs to counter hybrid threats. These research results support looking for new and also other promising innovations to the pan-European practitioners' and other relevant actors' (industry, academia, NGOs) needs in the project and European wide.

The event highlights the process and measures how innovations have been identified and analyzed to the EU-HYBNET project's identified pan-European practitioners' and other relevant actors' (industry, academia, NGOs) gaps and needs to counter hybrid threats. The event also shortly explains an assessment methodology used to analyze innovations. In addition, the event will tell about the innovation prioritization and main findings in different target areas; some promising innovations will be highlighted. In the event, the project will tell about its' future actions in the innovation definition and recommendations for the uptake.

When? 4th of October 2021 at 09.30-11.00 CEST

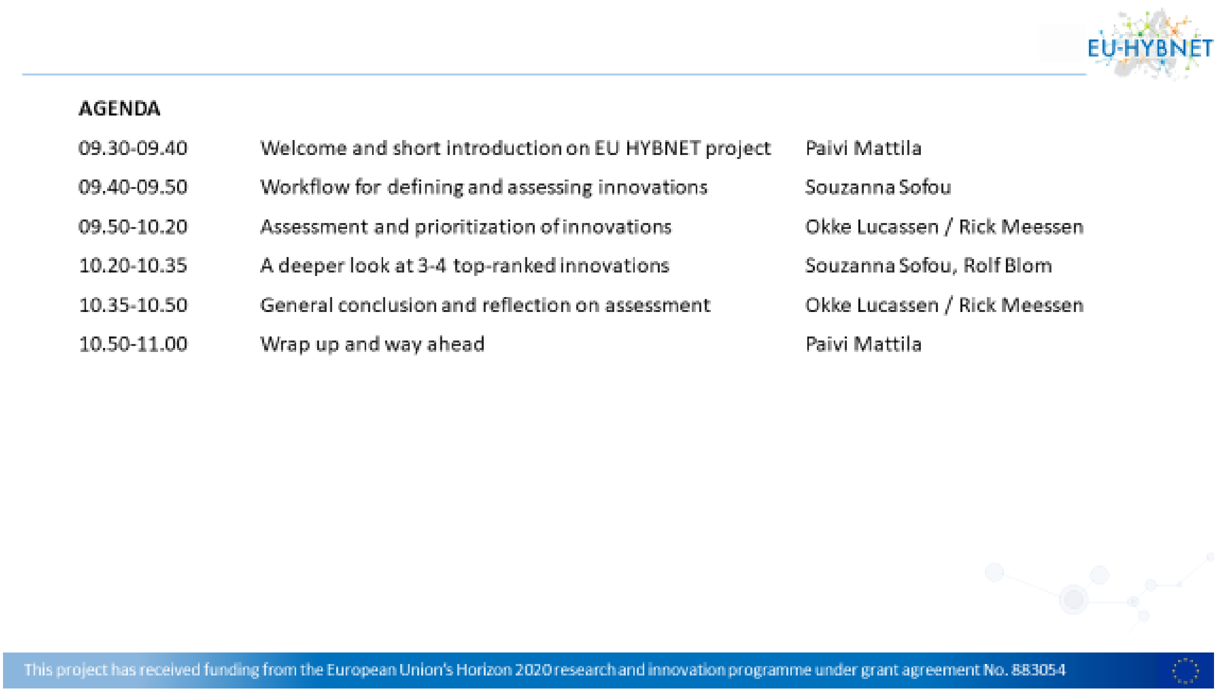
Registration Link: https://forms.office.com/Pages/ResponsePage.aspx?id=1-m58GaNFkucHGsHxHligJ0tlscy-qZLpuHyVgZM_NBUQlITSUNaVTAxQlhDOU5XOVJPTlg4NklSQi4u

For more information, please contact:

EU-HYBNET Event organiser: Rick Meessen (TNO) rick.meessen@tno.nl

EU-HYBNET Coordinator: Päivi Mattila (Laurea) paivi.mattila@laurea.fi

.



AGENDA

09.30-09.40	Welcome and short introduction on EU HYBNET project	Paivi Mattila
09.40-09.50	Workflow for defining and assessing innovations	Souzanna Sofou
09.50-10.20	Assessment and prioritization of innovations	Okke Lucassen / Rick Meessen
10.20-10.35	A deeper look at 3-4 top-ranked innovations	Souzanna Sofou, Rolf Blom
10.35-10.50	General conclusion and reflection on assessment	Okke Lucassen / Rick Meessen
10.50-11.00	Wrap up and way ahead	Paivi Mattila

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054