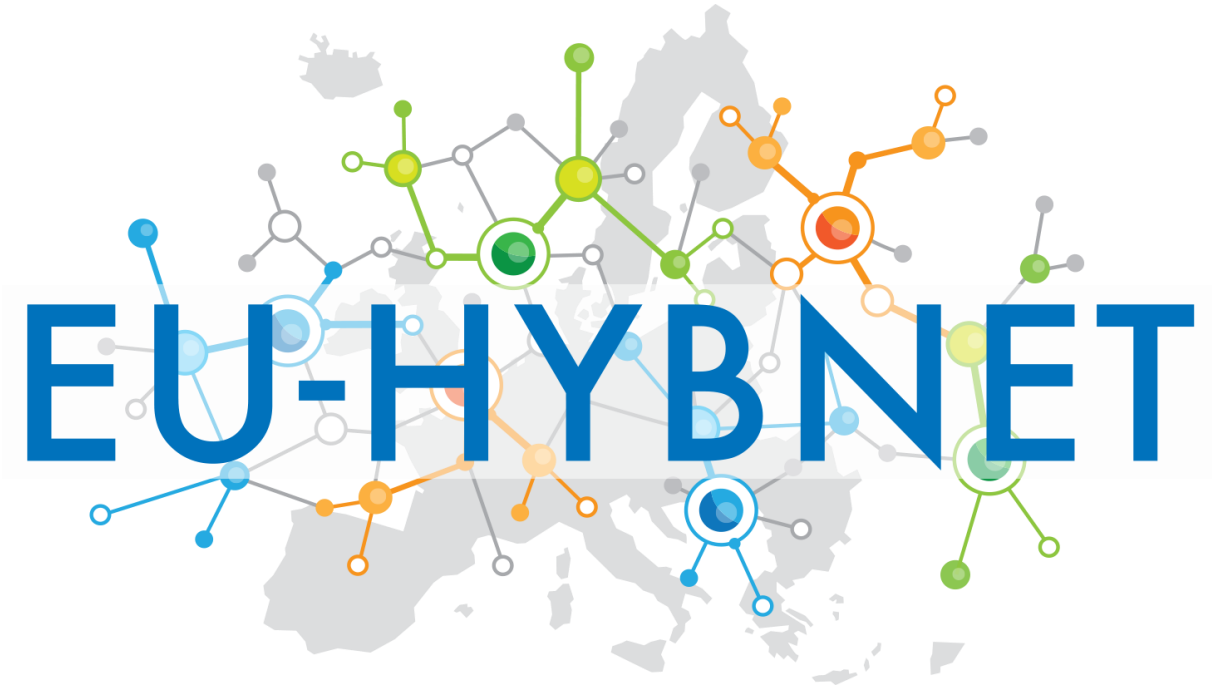


SIXTH SIX MONTH ACTION REPORT

DELIVERABLE 1.9

Lead Author: Laurea

Contributors: All partners
Deliverable classification: Public (PU)

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

D1.9 SIXTH SIX MONTH ACTION REPORT

Deliverable number:	**1.9**	
Version:	**1.0**	
Delivery date:	**28/07/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	Päivi Mattila, Tiina Haapanen	**Laurea**
Contributors:	Rachele Brancaleoni Rolf Blom	**UCSC** **RISE**
	Input to the report from all consortium partners due to their project work in various Tasks and events as contributors	**MTES, URJC, Hybrid CoE, PPHS, UiT, KEMEA, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, Maldita, Espoo, COMTESSA, ZITiS, L3CE**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	26/04/2023	Tiina Haapanen/ Laurea	1st draft
0.2	05/05/2023	Tiina Haapanen/ Laurea	Content delivery
0.3	11/05/2032	Tiina Haapanen/ Laurea	Content delivery
0.4	05/06/2023	Päivi Mattila/ Laurea	Content delivery
0.5	15/06/2023	Päivi Mattila/ Laurea	Content delivery
0.6	10/07/2023	Päivi Mattila/ Laurea	Content delivery
0.7	21/07/2023	Rolf Blom/RISE	Review
0.8	27/07/2023	Rachele Brancaleoni/ UCSC	Review
0.9	28/07/2023	Päivi Mattila/ Laurea	Final editing, text ready
1.0	28/07/2023	Päivi Mattila/ Laurea	Document to be submitted for the EC

DISCLAIMER

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

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

© Copyright in this document remains vested in the Project Partners

TABLE OF CONTENT

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) 1.9 "*Sixth Six Month Action Report*" in project month (M) 36/April 2023 is to describe how the project has proceeded from M31 until end of M36 of the project (November 2022 – April 2023) according to the European Commission (EC) defined, *"three lines of action*" which are mandatory to report according to the Horizon2020 Secure Societies Programme/General Matters-01-2019 funded projects. The *"three lines of action*", also mentioned in the EU-HYBNET Description of Action (DoA) are:

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

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

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

Furthermore, D1.9 also highlights what actions and results are expected from EU-HYBNET during the next six-month period (May 2023- October 2023).

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 D1.9 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 31-36 (Nov 2022 – Apr 2023) have contributed to the EC's requested "three lines of action" activities.
- Section 4. Conclusion and next steps for the upcoming six-month period of the project (May-October 2023).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.9 "*Sixth 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 D1.9, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.9 is to provide a general update on how the project reaches the results mentioned in the project objectives and KPIs. We have highlighted this in the figure below, showing the role of WP1 to support and guide project WPs 2-4 where the main project activities take place and the core project results are achieved.

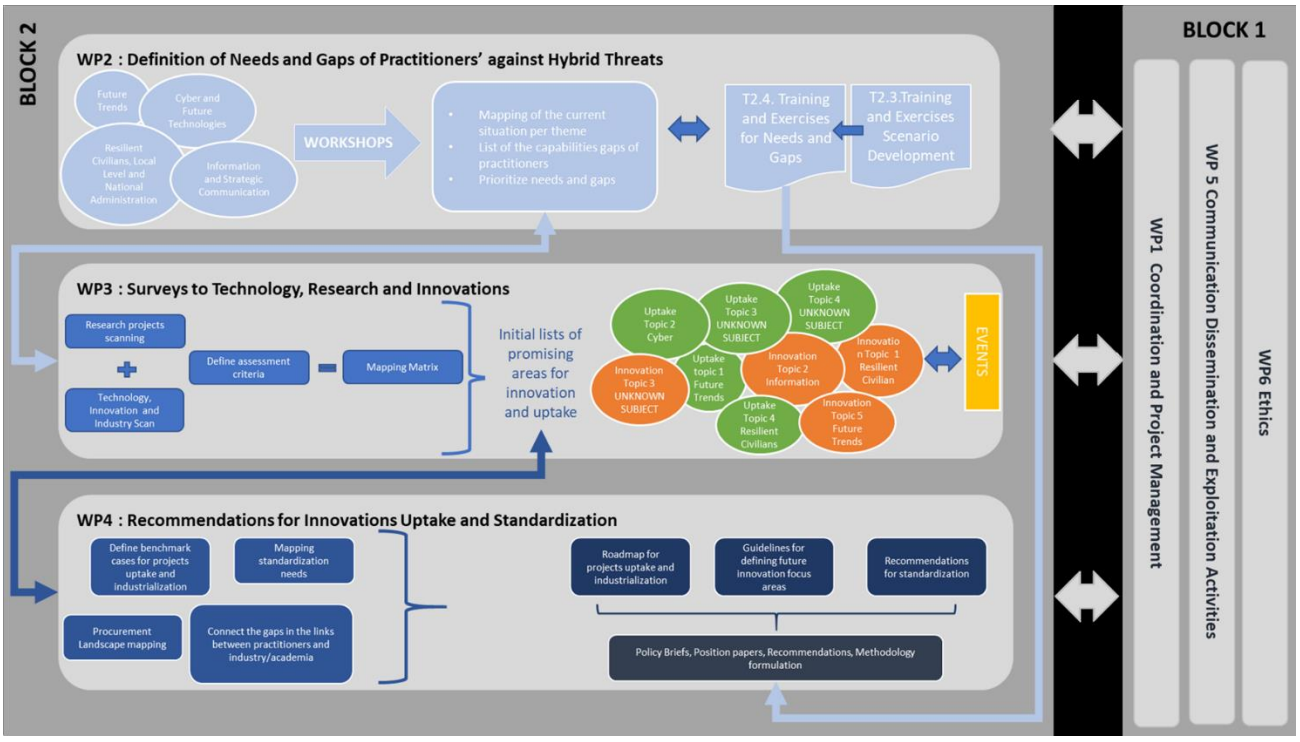


Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in D1.9 are linked to the project milestones (MS) achieved during the last six-month period. The milestones relevant to D1.9 are following:

Milestone No.	Milestone (MS) name	MS related Task	Due project month
14	Cycle III	All	35
27	2nd Policy briefs, Position Papers or Recommendations documents are published	All	36
7	3rd EU-HYBNET Project Management Board Meeting	1,4,5	36
36	3rd Annual Workshop	All	36

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The sixth Six-Month Action Report (D1.9) main author is Laurea, the organization responsible for the delivery of D1.9. However, EU-HYBNET work package (WP) and task (T) leaders have also provided information on the tasks they are responsible for and have been working on during the sixth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager have contributed to D1.9 by providing general remarks on the project's general progress and innovation uptake.

3. THREE LINES OF ACTION REPORTING

This chapter describes EU-HYBNET's activities, especially in Work Packages (WPs) and Tasks (T) relevant to the Three Lines of Action during the project past six months, namely period May - October 2022. According to the EC's request, EU-HYBNET should report according to the following Three Lines of Action:

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

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

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

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

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

The starting point for the first "Three Lines of Action" reporting is coming from the EU-HYBNET Task (T)2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" (lead by Hybrid CoE) and T2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC) who identified during the beginning of the second project cycle (M18-M34/ October 2021 – February 2022) practitioners'[1] and other relevant actors' (industry, SMEs, academia, NGOS) gaps and needs, vulnerabilities to counter hybrid threats. The work conducted in T2.1 and T2.2 contributed to deliverable (D) 2.10 "Deeper analysis, delivery of short list of gaps and needs" (M22/ February 2022) where the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats were listed. Therefore, the D2.10 signified in the second project cycle (M18 – M34/ October 2021 – February 2023) the starting point for the EU-HYBNET project to start monitoring and mapping technological and non-technological/human-science based innovations, solutions from existing research and innovation (R&I) projects and other possible sources or providers (e.g. industry, academia, NGOs) to cover the identified gaps and needs and with a goal of recommending the uptake or the industrialization of results.

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

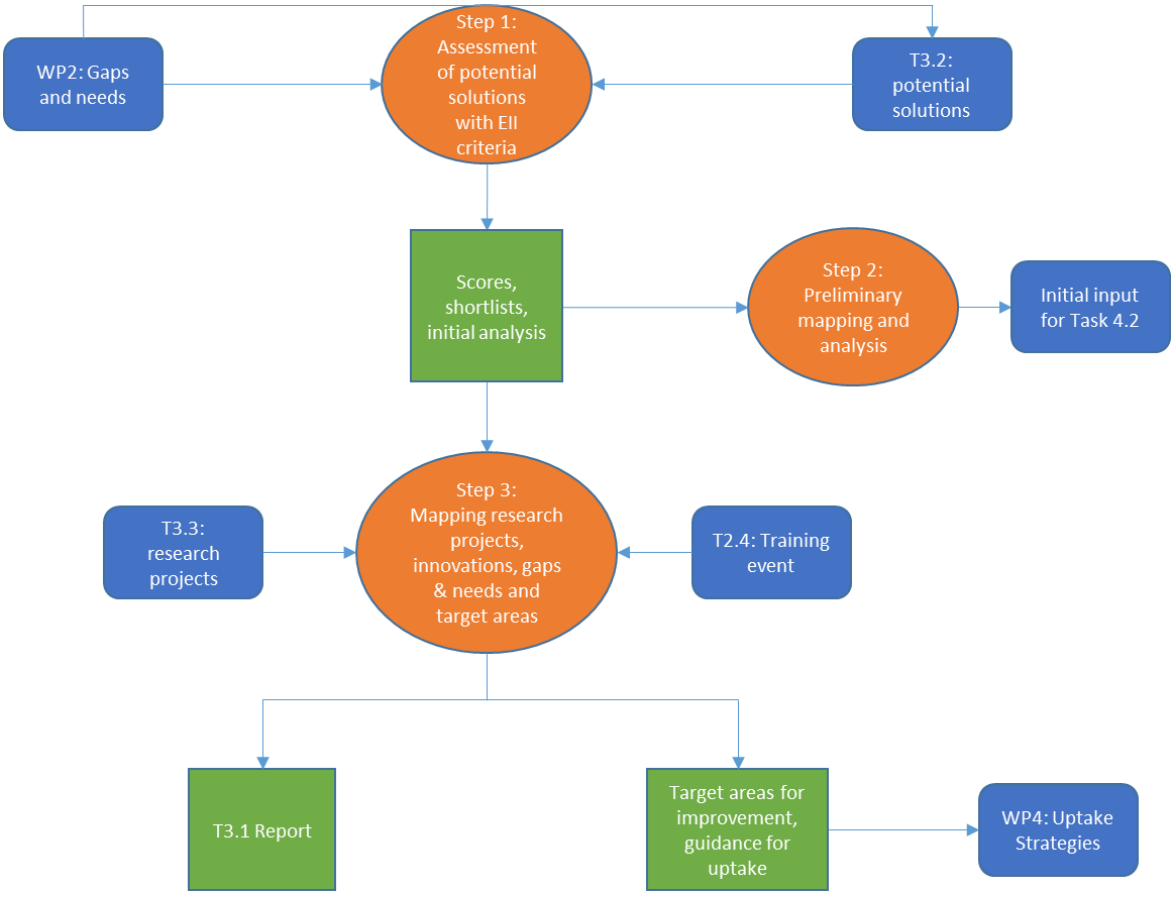
During the previous reporting period many innovations identified in T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) and T3.2 "*Technology and Innovations Watch*" (Lead by Satways) were going through during this reporting period thorough analyses of T3.1 "*Definition of Target Areas for Improvements and Innovations*" (Lead by TNO). Because T3.1 delivers final analysis of the most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats, the results from T3.1/ D3.2 "*Second interim-report mapped on gaps and needs*" (M32/ Jan 2023) are reported below in sub-chapter 3.1.1. below.

Next to T3.1 important innovation analysis relevant to the first Three Lines of Action reporting has been conducted WP4 "*Recommendations for Innovations Uptake and Standardization*" T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE)/ D4.5 "*2nd Innovation uptake, industrialization and research strategy"* (M34 / Feb 2023, RISE). The results achieved in T4.2 according to the three lines of actions topic **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** are described in the following sub-chapters (3.1.2.) alike results from WP5 "*Communication, Dissemination and Exploitation Activities*" T5.3 "*Project Annual Workshops for Stakeholders*" (Lead by Laurea). In T5.3 EU-HYBNET Annual Workshop event was arranged on 20th of April in Bucharest where sound projects to identified pan-European security practitioners' gaps and needs were provided pitching opportunities. More on the selected projects in sub-chapter 3.1.3 below.

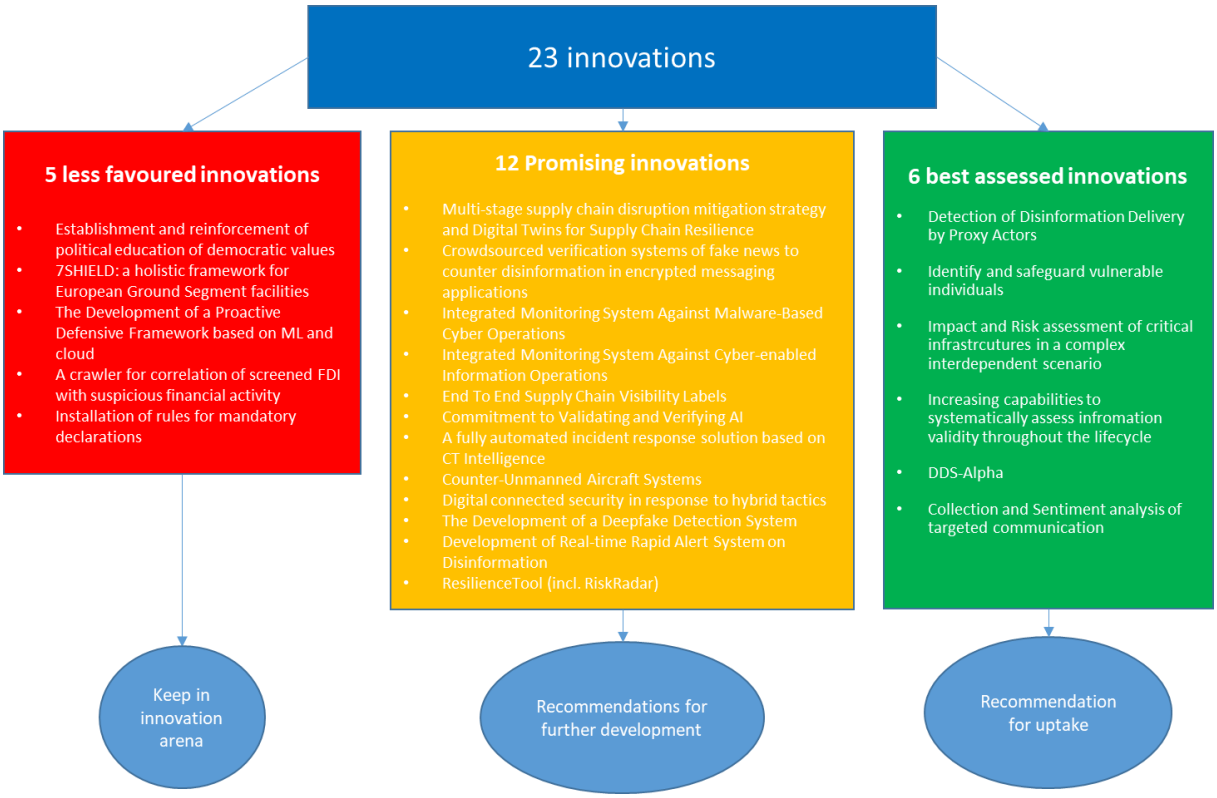
3.1.1 EU-HYBNET T3.1 DEFINITION OF TARGET AREAS FOR IMPROVEMENTS AND INNOVATIONS

During the reporting period the many innovations identified in T3.3 and T3.2 have been set under thorough analyses of T3.1 "*Definition of Target Areas for Improvements and Innovations*" (Lead by TNO) because T3.1 is to deliver the final analysis of the most promising innovations to identified, present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats. T3.1/ D3.2 "*Second interim-report mapped on gaps and needs*" (M32/ Jan 2023) results are presented below.

In T3.1 a three-step analysis approach was used in order to ensure that all relevant project information is imbedded to analysis and research. 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 23 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 23 innovations 5 less favoured innovations, 12 potential and promising innovations and 6 best assessed innovations. The process and thorough analysis of the innovation analysis is described in detail in T3.1/D3.2 "*2nd interim-report mapped on gaps and needs*" (by TNO, M33/ Jan 2023). The picture below describes the innovation assessment and prioritization results – the picture is from D3.2 by TNO:



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**
Detection of Disinformation Delivery Proxy Actors	14	5	5	4
Identify and safeguarding vulnerable individuals	13	5	5	3
Impact and Risk assessment of critical infrastructures in a complex interdependent scenario	12	4	5	3
Increasing capabilities to systematically assess information validity throughout the lifecycle	12	4	4	4
DDS-alpha	12	4	4	4
Collection and sentiment analysis of targeted communication	12	4	4	4

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 23 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 D2.21 "Training and

exercises delivery on up-to-date topics" (L3CE, M29). 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 six best assed innovations uptake are following:

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

Primary Context: Exploitation of existing political cleavages

Idea/Innovation proposed: "Detection of Disinformation Delivery Proxy Actors". The innovation is among the six best assed innovations, No. 1. Total score 14 points. Projects linked to this idea following:

- **Project: WEVERIFY** H2020 project aimed to "address the advanced content verification challenges through a participatory verification approach, open-source algorithms, low-overhead human-in-the-loop machine learning and intuitive visualizations" (European Commission, 2018)
- **Project:** Open Distributed Digital Content Verification for Hyperconnected Sociality (**SOCIALTRUTH**) aimed to create a more open, democratic, scalable, and decentralized environment for content verification (European Commission, 2018)
- **Project :** The Co-Creating Misinformation-Resilient Societies project provided tools for citizens, journalists and policymakers to better identify misinformation and to improve their own understanding on the spread of misinformation (**Co-Inform**) (European Commission , 2014)
- **Project:** The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (**COMPROP**) project showcased how malicious entities were able to abuse computational propaganda to produce conflicting stories, leading to a general lack of knowledge and awareness amongst consumers of the disinformation (European Commission, 2016).
- **Project:** Information and Misinformation Economics: Design, Manipulations and Countermeasures (**IMEDMC**): this research project aims to improve understanding of information designs and flows, and how these may be manipulated (European Research Council, 2021).
- **Project: Open Your Eyes: Fake News for Dummies** is a Erasmus+ project dedicated to improve the digital literacy of adult learners by providing them with tools to identify fake news and fight the spread of disinformation online (Dlearn, 2020).
- **Project:** The Consequences of the Internet for Russia's Informational Influence Abroad (**RUSINFORM**) project aims to increase understanding of Russian information influencing operations abroad. Whilst it does not aim to develop specific technologies, it may improve defensive tools by leveraging a more holistic understanding of how Russia uses the internet for its influence operations abroad (European Commission, 2019).
- **Project:** The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (**COMPROP**) project aimed to improve understanding of how

algorithms and automation can be used to manipulate public opinions during elections and/or political crises. It also showcased how malicious entities were able to abuse computational propaganda to produce conflicting stories, leading to a general lack of knowledge and awareness amongst consumers of the disinformation (European Commission, 2016).

Primary Context: Exploitation of critical infrastructure weaknesses and economic dependencies

Idea/Innovation proposed: "*Impact and Risk assessment of Critical Infrasturctures in a complex interdependent scenario*". The innovation is among the six best assed innovations, No. 3. Total score 12 points. Projects linked to this idea following:

- **Project:** Strategic programs for advanced research and technology in Europe (**SPARTA**) aims to develop a framework of 'Comprehensive Full-Spectrum Cybersecurity Threat Intelligence', by developing technologies and models that enable orchestration of situational awareness processes, identification, intelligence, and counteraction across multiple stakeholders' organizations (European Union, sd)
- **Project:** The Protection of Critical Infrastructures from advanced combined cyber and physical threats (**PRAETORIAN**) project aims to produce a toolset that helps critical infrastructure operators' decision-making by combining physical situational awareness tools and cyber situational awareness tools into a hybrid and comprehensive situational awareness system (European Union, 2023).
- **Project:** The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with a focus on district or regional protection (**PRECINCT**) helps connect private and public critical infrastructure stakeholders.
- **Project:** The INtelligent Security and Pervasive tRust for 5G and Beyond (**INSPIRE-5Gplus**) project tries to apply Machine Learning, AI, and blockchain technologies to help improve control of systems and eliminate vulnerabilities for infrastructure operators (European Commission, 2019)
- **Project**: Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (**EU-LISTCO**) project aims to analyse when areas of limited statehood (ALS) and contested orders (CO) in the EU's Southern and Eastern neighbourhood, may threaten the stability and security of the EU. It examines conditions of deterioration, and how preparedness of the EU and its member states may foster resilience in the neighbourhood (European Commission, 2022)

Context – EU-HYBNET Project Core Theme: Information and Strategic Communications

Primary Context: Information manipulation with the aim of destabilization

Idea/Innovation proposed: "*Increasing capabilities to systemically assess information validity throughout the life cycle*". The innovation is among the six best assed innovations, No. 3. Total score 12 points. Projects that support the named idea/innovations uptake are listed below. However, the projects are same that were seen to support development and uptake of the idea/innovation mentioned under *Core Theme: Resilient Civilians, Local Level and National Administration*. Therefore,

only the project's names are mentioned below but more detailed descriptions of theme can be read form previous sub-chapter above. The projects in question are:

- **Project: WeVerify**
- **Project:** Open Distributed Digital Content Verification for Hyper-connected Sociality **(SOCIALTRUTH**)
- **Project:** The Co-Creating Misinformation-Resilient Societies (**Co-Inform**)
- **Project:** Information and Misinformation Economics: Design, Manipulations and Countermeasures (**IMEDMC**)
- **Project:** The Consequences of the Internet for Russia's Informational Influence Abroad (**RUSINFORM**)
- **Project:** The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (**COMPROP**)

Primary Context: Information manipulation with the aim of destabilization

Idea/Innovation proposed: "*DDS-Alpha (EEAS)*". The innovation is among the six best assed innovations, No. 3. Total score 12 points. Projects that support the named idea/innovations uptake are listed below. However, some of the projects are same that were seen to support development and uptake of the idea/innovation mentioned under *Core Theme: Resilient Civilians, Local Level and National Administration*. Therefore, new projects descriptions are given but already mentioned project's project names is mentioned below because more detailed descriptions of the already named projects can be read form previous sub-chapter above. The projects in question are:

- **Project:** The Consequences of the Internet for Russia's Informational Influence Abroad (**RUSINFORM**)
- **Project:** The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (**COMPROP**)
- **Project: Open Your Eyes: Fake News for Dummies**
- **Project:** The project **PersoNews** concerns the profiling and targeting of news readers, and the implications for the democratic role of the digital media, user rights and public information policy (European Commission, 2015). This project analysed how various social media platforms use algorithms to select what material to recommend to its consumers. This project could be beneficial to better understand the landscape and information flows of such platforms, that could benefit this innovation on the collection and analysis of sentiments through targeted communications.
- **Project:** The project **AI4Dignity** is a project that aimed to merge capabilities of AI technologies with human interactions and community-based fact-checking (European Commission, 2021). This project was especially leveraged to apply AI in pursuit of the detection of hate speech. Whilst important work, this project was relatively small. Despite its size, the implications should be better leveraged in related research and innovations.

Primary Context: Promoted ideological extremism and violence

Idea/Innovation proposed: "*Collection and Sentiment Analyses of targeted communication*". The innovation is among the six best assed innovations, No. 3. Total score 12 points. However, the projects

are same that were seen to support development and uptake of the idea/innovation mentioned under *Core Theme: Resilient Civilians, Local Level and National Administration*. Therefore, only the project's names are mentioned below but more detailed descriptions of theme can be read form previous sub-chapter above. The projects in question are:

- **Project:** The Consequences of the Internet for Russia's Informational Influence Abroad (**RUSINFORM**)
- **Project:** The Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (**COMPROP**)
- **Project: PersoNews**
- **Project: AI4Dignity**

Primary Context: Promoted ideological extremism and violence

Idea/Innovation proposed: "*Identify and safeguarding vulnerable individuals*". The innovation is among the six best assed innovations, No. 2. Total score 13 points. However, the projects are same that were seen to support development and uptake of the idea/innovation mentioned under *Core Theme: Resilient Civilians, Local Level and National Administration*. Therefore, only the project's names are mentioned below but more detailed descriptions of theme can be read form previous sub-chapter above. The projects in question are:

- **Project: Open Your Eyes: Fake News for Dummies**
- **Project:** The Consequences of the Internet for Russia's Informational Influence Abroad (**RUSINFORM**)

On the whole, according to T3.1 clear link has been made between the identified innovations and research projects working on similar issues that may be mutually beneficial. In addition, there are some research projects that are not relevant to any specific identified potential solution or innovation, but could still be useful in relation to the overall primary context. As such, whilst these research projects might not have a direct relation into improving potential solutions and innovations, they may nonetheless help improve the overall framing and understanding of the issues addressed within the primary context. By extension, it may also improve experts and practitioners' broader understanding of interrelated issues, and indirectly improve those working on innovations and solutions under development.

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. This finding will support to recommend EC funded projects (e.g. RUSINFORM, COMPROP, IMEDMC) innovation uptake for practitioners who especially work on disinformation and IMI/ information manipulation and interference. 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) contributes 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***" alike T4.2 provides input to the second Three Lines of Action "Common Requirements as Regards Innovations that Could Fill in Gaps and Needs" and the third Three Lines of Action "Priorities as regards of increasing of knowledge and performance requiring standardization". The T4.2 contribution to the first Three Lines of Action is described below.

T4.2 delivered D4.5 "*2nd Innovation uptake, industrialisation and research strategy"* in M34 (February 2023) and the document described four most promising innovations identified by EU-HYBNET to the innovation uptake recommendations. The four most promising innovations to cover the 2nd project cycle's identified pan-European security practitioners' gaps and needs to counter Hybrid Threats are following according to D4.5.:

- **WINS**/ "*What Information Needs to be Shared between Critical Infrastructure (CI) entities to detect hybrid threats and attacks, and to be prepared for them*". Methodology.
- **EESCM**/ "*Enhanced and Extended Supply Chain Management*". Methodology.
- **MIMI**/ "*A Market place for Information Manipulation and Interference Information*". Platform and approach.
- **GECHO**/ "*Gatekeeping ECHO chambers*". Methodology for information sharing and cooperation, also new technological solutions to support the cooperation.

All four above mentioned innovations and research projects that support the innovation uptake are described below

WINS/ *"What Information Needs to be Shared between Critical Infrastructure (CI) entities to detect hybrid threats and attacks, and to be prepared for them"*

Scope of WINS - General description: *WINS* is a **methodological approach to discover what information needs to be shared to enhance Critical Infrastructure (CI) entities[2] resilience to counter hybrid threats**. WINS builds on CISAE innovation that was identified as promising innovation and solution during the 1st EU-HYBNET project working cycle to support CI entities to counter hybrid threats. ***CISAE*** (A common Information Sharing and Analysis environment) is answering to the question of **how to share CI information between CI stakeholders**. Furthermore, pan-European maritime security authorities Common Information Sharing Environment (CISE) approach developed in various EC funded projects, e.g. EUCISE2020 (https://cordis.europa.eu/project/id/608385), was seen as sound approach to establish CISAE. Therefore, in the information sharing part of the CISAE, we refer to the

[2] Critical entity definition according to CER Directive Article 2/ (1) is following "Critical entity means public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column in the table of in the Annex". CER Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829.

documentation of the European Maritime Security Agency (EMSA) CISE specifications https://www.emsa.europa.eu/we-do/surveillance/cise.html

Projects relevant to WINS uptake: EUCISE2020 project https://cordis.europa.eu/project/id/608385 and more about CISE https://www.emsa.europa.eu/we-do/surveillance/cise.html

Description of the projects relevance: The core concept, alike in CISE, is to have CISAE nodes in each participating Member State to which local systems can be connected. The CISAE nodes exchange information in a common format which is then translated into the formats of the Member States' local systems. Information sharing is discretionary and controlled by the information owner/source. End to end data is used for information sharing. Data fusion and analysis tools may be implemented locally in each Member State, in joint efforts or as a common system function. Storage tools may be introduced when required for the analysis and/or for logging. These tools can be connected to or implemented in CISAE nodes. The CISAE will be easily extended to include new users and organizations, while local systems and analysis tools can be connected and integrated stepwise. The CISAE must have extremely high cyber security. It should build on established principles and best practices for how information exchange between organisations in Member States is protected. The CISAE will not, in the information sharing part, be particularly sensitive to changes in threat vectors. Analysis tools may however exhibit such sensitivity.

WINS – CISAE - CISE Implementation: The system architecture will be similar to the architecture of the EMSA CISE hybrid model as shown in the Figures A (Illustration of how legacy systems are connected to EMSA CISE). Figure B illustrates of CISAE connection with the new analysis function to existing CISE approach.

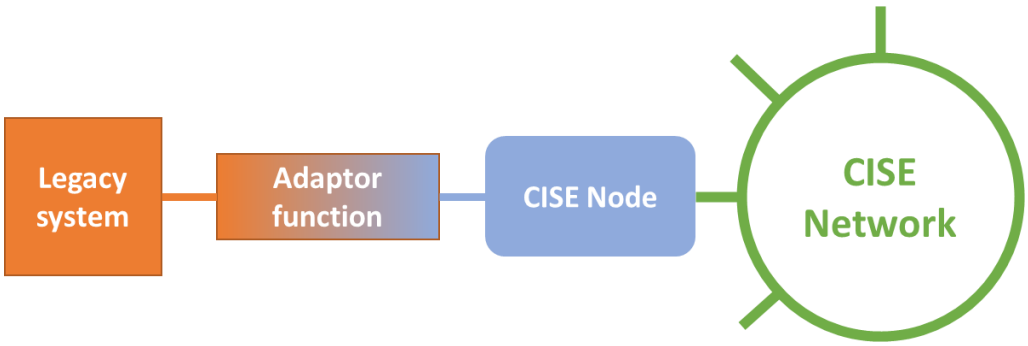


Figure A. Illustration of how legacy systems are connected in EMSA CISE.

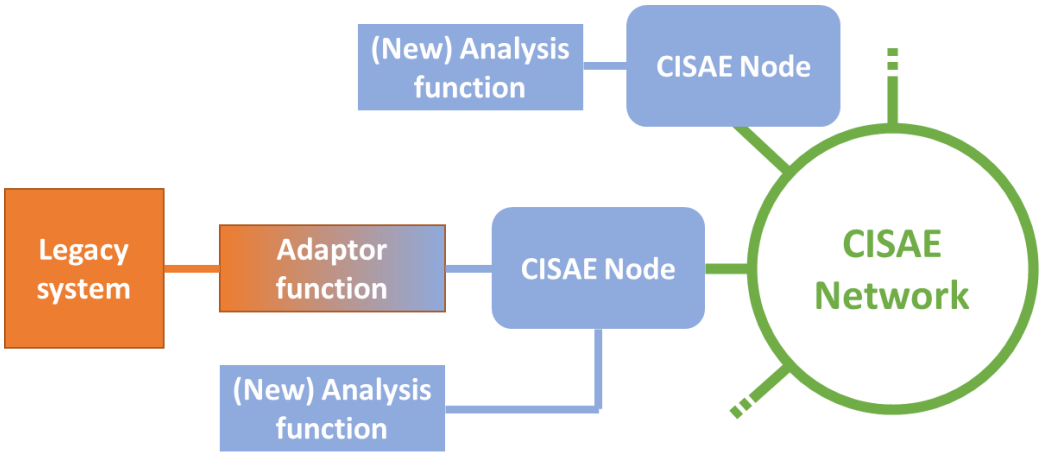


Figure B. Illustration of CISAE connection with new analysis function

EESCM/ "*Enhanced and Extended Supply Chain Management*"

Scope of EESCM - General description: ***EESCM*** **(Enhanced and Extended Supply Chain Management)** is a methodological approach and solution focusing on how to enhance and extend the supply chain management scope so as to take more aspects into account, provide a better understanding of the real issues and how to minimize disruption impacts. Scope of EESCM is to focus on Supply chain management policies and methods for Critical Infrastructures (CI) and industry, followed by enchased tooling (e.g. Digital Twins). Furthermore EESC mission is to support CI service providers and product suppliers by building capabilities in impact minimisation and rapid recovery in response to wide supply chain disruptions, including services. The aim of the proposed solution is to provide insights, methodology and frameworks for the industry. New approach of supply chain management then will be taken over by technological solution providers to include new functionalities in their tools.

Projects relevant to EESCM uptake: In the D4.5 no specific project was mentioned to support EESCM uptake while it was underlined that Digital Twins is the needed solution for EESCM creation. Therefore, an European Commission (EC) funded project PRECINCT ("The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats") that EU-HYBNET has already earlier identified as sound CI entities resilience building project can be mentioned in the context of EESCM as a project that supports EESCM creation due to the project's focus to create digital twins for CI entities for enhanced crises response, recovery and preparedness planning. PRECINCT Webpage: https://www.precinct.info/

Description of the project's relevance: The EESCM is to develop easy to follow framework to describe the wide scope supply chain concept. It should include critical services, geopolitical risks, deeper coverage of value chain and other relevant aspects. That can be further used for policy formulation, recommendations and other means to promote and improve it. Relevant legislation on EU and national level can be final stage to anchor the new approach to the supply chain management. In parallel to the conceptualization efforts methods and tools for wide scope supply chain management should be developed, while there are innovative solutions already available in the market e.g. approaches and solutions developed in PRECINCT project. After all, PRECINTC is to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management

approach which will yield a protected territory for citizens and infrastructures. Furthermore, PRECINCT advances state of the art in security tooling will help CI private and public actors with comprehensive and installation-specific approaches to secure existing and future connected and co-dependent installations. To achieve this target, the PRECINCT project will be addressed in a multi-faceted way. PRECINCT delivers **Digital Twins** solution that will help improving accuracy and automation in identification, remediation and threat elimination where the above models can be advanced towards more detailed models in the context of specific hazards. The application of Digital Twins to the multi-hazard risk management yields a circular process of anticipating, preventing and protecting events, responding during the events, and recovering and learning after events. Learning from experience closes the loop by reducing the vulnerabilities and improving the capabilities of the system, which then becomes less vulnerable to future events and more resilient to cope with future disruptions.

EESCM Implementation: To bring the EESCM solution to practice, providers of supply chain management related services (tools and training) should enhance current instruments with new concept, e.g. such coming from PRECINCT. In addition, for doing so the policy and guidance should be set by EU and MS level policy makers. It is presumed that if such recommendations, supported with easy-to-follow framework, are developed and well disseminated, tool and training providers will follow them, adding new capabilities in their instruments. Digital Twins is the approach currently used to model supply chain and optimisation means (e.g. PRECINCT project) and it can be adapted to the widened scope that includes services, geopolitical and other hybrid threats related aspect. Enhanced tools should also be able to provide reliable, real life based, modelling of cascading effects, impact minimisation and recovery simulation capabilities. For these needs PRECICNT is partially providing the needed solutions.

MIMI/ *"A Market place for Information Manipulation and Interference Information"*

Scope of MIMI - General description: It has been recognized that a solution for efficient sharing of Information Manipulation and Interference Information (IMII) between concerned stakeholders is a key element in the EU Member States' (MS) efforts to improve societal resilience against national and foreign Information Manipulation and Interference (IMI) activities. This fact is corroborated by the actions and activities by the European External Action Service (EEAS)/Strategic Communication (Strat.Comm.) directed at designing and implementing such an IMII sharing platform. The need is thus established but the means to ensure wide sharing and exchange of IMII still remains to be comprehended. Therefore, MIMI has been proposed to support the EEAS's IMI measures. On the whole, as an answer to the user challenges, EU-HYBNET proposes that a market and market place for IMII is established. For this to be possible, there is a need for:

1. *Trusted and secure IMII sharing platform*
2. *Initial business model which is accepted by all stakeholders*
3. *Integration of a charging solution in the sharing platform which is compliant with the business model*.

The requirement 1) for a *trusted and secure IMII sharing platform* is satisfied by the EEAS/Strat.Comm.'s DDS-alpha innovation. However, EU-HYBNET T4.2 noted that it is important to also implement functionality to make sure that no information leaks to "external agents" or that contaminated information can be entered into the platform. This effort must be sustained during the

formation and the operation of the MIMI to ensure that both the functioning of the whole system and the information that moves through it are reliable. This observation is true for MIMI but it is of course also true for the DDS-alpha platform in itself. Detailed solutions for *2) and 3)* would need to be developed in cooperation with the IMII stakeholders to provide a working solution. This proposed solution is called **MIMI – a Marketplace for IMI information**. In EU-HYBNET T4.2 it was noted that business agreements, contracts and payments for services should be handled by standard procedures and are not part of the solution.

Establishment of a MIMI should also promote the building of supply chains in the area. The market place would stimulate the establishment of multiple actors that specialize and compete in different segments of the supply chain with different focus. There may be actors that mine the Internet, others monitor media outlets or the darknet, searching for relevant data and content, and in this way produce baseline IMII. Others may specialize in analysis of such baseline IMII data to detect certain aspects of IMI, like fake accounts, fake media and hate speech, in different cultural regions and languages. Still others, may base their work on already analysed IMII data in order to get an overarching situational awareness or to base decisions on where and how to intervene. If such a market place is established, it would in the best of worlds lead to a market place in which highly competent and specialized competing actors and this would in the end give high quality results and end products. Lastly, it is noted that although the setting of this innovation is for DDS-alpha, it would be applicable for any other sharing platform like the Common Information Sharing and Analysis Environment (CISAE) for disinformation, proposed in the first EU-HYBNET project cycle (see D4.4[3] and the EU-HYBNET Policy Brief No3.– Information Manipulation and Interference – February 2022[4]).

Projects relevant to MIMI uptake: In the last few years, the EU has started to take a stronger role in facilitating connections between civil society actors, mainly through two overlapping projects, also relevant to the development of MIMI.

In short, “the Social Observatory for Disinformation and Social Media Analysis” (SOMA) project (duration Nov/2018 – April/2021) has been established to lay the basis for a Europe-wide network of fact-checking organisations. But in practice, SOMA only attracted a small number of members, most of whom did not appear to make much use of the project platform. SOMA’s activities have largely been taken over since June 2021 by the more ambitious European Digital Media Observatory (EDMO) that can also be seen as a project. EDMO is a Europewide network of not only fact-checking organisations but also academics, researchers and media institutions. MIMI would especially rely on the basis of EDMO.

Furthermore, as mentioned above, establishing MIMI is also linked to the creation of CISEA platform that is based on the European Maritime security authorities Common Information Sharing Environment (CISE) that has been build in EUCISE2020 project. More about CISAE and CISE above in the context of WINS innovation description. EDMO https://edmo.eu/ and EUCISE2020:

[3] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e29c595e&appId=PPGMS

[4] https://euhybnet.eu/wp-content/uploads/2022/02/EU-HYBNET_Policy-Brief_-Information-Manipulation-and-Interference_Feb-2022.pdf

https://cordis.europa.eu/project/id/608385 and https://www.emsa.europa.eu/we-do/surveillance/cise.html

Description of the projects relevance: EDMO is built around a European level of partner organisations, with several national and regional hubs that are in the process of being set up, and its goal is to strengthen cooperation, raise awareness and empower citizens to respond to online disinformation. To this end, it conducts original research, maps and supports existing fact-checking and research activities, and seeks to build a European community of fact-checkers that will collaborate continually, contributing to a culture of cross-border cooperation. EDMO's structure is, therefore, by design, cross-sector, cross-border and cross-purpose, in that it aims to develop research and understanding about disinformation while also working practically to counter it. Although each of its national and regional hubs is composed of different organisations working together in different ways, the various national experiences should allow for exchange and mutual learning between countries. This transnational perspective, informed by expertise on national and regional dynamics, helps monitor the spread of disinformation more effectively, regardless of its origin, and contribute to finding and coordinating effective responses against it. From this perspective EDMO could well support uptake of MIMI innovation.

MIMI Implementation: Although the setting of MIMI is for DDS-alpha, it would be applicable for any other sharing platform like the Common Information Sharing and Analysis Environment (CISAE) for disinformation. Idea on CISAE is already described above while in the case of WINS innovation. The need for CISAE, or similar platform, is crucial because the present DDS-alpha platform format needs to be extended with a service platform on top of DDS-alpha. This service platform should include DDS-alpha extensions for charging and service control. Lastly, to bring the MIMI solution to practice, also possible hosts of planned MIMI market place should be defined – discussion with EDMO and EEAS on their interest for the owner of the market place would be ideal.

GECHO/ "*Gatekeeping ECHO chambers*"

Scope of GECHO - General description: The ultimate objective of GECHO is to develop easy to follow validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. To make it become the powerful tool it should become, there is need for supporting research in several areas related to the factors influencing the radicalisation process:

a) The state-of-the-art of existing frameworks, methods and tools.
b) Methods used by groups promoting violent extremism in their online recruiting activities.
c) Relevant differences in cultural, language and community codes
d) What makes a person vulnerable
e) Frameworks, methods and tools for creation of practical means for prevention.
f) Methods for evaluation and validation of the effectiveness of countermeasures

The research and development of GECHO frameworks, methods and tools for creation of the practical means for recruitment prevention should start from the current state-of-the-art. Different components exist today but may need validation and/or updates to become more generic, others need

to be developed; what is missing is the overarching framework – the creation of a systematic knowledge base with validated intervention means. The proposed way to proceed is to use an incremental, step-by-step approach in building the frameworks, the tools and methods. However, as the target arena is agile both in the way that the extremist groups behave and appear online, and in the development of knowledge and technology in countermeasure methods and tools continuous development and updates will be required. Also, for this research a project organization is required.

The GECHO solution will target stakeholders at different levels and with different application areas. Dissemination and training activities will be needed for the uptake of the developed working methods and tools.

Projects relevant to GECHO uptake: There are many initiatives implemented within EU funded projects, and the projects are listed below:

- **Participation**[5] is project which primary purpose is to prevent extremism, radicalization and polarization that can lead to violence through more effective social and education policies and interventions that target at risk groups to be performed through the establishment of a holistic framework and the involvement of social actors, local communities, civil society, and policymakers;
- **INDEED**[6] builds from the state-of-the-art, utilizing the scientific and practical strengths of recent activities – enhancing them with complementary features to drive advancements and curb a growing rise of radical views and violent behaviour threatening security. Project's methodological framework is based on the '5I' approach i.e. 5 project phases: Identify; Involve; Innovate; Implement; Impact;
- **Dominoes** (Digital Competences Information Ecosystem)[7] is a project dedicated to the investigation of hybrid threats, propaganda and disinformation which overall objective is to reduce societal polarization by combating fake news and online disinformation in two target groups: university professors employed by the partner universities/civil society trainers and M.A. students in the partner universities.
- **VOX-Pol Network of Excellence**[8] is a FP7 started Virtual Centre of Excellence for Research in Violent Online Political Extremism, which still is very active. The aim of VOX-Pol is the comprehensive exploration of the many varieties of Violent Online Political Extremism, its societal impacts, and responses to it. To this end, project partners combine complementary expertise from a range of disciplines (e.g. Communications, Computer Science, Criminology, Ethics, International Relations, Politics).

In the Horizon Europe Work Programme on Civil Security for Society, there is a RIA call[9] for 2024 on Radicalisation and gender, with focus on improved understanding of motivation for supporting extremist ideologies, by women and girls, by men and boys as well as of the role of group dynamics. Another target is to develop modern and validated tools, skills and training curricula to identify early symptoms of radicalization. This project is well aligned with the proposed solution detailed above.

Description of the projects relevance: There are a lot of projects alike organizations and initiatives that focus on the main issue of GECHO, namely fighting against radicalization/terrorism in a global way.

[5] https://participation-in.eu/
[6] https://www.indeedproject.eu
[7] https://projectdominoes.eu/
[8] https://www.voxpol.eu/
[9] HORIZON-CL3-2024-FCT-01-04: Radicalisation and gender

However, what is missing is following and for these actions the named projects, alike future projects are needed to deliver solutions:

- A platform for online situational awareness with respect to violent extremism and terrorism. The platform should comprise functions for real-time sharing of available information.
- AI based tools for rapid and accurate discovery of new sites related to violent extremism. Monitoring of activity levels at known sites and visits by new users.
- A standardized taxonomy which is accepted by all stakeholders together with standardized formats for descriptions, their coding and communication.
- Automatic identification and rapid launch of automatic countermeasures and human interventions online and IRL, based on validated frameworks and methods.
- Targeted and coordinated research and development to provide systematic knowledge at a European level on all aspects of how to build resilience in vulnerable young people against online entrapment in violent extremism and terrorism.

GECHO Implementation: The starting point to create GECHO solutions is to develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. Enable sharing of situational data between stakeholders. The platform can be based on above mentioned EU-HYBNET innovations such as CISAE. If so, the CISAE principles proposed to be standardized. An alternative route would be to use an extended DDS-alpha platform as described in the EU-HYBNET MIMI innovation description above.

On the whole, GECHO lies strongly on the use of AI, and therefore there is need to develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites. In this work use of federated learning should be considered and how anonymization and GDPR requirements can be fulfilled. Furthermore, there is a need for research and compilation of training sets to guarantee that AI based solutions easily can be developed and tested.

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

EU-HYBNET T5.3 “Annual Workshop for Stakeholders” is dedicated to arrange the EU-HYBNET Annual Workshop on a yearly basis. The 3rd Annual Workshop (AW) was arranged in M36 (April 2023) in Bucharest, Romania. Program and more about the AW in EU-HYBNET D5.12 “*Annual Workshop Report 3*”. According to DoA Annual Workshop is arranged to disseminate project findings for large scale of stakeholders and to ensure vivid interaction with industry, academia and other providers of innovative solutions outside of the consortium with a view to assessing the feasibility of the project findings and possible recommendations to innovations uptake and standardization. Annual Workshops will foster network activities, raise awareness of the project and bring together relevant practitioners and stakeholders who may join to the EU-HYBNET network and its activities. Eventually the goal of Annual workshops is to bring sustainability of the project activities and increase relevant members in network.

As one of the EU-HYBNET Annual Workshop (AW) goal is to focus on promising innovations and their uptake and recommendations, in the 3rd Annual workshop a session was dedicated to pitches of innovations and innovative solutions. Prior to AW, the EU-HYBNET announced possibility for innovative solutions providers to suggest their innovation as a sound solutions to counter hybrid threats. In the EU-HYBNET announcement "Call for Pitches" the areas where innovation pitches were wished to have were reflecting the EU-HYBNET identified gaps and needs to counter hybrid threats in the four core themes of the project. This call resulted to various pitches of which three (3) were chosen to 3rd Annual Workshop. The selected pitches were delivering innovative solutions to foreign information manipulation and interference measures and to border management. The pitches were given by following organizations and a Commission funded project on following innovations or innovative solutions:

1. **Provider:** Maltego https://www.maltego.com/
   Innovation: *Countering Disinformation with Maltego*

2. **Provider:** TrustServista https://www.trustservista.com/
   Innovation: *TrustServista – AI-powered Content Analytics and Verification Platform*

3. **Provider:** University of Malta, CRiTERIA -project https://www.project-criteria.eu/
   Innovation: *CRiTERIA - Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks (Horizon funded project, GA No. 101021866)*

The Innovative solution "*Comprehensive data-driven Risk and Threat Assessment Methods for the Early and Reliable Identification, Validation and Analysis of migration-related risks*" presented by University of Malta is part of the CRiTERIA H2020-project (GA101021866), and hence also highlighted the importance for cooperation between CRiTERIA and EU-HYBNET. In short, if other EC funded projects' solutions and innovations are seen promising to counter hybrid threats, EU-HYBNET is interested in promoting them alike underlining for the projects' their solutions importance also to measures countering hybrid threats.

Next to "Call for Pitches" EU-HYBNET invited three (3) other projects to the 3rd EU-HYBNET Annual Workshop to present their solutions that are seen to deliver sound solutions to the EU-HYBNET's identified critical pan-European security practitioners' and other relevant actors' gaps and needs to counter hybrid threats. The projects who provided presentations were:

- **CYCLOPES/** Fighting Cyber Crime – Law Enforcement Practitioners' Network (GA No. 101021669) https://www.cyclopes-project.eu/
  - Connection to EU-HYBNET's identified Hybrid Threat area: *Offensive cyber capabilities* and *Disruptive innovations (5G, AI)*
- **CRESCEnT**/ CoveRagE and Strategic communication in CasE of security Threats – the development of critical thinking and responsible reaction (GA 2018-1-RO01-KA202-049449) https://crescentproject.eu/
  - Connection to EU-HYBNET's identified Hybrid Threat area: *Offensive cyber capabilities* and *Disruptive innovations (5G, AI)*

- **DOMINOES /** Digital Competences Information Ecosystem (GA 2021-1-RO01-KA220-HED-000031158) https://projectdominoes.eu/
    - Connection to EU-HYBNET's identified Hybrid Threat area: *Information manipulation with the aim of destabilization*

These projects' solutions are especially important to EU-HYBNET T3.2 "*Technology and Innovations Watch"* and T3.3 "*Ongoing Research Projects Initiatives Watch*" to proceed with their analysis and **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** as their work is to be started after D2.7 "*Long list of defined gaps and needs*" (April 2023) and D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (July 2023). Further findings on 3rd Annual workshop will be reported in D5.12"Annual Workshop report 3" (M37/ May 2023).

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

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 T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE), T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) and in T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE). However, during this document reporting period, project months (M) 31 – 36 (November 2022 – April 2023) the third cycle of the project (M35 -M52/ March 2023 – August 2024) 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 M35 (March 2023). Therefore, in this reporting period preliminary views on new gaps and need of pan-european security practitiners to counter hybrid threats have been achieved while the analysis is still on-going. The results from each of the named EU-HYBNET Tasks are described in the forthcoming sub-chapters.

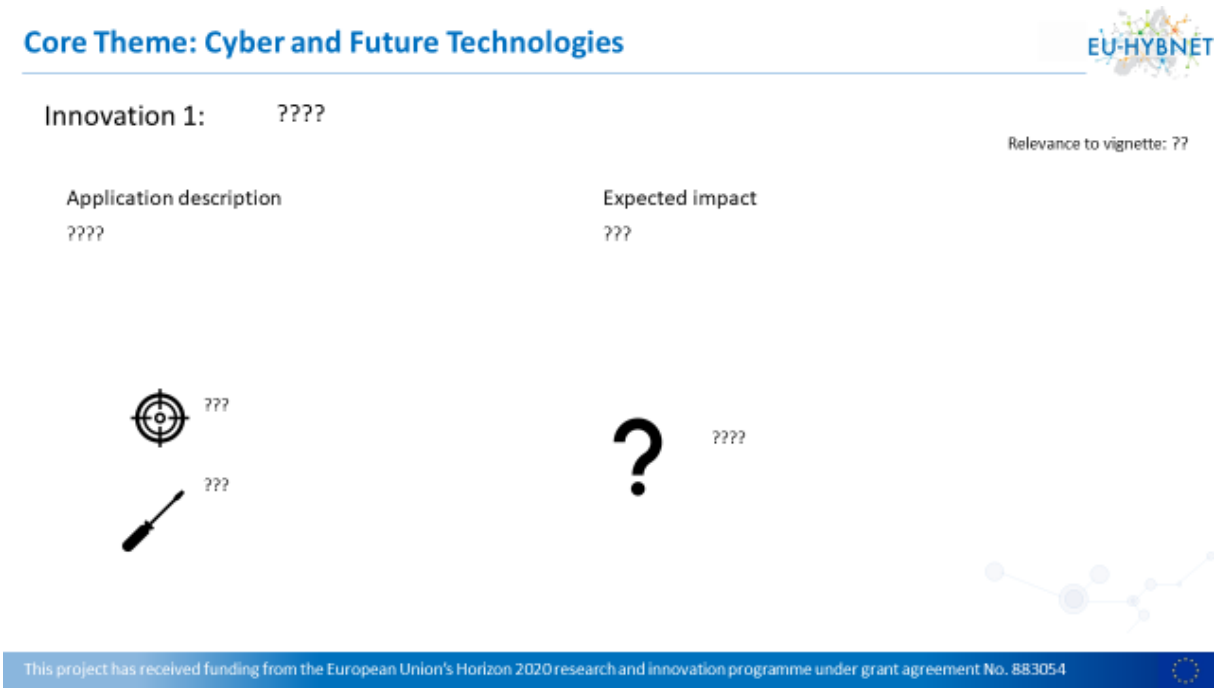
Also WP4/ Task (T) 4.3 "*Recommendations for Standardization*" (lead by the Polish Platform for Homeland Security/ PPHS) has contributed to the second three lines of action while the results are especially relevant to the third Three Lines of Action and hence reported under this topic/ Chapter 3.3. subchapter.

3.2.1 EU-HYBNET T2.4 TRAINING AND EXERCISES FOR NEEDS AND GAPS

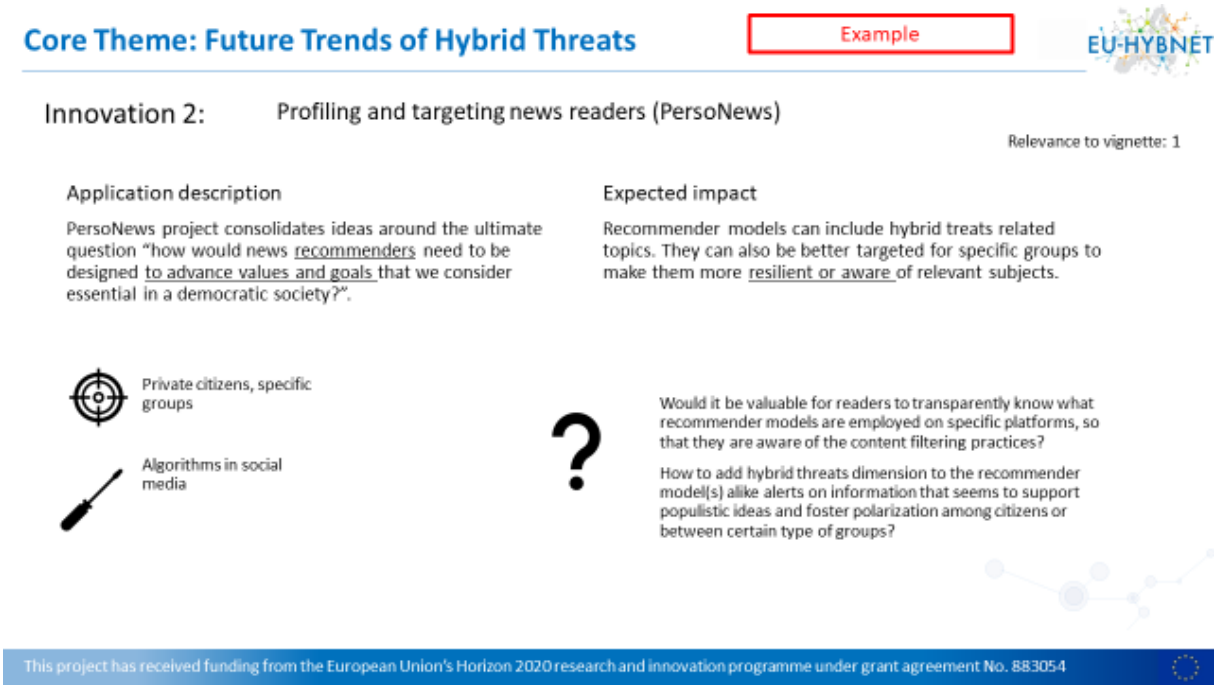
EU-HYBNET T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE) provides input to the second Three Lines of Action **Common requirements as regards innovations that could fill in gaps and needs** from the EU-HYBNET training activities side. In short, T2.4 arranges testing environment for some selected promising innovations according to T2.3 training scenario suggestions. The testing is important in order to gain EU-HYBNET's Network members' (pan-European security practitioners, academia, industry, SMEs and NGOs) views on the soundness of the proposed innovations to gaps and needs. Results of 2nd training event (hybrid format in Vilnus, 29-30/9/2022) have been describe in "*5th Six Month Action Report*"/D1.10 (M30/ Oct 2022) and in D2.21/ "*Training and Exercises Delivery on Up-to-Date Topics"* (M29/ Sep 2022). However more thorough analysis of the training event and innovation recommendations also from common requirements perspective were delivered in T2.47 D2.24 "*Training and Exercises Lessons Learned Report*" (M31/ Dec 2022) and D2.27 "*Training and Exercises Scenario and Training Material*" (M34/Feb 2023). During this reporting period, based on the training event a training material was created to help innovation uptake, and hence also the results especially from D2.27 are reported below in the context of second Three Lines of Action "**Common requirements as regards innovations that could fill in gaps and needs".**

The 2nd EU-HYBNET Training and Exercises event was built around the scenario and injects from T2.3/D2.18 and promising innovations were pre-selected to be tested according to the scenario and injects. To consider usability and soundness of presented, pre-selected innovations (technological on

non-technological) in each of the EU-HYBNET Core Themes, a Power Point document was shared to training participants to ease their innovation analysis. The PowerPoint template is presented below in two version: (1) an empty version and (2) a filled version after the training event and full scale analysis. The pictures below are to highlight how the analysis and common requirements were collected from the participants.



An example of the Power Point that provides the starting point to the training to analyse the presented situation and suggested innovations as solutions.



An example of the Power Point that provides the end point to the training and highlights the usability and needs of a possible innovative solution to be used in the future.

According to the discussions among the training participants following remarks of the highest ranked innovations were done, including remarks to common requirements of the innovations. The innovations were following:

1.Open source intelligence (OSINT) related tools (e.g. HENSOLD innovation)

Identified points for further considerations:

- Visual representation of key results of the request is very important.
- Verification and traceability of information included is essential.
- Some machine learning (AI) features can be added in the future for improved request execution.

2.Support of critical infrastructure in securing their services provision in case of direct attacks or supply chain breakdowns (e.g. Digital Twins, 7Shield)

Identified points for further considerations in the case of Digital Twins:

- Requires more information, but might be considered interesting solution for industry and critical supplies.
- Can be considered for the future as potential subject for regulation.

Identified points for further considerations 7Shield project:

- It does not contribute to the prevention of crisis or attack but rather works for during and post crisis stages.
- Works good for higher coordination and management capabilities involved in mid and high-level decision making processes.
- Especially useful for information sharing cross institution and cross-borders among alliance partners.
- Allows better to organize responsible capabilities for different actions.
- Data correctness is key factor for platform to be trusted.
- It should be developed further from security and high availability perspective as such a solution immediately becomes strategic target (decentralization should be a solution).

3.Information about hybrid treats and relevant operations exchange and structurisation providing faster and more focused response (e.g. DDS-Alpha)

Identified points for further considerations:

- Too early to evaluate at operational level. Considered interesting and valuable.

- Were considered helpful with regard to data collection and management but was also highlighted their limitations from the perspective of how to counter the threats.

4.Innovations, that provide possibilities for collective response to hybrid treats. Focusing on involvement at different levels, from crowd sourcing to international collective actions

Identified points for further considerations e.g. Defence Framework:

- How to ensure that infomration is correct?
- In case on attack situation is changing too fast for system to learn and train on the data to address it correctly.
- Typically, attacks are uniquely designed and there is high probability that it will miss the new major attacks.
- Very dependent on data quality and there is not clear presentation how data quality will be addressed.
- New technologies and software upgrades are released on daily basis that it is hardly imaginable how to maintain such a framework actuality.

Next to above mentioned innovations specified remarks on common requirements, also some general points for considerations were given – they were following:

- Means for verification in different processes, starting from fact checking, debunking and going to decision making protection, it is critical to ensure machine learning credibility.
- In the case of use of any innovation it is important to address cascading effects. Therefore timely, precise communication, also with citizens, is a critical feature. All institutions having precise situational awareness to information is a key to counter measures.
- In large scale crisis it is mandatory to enable local/regional autonomous handling of life critical functions, therefore localized situational awareness and coordination should be considered as improvement. Innovations that support this are much appreciated.
- Integration of automated response protocols would be considered as one of features helping a lot to efficiently handle first stage after crisis incident report.
- For cyber incidents quick analysis features can be considered additionally (who is behind analysis, attack scale assessment).

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

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**".

As described in this document Chapter 3.1.2 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 identified to further analysis and strategy development:

- *WINS/ "What Information Needs to be Shared between Critical Infrastructure (CI) entities to detect hybrid threats and attacks, and to be prepared for them"*. Methodology.
- *EESCM/ "Enhanced and Extended Supply Chain Management".* Methodology.
- *MIMI/ "A Market place for Information Manipulation and Interference Information".* Platform and approach.
- *GECHO/ "Gatekeeping ECHO chambers".* Methodology for information sharing and cooperation, also new technological solutions to support the cooperation.

Alike during the 1st project working cycle, also during the 2nd cycle, T4.2 used its' Innovation Canvas that has been especially tailored for EU-HYBNET's purposes on innovations uptake and common requirements analysis. The T4.2 Innovation Canvas created in T4.2 is following:

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 and common requirements to it. The subtopics under each of the four main topics are following and their rationale is explained in more details in T4.2 D4.5 (M34/ Feb 2023):

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 D4.5. 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.

1.WINS/ "What Information Needs to be Shared between Critical Infrastructure (CI) entities to detect hybrid threats and attacks, and to be prepared for them". Methodology.

INNOVATION

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

  The innovation **Impact and Risk assessment of critical infrastructures in a complex interdependent scenario** has been transformed into a solution which present a methodology for how to establish what information dependent CI entities need to share in order to enhance their resilience against cascading effects and to counter hybrid threats.

  SCOPE: A methodological approach to discover what information CI entities need to share in order to enhance CI entities resilience and to counter hybrid threats.

VISION: WINS will help CI entities and law enforcement (LE) officials to recognize new forms of hybrid threats/attacks, and further fulfil requirements in this respect given in CER- and NIS-2 Directive.

MISSION: Deliver pan-European and cross-sectoral CI methodological (even standardized) approach for analysis of CI entities' critical vulnerabilities also in the context of hybrid threats/attacks. The collection of CI entities' vulnerability data is based on risk assessments and stress tests and an attack tree approach. If the CI entities share the data with competent authorities, interconnected services and other relevant stakeholders, this will eventually support CI entities to be more prepared for hybrid attacks/threats.

STRATEGY: Promote and facilitate discussions of the benefits to use and to implement WINS methodology among CI entities. Initiate a project to in detail define the steps in the WINS methodology and a guide to how it should be implemented. Initiate development of supporting tools. To promote that the WINS methodology uptake is to define *what relevant CI Data and information needs to be focused on and shared* to detect hybrid incidents based on the CER directive requirements so that CI entities may prevent future incidents.

LIMITATIONS: WINS is based on solely the interest of CI entities to conduct risk assessment (incl. e.g., stress test) with the suggested methodology. Furthermore, WINS is based on solely the information that CI entity/entities provide and voluntary exchange. Based on that analysis, an agreed data-model/methodological approach can be built to have European CI awareness picture as requested in the CER directive. Now CER Directive strives "Critical entities of particular European significance" for information sharing on severe incidents, not on voluntary basis, but sanctions. In short, to avoid sanctions the "Critical entities of particular European significance" would be more inspired to share information voluntarily also with other CI entities to enhance their resilience to crises and disruptions. Sharing CI data and information could be also done by the "data-market-house" -principle, where CI entities agree on data sharing at a certain cost.

RATIONALE: This innovation relies solely on novel methodological approach to gain relevant information and data, and their categorization that CI entities provide from their perspective; when doing their analysis in "What If"-scenarios and according to the "Attack tree" approach the CI entities may realize that they also need open data or restricted data from other domains. In general, to detect signs of hybrid threats and measure that are part of them (e.g. industrial espionage, FDI, creating economic dependencies, territorial water violation) there is a need for data also from other sectors and across borders due to the interlinked CI environment and hybrid threats landscape. Sharing of data for preparedness is not mentioned in CER Directive but this element would empower the directive's goals. Therefore, WINS will support CER Directive's enhanced implementation. In addition, WINS will support EU-level cooperation between different domains. This is seen to provide a more comprehensive resilience picture among pan-European CI entities and pan-European response to hybrid threats via the CI domain. Also, to detect hybrid threats targeted to other domains but also conducted through infrastructure domain.

- **<u>Added value proposition.</u>**

NEED: Existing CI protection (mainly based today on asset protection) has led to a situation where increased interdependencies and related risk of cascading effects across sectors are not sufficiently considered, especially to detect hybrid threats. Today, the used risk management approaches are sector and country-specific, which does not allow the forming of a coherent risk awareness between sectors or countries. There is a need for future wider attention from EU MSs and owners and operators of CI. This has clearly been stated in the new CER Directive and "Strategic Compass for Security and Defence". Identifying the most critical weaknesses in CI resilience (incl. protection) by noticing also other domains (e.g., economy, legal) influence the CI entity's action and sharing CI anomaly detection data/information will enhance CI resilience due to the analysis of what can be made once one has sufficient data available (near real-time).

Most of the critical infrastructure sectors are becoming more and more interdependent on various sectors at the same time and rely on interconnected networks and devices. Due to this interconnectedness, failures in one country or one critical sector may lead to cross-sector and/or cross-border cascading effects. The lack of awareness makes it difficult for the CI entities to anticipate these risks, which can in turn influence their ability to provide essential services in case of disruptions. Adversaries may be keen to benefit from interconnectedness and cross-sector and/or cross-border cascading effects in forming hybrid threats targeting the CI domain. Indeed, there is a need for large-scale data mining of cross-sectoral and cross-border information from CI entities which is a key enabler for CI resilience and esp. protection against external and internal threats (e.g. FDI, promoting social unrest, electronic operations, creating and exploiting infrastructure dependency incl. civil-military dependency). The focus must shift away from asset protection to one that is more systemic in nature and which recognizes interdependencies across a range of different sectors. Key aspect here is to define the CI external incident data and the hybrid threats element in it.

IMPACT: The main impact of the proposal will allow cross-sectoral and cross-border anomaly information discovery and exchange which will help to build resilience against external threats, identify systemic risks and detect hybrid threats in different CI domains but also in other domains that target to harm CI entities. The purpose is to deliver comprehensive CI awareness that delivers powerful awareness for decision-making at the following levels: domain-specific, national and EU-level in the CER Directive requirements.

VIABILITY: The viability for the solution is linked to the goals of CER Directive. The proposed techniques, use of "What if"-scenarios and attack trees are established methods.

- **<u>Stakeholders and domains</u>**

  Gaps and needs: The solution is related to the following gaps and needs as defined by EU-HYBNET deliverable (D) 2.10 "*Deeper analysis, delivery of short list of gaps and needs*".[10]

  - Threat "**Exploitation of critical infrastructure weaknesses and economic dependencies"** under the project's Core Theme "Resilient Civilians, Local Level, National Administrations"

[10] EU-HYBNET Deliverables D2.10 "Deeper analysis, delivery of short list of gaps and needs" in CORDIS https://cordis.europa.eu/project/id/883054/results.

Conceptual Model domains: The solution is foremost related to the following domains:

- Infrastructure
- Information
- Cyber

Stakeholders: CI entities, public and private companies to alert relevant law enforcement (LE) officials and authorities on hybrid threats to prevent escalation.

RESOURCES

- **Required development resources**
  The use of the WINS methodology does not require much from the methodology development side because it is to provide the frames for CI entities' own, more specific planning. However, the use and implementation of the WINS methodology by CI entities will ask for resources for planning and testing, and analysing, also to update the plans and views periodically. In short, the use of WINS should be an ongoing activity to be able to cope with new threats and attack vectors - competition for resources may be an issue in this area.

- **Required operating support system**
  EU-HYBNET had suggested during the 1st project working cycle an innovation focusing also on CI protection but called "CISAE" (A common Information Sharing and Analysis environment), and the *CISAE* was answering the question of ***how*** *to share CI information between CI stakeholders*. Now, the WINS *is answering the question and providing a methodological solution:* ***what*** *information needs to be shared to enhance CI entities' resilience to counter hybrid threats.*

  Therefore, to gain the comprehensive benefit of WINS by CI entities and law enforcement authorities pan-European-wide next to a **WINS CISAE** is much welcomed as a CI operating support system.

  In the case of CISAE, the following approach is suggested. A governance body or ENISA which would control the specifications and would oversee the operational procedures of the CISAE (incl. maintenance, updates and upgrades) would be needed. In the case of CISAE the governance body should also provide a forum for the CISAE stakeholders to discuss and share experiences and agree on CISAE improvements and extensions and the possible novelties in the use of WINS methodology. In other words, the governance body could initiate activities and research for the development of new analysis tools and approaches to WINS with CISAE.

- **CAPEX & OPEX**
  EU research projects supported by the European Commission, c. 5 -8 MEURO over 3 - 4 years. Operating costs of the WINS methodology in CI entities would limit under 1 MEURO. However, the development of the CISAE asks for more funding as explained in earlier EU-HYBNET deliverables D4.4. "*1st Innovation uptake, industrialisation and research strategy*".[11]

UPTAKE

- **Competition and market**
  The proposed methodological approach is novel in the sense that it highlights how CI entities may pay attention to hybrid threats/attacks when considering their resilience to critical risks and their key vulnerabilities. Still, there is a need to have a roadmap of how the suggested methodological approach

[11] EU-HYBNET Deliverables D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

could be accepted by pan-European CI operators widely because only in this case the CI entities may benefit fully from the commonly used methodology. After all, there are several initiatives to increase security in critical infrastructures while, and as said, the hybrid threats focus is now the novelty in WINS.

- **Funding and organization of uptake and industrialization efforts**
  The road mapping indicates that it needs to be an EU initiative behind the realization and development of the proposed CISAE -WINS. The development of a CISAE-WINS 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 an add-on to the already ongoing efforts.

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

  Barrier 1: Technological barrier
  A technological barrier would involve problems concerning integration or interoperability of sharing the discovery of anomalies related to hybrid threat campaigns as a result of the use of WINS methodology. More specifically, interoperability problems between CI entities could arise from the obsolescence of specific technological components or services, whereas difficulties with integration may come from unexpected delays in subsystem definition or implementation.

  Barrier 2: End-user skills

  WINS methodological approach asks knowledge and understanding of both Attack Tree approach and hybrid threats. However, the knowledge of both can be fairly well achieved and does not require a lot of resources.

  Barrier 3: Regulation, Ethical and Societal acceptance

  WINS methodological approach is to discover vulnerabilities of CI entities and hence the information is often sensitive. However, information on hybrid threat campaigns may also include open data and hence this may be shared between CI entities. Therefore, before sharing the data between CI entities a thorough analysis of societal impact assessment (SIA) and ethical issues needs to be conducted.

  Compliance with different types of regulation follows naturally from cooperation with public authorities and integration with existing security data-sharing environments.

  Barrier 4: Economic

  Notable economic barriers may emerge, if costs from the implementation would climb unexpectedly.

  Barrier 5: Operational barrier

  To implement the required operational structures and cooperation in information sharing, institutional and legal framework is missing.

  Barrier 6: Engagement

  To engage the relevant practitioners, end-users, and organizations in all EU MSs and to encourage them all that this is the best way to proceed.

2.EESCM/ "Enhanced and Extended Supply Chain Management". Methodology.

INNOVATION

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

The innovation **Multi-Stage Supply Chain Disruption Mitigation Strategy and Digital Twins for Supply Chain Resilience** has been transformed into a solution focussing on how to enhance and extend the supply chain management scope (EESCM, Enhanced and Extended Supply Chain Management) to take more aspects into account, provide a better understanding of the real issues and how to minimize disruption impacts.

SCOPE: Supply chain management policies and methods for Critical Infrastructures and industry, followed by enchased tooling.

VISION: An extended and evolved supply chain management reducing the effects of natural and antagonistic disruptions.

MISSION: Support CI service providers and product suppliers by building capabilities in impact minimisation and rapid recovery in response to wide supply chain disruptions, including services.

STRATEGY: Initiate and facilitate discussions for wider understanding of supply chain resilience building by including more components and layers.

Propose relevant legislation and regulations, as required, to enforce expected CI resilience.

Evaluate and, if needed, propose changes and extensions of available instruments for supply chain management. Support the instruments availability for all relevant organizations.

LIMITATIONS: There are no hard limitations. EESMC intends to cover as broad scope as possible. Limitations might appear in the instrument development stage.

RATIONALE: The period of the recent COVID pandemic followed by the Russian aggression on Ukraine brought new challenges into sectors that are critical for the safe, secure and smooth operation of our society and industries. The experienced heavy disruptions in supply chains were critical**.** Thus, there is a need to build EU autonomy in critical industrial sectors and a key aspect is to understand how supply chains are operating and which interdependencies there are.

- **Added value proposition.**

NEED: Current developments in energy sector clearly shown European dependence on raw materials from Russia. This situation so far resulted in numerous cascading effects (e.g.: providing vast feed for adversary communication, decision making process, potential influence on elections, etc.). There are plenty of other examples, occurring from trade with China or countries under Russia's and China's influence, to illustrate the need to reassess supply chain contingency measures and support industry or even higher-level organizations (associations, groups of interdependent providers of critical products or services) with tools to move to the widened scope of the assessments. The importance of building stability in supply chains are not solely the issue of industry, but also relates heavily to hybrid threats.

IMPACT: The proposed solution (policies, methodologies, followed by relevant tooling) will increase possibilities to react to natural or man-made disruptions in supply chains in general from the current international production interdependencies point of view. The impact of using proper tools to support risk evaluation and alternative supplies, widening supply management scope, will be on impact minimisation and rapid recovery capabilities responding to supply chain disruptions.

VIABILITY: The proposed solution is more of an incremental change than a disruptive step. Thus, it should be relatively straightforward, although not uncomplicated, to develop the proposed EESCM.

There are existing tools, as it is described in the Setting the scene section, that can be taken as a basis for EESCM services. Here we especially consider the use of Digital Twin based solutions which can be extended and enhanced to provide the capabilities required to broaden the scope (including services and geopolitical aspects) and make proper impact assessment, based on real examples. Also strengthen the impact minimisation and recovery components. Even though solutions are available, there is still challenges to understand the scope of supply chain and aspects of hybrid threats within the chain.

The aim of the proposed solution is to provide insights, methodology and frameworks for the industry. New approach of supply chain management then will be taken over by technological solution providers to include new functionalities in their tools.

- **Stakeholders and domains**

Gaps and needs: The solution is related to the following gaps and needs as defined by WP2 in D2.10:

  - Critical threat of Geopolitical heavyweight of domestic policy and the need to Improve geostrategic synergies towards new global frontiers.

Domains: The solution is dedicated for few domains: Infrastructure, Cyber, Space, Economy, Military/Defence, Legal and Political.

Stakeholders: The core stakeholders related to this solution are policy makers and owners/operators of critical infrastructure. In the secondary group other industry and education & training providers should be included.

Policy makers: inclusion of wide scope supply chain in related documents and development of relevant support measures.

Owners / operators of CI: inclusion of wide scope supply chain concept in contingency planning and application of innovative solutions in supply chain risk management.

Other industry: inclusion of wide scope supply chain concept in contingency planning and application of innovative solutions in supply chain risk management were considered relevant.

Education & training providers: conceptualization of the wide scope supply management and provision of relevant training.

RESOURCES

- **Required development resources**

  The set-up of the governance body or to include subject in the agenda of Critical Entities Resilience Group, to be established under CER-Directive, and to define the detailed, evidence based, research program for wide scope supply chain framework should not require any major resources.

  The roadmap proposes to start with the development of the wide scope framework. We find it reasonable to start two-three one-year projects for these tasks with total budget of 4 MEURO. Coordination of research activities should of course be encouraged/enforced.

  Testing can be made in a similar manner, so after two years period the complete enough framework is ready for deployment.

  Assessment of availability and completeness of methodologies and tools can also be done within one-two year with similar funding. At this point it should be decided if additional efforts are needed for functionalities development.

  Governance body or the above-mentioned Group, could start implementation of regulatory measures or recommendations.

  Additional supporting funding requirements in line with CER-Directive can be estimated at this point also.

- **Required operating support system**

  The logic proposed in the roadmap suggests, that initiation of the framework and preparation of tools can be organised at EU level. National supportive funding can later be decided individually by MS.

  The same applies to the tooling issue. If the framework becomes obligatory (as a standard, as a requirement of other form), industry will provide commercial solutions for the market. Those can be developed as bay-in solutions or provided as service.

  The governance body should remain active, mainly focusing on impact assessment and update.

  It might lead to some complex initiatives, requiring EU level interventions, to minimise potential disruptions. Governance body should consider managing such issues as well.

- **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 8 – 12 MEURO.

  It is difficult to assess potential costs for implementation of functional requirements if they appear to be needed. Part of costs can be taken by solution providers. The same applies to the national level support instruments.

  The total cost to launch such an action as proposed here would then be in the order of 10 – 15 MEURO over 3 - 4 years. Other costs can occur at later stages, but expected to be absorbed by solution providers or MS.

UPTAKE

- **Competition and market**

There are several methodologies and tools for supply management available, as described in the Setting the scene section. Risk of disruptions is also addressed in contingency planning. This proposes that the market is well functioning in the area.

The proposed change at the high level includes widening the scope by adding services and geopolitical aspects, enabling more precise, real live based, impact assessment, capabilities to assess impact minimisation and recovery time scenarios.

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

  There are no specific thresholds for uptake, as innovations considers wider scope and different focus of activities already implemented and services / solutions already available and used by many relevant entities. Funding is required at the initial stage to move the subject to other level.

- **Barriers**

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

  - To convince the EU that this is the right way to proceed. Supply chain management is a subject of each organization and might contain confidential information.
  - It might be challenging to agree on the wider scope interpretation, especially inclusion of geopolitical and other aspects related to hybrid threats in the framework.
  - Development of new understanding is rather time consuming while regulatory measures might be not well accepted. Actual resilience should be developed by a big number of organization and probability versus costs should be estimated.
  - Widened scope and shifted focus might require additional funding for organisations. It is not clear how much of new concept of the supply chain management can be implemented on voluntary bases.
  - New concept, especially inclusion of geopolitical aspects, might disclose some sensitive information.

3.MIMI/ "A Market place for Information Manipulation and Interference Information". Platform and approach.

INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**
  The innovation **DDS-alpha** (the Disinformation Data Space – alpha) has been transformed into a solution focussing on how to build a market and **A Market place for IMI Information (MIMI)**.

  SCOPE: A European IMII sharing solution.

  VISION: A secure and trusted market place for IMII sharing which is embraced by IMI data providers, analysts and consumers.

  MISSION: Build a European community of IMI data providers, analysts and consumers which embrace the idea of a market-based IMII sharing solution.

Define and agree the business model.

Define and agree functional requirements on the sharing platform for a secure and controlled information exchange supporting the business model.

STRATEGY: Develop a strong and convincing storyline proving the benefits of a general IMI exchange which takes all existing barriers into account. Elect evangelists.

Study existing business models used by stakeholders for existing IMI exchange solutions. Synthesize a business model acceptable for all which would stimulate current stakeholders to exchange IMI information.

Design a service platform on top of DDS-alpha including required DDS-alpha extensions required for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it only considers the sharing aspects and how to stimulate stakeholders to share their IMII.

RATIONALE: It has been recognized that one barrier is the problem of having access to all required information when aiming for exact and detailed real-time data and situational awareness covering all aspects of IMI activities and campaigns. With the proposed MIMI solution, the barrier would be reduced/eliminated as there would be a direct business value in sharing.

- **Added value proposition.**

NEED: Sharing of IMII is needed to enable production of high quality and detailed situational awareness regarding IMI activities and campaigns.

IMPACT: Increased sharing of observations and IMII base as well analysed data would improve situational awareness in terms of quality and timeliness and improve the possibilities for speedy mitigating actions and interventions. MIMI will serve the governmental and security sectors, which require in-time and complete information to enable fast reaction. Private sector companies (particularly online platforms) may benefit from a systematic inflow of threats observed and flagged to them for interventions.

A market-based solution like MIMI, with a mixture and private companies, organizations and government institutions at different levels as stakeholders, would most likely develop into an efficient market economy solution and thus be driving force behind increased sharing of IMII. The alternative is to regulate sharing, which will remove many incentives as it will mainly be a cost driver

VIABILITY: That there is a market for threat information is clearly verified by e.g., the business around CTI with several (vertical) companies. Furthermore, the DDS-alpha initiative from EEAS StratCom shows the need and when there is a need there is a market.

- **Stakeholders and domains**

GAPS AND NEEDS: The solution is related to the following gaps and needs as defined by WP2 in D2.10[12]:

[12] EU-HYBNET Deliverables D2.10 “Deeper analysis, delivery of short list of gaps and needs” in CORDIS https://cordis.europa.eu/project/id/883054/results.

- Lack of tools to tackle information manipulation / Lack of data on disinfor-mation impact impairs anticipation.
- Lack of awareness of interference / Lack of horizontal public private governance and risk assessment.

CONCEPTUAL MODEL DOMAINS: The solution is in the Information domain.

STAKEHOLDERS: Actors specialized in monitoring of disinformation campaigns or the collection and analysis of IMII will also be important stakeholders. Core stakeholders are of course also the Member States' practitioners involved in monitoring, handling and countering disinformation campaigns. Private platform and media companies will also be important stakeholders in a MIMI solution.

RESOURCES

- **Required development resources**
  The roadmap proposes an EU funded project to establish MIMI. Resources will be required for the "marketing" of MIMI, investigation and proposal of relevant business models. Furthermore, the development and a first implementation of the service platform will be required. We find it reasonable that a three-year 4 MEURO project would be able to perform the required actions and achieve the goals.

- **Required operating support system**
  Organizational support after the establishment of MIMI would be the work performed in the suggested MIMI interest group. The work in the interest group should be financed by its members but would not require any substantial resources. Any required updates of the service platform should be integrated in the future developments of DDS-alpha.

- **CAPEX & OPEX**
  As the roadmap only proposes the set-up of one EU funded projects to establish MIMI the CAPEX would be 4 MEURO. Thereafter operational costs will part of the DDS-alpha operational costs and are hard to estimate, however these costs should be limited.

UPTAKE

- **Competition and market**
  MIMI is a unique solution and there are no similar competing solutions. Possible competition could appear from already established players that work in vertical silos.
- **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 MIMI. This solution would most likely never happen without such an initiative and the required corresponding funding. There is also a need that MSs embrace the idea and that national stakeholders are prepared to join in using MIMI. Furthermore, we note that the EU already has a number of activities in the area of handling and understanding disinformation and that MIMI just would be a relatively small extension of the already ongoing activities.
- **Barriers**

  The only identified barrier, which the MIMI solution actively tries to break down is the acceptance to use a marketing solution for IMI sharing.

There may also be efforts from antagonistic actors, trying to stop the establishment of MIMI by claiming that it would increase the surveyance and control of citizens in MSs and impact and limit their freedom of expression.

4.GECHO/ "Gatekeeping ECHO chambers". Methodology for information sharing and cooperation, also new technological solutions to support the cooperation.

INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**
  The innovation **Identify and safeguarding vulnerable individuals**[13] has been transformed into a solution that **monitors the online environment, identifies where and how interventions are needed, thereafter launching the appropriate actions to build resilience in vulnerable young people against possible entrapment in violent extremism and terrorism**. The solution is called Gatekeeping ECHO chambers (GECHO).
  GECHO is for countering violent extremism and terrorism, as antagonistic states and organizations may use support of local groups that promote violent extremism and terrorism as one tool in their hybrid threat toolbox. This to widen sociocultural cleavage and reduce trust in the society.

  SCOPE: Building resilience in vulnerable young people against online entrapment in violent extremism and terrorism.

  VISION: Young people will be resilient against online content that advocate, incite, promote or justify hatred, violence, terrorism and discrimination.

  MISSION: Ensure that young people when traversing online environments promoting ideas of hate, violence, terrorism and discrimination also encounter, absorb and internalise content/information, which counter such ideas.

  STRATEGY: Develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. Enable sharing of situational data between stakeholders.

  Develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites.

  Develop easy to follow validated frameworks, methods and tools for creation of practical locally adaptable means for prevention of online recruitment of young people into groups promoting violent extremisms and terrorism.

  Ensure that a research networking organization exists which promotes and coordinates required research efforts needed to better understand the drivers behind radicalization, to develop countermeasures and validate their impact.

  Establish a systematic knowledge base and means for collecting and sharing of frameworks, methods, tools and research results in a searchable database. Liaise, cooperate and share information with existing practitioner networks.

[13] See D3.4 First Mid Term Report on Improvement and Innovations, Section 4.3.2 p80.

Initiate training activities for first line practitioners to

1. Get to know the proposed frameworks, methods and tools presented, including online behaviour guidelines.
2. Understand the reasoning behind proposed countermeasures and interventions.
3. Become proficient in their use and how to adapt them to different online environments.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern direct identification of vulnerable individuals as this most often would be in conflict with GDPR and that it is mainly targeting young people.

RATIONALE: Countering/Preventing violent extremism and terrorism is a wide area and concerns many aspects, but at the core it is about reducing the number of supporters and followers. One way of achieving this is to focus on the most vulnerable groups and counteract on their radicalization. As online platforms play an increasingly important role in the recruitment process and are abundant and easily accessed it is a logical consequence to spend substantial efforts in developing online countermeasures.

- **Added value proposition.**

NEED: There is a need to provide means to reduce the number of followers and supporters of groups that promote violent extremism and terrorism. This need is validated by the many initiatives from different global, EU and national organizations and networks working in the general area preventing/countering violent extremism and terrorism.

IMPACT: In GECHO, the proposed platform for surveillance and situational awareness will allow that countermeasures against recruitment into groups of violent extremisms and terrorism can be launched with high precision, earlier and more effectively than has been possible before. The proposed research will review existing, develop new, and validate efficient and rapid automatic countermeasures together with human intervention strategies. The proposed countermeasures will be integrated in frameworks for deployment in different extremism environments and have easily adaptable methods and tools to become fit for purpose. In the research one strand of actions is targeting a better understanding of drivers and what constitutes effective counter means.

VIABILITY: The viability of the GECHO surveillance and situational awareness platform solution can be deduced from activities in related areas like EEAS Stratcom activities around FIMI [14] and the development of a Disinformation Data Space (the DDS-alpha platform[15]). Another platform was proposed in the first cycle project cycle of EU-HYBNET, the CISAE for disinformation[16] which easily can be adapted for the current target area. To ensure that a research networking organization would exists it could be possible to delegate this responsibility to an existing body e.g., the RAN (the Radicalization Awareness Network) or expand the VOX-pol network of excellence mandate. If judged more efficient a new networked research organization like EDMO,

[14] EEAS Stratcom, 2022 Report on EEAS Activities to Counter FIMI.
https://www.eeas.europa.eu/sites/default/files/documents/EEAS-AnnualReport-WEB_v3.4.pdf
[15] Innovation the DDS-alpha description can be found in D3.2.
[16] EU-HYBNET Deliverables D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS
https://cordis.europa.eu/project/id/883054/results

the European Digital Media Observatory (EDMO) could be initiated. EDMO is a Europe wide network built around a few core partner organisations and several national and regional hubs.

- **Stakeholders and domains**

GAPS AND NEEDS: The solution is related to the WP 2 defined gap and need *Promoted ideological extremism* in Core Theme *Information and Strategic Communications*, see D2.10. It is also related to Core Theme *Resilient Civilians, Local Level and National Administration.*

CONCEPTUAL MODEL DOMAINS: The solution is related to the following domains:

- Cyber,
- Culture,
- Social,
- Legal,
- Intelligence and
- Information.

STAKEHOLDERS: The core stakeholders of course are the Member States first line practitioners, e.g., social care workers, police, teachers and NGOs like RAN, that meet vulnerable individuals in danger of becoming radicalized. Furthermore, local level as well as support functions will be heavily involved in the monitoring of online activities and launch of countering activities. Finally, the research community and ministry level functions will have to be involved in providing resources to research, to develop countermeasures, and to build and maintain overarching situational awareness. The responsibility for the realization of the solution will lie on ministry level and the commission. Actors specialized in monitoring of online activities by violent extremism and terrorism groups as well as tech companies developing tool for such monitoring will also be important stakeholders.

RESOURCES

- **Required development resources**

The roadmap proposes one or more EU finance projects to establish the required knowledge base and to develop the framework, methods, tools and training material. The required development resources for this part of the work will be researchers in P/CVE and related areas. We find it reasonable to start three, three-year 3 MEURO projects for these tasks, out of which one should be on AI tools and methods. The establishment of a more permanent research cooperation community, based on the same principles as for EDMO, would likely have a somewhat lower cost than the EDMO had and could be in the order of 4 MEURO. Extending it with satellite nodes as EDMO has, would be in the same order.

The set-up of the governance body and to define the detailed, evidence based, research program following the proposed solution should not require any major resources.

The work on local and regional levels with adaptations of the methods and tools will require involvement of local experts and admin personnel. It is hard to estimate the total efforts required before knowing what the framework, methods and tools 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 experts and

authorities, 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, methods, tools, and training material with their local adaptations will look like. But the update and upgrade work will most likely require efforts in the order of several 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 15 MEURO.

  The initial local adaptions would, if they require 1 - 3 man-years per Member State and end up to about in same order. The same effort would probably be needed for the continues updates and grades the coming years.
  The total cost to launch such a comprehensive action as proposed here would then be in the order of 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be of the same order, that is 3 – 4 MEURO per year but financed by each Member State.

UPTAKE

- **Competition and market**
  There are a great number of initiatives in the field of P/CVE and there are tools and training material available. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the GECHO solution. Examples on ongoing initiatives in can be found in the setting the scene section.

- **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 and national support for the required local adaptations. The proposed coordinated work would most likely never take place without such an initiative and the required corresponding funding.
- **Barriers**
  Required actions that may became 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 P/CVE is high on the EU agenda.
  - To engage the MSs in the work and get them involved.
  - To attract the right competencies and expertise for the required research and development activities
  - To get acceptance from and liaise with already existing groups and initiatives in the area of P/VCE.
  - To organize the funding of the research activities and the related local adaptations.

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

During the reporting period EU-HYBNET T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) delivered also insights to the second Three Lines of Action in the 3rd Future Trends Workshop

(FTW) arranged by EOS and MVNIA in Bucharest during 19/4/2023. Comprehensive description on FTW is delivered in D.3.16 "3rd *Future Trends Workshop Report*" (by MVNIA, M35/May 2023). The chapters below summarizes key findings of FTW from D3.16 what comes to Second Three Lines of Action "**Common requirements as regards innovations that could fill in gaps and needs**".

EU-HYBNET 3rd Future Trends Workshop (FTW) provided a platform of interaction on emerging hybrid threats in the EU's neighbourhood, their implications for the future of EU security and potential innovations to counter them. Discussions between academics, researchers, institutional stakeholders at national and EU level, civil society representatives and practitioners were extremely useful as they allowed enhancing of awareness, shaping of new perspectives, better understanding of the interdisciplinary character of the challenges addressed while, at the same time, facilitated transfer of knowledge.

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

Break-out session #1: Future Trends in Cyber and Future Technologies

Description. This session looked at the current EU security environment as a whole and addressed hybrid threats arising from Cyber and Future Technologies to allow participants to identify the most pressing future trends in this field, as well as the innovations that could support the work of pan-European practitioners. The discussion was split in three building blocks:

1. persistent and recurring threats already identified by practitioners in the first two cycles of the EU-HYBNET project (e.g., threats related to quantum computing);
2. developing trends identified by the 3rd EU-HYBNET Gaps and Needs assessment as well as the European Commission (e.g., vulnerabilities related to space and GPS navigation infrastructure);
3. new and shifting trends in the tech sector (e.g., foreign investments in social media platforms, filtering techniques applied by social media gatekeepers, social change brought by AI developments and initiatives, the metaverse, AI and ML operations, supply chain dependencies and their impact on clean tech). Participants will also have the opportunity to discuss innovative solutions and receive a demonstration of how the technology is working.

Innovations. In the frames of the three topics/ blocks, various innovations that were brought under discussion. The list below summarizes the names of the innovations and key slogans on the priority requirements for their development and uptake. Innovations were:

- DLT/Distributed Ledger Technologies -> Financial market change (oil/gas, strategic resources, monetary power)
- AI Technologies -> content & information market change, cheap fakes, mass adoption, data economy
- Cyber offensive technologies -> EU capabilities
- Crisis of trust -> age of mass anxiety, slowdown of progress & collaboration
- Rise of decentralized businesses and infrastructures
- Quantum computation capabilities, HPC -> who first?
- Innovation maturation, uptake and operationalization speed
- Control of strategic innovation & knowledge development dissemination, access, export
- Global education and students from foreign territories
- Innovate as you go
- Adoptability by design (organization, competence, infrastructure)
- Capability to act and respond autonomously (decentralized battlefield concept)
- Future tech inclusion in primary and secondary education, issue with teachers
- Cyber attacks backed by AI, autonomous AI operations
- Cyber defence backed by AI
- Increasing collaboration with increased transparency

In general, participants agreed that quantum computing, cyber technologies, use of AI, social media security etc. represent instruments potentially weaponizable against democratic order and that should be approached in a security by design perspective. As features of an optimal approach, were mentioned: rapid adaptation, need to adopt emerging technologies, provide security by design formulas, digital education etc.

Break-out session #2: Hybrid threats in the Arctic

Description. This session started from the premise that the Arctic region is already (and will continue in the future) to be experiencing increased targeting via diverse non-conventional hybrid threats. This is particularly relevant given the ongoing accession talks of Finland and Sweden into NATO. The northern part of Europe is still very vulnerable due to small population concentration (compared to the south), poor infrastructure (e.g., supply lines, roads), lack of investment, vulnerability to "sympathetic" narratives etc. The region is very remote and forms a key part of the EU's external borders in the current geopolitical environment, while also being close to critical third-country-owned military bases. Third-country defence in the area is more than likely to be of a non-conventional nature

than conventional, and could involve the manipulation and destabilization of the northern regions, to cut them off from their capitals if not physically (territorial capture) then by all other means necessary including cyber-attacks on infrastructure, sabotage (including water sources), mis- and disinformation, and attempts to network and build up 5th columns. This could destabilise the entire northern region of Europe.

Innovations. The key take away was that innovations that will support foresight to hybrid threats are much needed under various topics. After all it was concluded that the Arctic region is likely to remain a vulnerable target for hybrid threats, due to its geographical profile which makes hybrid tactics difficult to detect (wide surface, dispersed population, severe climate conditions, limited infrastructure and reconnaissance capabilities).

Break-out session #3: Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats

Description. Starting with an overview of current security threats arising from disinformation as a hybrid threat, in this session participants worked towards identifying the challenges and needs of practitioners in countering this phenomenon, existing technological and non-technological solutions as well as the need to adopt a more anticipatory outlook. What trends can be identified for the future outlook of disinformation? The EU Code of Practice on Disinformation was discussed and evaluated: how does it address disinformation used by foreign actors especially given the current threat landscape, as well as emerging trends (AI-produced disinformation, ownership changes in signatories etc)? The French Ministry of Ecological Transition also presented their perspective and needs when it comes to protecting strategic assets, values and the economy against disinformation. Taking into consideration these trends, participants discussed required innovations that could assist the work of hybrid threats practitioners through an integrated and anticipatory approach.

Innovations. During the session there was discussed the need for a multidimensional and comprehensive response to propaganda and disinformation, based on both strict regulations and self-regulatory initiatives. Among the necessary steps forward there was mentioned the need for better consolidated cooperation between state institutions and private sector, and the need to focus not only on external actors, but also those internal to democratic societies. As promising practices and regulations, participants mentioned the Digital Services Act, The Code of Practice on Disinformation Signatories, the French inter-institutional working group on the topic.

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

As mentioned in chapter 3.2, during this document reporting period the third cycle of the project (M35 -M52/ March 2023 – August 2024) 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 M35 (March 2023). Because the gaps and needs analysis and deliverables are consortium only (CO), only general themes on present gaps and needs can be mentioned in future EU-HYBNET public deliverables. However, the general topics will ease EU-HYBNET

to map and to analyze promising innovations to the gaps and needs in order to serve pan-European security practitioners and other relevant actor (industry, sMEs, academia, NGOSs) to counter hybrid threats. The general formulation will base on T2.1 "*Needs and Gaps Analysis in Knowledge and Performance*"/ D2.7 "*Long list of defined gaps and needs*" (by Hybrid CoE) and T2.2"*Research to Support Increase of Knowledge and Performance*"/ D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (by JRC). In the next six month action report (D1.11, M42/ Oct 2023) general themes will be described in order to provide contribution to the second Three Lines of Action "Common requirements as regards innovations that could fill in gaps and needs".

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

In EU-HYBNET the WP4 *"Recommendations for Innovations Uptake and Standardization*" and two of its Tasks have delivered main contribution during the reporting period to the Three Lines of Action "**Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation**" – the WP4 Task has especially been Task (T) 4.3 "*Recommendations for Standardization*" (lead by the Polish Platform for Homeland Security/ PPHS) but also T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE) have provided valuable findings. The following subchapters describe the contribution from each of the named tasks.

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

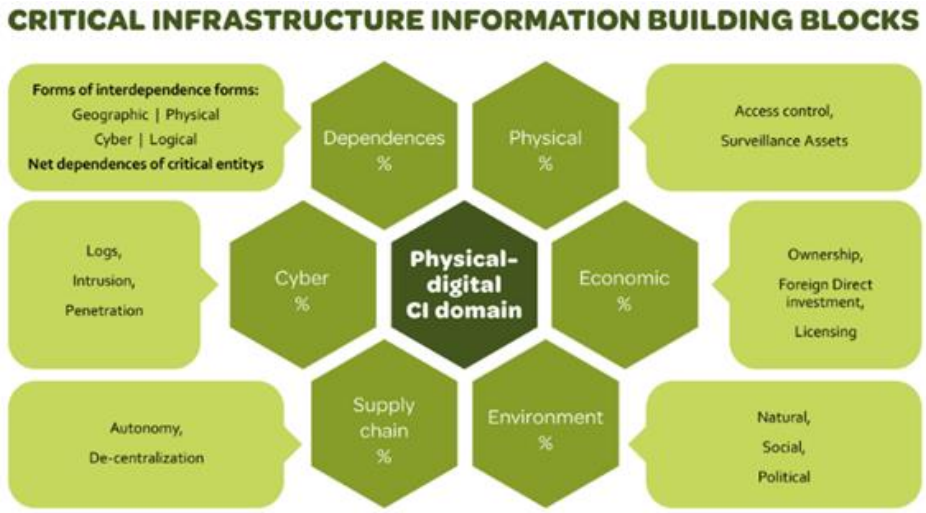
The T4.2 "*Strategy for Innovation Uptake and Industrialization*" (lead RISE) contribution to the third Three Lines of Action "**Priorities as regards of increasing of knowledge and performance requiring standardization**" is well highlighted in T4.2/ D4.5 "*2nd Innovation uptake, industrialisation and research strategy"* in M34 (February 2023). In short, D4.5 describes four most promising innovations (acronyms: WINS, EESCM, MIMI, GECHO) for innovation uptake and in the analysis also insights to existing standards or standardized actions are highlighted to support the uptake. Each of the T4.2/D4.5 identified and promoted innovation with relevant standards or standardizations needs are described.

WINS/ *"What Information Needs to be Shared between Critical Infrastructure (CI) entities to detect hybrid threats and attacks, and to be prepared for them".* Methodology.

The central idea of WINS is that Risk management is key to finding the right data to be shared. In short, WINS is an innovation to serve critical infrastructure (CI) risk management that is often static and done in silos without a common view or understanding of risks. The data analysis tool is needed to detect and identify risks continuously across sectors, feeding risks for CI assessment on anomaly to data sharing, which was the EU- HYBNET CISAE proposal 2021 answering to the research question on **how** to share information. However, now WINS proposal introduces a collaborative multi-criteria data management methodology example for identifying, assessing, analysing, and managing CI risks. This allows the adoption of multiparty interdependency and cross-impact analysis for the EU MS and CI entities.

In general, existing data models are mostly isolated to single organizations or single domains and the overall risk landscape is missing. The state-of-the-art explicitly determines the structured data in relational database frameworks. State-of-the-art data management focuses on an integrated, modular environment to manage organizational application data. Also, corresponding risk prediction tasks are scoped to one domain only. Managing prediction of emerging risk functionality over a multi-organizational domain environment is limited. Therefore, in WINS proposes the use of "*What-if*"

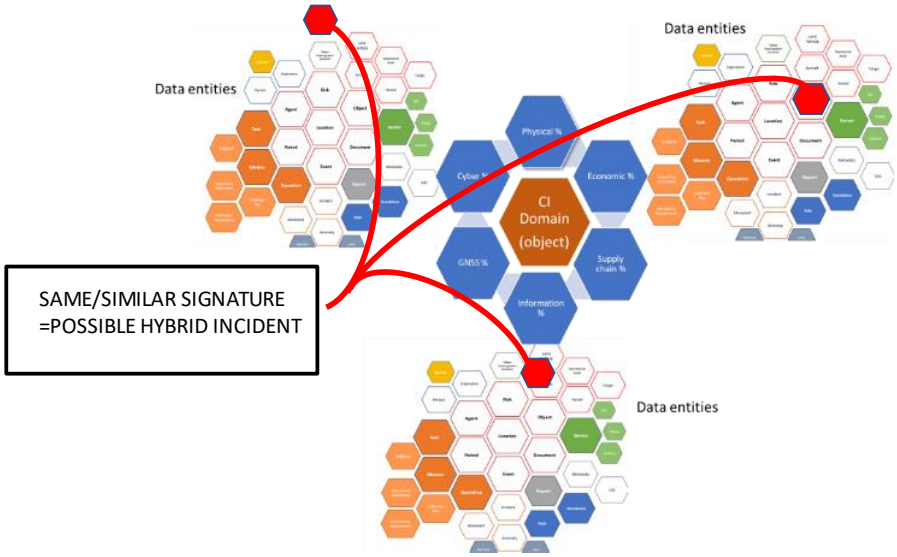
scenarios and an “Attack tree” approach so that each CI community can identify risk areas and their data/information details to be shared. According to the following example, risk related data can be e.g. divided into 6 different risk areas where data is collected from each particular risk category into the one holistic risk data landscape of the critical infrastructure domain.



Picture above provides an example of risk data environment where risk awareness can be built. The approach could lay basis for a standard.

Critical infrastructure (CI) systems and sub-systems continuously generate aggregated data in the format of key performance indicators, counters, events, and alarms from all their components. It is worthwhile to analyse and correlate all these different types of data to one data environment, where the detection of anomalies gives early indicators of compromise/attack. This systemic anomaly detection solution allows CI providers to early detect hybrid threats and early prevent larger effects on the European CI. Even though it is not part of CI entities duties to detect that something what occurs is in fact that part of a broader hybrid threat campaign, still this information discovery may now be reached and support CI entities to be prepared for further challenges and/or support to reduce and cut the strength of the hybrid threat campaign. E.G. by knowing that certain foreign direct investments together with cyber espionage and riots have in other similar CI entities cases followed by exploiting thresholds, gaps and uncertainty in law and harming in this way CI entities functions may provide situational awareness on emerging risk and hybrid threat campaign.

In order to establish WINS, a proposal is to classify hybrid threats related incidents. If there is a systematic attack approach with the same signature (anomaly) repeating (digital or operational procedure), we can assume that there is a hybrid threat campaign with various elements ongoing, if we can connect this incident to simultaneous influencing to decision-making; all play their parts. This data-model approach supports the decision-support approach for CI entities’ risk (anomaly) findings.



Picture above describes how connecting dots will lead the operator to the roots of the hybrid threat attack/ activity. Again, standardized approach would support comprehensive surveillance picture.

The creation of a comprehensive WINS methodology for pan-European CI entities would require the set-up of EU research projects supported by the European Commission alike creation of standards that would support WINS uptake.

EESCM/ "*Enhanced and Extended Supply Chain Management".* Methodology.

The importance of supply chain in many aspects is described in different EU strategic documents, e.g., the plan of action for strengthening the EU's security and defence policy A Strategic Compass for Security and Defence[17] highlights the subject in scope of global competition, overall economic security, space industry, disruptive technologies. The document also states that to reduce dependencies "In 2023, we will assess, together with the Commission, the risk for our supply chains of critical infrastructure (CI), in particular in the digital domain, to better protect the EU's security and defence interests." Also, CER- Directive[18] acknowledges the importance of supply chain pointing out the recovery from incidents, including business continuity measures and the identification of alternative supply chains, as one of the key resilience measures of critical entities. The CER-Directive also establishes the governance system, that is very much relevant to the solution proposed.

The above depicted situation shows that there are three main aspects that needs to be covered, also in the view of possible standards:

- To increase the resilience of the critical infrastructure (CI) by creating an understanding of the need to extend the scope of supply chain management. This aspect includes not only the wider

[17] https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
[18] EUR-Lex - 52020PC0829 - EN - EUR-Lex (europa.eu) Article 11.

consideration of materials and supplies, but also inclusion of services and the aspect of origin. It is also essential to extend the depth of supply chain management, covering end-to-end chain.

- To model and estimate with greater accuracy the consequences and cascading effects of supply change disruptions and go from theoretical estimates to real and verified developments. Actual disruptions and their impacts must be used for a thorough check models and their calibration. Improved models would offer opportunities not only to evaluate the resilience of supply chains, but also to develop mitigating strategies.

- To support organizations with state-of-the-art instruments to enable proper supply chain management and alternative sourcing. There are existing commercial tools for supply chain management. However, the required broadened scope is not covered. A viable development would be to consider the use of Digital Twin based solutions which can be extended and enhanced to provide the capabilities required in the broadened scope and to make proper optimisations, impact assessments and risk identifications, as described in the EU-HYBNET project deliverable D3.4 section 1.1.2.

The EU-HYBNET project deliverable D3.4 section 1.1.2. proposed on of the tools – anyLogistix[19]. But there are many others in the market. Just to name the few: Shippabo[20], Magaya Supply Chain[21], FreightPOP[22], Precoro[23], Lagiwa WMS[24], SAP supply chain[25] and many more. They have different functionalities, but all provide possibilities to digitalise the procurement process, vendor and supply management, warehouse management, optimization, assets productivity maximisation, alternative supply modelling and many other sector specific or generic components. At the same time, we note that even though many tools are available, there are still challenges to understand and define the relevant scope of supply chain management in view of hybrid threats within the chain. Current tools are focused on goods mainly and hardly include services. There is no proper functionalities enabling geopolitical risk and impact assessment, they do not include cascading effects or other threats of hybrid nature, they lack impact minimization and recovery planning features. Current instruments are build based on the traditional understanding of supply chain, while the proposed solution is focused on wider concept of supply chain and not on optimization of current procedures. Again, standardized approach is seen as a ned to empower the situation.

MIMI*/ "A Market place for Information Manipulation and Interference Information".* Platform and approach.

It has been recognized that a solution for efficient sharing of IMI (information manipulation and interference) Information (IMII) between concerned stakeholders is a key element in the EU Member States' efforts to improve societal resilience against national and foreign IMI activities. This fact is corroborated by the actions and activities by the EEAS Strat.Com. directed at designing and

[19] https://www.anylogistix.com/business-challenges/supply-chain-risk-assesment/
[20] www.shippabo.com
[21] www.magaya.com
[22] www.freightpop.com
[23] Best Procurement Software for Small and Midsize Businesses | Precoro
[24] www.logiwa.com
[25] www.sap.com/products/scm.html

implementing such an IMII sharing platform where Disinformation Data Space (DDS-Alpha) has played a noticeable role. This is also communicated in the EU-HYBNET Policy Brief no 3, *Build Societal Resilience – Share IMI* Information* that was written together with RISE and EEAS/Strat.Comm. The need is thus established but the means to ensure wide sharing and exchange of IMII still remains to be comprehended.

*All providers of IMII see the IMII as an asset in their operations and business and thus would providing free access to this asset be problematic for most stakeholders. Furthermore, private companies and organizations might be hesitant or not at all willing to freely share IMII, either because of the IMII business value (like Cyber Threat Intelligence) or that the information may be business sensitive. To overcome these challenges and issues and to provide a solution which complies with the mentioned baseline requirements, EU-HYBNET propose that a market and market place (MIMI) for IMII is established. For this to be possible there is a need for a

1. Trusted and secure IMII sharing platform
2. Initial business model which is accepted by all stakeholders
3. Integration of a charging solution in the sharing platform which is compliant with the business model.

The requirement 1) for a trusted and secure IMII sharing platform is satisfied by the EEAS/Strat.Comm. DDS-Alpha innovation because with DDS-alpha, a taxonomy and standards for describing and coding of IMI observables is established; This greatly facilitate the sharing of information. The main standards used are STIX, a language and serialization format for exchange of Cyber Threat Information (CTI) and TAXII, a CTI data exchange protocol. This are also then promoted as standards for future initiatives tackling information manipulation and interference Information (IMII). One of such an initiative is the EU-HYBNET's proposed solution MIMI.

GECHO/ "*Gatekeeping ECHO chambers".* Methodology for information sharing and cooperation, also new technological solutions to support the cooperation.

EU-HYBNET recommends to develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. The goal is to enable sharing of situational data between stakeholders. To achieve this goals there is need for development of easy to follow validated frameworks, methods and tools for creation of practical locally adaptable means for prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. This innovation is labelled as "GECHO".

An EU standardized platform for (semi-)real-time collection and sharing of such information would be a starting point in the creation of GECHO. The viability of the GECHO surveillance and situational awareness platform solution can be deduced from activities in related areas like EEAS Stratcom activities around FIMI [26] and the development of a Disinformation Data Space (the DDS-alpha

[26] EEAS Stratcom, 2022 Report on EEAS Activities to Counter FIMI.
https://www.eeas.europa.eu/sites/default/files/documents/EEAS-AnnualReport-WEB_v3.4.pdf

platform[27]). Another platform was proposed in the first cycle project cycle of EU-HYBNET, the CISAE for disinformation[28] which easily can be adapted for the current target area of GECHO - The core concept would be to have situational awareness entities in all participating Member State that share and exchange information in a common standardized format based on (extensions) to existing standards like STIX and TAXII. It is seen that the development of the GECHO platform for surveillance and situational awareness would require the setup of a project organization to formulate detailed requirements and use of standards (or to be standardized formats) for information sharing. An integral part of the project would be to take care of the initial development of the AI-based tools required. A steering group of key stakeholders should oversee the project work. A possible driver for the platform development work could be EUROPOL.

Furthermore another vital starting point to establish other key components to establish GECHO are further research on underlying factors for being attracted to violent extremism and on how interventions and countermeasures should be realised. For research EU and international research networks and sharing their results and solutions in order to gain standardized approaches and best practices would be a central activity to take care of as well.

To ensure that a research networking organization would exists, it could be possible to delegate this responsibility to an existing body e.g., the RAN (the Radicalization Awareness Network) or expand the VOX-pol network of excellence mandate. If judged more efficient a new networked research organization like EDMO, the European Digital Media Observatory (EDMO) could be initiated.
In general, the need to established GECHO is in-line with present EU initiatives. In short, EU has adopted the EU Counter-Terrorism Strategy [29] and the Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism[30]. These strategy documents together with the Final Report[31] from the High-Level Commission Expert Group on Radicalisation (HLCEG-R) and the recent new Counter-Terrorism Agenda[32] provide a number proposals for countering violent extremism and terrorism. We note here that

- There is an EU strategic commitment to prevent people from being drawn into terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment to terrorism, in Europe and internationally;
- The responsibility of combating radicalisation and terrorist recruitment lies primarily with the Member States, but that EU efforts in this field can provide an important framework to share good practices; The good practices may support to create standards for future work.
- There is a need to develop a strategy to address radicalisation in all of its forms; and
- Measures to counter radicalisation and recruitment need to take account of the diversity of modern society and modern communications.

[27] Innovation the DDS-alpha description can be found in D3.2.
[28] EU-HYBNET Deliverables D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results
[29] EU counter-terrorism strategy
[30] Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism
[31] https://op.europa.eu/en/publication-detail/-/publication/04756927-97bc-11e9-9369-01aa75ed71a1/language-en
[32] Counter-Terrorism Agenda

Furthermore, to fight against terrorism, the European Commission has put forward a series of voluntary and legislative measures and initiatives to help mitigate the terrorist and radicalization threat. One relevant example is the regulation on addressing the dissemination of terrorist content online33 as of 7 June 2022. The regulation sets out EU-wide rules to tackle the misuse of hosting services for the public dissemination of terrorist content online. The regulation sets out a number of measures to address the public dissemination of terrorist content online. Based on the Regulation, terrorist content must be taken down within one hour after it is identified online. This applies for online platforms offering services in the EU, to ensure the safety and security of citizens. At the same time, the Regulation puts in place strong safeguards to guarantee that freedom of expression and information are fully protected. One may note here that we speak about standardized approaches.

To conclude and to support uptake of GECHO, we want to first reference one successfully developed and widely deployed method and then one study report. The first refence is to a solution from Moonshot, the Redirect Method[34]. It is an open-source methodology that uses targeted advertising to connect people searching online for harmful content with constructive alternative messages. Piloted by Jigsaw and Moonshot in 2016 and subsequently deployed internationally by Moonshot in partnership with tech companies, governments and grassroots organizations, it uses pre-existing content made by communities across the globe, including content not created for the explicit purpose of countering harm, to challenge narratives which support violent extremism, violent misogyny, disinformation and other online harms. The study report is a report in Swedish titled *Webbpoliser, gaming och kontranarrativ : Digitalt förebyggande arbete mot extremism och våldsbejakande extremism*[35] (Google translate: *Web police, gaming and counternarratives: Digital prevention efforts against extremism and violent extremism*) by Linda Ahlerup and Magnus Ranstorp at the Swedish Defence University. It discusses the digital arena and preventive measures with respect to violent extremism and reviews 15 innovative and successful methods and tools[36] for how to use the digital arena in preventive work. One conclusion is that there is a need for many different initiatives with different functions and focus areas and that they often need to be integrated in a wider strategy and plan of actions. If an standardized approach or best practices could be discovered even more clearly that is seen optimal.

As a conclusion it can be stated that there are a lot of organizations, initiatives and projects that focus on fighting against radicalization/terrorism in a global way but what is missing are:

- A platform for online situational awareness with respect to violent extremism and terrorism. The platform should comprise functions for real-time sharing of available information.
- AI based tools for rapid and accurate discovery of new sites related to violent extremism. Monitoring of activity levels at known sites and visits by new users.
- A standardized taxonomy which is accepted by all stakeholders together with standardized formats for descriptions, their coding and communication.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784
[34] https://moonshotteam.com/the-redirect-method/
[35] Webbpoliser, gaming och kontranarrativ: Digitalt förebyggande arbete mot extremism och våldsbejakande extremism
[36] The 15 solutions studied are: Gamen met de politie (the Netherlands), Les Promeneurs du Net & Web Citizen Training Program (France), Veebikonstaabel (Estonia), Counter Conversations (England), Seriously (France), Malmö – Trygg och säker digital stad (Sweden), Politiets Online Patrulje (Denmark), Politiets nettpatruljer (Norway), Project RETHINK, The Redirect Method, MoonShot, Islam-ist och Tränen de Dawa (Germany), Jamal al-Khatib, Extremkoll.se, Prevent Duty Training (England), streetwork@online, (Germany)

- Automatic identification and rapid launch of automatic countermeasures and human interventions online and IRL, based on validated frameworks and methods.
- Targeted and coordinated research and development to provide systematic knowledge at a European level on all aspects of how to build resilience in vulnerable young people against online entrapment in violent extremism and terrorism.

3.3.2 EU-HYBNET T4.3 RECOMMENDATIONS FOR STANDARDIZATION

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

In every EU-HYBNET working cycle (M1-M17/ cycle I, M18-34/ cycle II, M35-51/ cycle III, M52-M60/ cycle IV), T4.3 is the final project Task that will highlight the key selected project innovations that are seen as a sound solution for the identified working cycle gaps and needs and answering to the pan-European security practitioners and other relevant actors' needs. Therefore during the reporting period in T4.3/D4.9 "*2nd report on standardization recommendations*" it is highlighted what are the best practices, key regulations and even standards that eventually support the EU-HYBNET's recommended innovation uptake for pan-European security practitioners' and other relevant actors use.

The D4.9 followed the innovations from T4.2 (WINS, EESCM, MIMI, GECHO) while decided to broden the scope by focus on six innovations which were considered initially as basis for T4.2 innovations. Therefore, the T4.3 had following six innovations related to T4.2 innovations (WINS, EESCM, MIMI, GECHO):

1. DDS-alpha (Core theme: Information and Strategic Communication) –> MIMI
2. Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience (Core theme: Future Trends of Hybrid Threats) -> EESCM
3. Detection of Disinformation Delivery Proxy Actors (Core theme: Resilient Civilians, Local Level and National Administration) -> GECHO
4. Development of Real-time Rapid Alert System on Disinformation (Core theme: Resilient Civilians, Local Level and National Administration) -> MIMI
5. Identify and safeguarding vulnerable individuals (Core theme: Information and Strategic Communication) -> GECHO
6. What Information Needs to be Shared between CI entities to detect hybrid threats (Core theme: Resilient Civilians, Local Level and National Administration) -> WINS

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

DDS-alpha

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		
Best Practices **(medium term)**	A recommended solution in the context of DDS-Alpha is called MIMI – a Marketplace for IMI information. For the establishment of MIMI there is a need to establish an organization which drives the building a European community of interested partners. This could be organized as a time limited project. The project should: • Develop a strong and convincing storyline showing the benefits of using MIMI and elect evangelists to convince stakeholders of the value in using MIMI. • Liaise with the DDS-alpha community/interest group to prepare for future joint developments. • Define and propose a suitable business model. • Define the requirements for the service platform on DDS-alpha, including required DDS-alpha extensions for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations. It must contain functionality for – Secure and controlled information exchange – Interfaces for control of service level agreements between users and providers • Implement and verify required functional extensions of DDS-alpha. Publish extensions as open source. • Set up a MIMI interest group which can maintain and extend MIMI. • Transfer maintenance operations of the service platform to the organization handling DDS-alpha. When MIMI has been established as a working solution, the required maintenance of the idea would be handled by the interest group.	**EEAS** **ENISA** **EU INTCEN**
Additional recommendations within T4.3		

Standardisation **(medium term)**	There is a need for implementing a Standard regarding the exchange of Data between the stakeholders The main standards in use are STIX, a language and serialization format for exchange of Cyber Threat Information (CTI) and TAXII, a CTI data exchange protocol. CTI documentation is here. Relative to the DDS-Alpha Innovation we could examine the applicability of already existing standards as per ISO 20614:2017 (Information and documentation — Data exchange protocol for interoperability and preservation), CEN/TS 16157-10:2022 (DATEX II data exchange specifications for traffic management and information|||), where we may observe analogies with the DDS-Alpha operational needs and finally an interesting analysis EU-SysFlex (PROPOSAL FOR DATA EXCHANGE STANDARDS AND PROTOCOLS) conducted in the context of Horizon 2020 (https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf) where interesting conclusions are illustrated in section 5.3 regarding Data exchange standards in General.	**ENISA**

Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		
Legal/Standardisation/Best Practices **(short/medium/long term)**	The innovation Multi-Stage Supply Chain Disruption Mitigation Strategy and Digital Twins for Supply Chain Resilience has been transformed into a solution focusing on how to enhance and extend the supply chain management scope (EESCM, Enhanced and Extended Supply Chain Management) to take more aspects into account, provide a better understanding of the real issues and how to minimize disruption impacts. In the short term the recommended actions required for the implementation of the innovation put forward above should address the target audience (for example, policy makers, providers of tools and training) and stakeholders concerned with preserving the integrity of Critical Infrastructures under fire. This should include setting up a governance body that is capable of defining the final scope of an innovative supply chain resilience framework and ensure that the critical components of the framework are consistent with existing legal / standardization and	**Council of the EU, European Parliament and European Commission** **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829** **The Critical Entities Resilience Directive (CER) (critical-entities-resilience-directive.com)**

		best practice related strategies and directives of EU and EC, which are delineated and explained below and include a Proposal for a DIRECTIVE on the resilience of critical entities; The Critical Entities Resilience Directive (CER); and the Strategic Compass for Security and Defence. More specifically, within the context of the CER, the Commission may also adopt legal acts laying down procedural arrangements necessary for the smooth functioning of the burgeoning **Critical Entities Resilience Group**, which shall support EC and be composed of representatives of the Member States and the Commission, facilitating strategic cooperation and exchange of information. The key recommendation here is to ensure that this **Group** will also address the evolving needs of the extended supply chain management framework. Furthermore, for the medium term, within the context of these EU / EC level actions and the supply chain resilience framework, we recommend strict adherence to supporting the development of enhancements to the aforementioned actions with special attention to: • developing and testing the framework on a sub-set of industries at the EU or regional level to evaluate resilience capacities; • ensuring that the final framework is adequately robust across industry sectors and can also be implemented in education/training environments; including a set of newly developed guidelines for the further development of tools and methodologies. Finally, in the long term, to bring the EESCM solution to fruition, providers of supply chain management related services (tools and training) should enhance current instruments with novel concepts. To effectively accomplish this, the strategies and guidance should be set by EU and MS level policy makers. In this context, the Digital Twins approach is crucial and although currently used to model supply chain and optimization techniques, it can also be adopted to widen the scope of its capabilities. This would include expansion of services, geopolitical concerns and hybrid threat challenges; as well as enhanced tools capable of providing reliable, real life based, modelling of cascading effects; including impact minimization and recovery simulation capabilities. Supply chain is in the scope of current standards. ISO family includes ISO 9001 focusing on the quality of supply chain, ISO 26000 and ISO 20400:2017 focusing on sustainability. ISO 2800 is specifically designed for supply chain security management, but the scope remains on transportation of products. The same can be observed in other recommendations or standards related to supply chain management, provided by Association for Supply Chain Management	**EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)** **www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf** **IBM, What is a digital twin?** **ISO - ISO 9001 - What does it mean in the supply chain?** **ISO 20400:2017 - Sustainable procurement — Guidance** **ISO 28000 - Supply Chain Security Management | BSI (bsigroup.com)** **SCOR Digital Standard | ASCM** **SCRM (asisonline.org)**

	(ASCM), American National Standards Institute (ANSI). The European Committee for Standardization (CEN) and the European Committee for Electronical Standardization (CENELEC) are developing sectorial standards, that in some cases include supply chain aspects. All the above mentioned initiatives are considering supply chain from the traditional point of view, focusing on goods and transportation. However, challenges remain. For example, understanding and defining the relevant scope of supply chain management in the context of hybrid threats. The current tools are mainly focused on goods but hardly include services. In addition, these lack functionalities that could deal with geopolitical risk, impact assessment and minimization, cascading effects, including recovery planning features, or other threats of a hybrid nature. Current instruments have been developed on a traditional understanding of the supply chain, while the proposed solution is focused on a much wider concept of supply chains and not on expedient optimization procedures.	
Additional recommendations within T4.3		
Best Practices **(medium term)**	**Strategic Compass for Security and Defence** (approved 21 March 2022) provides the European Union with an ambitious plan of action for strengthening the EU's security and defence policy by 2030**.** The **Compass** is ambitious, formally approved just after Russia's attack on Ukraine. It covers security and defence strategies in relation to global competition, overall economic security, the space industry, disruptive technologies, and associated risks to EU's supply chains related to Critical Infrastructure.	**Council of the EU and European Commission** **www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf**

Detection of Disinformation Delivery Proxy Actors

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations within T4.3		

Legal **(medium term)**	Set up a national agency to monitor, detect and analyse the operation used by foreign actors to disseminate and amplify online content hostile to nation with the aim of damaging the nation's interest. France set up VIGINUM (The Vigilance and Protection Service against Foreign Digital Interference) to combat information manipulation. Formed in 2021 and attached to the General Secretariat for Defence and National Security (SGDSN). The main mission is to protecting digital public debate against information manipulation campaigns involving foreign actors intended to harm France and its fundamental interests. VIGINUM has an ethical and scientific committee, and its mandate is strictly regulated by law. The agency employs mainly analysts, data engineers and digital media experts who work with open sources information. According to Report, VIGINUM has detected 84 potentially inauthentic phenomena as of 22 July 2022 phenomena on digital platforms and 60 of them during the 2022 French election period.	**EU MS governments related to national security and defence**
Legal **(short term)**	Legal solutions to be introduced on the EU level that will increase transparency of online platforms – e.g. sharing of and accessing relevant data of social media platforms, increasing transparency of political advertisements, increasing transparency and understanding of micro targeting, algorithms and content moderation activities	**European Institute for Security Studies** **EEAS** **European Parliament** **Committees** **Communications Networks, Content and Technology**
Legal **(short term)**	Code of Practice of Disinformation to be signed by relevant players to be signed obligatorily and not voluntarily, as it is currently	
Best Practices **(short term)**	Supporting independent, quality, fact-based journalism, including independent public-service broadcasting, and encouraging media literacy campaigns to develop trust in the media and understanding of what constitutes good information will continue to play important roles.	
Best Practices **(short term)**	Promote and support audiences' use of reliable sources of information, including traditional media. Enable young people to access paid news services on preferential terms, for example, through school subscriptions.	

Best Practices **(short term)**	Support the activities of independent fact-checking organizations that publish specific data on disinformation campaigns delivered by proxy actors and whose personnel have the competence and tools to professionally detect and describe such phenomena. In this context, also promote broad cooperation, especially between the journalistic and fact-checking communities with social-media platforms.	**European Commission – DG EAC – Education, Youth, Sport and Culture - EAC.B YOUTH, EDUCATION AND ERASMUS+** **European Parliament – Committee on Culture and Education**
Best Practices **(short term)**	Aim to ensure that social media users are not only competent in recognizing disinformation messages, but also have the widest possible access to data on, for example, where a message came from, how it spread, etc. The idea would be to make the circulation of messages on social media as transparent as possible.	
Best Practices **(medium term)**	Media-literacy teaching should be stretched across all age groups including kindergarten groups and seniors. For schoolchildren and students countering disinformation classes should be part of the core curriculum. Teachers who are responsible for those classes should first be thoroughly educated themselves so that they are well prepared to share the knowledge with children and students. As the landscape of disinformation is constantly evolving, teachers should undergo regular up training sessions (also with practitioner e.g. journalists and civil society representatives) to make sure they are updated. For older groups, media-literacy teaching can take different forms – lectures, discussion panels, workshops, awareness campaigns etc. with age and education-appropriate tools. It is important for media-literacy teaching to be rather group specific than include everyone.	
Best Practices **(short term)**	Creating guides tailored to selected target groups – social and digital media users. Guides in a practical and understandable way should inform on how to recognise fake news and what can be done in this case. Those guides should be consistent within all MSs but taking into consideration different topics specific for various countries/regions. Once created, those guides should be incorporated into media-literacy teaching classes and events (as described above).	

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations within T4.3		
Best Practice (medium term)	Complete and finish the works on the upscale of Rapid Alert System: FIMI toolbox making it 24/7 operational information tool in cause of time-criticality, especially in times of large-scale crises as pandemics, irregular immigration flows, etc. The main outcome of the innovation proposal could be better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups.	**National Governments – Entities responsible for Public Security Issue Coordination, in Poland: Government Centre for Security** **European Parliament - Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation** **Association of European Journalists** **International Fact Checking Network** **EU fact checking networks** **EU project working on countering disinformation e.g. EDMO**
Best Practice (short term)	'Countering disinformation' units to be established in EU and in each country (national and local levels), making sure those units are consistent, have similar duties, responsibilities, access to the same tools and are in constant contact with one another sharing information.	
Best Practice (medium term)	Multisectoral cooperation supporting pre-bunking and debunking efforts to counter disinformation campaigns. Preparing proactive and tailored responses, Creating blueprints and/or best practices that can be initiated in order to predict the likely impact of disinformation campaign and respond accordingly to ongoing disinfo campaigns by initiating the relevant protocol.	
Best Practice (short term)	Work on unified terminology for combating disinformation – fake news, misinformation, disinformation, malinformation, FIMI etc. Currently terms "disinformation" or "fake news" are often used as to cover a range of disinformation activities.	
Best Practice (short term)	Cooperation with fact-checking organizations at the national and supra-national level, with the aim of quickly detecting disinformation messages and obtaining full and certain knowledge that a given message is actually disinformation. This kind of cooperation will minimize the likelihood of bias in the evaluation of messages by applying the solutions developed by fact-checkers.	

Best Practice **(medium term)**	Building on scientific knowledge in the detection and recognition of disinformation messages. Thus, continuous cooperation with researchers of disinformation messages on how to detect and recognize such messages, trends in this area, the most important actors and changes in the media that favour the spread of disinformation messages.	**European Commission: DG Connect: Directorate H Digital Society, Trust & Cybersecurity** **Council of European Municipalities and Regions (CEMR)** **Council of Europe: Congress of Local and Regional Authority Secretary General** **European Committee of the Regions – thematic commission CIVEX: Commission for Citizenship, Governance, Institutional and External Affairs** **European Institute for Security Studies** **EEAS**
Best Practice **(medium term)**	Creation of a structure that will include entities of different nature - governmental, public, non-governmental organizations, research centers, etc. Adopt common standards of operation and ensure continuous and uninterrupted flow of information between these institutions.	
Best Practice **(short term)**	It is particularly important to ensure that relationships are built and maintained with entities that will be able to communicate the results of the FIMI toolbox work to the broader public (to the extent established). These entities are primarily the media, but also fact-checking organizations, NGOs, research institutes, local government units, etc.	
Standard **(medium term)**	Incorporate fact-checking curriculum for journalism students within all European higher education schools which offer journalism faculties.	

Identify and safeguarding vulnerable individuals

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		

Best Practices/Standardisation (medium term)	Develop a sharing and analysis platform for GECHO (Gatekeeping ECHO Chambers). The innovation Identify and safeguarding vulnerable individuals has been transformed into a solution that monitors the online environment, identifies where and how interventions are needed, thereafter launching the appropriate actions to build resilience in vulnerable young people against possible entrapment in violent extremism and terrorism. The solution is called Gatekeeping ECHO chambers (GECHO). GECHO is for countering violent extremism and terrorism, as antagonistic states and organizations may use support of local groups that promote violent extremism and terrorism as one tool in their hybrid threat toolbox. This to widen sociocultural cleavage and reduce trust in the society. GECHO proposes the establishment of a platform for information sharing, monitoring, analysis and joint actions between organizations in the MSs to provide detailed and local situational awareness about activities in online environments related to violent extremism and terrorism. This to allow efficient interventions against recruitment activities and to safeguard young people from such influence. Develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. Enable sharing of situational data between stakeholders. The platform can be based on the CISAE principles proposed to be standardized in the first project cycle. An alternative route would be to use an extended DDS-alpha platform. Develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites. In this work use of federated learning should be considered and how anonymization and GDPR requirements can be fulfilled. Furthermore, there is a need for research and compilation of training sets to guarantee that AI based solutions easily can be developed and tested. Establish research network with focus on GECHO needs. The ultimate objective of GECHO is to develop easy to follow validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. To make it become the powerful tool it should be, there is a need for supporting research in several areas related to the factors influencing the online radicalisation process: a) Review state-of-the-art of existing frameworks, methods and tools to prevent radicalization. b) Methods used by groups promoting violent extremism in their recruiting activities. c) Relevant differences in cultural, language and community codes d) What makes a person vulnerable?	**The European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online activities by violent extremism and terrorism groups as well as tech companies developing tool** **EU Member States stakeholders (social care workers, police, teachers, NGOs)** **Europol** **The Radicalisation Awareness Network (RAN Practitioners)** **The VOX-Pol Network of Excellence (NoE)** **European Digital Media Observatory (EDMO**

		e) Frameworks, methods and tools for creation of practical means for intervention and prevention. f) Methods for evaluation and validation of the effectiveness of countermeasures	
Additional recommendations within T4.3			
Best Practices **(short term)**		Join the Transparency Centre signatories. By joining the 2022 Code of Practice on Disinformation, new signatories will be part of an EU-wide forum bringing together a variety of relevant players who seek to strengthen their actions, share best practices and improve cooperation in order to mitigate the risks stemming from disinformation in the EU. Potential signatories can get in contact with the Task-force through the website.	**Providers of online services (social media, private messaging applications, search engines)** **Providers of online advertising industry** **Providers of e-payment services, e-commerce, crowd-funding, donation systems** **Fact-checkers** **Civil society organizations specializing in countering disinformation**
Best Practices/Legal **(long term)**		Finnish Education System and approach to counter disinformation. According to the Media Literacy Index 2022[37] which assess the potential vulnerability of 41 societies in Europe to disinformation, Finland is first in the ranking and also shows that countries in the Southeast and East Europe are more vulnerable to the phenomenon (in Report takes into account such factors are media freedom, education, trust in people and e-participation). Education as one of essential component in aforementioned Report is also the cornerstone to resist information warfare considering by Finland's government. The curriculum was revised in 2016 to teach children the skills they needed to spot the kind of fabricated information on social media. Wide spreading	**Ministries of Education in EU countries** **The European Education Area**

[37] https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf

	critical thinking skills among pupils/students along with coherent government response is the main tool to combating disinformation campaigns and creating more resilient society. Finnish teachers in maths classes showing how statistics can be manipulated is a good example.	
Legal **(medium term)**	Legislation allowing to verify kids' age in social media. The French government is very close to implementing age verification and parental consent for social media platforms. The aim is to protecting children from harmful online content not intended for their age group. On march 2023 the National Assembly of France voted overwhelmingly in favour of the legislation and then it is up to the Senate to pass the bill into law. That legislation will allow to force social media and adult sites to verify their users' age and request parental consent for anyone under the age of 15. Parents will also be empowered to terminate social media accounts for their children if they're under 15. Such legal arrangements could be an appropriate approach for all EU Member States.	**Legislative authority in UE Member States**
Best Practices **(short term)**	Increasing resilience and reducing vulnerability to disinformation on local and regional level Local media are an important part of the fabric of local communities. They provide news that more deeply concerns readers' day-to-day experience. Quality local media promote transparency and accountability from local government and therefore trust in local politics. When citizens do not have access to local media it pushes them towards getting news through social media and messaging app groups, the latter of which are very hard to monitor because their encrypted nature. Therefore "A handbook on good practice in countering disinformation at local and regional level' was developed for the Committee of the Regions, CIVEX Commission (Commission for Citizenship, Governance, Institutional and External Affairs). A Handbook contains: - A typology of different areas of action to combat online disinformation (awareness raising, development of media literacy, strong public communication, promoting involvement of civil society stakeholders and citizens and support for local media) at local and regional level, including of action already taken; - Three in-depth case studies of intervention undertaken to counter disinformation and identifies lessons that local and regional authorities (LRAs) could use for similar initiatives; - Gathered together lessons learned from research to provide practical recommendations for LRAs going forward.	**Local and Regional Authorities in EU Member States**

	The recommendations aim to provide some guidance to LRAs on how to go about countering disinformation, based on practices that have shown to be successful	
Best Practices **(medium term)**	Create and support the operation of multidisciplinary research and project teams. Such teams would analyse factors influencing the particular vulnerability of given individuals or environments to disinformation and the media-psychological mechanisms of its impact. Then, on the basis of this knowledge, they would design effective communication tools to influence these individuals or environments.	**Local and Regional Authorities in EU Member States** **European Commission** **Research institutions**
Best Practices **(medium term)**	Build awareness of social media users on how harmful extremist groups operating on the Internet can be and what consequences their disinformation tactics (especially hate speech) can lead to.	**Local and Regional Authorities in EU Member States** **NGOs**
Best Practices **(medium term)**	Decentralization of educational processes in the field of media competences, delegating such activities to non-governmental institutions that operate in the local environment and have the best understanding of the needs and opportunities for education in this area. These types of organizations also have the knowledge and contacts that allow them to reach the groups most at risk of disinformation with their educational activities. Involvement of local opinion leaders in these activities.	**Local and Regional Authorities in EU Member States** **NGOs**

What Information Needs to be Shared between CI entities to detect hybrid threats

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution

Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)			
Legal/Standardisation/Best Practices **(short/medium term)**	The innovation Impact and Risk assessment of critical infrastructures in a complex interdependent scenario (Acronym CIRP) has been transformed into a solution which present a methodology for how to establish what information dependent CI entities need to share in order to enhance their resilience against cascading effects and to counter hybrid threats**.** The solution proposed is called WINS, What Information Needs to be Shared between CI entities to detect hybrid threats and attacks, and to be prepared for them? The vision on the solution is to help CI entities and law enforcement (LE) officials to recognize new forms of hybrid threats/attacks, and further fulfil requirements in this respect given in CER- and NIS-2 Directive. Earlier innovation focusing on CI protection (from EU-HYBNET 1st working cycle) was an innovation called CISAE (A common Information Sharing and Analysis environment), and the CISAE was answering the question of how to share CI information between CI stakeholders. Now, the CIRP innovation is reconsidered and reformulated as an innovation called "WINS" that will build on CISAE. WINS is answering the question: what information needs to be shared? Therefore, the key element in WINS is a suggested methodological approach to discover what information needs to be shared to enhance CI entities resilience to counter hybrid threats. It is recommended to deliver pan-European and cross-sectoral CI methodological (even standardized) approach for analysis of CI entities' critical vulnerabilities also in the context of hybrid threats/attacks. The collection of CI entities' vulnerability data is based on risk assessments and stress tests and an attack tree approach. If the CI entities share the data with competent authorities, interconnected services and other relevant stakeholders, this will eventually support CI entities to be more prepared for hybrid attacks/threats. Research and development of supporting tools for WINS. To make the WINS solution a practical and efficient tool to identify which information to share, supporting tools for handling the required base information about the CI entities, the formation of attack trees and the following sensitivity and risk analysis will be needed. It is thus recommended to start such research and development work. CISAE standardization. This recommendation is a repetition of a recommendation from the first project cycle. We include it once again as it a proposed basis for the WINS solution. The recommendation is to develop and standardize a framework for the implementation of information sharing and analysis environments (CISAEs). Build the information sharing functionality on the EMSA CISE, solution. Define principles for how analysis functionality can be implemented and analysis results be shared. The work should cover the needs for situational	**European Parliament** **European Commission**	

		awareness in EU critical infrastructures and for monitoring and handling of disinformation campaigns. For further details see Deliverable 4.5 However, it is good to notice that Technical Committee ISO/TC 292 Security and resilience works with standardization in the field of security to enhance the safety and resilience of society. ISO/TC 292 was established on January 2015. The actual development of the standards is done in various Working Groups which focus on certain areas within the field of security and resilience. Working Group 6 is responsible for drafting standards in the area of Protective Security which is the framework, policies and processes implemented to identify, respond to and reduce the risk of harm from malicious acts. Working In this field, the Group has ongoing project dedicated to provide Guidelines for the development of a security plan for an organization (ISO 22343:2023). This document gives guidance on developing and maintaining security plans. The security plan describes how an organization establishes effective security planning and how it integrate security within organizational risk management practices. The document is applicable to all organizations regardless of type and nature (in the private, public or non-profit sectors, that wish to develop effective security plans in a consistent manner. The intent of the document is to provide the fundamental elements necessary to improve and sustain the protection of an organization. Other identified relevant standards to WINS development are: • ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity • ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity • ISO 31000:2018 Risk management – Guidelines • ISO/TS 22375:2018, Security and resilience – Guidelines for complexity assessment process		
Additional recommendations within T4.3				
Best Practices (short/medium term)		ENISA provides state-of-the-art advice and counsel to EU national authorities on safeguarding critical infrastructure such as power grids, telecoms and mass transportation systems essential to the national and cross-border security of essential services.	**ENISA**	

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

4. CONCLUSION

4.1 SUMMARY

In the chapter above it is described how the EU-HYBNET project activities from the past six project months (November 2022 – April 2023) contributed to the Three Lines of Action. In addition, chapters have described how the work in the project Tasks has been conducted now when the 2nd project cycle has started to deliver results from this cycle as well. Furthermore, the goal of the document has partly also been to highlight what kind of results EU-HYBNET is expected to achieve in the Three Lines of Action during the next six months reporting period.

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

In Section 3. we showed how the EU-HYBNET project tasks and project actors have contributed 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 end of the second project cycle (2nd cycle duration: M18-M34/ October 2021 – February 2023) have been now explained to the EC. The next Six Month Action Report (in Nov 2023) will describe the first 3rd cycle results and findings to the Three Lines of Actions, and how the project has been able to implement the findings even more to the benefit of pan-European practitioners to counter hybrid threats. In addition, the next report will describe the project activities in the beginning of the 3rd project cycle (March 2023 – August 2024). Definitely, best practices and lessons learned and key findings will be taken into further work in the third cycle and Three Lines of Action related work in different EU-HYBNET project work packages and Tasks. The following six (6) deliverables will be delivered during next six-month period. No milestones take place M37-M42.

Deliverables (D):

T3.4 Innovation and Knowledge Exchange Events

- D3.16 3rd Future Trends analyses Workshop Report (MVNIA), M37

T5.3 Project Annual Workshops for Stakeholder

- D5.12 Annual Workshop Report 3 (MVNIA), M37

T2.2 Research to Support Increase of Capacity and Knowledg

- D2.11 Deeper analyses, delivery of short list of gaps and needs (JRC), M39

T3.2 Technology and Innovations Watch

- D3.5 Second mid-term report Improvements and Innovations (SATWAYS), M41

T3.3 Ongoing Research Projects Initiatives Watch

- D3.9 Second mid-term report Innovation and research monitoring (L3CE), M41

T1.1 Administrative and Financial Planning and Coordination

- D1.11 7th six month action report (LAU), M42

Milestones (MS):

- N/A

As the deliverables, the EU-HYBNET project will deliver many more results to the Three Lines of Action in the forthcoming months. The aim and value of the Six Months Action report is to track the results and to highlight their importance for the project proceeding, and to empower the pan-European measures and extension of the pan-European network to counter hybrid threats.

Furthermore, new project results to the Three Lines of Action will be reported especially because deliverables focusing on present pan-European security practitioners gaps and needs to counter hybrid threats (by T2.1, T2.2) alike first insights of promising innovations to gaps and needs (by T3.2, T3.3) will be ready. This is followed by research results on promising innovation analysis (T3.1). Furthermore, analysis on EU-HYBNET Dissemination, Communication and Exploitation activities will support the project to consider new ways to tell about the project's results for the pan-European stakeholders.

Lastly, EU-HYBNET will continue to share the key findings with DG HOME and other relevant DGs, EU Agencies and Offices via emails, invitations to the project events, and of course to contribute to EC's possible requests for information. In addition, cooperation with EEAS/Strat.Comm in the context of Foreign Information Manipulation and Interference/FIMI tool development will continue. This all is to benefit the pan-European stakeholders from the EU-HYBNET results and to enhance joint measures to counter Hybrid Threats.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threat –project, No. 883054
EC	European Commission
EU	European Union
GA	Grant Agreement
DoA	Description of Action Part A and B
H2020	Horizon2020, EC funding Program for EU projects' funding
FP7	The EC's 7th Framework Program to EU project funding
D	Deliverable
CO	Consortium only deliverable
WP	Work Package
T	Task
M	Month
MS	Milestone
OB	Objective
KPI	Key Performance Indicator
NoP	Network of Practitioners project
R&I	Research and innovations
EU MS	European Union Member State
G&N	gaps and needs
ISO	ISO Standard is a formula that describes the best way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials – standards cover a huge range of activities. Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators
IKEW	Innovation and Knowledge Exchange Event
BOS	Break Out Session
ISW	Innovation Standardization Workshop
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
Open CTI	OpenCTI is a comprehensive tool allowing users to capitalize technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of analysed information to its primary source (a report, new article, etc.) when solving the traits of disinformation
PRECINCT	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection -Project
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges -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
ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement –Project
PersoNews	Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy –Project
EU-LISTCO	Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders –Project
CYBERCULT	Strategic Cultures of Cyber Warfare -Project
INSPIRE-5GPlus	INtelligent Security and PervasIve tRust for 5G and Beyond -Project
ISOCRYPT	Isogeny-based Toolbox for Post-quantum Cryptography -Project
PROGRESS	Protection and Resilience Of Ground-based infRastructures for European Space Systems -Project
WeVerify	In the Wider and Enhanced Verification for You -Project
IMEDMC	Information and Misinformation Economics: Design, Manipulations and Coutermeasures -Project
RUSINFORM	The Consequences of the Internet for Russia's Informational Influence Abroad –Project
Open Your Eyes	Open Your Eyes: Fake News for Dummies –Project
COMPROP	Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe -Project
CONCORDIA	Cyber Security Competence for Research and Innovation -Project
ECSCI	European Cluster for Securing Critical Infrastructures
DDS-aplha	DDS-alpha is the Disinformation Data Space
STIX	STIX standard: Standard Threat Information Expression
CI	Critical Infrastructure
CISAE	Common Information Sharing and Analysis Environment. Similar innovation as CISE while focusing to other domain than maritime CISE.
CISE	
EMSA	European Maritime Security Agence
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
RAS	Rapid Alert System in EEAS
EDMO	European Digital Media Observatory
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria

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

.

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.

.