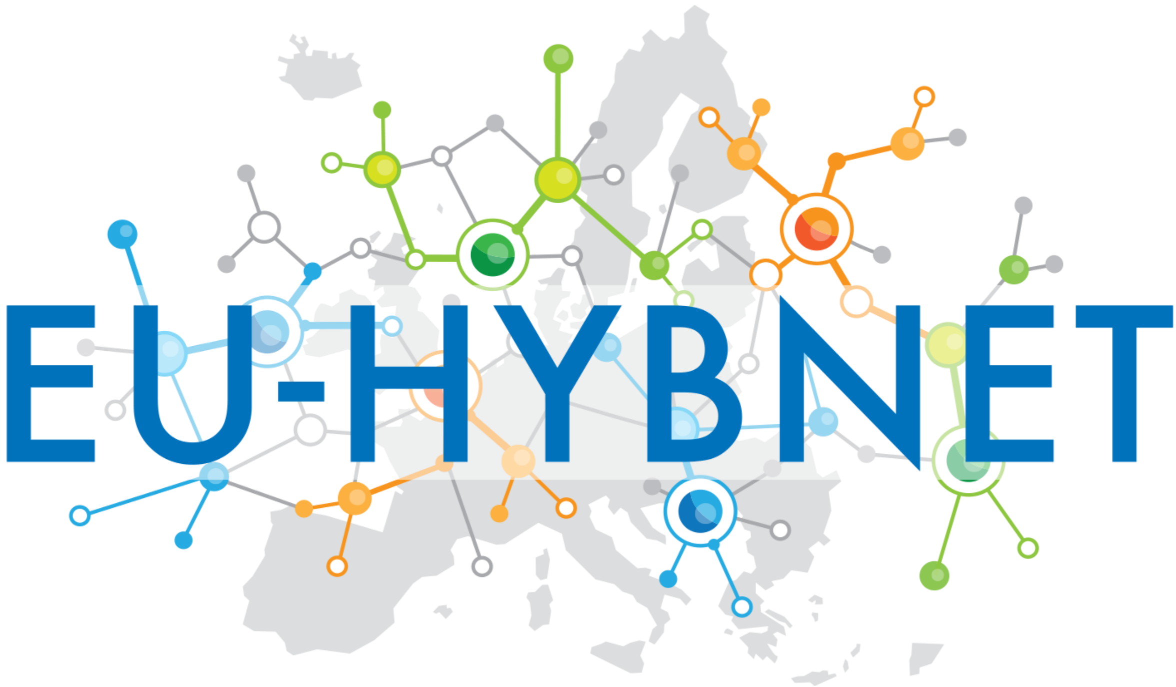

SEVENTH SIX MONTH ACTION REPORT

DELIVERABLE 1.11

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

D1.11 SEVENTH SIX MONTH ACTION REPORT

Deliverable number:	**1.11**	
Version:	**0.1**	
Delivery date:	**21/11/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	Päivi Mattila, Tiina Haapanen	**Laurea**
Contributors:	Gunhild Hoogensen-Gjorv	**UiT**
	Input to the report from all consortium partners due to their project work in various Tasks and events as contributors	**MTES, URJC, Hybrid CoE, PPHS, KEMEA, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, RISE, UCSC, Maldita, Espoo, COMTESSA, ZITiS, L3CE**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	18/10/2023	Päivi Mattila/ Laurea	1st draft of text
0.2	19/10/2023	Päivi Mattila/ Laurea	Text editing
0.3	20/10/2023	Päivi Mattila/ Laurea	Text editing
0.4	30/10/2023	Tiina Haapanen/ Laurea	Text editing
0.5	01/11/2023	Päivi Mattila/ Laurea	Text editing
0.6	03/11/2023	Päivi Mattila/ Laurea	Text editing, document for review
0.7	21/11/2023	Gunhild Hoogensen-Gjorv/ UiT	Review
0.8	21/11/2023	Päivi Mattila/ Laurea	Final editing, text ready
1.0	21/11/2023	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.

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) 1.11 "*Seventh Six Month Action Report*" in project month (M) 42/OCT 2023 is to describe how the project has proceeded from M37 until end of M42 of the project (May 2023 – October 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, D1.11 also highlights what actions and results are expected from EU-HYBNET during the next six-month period (November 2023 - April 2024).

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 D1.11 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 37 - 42 (May 2023 – October 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 (November 2023 - April 2024).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.11 "*Seventh 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 D1.11, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.11 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.

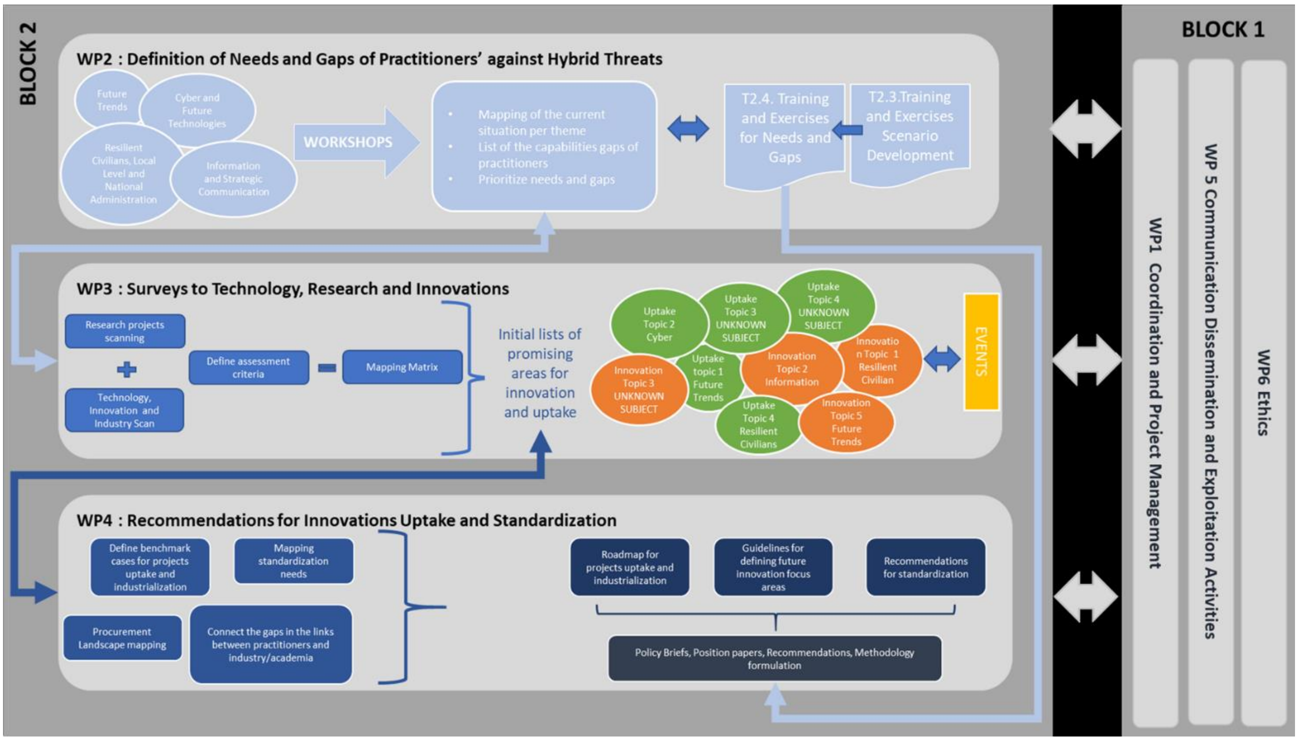
BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

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

In addition, the project results and findings described in EU-HYBNET Six Moth Action Reports are often linked to the project milestones (MS) achieved during the last six-month period. However, during D1.11 reporting period no project Mileston(s) was set to the project and hence no reporting on Milestone(s) this time.

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The seventh Six-Month Action Report (D1.11) main author is Laurea, the organization responsible for the delivery of D1.11. However, EU-HYBNET work package (WP) and task (T) leaders have also provided information on the tasks they are responsible for and have been working on during the sixth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager and Network Manager have contributed to D1.11 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 2023. 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 especially T2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC) who identified during the beginning of the third project cycle (M35 -M52/ March 2023 – August 2024) practitioners'[1] and other relevant actors' (industry, SMEs, academia, NGOS) gaps and needs, vulnerabilities to counter hybrid threats. The work conducted in T2.1 contributed to T2.2 who delivered during the reporting period deliverable (D) 2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (M39/ July 2023) where the most important pan-European practitioners' and other relevant actors' gaps and needs to counter hybrid threats were listed. Therefore, the D2.11 signified in the third project cycle (M35 – M52/ March 2023 – August 2024) the starting point for the EU-HYBNET project to start monitoring and mapping technological and non-technological/human-science based innovations, solutions from existing research and innovation (R&I) projects and other possible sources or providers (e.g. industry, academia, NGOs) to cover the identified gaps and needs and with a goal of recommending the uptake or the industrialization of results.

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

During this report's (D1.11) reporting period many innovations were identified in T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) and T3.2 "*Technology and Innovations Watch*" (Lead by Satways). More on the identified projects and their promising innovations in sub-chapter 3.1.1-3.1.2 below.

Next to T3.3 and T3.2 important innovation mapping relevant to the first Three Lines of Action reporting has been conducted also in 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 T3.2 TECHNOLOGY AND INNOVATIONS WATCH

In T3.2 "*Technology and Innovations Watch*" (lead by Satways) work focused on analysis on innovations that could be seen as solution to the identified pan-European security practitioners' and other relevant actors' gaps and needs, threats to counter hybrid threats listed in T2.2/ D2.11 according to the EU-HYBNET project's Four Core Themes (Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communication). The work in T3.2 focused mainly on technical innovations delivered by industry while also some of the innovations were deriving from EU Member States' (EU MS) national and European Commission (EC) funded projects and were non-technological in their nature. These innovations are described in detail in D3.5 "*Second Mid-Term Report on Improvement and innovations*" (M41/ September 2023). However, the most important analysis from D3.5 to the "*First Three Lines of Action*" is reported below according to EU-HYBNET's Four Core Themes below.

The table below all the innovations identified as possible solutions to the identified threats; however, not all of the innovations are based on projects and hence if this is the case, the innovations are not described with more details in sub-chapters below. The innovations based on projects are highlighted in yellow in the table.

CORE THEME		**PRIMARY CONTEXT, Threat**	**IDEA/ INNOVATION PROPOSED**
1. FUTURE TRENDS OF HYBRID THREATS	1.1	Political Failure	Mobile application to pinpoint acts of harassment/violence on the street and online
	1.2	New Agit-Prop	Anti agit-prop and hostile conspiracy warning platform
	1.3	Alternative Reality	WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories
			EXPERIENCE. The "Extended-Personal Reality": augmented recording and

			transmission of virtual senses through artificial-IntelligENCE
2. CYBER AND FUTURE TECHNOLOGIES	2.1	Stealing Data/Attacking individuals	BREACH GUARD Or Any Other Similar Available Solution
			NORDLAYER Or Other Similar Solution
			Shield, Watson Studio, Or Any Other Similar Available Solution
	2.2	Online Manipulation/Attacking democracy	Code of Practice on Disinformation
			Starlight Disinformation-Misinformation toolset
	2.3	Attack on Services	AI And Machine Learning Technologies
			Advanced Surveillance Systems with Perimeter security
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1	Spreading Violence	Expansion of the AVMS Directive
			NETWORK OF ANTI SLAPP FINANCIAL AND LEGAL SUPPORT
	3.2	Attack on social structure	Offline-Face-Secure-Access- (OFSA)
			Passive Authentication for Secure Identification- PASID
			AI-enhanced Disaster Emergency Communications
	3.3	Undermine Inside institutions	Advanced analytical and investigative capabilities via GRACE Platform and approach
			Antidote' to hostile messaging delivered by private messaging apps
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1	Media conundrum	Media Pluralism Monitor (MPM)
	4.2	Sectarianism	"BAD NEWS" Prebunking Game platform
	4.3	Attack on Information	Real-Time Fact-Checking Browser Extension
			BLOCKCHAIN-BASED VERIFICATION

<u>EU-HYBNET Project Core Theme: Resilient Civilians, Local Level and National Administration</u>

Threat: Spreading violence

- *No defined projects*

Threat: Attack on social structures

- *No defined projects*

Threat: Undermining institutions' internal organisation

The projects that are seen to deliver a possible solution to the threat are following:

GRACE (Global Response Against Child Exploitation)

GRACE project is funded by the EC (https://cordis.europa.eu/project/id/883341) and it has developed an innovative, AI-powered information sharing platform for European law enforcement authorities (LEA) investigations on child sexual exploitation and abuse material (CSEM). The AI-powered platform has answered for LEAs challenges to referrals of CSEM because the CSEM material has been in big growth on-line and the amount of material has exceeded the capacity of LEAs. The huge amount of data that needs to be analysed is a challenge in the case of hybrid threats as well and hence the GRACE projects platform and way how to share sensitive data is seen as a promising solution for authorities who are dealing analysis of signs of hybrid threats.

EU-HYBNET Project Core Theme: Cyber and Future Technologies

Threat: Stealing data attacking individuals

- *No defined projects*

Threat: Online manipulation attacking democracy

The projects that are seen to deliver a possible solution to the threat are following:

STARLIGHT

STARLIGHT project (https://cordis.europa.eu/project/id/101021797) is one of the flagship projects dedicated to deliver easy deployable toolset to address various need of LEA and other security practitioners driven by constantly changing tech driven crimes modus operandi. In particular, STARLIGHT has one direction dedicated for disinformation and misinformation related threats. This direction is composed of several organisations developing different tooling enabling deep access of information in social platforms and tools to detect different misleading aspects of the information. Starlight Disinformation-Misinformation toolset consist of the following toolset for version 1 and will be constantly expanding:

Tooling	Content Type	Language	Domain	Provider
Telegram Crawler	Telegram content (groups, posts, text, media)	Multi-lingual	Social networks, Discussion Forums	AIT
DeepFake detection	Is Images, Media amended	Multi-lingual	Any	AIT
Forbiden Symbol Detection	Forbidden symbolics detector	Multi-lingual	Any	AIT
Geolocalization	Recognition of recording location	Mutli-lingual	Any	AIT
Toxicity	Toxic, offensive content, comments, hateful language	German	Social Networks, Article	AIT
Story Clustering	Provides reposting chain	Multi-lingual	Social Networks, Article	AIT
Twitter Crawler	Twitter content (groups, posts, text, media)	Multi-lingual	Social Networks	AIT
Bot Detection	Is the post a bot	Multi-lingual	Social Networks	AMS
Clickbait detection	Is the post a clickbait	Multi-lingual	Social Networks	AMS
SPAM Detection	Is the post a SPAM	Multi-lingual	Social Networks	AMS

Sentiment Analysis	Provides semantic analysis of the post content based on basic emotions model	English	Social Networks, Article	AMS
Fake content Meta Detection Engine	Any post URL	Multi-lingual	Social Networks	ICCS
Toolset Integration interface	All of above	English	NA	ICCS, L3CE, AIT, AMS

There are tools dedicated to access information on general internet, communication platforms such as Telegram or X (Twitter) platforms, but majority are focused on detection of fault or forbidden content. Majority of them can work on different languages. All of tools listed are planned to be integrated in one interface, making them easier to use. At this point of time Starlight project is developing solutions for LEA, but it can be developed further for different target groups and serves as a good example of what is needed to handle artificial amplification complexity. On the whole, STARLIGHT's solution provides toolset that gives possibility easy and semi-automated way to analyse any content or communication reliability, trustworthiness and identifies amplification techniques applied as well how much of it is being "faked" or created artificially. In addition, it provides insights about extremists, radical, criminal content usage.

Threat: Attack on services

- *No defined projects*

EU-HYBNET Project Core Theme: Information and Strategic Communications

Threat: Media conundrum

- *No defined projects*

Threat: Antagonizing victimization narratives in the informational space

- *No defined projects*

Threat: Attack on information

- *No defined projects*

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

Threat: Political deficiency

- *No defined projects*

Threat: New agit-prop

- *No defined projects*

Threat: **Substitutive reality**

The projects that are seen to deliver a possible solution to the threat are following:

WeVerify

Keeping people safe is the number one priority for the European Union and governments across the world, and being able to respond quickly and effectively to the spread of misinformation is key. The InVID WeVerify plugin (https://weverify.eu/), funded through the EU's Horizon 2020 research and innovation programme (https://cordis.europa.eu/project/id/825297), has already proved to be a vital tool in tackling COVID-19 related disinformation across Europe and beyond.

WeVerify has a video plugin to debunk fake videos on social media that spread conspiracy theories. In short, WeVerify/ InVID is a plugin that allows fact-checkers, journalists and any other interested users to quickly get contextual information about videos posted on Facebook, Twitter and YouTube videos. It can also perform reverse image searches on many platforms and efficiently query them. It can fragment videos, to enhance and explore key frames and images through a magnifying lens, to read video and image metadata, to check media copyright licenses, and to apply forensic filters on still images, all of which are vital tools for anyone trying to check the authenticity and source of the material. The plugin can be found on "WeVerify", an open-source platform aiming to engage communities and citizen journalists alongside newsroom and freelance journalists for collaborative, decentralized content verification, tracking, and debunking

"EXPERIENCE (The "Extended-Personal Reality": augmented recording and transmission of virtual senses through artificial-IntelligENCE)

The EU-funded EXPERIENCE project (https://cordis.europa.eu/project/id/101017727) seeks to use VR to enhance daily life by allowing brand new ways of social interaction and personal expression. It will develop the technology required to help users easily create and manipulate their own unique VR environments, significantly improving their virtual experiences. The goal is to bring VR into areas such as mental health treatment, entertainment and education, promoting VR as a means of significantly improving the human experience.

The results coming from T3.2 will next go through more thorough analysis in T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) in order to find most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats.

3.1.2 EU-HYBNET T3.3 ONGOING RESEARCH PROJECTS INITIATIVES WATCH

During the EU-HYBNET's seventh six month Action Report reporting period (M37 - M42/ May 2023 - October 2023) T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) conducted vast research on research projects and research initiatives to discover innovations and results of the identified gaps and needs which EU-HYBNET could start to analyze and eventually recommend for uptake or industrialization. The research was accomplished in line with the EU-HYBNET four core themes (Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communication) and the identified gaps and needs, threats to each of the four core themes according to T2.2/ D2.11 results. T3.3 scanned following relevant EU Member State's (EU MS) and European Commission's (EC) research projects and identified potential innovative solutions. The results of T3.3 are presented in details in

D3.9 "*Second Mid-term Report Innovation and Monitoring*" (M41/ September 2023) but the most important analysis from D3.9 to the "*First Three Lines of Action*"/ "*Monitoring of research and innovation projects with a view to recommending the uptake or the industrialization of results*" is reported below according to EU-HYBNET's Four Core Themes.

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

Threat: Spreading violence

UNI_SEL, Universalism or selectivism? What citizens think about the institutional design of the future welfare state?

Start date 1 October 2021, End date 31 May 2024
Web: https://cordis.europa.eu/project/id/101023631

The social legitimacy of universal vis-à-vis selective welfare provision systems remains very much an open question. UNI-SEL explores cross-national, experimental and longitudinal data to identify under which circumstances (when, where and why) one social policy design option is more popular than the other. The findings will benefit the institutional design of the future welfare state as it will clarify the social legitimacy of universal vis-à-vis selective welfare.

ENGAGE, Engage Society for Risk Awareness and Resilience

Start date 1 July 2020, End date 31 December 2023
Web: https://cordis.europa.eu/project/id/882850

ENGAGE contributes to the target to make cities and human settlements inclusive, safe, resilient and sustainable. The setting is that society have to cope with hazards, requiring that all individuals specifically and the civil society at large, acquire the ability to rapidly respond to natural disaster and to man-made risks. The ability of societies to adapt and prosper depends on the collective action of the whole society. ENGAGE will show how individuals and local practices can interrelate effectively with planned preparedness and response, practitioners and technology and study the significant role citizens and communities play at the grassroots level. It will create innovative new ways of fostering trans-disciplinary collaboration and learning across disciplines. The ENGAGE results will have relevance for how to build civic engagement, political participation and community Involvement as well as for institutional design.

POLAR: Polarization and its discontents: does rising economic inequality undermine the foundations of liberal societies?

Start date 1 April 2020, End date 31 March 2025
Web: https://cordis.europa.eu/project/id/833196

POLAR studies if the trend of increasing economic inequality in Western societies is leading to societal problems, and when, to which extent and in what respects rising inequality may affect the nature of our societies. POLAR specifically examines patterns of social mobility, the extent of social cohesion, and the level of trust in democratic institutions. It also investigates to which extent rising inequality may interfere with societies' capabilities to allocate positions according to merit and talent, to engage in cooperative social relations, and to decide on political matters through fair and transparent democratic processes. The POLAR results will thus be relevant for understanding the role of economic conditions as the project will provide new empirical evidence on the purportedly negative relationship between inequality and social mobility, support for democracy, and social cohesion in the West.

PERGAP: The (Mis)Perception of Economic Inequality: The Impact of Welfare State Institutions on Social Perception and Preference Formation

Start date 1 December 2022, End date 30 November 2027
https://cordis.europa.eu/project/id/101042125

PERGAP will create a unique country-comparative dataset on institutional disparities and expand knowledge of the (self-)legitimizing mechanisms of public institutions. Different countries' social security systems provide different answers to the questions "who receives what and why?", and "who should get what and why?", which ultimately shape the way citizens see and justify the existing inequalities in society. Ultimately, it will lead to a comprehensive theoretical and empirical understanding of the impact of public institutions on social perceptions and preference formations. The rise of economic inequality in countries around the globe is causing societal and political concern. The project results will contribute to cross-cultural and cross-national studies, bringing a better understanding of how individuals' perception and response to inequalities varies between societies and social groups and how it influences civic engagement and community involvement.

PaCE: Populism And Civic Engagement – a fine-grained, dynamic, context-sensitive and forward-looking response to negative populist tendencies

Start date 1 February 2019, End date 30 April 2022
Web: https://cordis.europa.eu/project/id/822337

PaCE will analyse the causes, rise, specific challenges to liberal democracy, transitions related to leadership changes and consequences of these movements. PaCE will propose responses and develop risk analyses for each type of movement and transition by employing an agent-based simulation of political processes and conducts. The project developed an open source tool relying on machine learning algorithms for identifying and tracking populist narratives. The tool is not limited to populist narratives, it can be used to search for any topics in any language e.g., use of violence. It is also will result in specific interventions aimed at: the public, politicians, activists and educators. It also looked into the future and developed new visions concerning how to respond to populism.

ViEWS – a political Violence Early Warning System

Start 1 September 2022, End date 29 February 2024
Web: https://cordis.europa.eu/project/id/101069312

ViEWS is a political violence early warning system. Predicting political violence is useful for first responders and policymakers and ViEWS is a tool for research on high-quality forecasts of political violence. The project will design a plan to explore the system's societal potential and financial viability and will describe how to maximise the system's functionality for conflict prevention and mitigation, preserve and strengthen transparency and open-access publication strategies. This project is interesting as it is an example of how prediction methods can be developed and used for conflict prevention and mitigation.

ODYCCEUS: Opinion Dynamics and Cultural Conflict in European Spaces

Start date 1 January 2017, End date 30 June 2021
Web: https://cordis.europa.eu/project/id/732942

ODYCCEUs sought conceptual breakthroughs in Global Systems Science, including a fine-grained representation of cultural conflicts based on conceptual spaces and sophisticated text analysis, extensions of game theory to handle games with both divergent interests and divergent mindsets, and new models of alignment and polarization dynamics. The project gives an interesting example of an open modular an open-source platform that integrates tools for the complete pipeline, from data scraped from social media and digital sources to visualization of the analyses and models developed by the project.

Threat: Attack on social structures

The Countering Foreign Interference (CFI) project

CFI is an EU-funded project (funded by the Service for Foreign Policy Instruments) that started at the beginning of this year. The FCI project focuses on improving understanding of potential threats in the information space. It will utilize accumulating knowledge for developing improved tools and methods to identify, monitor and counter those threats. More specifically, the project will contribute to enhancing the EU's and Member States' capabilities and resilience towards foreign information manipulation and interference to support the European way of life and fundamental values. Thereby, the aims of the CFI project could involve matters related to interference in research and innovation but since the project has not produced publications, it cannot be verified[2].

Mutual Learning Exercise (MLE)

During this year MLE has started based on the European Commission's publication ***Tackling R&I foreign interference***[3]. The MLE is funded by EC's Policy Support Facility for Horizon Europe and has three focus areas, which all are relevant to the topic of this analysis: Awareness raising and stakeholder engagement, Understanding and identifying foreign interference threats, and Measures to counter foreign interference threats. Due to the relatively short running time so far of the MLE, it has not yet published reports on its progress. The MLE of foreign interference will organize a dissemination event in the spring of 2024 and it will end in November 2024[4]. In the meantime, we suggest that the progress and outputs of the MLE should be monitored. The MLEs produce typically several thematic reports that will offer up-to-date information about their progress. Therefore, we expect the upcoming reports of the MLE on Tackling R&I Foreign Interference will present additional insights on the identification of foreign interference and new innovative means to tackle such hybrid threats.

The EU Knowledge Network on China (EU-KNoC)

EU-KNoC initiative's objective was "to create an R&I Knowledge Network on China that connects European networks, centres, and experts working on China." It was launched by the EC's DG for Research and Innovation in the summer of 2020 and ended in autumn 2021. The initiative's work has continued in a follow-up project for EU-KNoC. The concrete outcomes of the original EU-KNoC initiative were a list of recommendations for future collaboration with China[5], which could be used as a benchmark for other partner countries as well. The recommendations included topics such as: information sharing considering specific needs of EU-MS, strengthening transparency of European

[2] https://www.iss.europa.eu/projects/countering-foreign-interference

[3] https://www.zsi.at/de/object/project/6522

[4] https://era.gv.at/governance/era-forum/mutual-learning-excercises/; https://www.zsi.at/de/object/project/6522

[5] https://data.consilium.europa.eu/doc/document/ST-1204-2021-INIT/en/pdf

cooperation activities with China, identifying common priority areas for cooperation, and toolbox for supporting STI [Science, Technology and Innovation] cooperation with China. In addition, EU-KNoC published a study *Annotated Collection of Guidelines and Meta-Checklist supporting the safe and successful international science and technology cooperation* in 2021 (Klueting et al., 2021). The latter publication has been updated by DLR in 2022 (Heinrichs & Klueting, 2022[6]C:\Users\paikuos\Downloads\"https:\www.science-diplomacy.eu\wp-content\uploads\2022\09\annotated-collection-2022.pdf"). The follow-up project of EU-KNoC collected information about the security measures in the European HEIs and RPOs through a survey at the beginning of 2023[7]. The results of the survey have not been published so far, or they are not publicly available, but they will be very interesting for their potential usefulness for countering hybrid threats in research and innovation.

As the EU-KNoC's review of guidelines (and DLR's updated version) has found out, there are dozens of different manuals published by individual higher education institutions, governments, and the EU. Most of the existing guidelines to tackle foreign interference in R&I have focused on China or been country-neutral with a general view on internationalization or a limited view on human rights, dual-use or export control (see DLR's document, Heinrichs & Klueting, 2022). Considering the recent cases of foreign interference, there is a specific and urgent need to produce guidelines for R&I interference from Russia. It has turned out that Russian spies have been able to develop credible fake identities that have not been detected before they have started employment or even worked longer time in European HEIs. This implies that the EU and the Member States must take the threat of foreign interference in HEIs more seriously because the cases are not always easily recognized. The EC's Staff Working Document *Tackling R&I Foreign Interference* (European Commission, 2022, p. 20) suggests that "additional tools may need to be developed (including context-specific risk assessments, checklists, screening mechanisms, and best practices) to support HEIs and RPOs in identifying and addressing gaps." These efforts would benefit from at least one of EU-KNoC's recommendations (slightly modified from the original EU-KNoC recommendation, see list of recommendations for the future collaboration with China above), which is building a continuous monitoring mechanism of foreign interference activities in the EU. The monitoring would entail information sharing between the Member States. Over time the monitoring mechanism would develop into a database of known cases of foreign interference in R&I in the European HEIs. This kind of database would also benefit from a collection of best practices that will be done in the MLE on foreign interference. A comprehensive database would serve the information needs of the pan-European security practitioners, in particular intelligence and police authorities.

Threat: Undermining institutions' internal organisation

EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective. GA No. 608385

Duration: 2014 – 2018
Web: **https://cordis.europa.eu/project/id/608385**

The main goal of EUCISE2020 has been to develop and to build a "Common Information Sharing Environment" (CISE) to European Union Member States (EU MS) various security maritime authorities in order to support their cooperation by using a dedicated platform for information sharing. In short, CISE

[6] https://www.science-diplomacy.eu/wp-content/uploads/2022/09/annotated-collection-2022.pdf
[7] https://eua.eu/partners-news/1001-survey-on-existing-approaches-for-responsible-international-r-i-cooperation-by-higher-education-institutions-and-research-performing-organisations-in-europe.html; https://survey.dlr-pt.de/index.php?r=survey/index&sid=596249&lang=en

is a service platform that is able to ensure interoperability among the legacy systems of EU MSs and maritime sectors of EU MS authorities based on agreed roles and rules. The CISE has been involving c. 60 European maritime authorities from 16 states, and the international and cross-sectorial information exchange network is currently operating among 12 nodes both national and European. Furthermore, the CISE has supported to (i) improve the harmonisation of intersectoral maritime awareness (ii) ensuring the EU MSs the direct control in the management of the information shared through the CISE intersectoral node and national nodes. Present CISE is hosted by EMSA/ European Maritime Security Authority and its' development will continue as mentioned in the "Strategic Compass for Security and Defence". This all speaks on behalf of its valuable approach to support multi-sectoral and multi-agency/institution information sharing needs in order to gain better awareness and cooperation in maritime security. While CISE has been focusing on maritime authorities' information sharing needs, the CISE approach can also be copied and developed to serve other security authorities' needs too, such as security agencies and offices focusing on hybrid threats. Due to the successful use of maritime CISE, the EC has granted funding also to other projects to build CISE for authorities focusing on security concerns in land borders and custom. The projects are ANDROMEDA and CONNECTOR.

ANDROMEDA/ An EnhaNceD Common InfoRmatiOn Sharing EnvironMent for BordEr CommanD, Control and CoordinAtion Systems. GA no. 833881

Duration: 2019 – 2021
Web : **https://cordis.europa.eu/project/id/833881**

The main goal of ANDROMEDA has been to benefit on the European Union's Common Information Sharing Environment (CISE) approach, and how with the support of CISE information may be shared seamlessly with a range of third actors, including police agencies and defence forces. In ANDROMEDA CISE is making different systems interoperable so that data and other information can be exchanged easily via modern technologies. ANDROMEDA will leverage on the developments, results and experience of CISE that is also partly gained in EC projects such as PERSEUS, CloseEye, MARISA, RANGER. Due to the success in CISE (maritime security authorities) and ANDROMEDA (land borders), also pan-European custom authorities has been interested in having similar system. Due to this noticed need a project called CONNECTOR has just been grant EC Horizon Europe funding. The CONNECTOR will kick off during October 2023.

CONNECTOR - Customs extended interoperable Common information sharing environment. GA No. 101121271

Duration: 2023 – 2025

CISE is not only to support various pan-European security authorities to increase their cooperation, but it also empowers the cooperation in national level due to the development of national nodes. In short, without the cooperation between the national security institutions and authorities in the specific security domain (e.g. in maritime domain/ border guards, navy, police, customs) development of the solution/CISE national node would not have been possible. In short, the pan-European CISE has pushed national security authorities and institutions to find and definite new ways of cooperation and information sharing reducing partly also the culture of secrecy between institutions and inside the institutions. An example of increased cooperation between national *strategic security institutions* is a FINCISE project from Finland **FINCISE 2.0 Project** CISE | The Finnish Border Guard (raja.fi) (Duration: 2022 -2024) where all Finnish Maritime Cooperation (FIMAC) authorities joined to CISE development and finding new ways for future cooperation. On the whole, the takeaway from the above mentioned CISE projects' is that the approach seems to work in various security domains and hence also hybrid threats related security authorities could consider to develop CISE for their purposes. Furthermore, CISE seems to support cooperation between strategic security institutions and diminish culture of secrecy between institutions, also in the institution.

STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats GA No. 740610

Duration: 2017 – 2021
Web: https://cordis.europa.eu/project/id/740610

What comes to platforms that support especially strategic security institutions' internal information sharing culture in different positions and parts of administration to proceed, esp. in a case of crises, a platform developed in an EC funded project STOP-IT, aims to this. Even though STOP-IT focuses on delivering a solution for authorities in water security and management, still the STOP-IT platform may provide an example to any other security domain and their institutions and authorities incl. hybrid threats.

STOP-IT has delivered an integrated, modular platform that supports strategic/tactical planning, real time operational decision making and post-action assessment for the key parts of the water infrastructure. Furthermore, the platform is scalable (scaling from small utilities to large ones); adaptable (including various modules addressing different needs, with expandability for future modules); and flexible (the utility managers can decide how to use it and it will be usable by experts, novices, and even non-technical staff). On the whole, the platform support to enhance cooperation skills and trust between the users because its use provides exercise(s) that may then ease the cooperation in the future in real cases. The platform has been developed to three different user categories in and organizations, but it can also host multi-agency/ institutions discussion and planning. The categories in the platform are: Decision Makers; Risk Officers and Modellers; Real Time Operators and Maintenance Managers.

Third Phase of the Consultation Forum for Sustainable Energy in the Defence and Security Sector, EDEN, (CF SEDSS III

Duration: 2019 – 2023
Web : https://eda.europa.eu/what-we-do/eu-policies/consultation-forum/phase-iii
Web: https://eda.europa.eu/docs/default-source/events/eden/annex-a-conf-prog-23-24-11-21.pdf

Positive experiences on enhanced cooperation and trust, also possibility to learn other organizations' manners to react to critical security challenges have been part of European Defence Agency (EDA) EDEN project that included exercise based on approaches in CORE Model[8]. According to the training & exercise experience, the CORE Model was seen much to support the understanding between various authorities and enhancing their cooperation. Therefore, approaches and methodologies to support strategic institutions to enhance their cooperation and information sharing, also building trust among actors, are much underlined are solid innovations to counter hybrid threats.

NOTIONES - Interacting network of intelligence and security practitioners with industry and academia actors GA No. 101021853

Duration: 2021 – 2026
Web: https://cordis.europa.eu/project/id/101021853

[8] https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en

Security frameworks designed by national intelligence communities according to specific threats to strategic institutions may also support to overcome the challenges in cooperation and information sharing. An EC funded project NOTIONES may deliver some views to this while at present the project merely focuses on technological solutions to security practitioners', and especially needs of intelligence services. After all, the key activities in NOTIONES are to build and maintain a pan-European ecosystem of security and intelligence practitioners in order to (**1**) monitor technologic opportunities and advancements and best practices and (**2**) define and refine requirements and standardization needs. NOTIONES project will last until 2026 and hence solutions that will serve to build security framework by national intelligence may be gained through the project.

EU-HYBNET Project Core Theme: Cyber and Future Technologies

Threat: Stealing data attacking individuals

FLUTE, Federate Learning and mUlti-party computation Techniques for prostatE cancer

Start date 1 May 2023, End date 30 April 2026
Web: https://cordis.europa.eu/project/id/101095382

FLUTE will demonstrate the practical use of federated learning and multi-party computation techniques having health data hubs located in three different countries. Flute will provide an example of a novel federated AI toolset to provide privacy protection, pushing the performance envelope of secure multi-party computation, used for diagnosis of clinically significant prostate cancer.

SECURED, Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

Start date 1 January 2023, End date 31 December 2025
Web: https://cordis.europa.eu/project/id/101095717

SECURED demonstrate technologies developed in health-related use cases like real-time tumour classification, telemonitoring for children and access to genomic data. It will do this by increasing efficiency, scaling up multi-party computation, data anonymisation and synthetic data generation, focusing on private and unbiased AI and data analytics. The results on how to increase efficiency in multi-party computation to allow private and unbiased AI and data analytics will be of great interest.

HARPOCRATES Data analytics and cryptography for privacy preservation

Start date 1 October 2022, End date 30 September 2025
Web: https://cordis.europa.eu/project/id/101069535

HARPOCRATES will design and demonstrate several practical cryptographic schemes (functional encryption and hybrid homomorphic encryption) for analysing data in a way that preserves privacy and enables a comprehensive approach where data analytics and cryptography are associated with increased privacy. This project will advance the encryption techniques used for privacy protection and can become part of generic solutions.

PAROMA-MED, Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications

Start date 1 July 2022, End date 30 June 2025

Web: https://cordis.europa.eu/project/id/101070222

PAROMA-MED aims to develop novel technologies, tools, services and architectures for patients, health professionals, data scientists and health domain businesses so that they will be able to interact in the context of data and machine learning federations according to legal constraints and with complete respect to data owners' rights to privacy protection to fine grained governance, without performance and functionality penalties of ML/AI workflows and applications. The project will develop a hybrid-cloud based delivery framework for privacy and security assured services and applications in a federative environment, in particular presenting privacy preserving processing and trusted data storage.

ENCRYPT, A Scalable and Practical Privacy-Preserving Framework

Start date 1 July 2022, End date 30 June 2025
Web: https://cordis.europa.eu/project/id/101070670

ENCRYPT will, based on different use cases, evaluate and validate Differential Privacy, Multi-Party Computation, Full Homomorphic Encryption (FHE) and Local Differential Privacy. The project will develop a scalable, practical, adaptable privacy-preserving framework, allowing researchers and developers to process data stored in federated cross-border data spaces in a GDPR-compliant way. The project will address the limitations of the studied Privacy Preserving (PP) technologies in several aspects such as scalability and performance issues, by going beyond the single-key FHE paradigm. Furthermore, it will investigate the combinations of several of these PP methods. The improvements will be of general interest in the implementation of privacy preserving solutions.

SPATIAL: Security and Privacy Accountable Technology Innovations, Algorithms, and machine Learning

Start date 1 September 2021, End date 31 August 2024
Web: https://cordis.europa.eu/project/id/101021808

SPATIAL will address the challenges of black box AI and data management in cybersecurity. To do this, it will design and develop resilient accountable metrics, privacy-preserving methods, verification tools and a system framework to pave the way for trustworthy AI in security solutions. SPATIAL will design and develop required critical building blocks to achieve trustworthy AI in security solutions. In particular, it will develop systematic verification and validation software/hardware mechanisms that ensure AI transparency and explainability in security solution development and system solutions that enhance resilience in the training and deployment of AI in decentralized, uncontrolled environments. Results will be of interest when designing future privacy preserving solutions.

Threat: Online manipulation attacking democracy

Research scan on this topic did not reveal research projects that would be specifically dedicated to the phenomena of fake attacks and their handling. It seems that it is considered still a practical discipline of the general preparedness framework, and decisions "real or fake" in the highly intense situation of limited awareness and time pressure is left to the experience and gut feeling of decision makers. We thus collected EU funded projects which are not completed at the time of preparation of this deliverable, which deal with the hazard monitoring / mitigation, which should consider including in their scenarios early identification of false positives, considering that false positive signals can be intentionally generated by adversaries.

European System for Improved Radiological Hazard Detection and Identification, RADION

Start date 1 September 2020 - 29 February 2024

Web: https://cordis.europa.eu/project/id/883204

To better defend itself against chemical, biological, radiological, nuclear and explosive (CBRNE) attacks and threats, Europe needs a specialised, efficient and sustainable CBRNE protection scheme. The EU-funded EU-RADION project therefore aims to offer an innovative solution for some of the shortcomings that exist in CBRNE protection. To this end, it will create an operational radiological threat detection and identification system consisting of several technological components. The components will include radiological threat dispersion modelling and analysis tools, test sensor platforms, including a swarm of mini unmanned ground vehicles, a tactical command tool, a network controller and a sensor integration unit. The project will play a role in improving European resilience against CBRNE attacks and threats.

Innovative Cluster for Radiological and Nuclear Emergencies, INCLUDING

Start date 1 August 2019 - 31 July 2024

Web: https://cordis.europa.eu/project/id/833573

Radiological and nuclear (RN) threats are more real than ever, and they know no borders. Safety in this field requires a wide collaboration of many actors. In Europe, the EU-funded INCLUDING project will build a dynamic cluster of 15 partners from 10 EU Member States acting in the INCLUDING Federation. An advanced web platform will shape a map of cooperation between governmental, security and medical institutions, industrial services and others. Partners will provide multidisciplinary knowledge, research, new technologies and infrastructure. Procedures will be formed for joint actions: field exercises, training and simulations. The project will be a base for a modern flexible network for better security in the RN field in Europe.

PReparedness against CBRNE threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society, PROACTIVE

Start date 1 May 2019 - 31 August 2023

Web: https://cordis.europa.eu/project/id/832981

Chemical, biological, radiological and nuclear (CBRN) risks represent a major concern for the EU. The role of professionals can be reinforced by preparation and civil society engagement. The EU-funded PROACTIVE project will evaluate the response of security professionals such as law enforcement agencies (LEAs) to the demands of civil society comprising vulnerable citizens. The estimation of the effectiveness of existing procedures will lead to innovative proposals for policymakers and security professionals and will support the EU Action Plan for CBRN threats. The project aims to create innovative tools, including an information platform for LEA use and a mobile app tailored to meet the needs of vulnerable groups.

Threat: Attack on services

- *No defined projects*

EU-HYBNET Project Core Theme: Information and Strategic Communications

Threat: Media conundrum

Harnessing Data and Technology for Journalism (JOLT), ID: 765140

From: 1 May 2018 to: 30 April 2022
Website: http://joltetn.eu/
Cordis: https://cordis.europa.eu/project/id/765140

JOLT aimed to deliver a world-class, multi-sectoral PhD research-training programme focused on harnessing digital and data technologies to advance economically sustainable and socially valuable journalism. Journalism is in profound crisis arising from declining advertising revenues, the dominance of US technology platforms, and the rise of online information-sharing including fake news. Journalism research has not kept pace with these changes. This is reflected in the lack of European, and indeed global, PhD programmes focussed on the intersections of journalism, data and technology. Europe lacks knowledge on the best-practice integration of data and digital technologies, strategies to overcome organization disruption, and on the political, social and ethical implications of digital journalism. JOLT addressed this lack by creating a multidisciplinary and multi-sectoral consortium of five leading European universities and twelve non-academic partners (four as beneficiaries) representing journalism NGOs, SMEs and large-scale media enterprises. JOLT's training programme was grounded in the universities' academic excellence and the complementarity of diverse non-academic partners. In addition to secondments with non-academic partners, all ESRs attended 3 industry workshops, 6 seminars on research and transferrable skills, and 3 summer schools, which drew on the cross-sectoral and multi-disciplinary expertise of all partners. JOLT's key measurable outputs were much-needed open-source tools and technical protocols, 30 journal articles, 30 conference papers, 15 policy and best-practice guidelines, and extensive media outreach conducted in collaboration with JOLT's media partners. JOLT acted as a pilot for the formalization of similar PhD programmes, creating a sustainable network of multi-disciplinary and cross-sectoral partners to advance research/innovation beyond the project, and support the renewal of a socially valuable and competitive European media sector.

MeDeMAP Mapping Media for Future Democracies, ID: 101094984

From: 1 March 2023 to: 28 February 2026
Website: https://www.medemap.eu/
Cordis: https://cordis.europa.eu/project/id/101094984

To set out future-proof pathways to strengthen democracy through improving accountability, transparency and effectiveness of media production and expanding active and inclusive citizenship, the project aims to clarify the extent to which certain media under which conditions perform which democratic functions for which audiences, thus making it apparent what is at stake for democratic media - and for democracy itself.

By applying an innovative multi-method design consisting of data science methods, large-scale quantitative analyses, in-depth qualitative approaches and participatory action research, the project will cover (1) perspectives of both representative and participatory notions of democracy as they exist in European societies, (2) the entire range of news media, regardless of distribution channel, mandate, ownership and source of financing, (3) the legal and (self-)regulatory framework under which media houses and journalism operate and people use media, (4) the media's potential to promote and support political participation (supply side), and (5) the media use patterns, communication needs and democratic attitudes of the audiences (demand side) in all EU Member States.

Based on the research results, an interactive multi-layer map of European political information environments will be created, whose layers reflect the legal and regulatory framework and the democratically relevant features of media supply and demand. In addition, the obtained "real" map is to be confronted with a map of how European citizens envision the future media landscapes. By comparing these maps, conclusions can be drawn from congruencies and discrepancies between them, good practice examples can be identified and guidelines can be derived to support developments that promote democracy and counteract phenomena that may jeopardize democracy. These guidelines will be addressed to policymakers, regulators, self-regulation bodies, media houses, journalists, NGOs and citizens.

MeDeMAP could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, even though it is mainly concerned with promoting democracy and counteracting phenomena that may jeopardize democracy. Since democracy in media and journalism is a crucial component of integrity and quality, the guidelines that will stem from the project will cover media use patterns and communication needs in all EU Member States, aside from the democratic attitudes, as mentioned in the project description. These media use patterns, but also communication needs, could provide invaluable insight into the steps required to lead to economic sustainability of journalistic media.

ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE, ID: 101094742

From: 1 March 2023 **to:** 28 February 2026
Website: https://resilientmedia.eu/
Cordis: https://cordis.europa.eu/project/id/101094742

Resilient Media for Democracy in the Digital Age (ReMeD) responds to the European Commission's call HORIZON-CL2-2022-DEMOCRACY-01-06: "Media for democracy – democratic media" and will tackle existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. ReMeD could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, in the same way project MeDeMAP can.

By gathering, analysing, comparing and contrasting data regarding professional journalists, alternative media content producers and citizens which operate in technologically mediated configurations, as well as the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape, ReMeD could, as a biproduct identify trends and qualitative indicators which could help better understand the demand of and thus the sustainability of quality journalistic media.

INJECT Innovative Journalism: Enhanced Creativity Tools, ID: 732278

From: 1 January 2017 **to:** 30 June 2018
Cordis: https://cordis.europa.eu/project/id/732278

INJECT's objective was to transfer new digital technologies to news organisations to improve the creativity and the productivity of journalists, to increase the competitiveness of European news and media organisations. To achieve this objective, INJECT extended and aggregated new digital services and tools already developed by consortium members to support journalist creativity and efficiency, and integrated the services and tools with current CMSs and journalist work tools in order to facilitate their uptake and use in newsrooms. The services undertook new forms of automated creative search on behalf of journalists, using public sources (e.g. social media) and private digital resources (e.g. digital libraries of political cartoons) to generate sources of inspiration for journalists who were seeking new angles on stories. The tools provide new interactive support for journalists to think creatively about new stories and reuse news content in new ways to increase productivity. To transfer the new services and tools to Europe's news and media organisations, INJECT established a new INJECT spin-off business, built up and expanded multiple vibrant ecosystems of providers and users of new digital technologies, and exploited its position at the heart of Europe's journalism industry to raise market awareness and take-up on the services and tools. With respect to Call ICT21, INJECT increased the competitiveness of one of Europe's most important creative industries – journalism - by stimulating ICT innovation in SMEs, by effectively building up and expanding vibrant EU technological ecosystems that met the emerging needs of Europe's new and existing news and media organisations.

Threat: Antagonizing victimization narratives in the informational space

Understanding the Impact of Narratives and Perceptions of Europe on Migration and Providing Practices, Tools and Guides for Practitioners. PERCEPTIONS (HORIZON 2020 Grant agreement ID: 833870)

Narratives on a "better life" that can become reality elsewhere have always been shaping human migration. The image or idea of a "promised land", however, might not be real, and newcomers are often faced with obstacles and challenges. Certain narratives and perceptions of Europe influence migration aspirations and false images can not only lead to problems when the image does not hold true, but it might also even lead to security threats, risks or radicalisation. It is, therefore, of the utmost importance to understand and investigate narratives about Europe, how these can lead to problems and threats, how they are distributed, and, in a next step, find ways to react and counteract on them. Perceptions on Europe are formed in the country of residence, and they are based on a multitude of sources. Social media and new communication networks, in addition, have increased the scope and the intensity of distribution of such narratives; and furthermore, so-called filter bubbles and echo chambers can lead to isolated misperceptions that are not corrected. Due to new communication technologies, false or incorrect claims become life on their own, raise expectations or disapproval. At the same time, however, these technologies and communication networks might also provide a channel to set an exaggerated image straight and to promote a more realistic narrative. It is, therefore, the aim of the PERCEPTIONS project to identify and understand the narratives and (mis-)perceptions of the EU abroad, assess potential issues related with the border and external security in order to allow better planning and outline reactions and countermeasures. For that purpose, the project will conduct research on the narratives and the myths that are circulating about the EU in countries West- and Central Mediterranean area. Based on the research insights, the consortium will develop a PERCEPTIONS framework model including policy recommendations and action plans.

Threat: Attack on information

NL4XAI - Interactive Natural Language Technology for Explainable Artificial Intelligence

Timeline: 01/10/2019 - 30/09/2024
Website: https://nl4xai.eu/

With the help of Explainable AI (XAI) systems, the project will address the problem of making AI self-explanatory and help transform knowledge into products and services for economic and social benefit. As a supplement to visualization tools, NL4XAI focuses on automatically creating interactive explanations in natural language (NL), as humans do naturally. The project's output is interesting since it works directly with natural language. The foundation models, like GPT from OpenAI, LLaMA from Meta (Facebook), and PaLM from Google, are also large language models. Understanding them profoundly and constructing self-explanatory and reliable AI language models are needed to tackle the abovementioned threat.

TAILOR - AI systems made safe, transparent and reliable

Timeline: 01/09/2020 - 31/08/2024
Website: https://tailor-network.eu/

The goal of TAILOR is to establish a robust academic-public-industrial research network that can provide the scientific underpinnings for trustworthy artificial intelligence (AI) by leveraging and combining learning, optimization, and reasoning to create AI systems that incorporate safeguards that make them trustworthy, safe, transparent, and respectful of human agency and expectations.

This is another project considering the safety development of AI systems. The output can be later used for foundation models, more specifically. Within this project, the results of WP3 are highly relevant for the abovementioned threat-gap-need. The dimensions of the project - Explainability, Safety, Fairness, Accountability, Privacy, and Sustainability - are inextricably linked to the project's guiding principles through ongoing requirements and challenges to create approaches that balance value and legal protection. The question, which the WP3 addresses are:

- How can we guarantee user trust in AI systems through explanation?
- How to formulate explanations as Machine-Human conversation depending on context and user expertise?
- How to bridge the gap from safety engineering, formal methods, verification as well as validation to the way AI systems are built, used, and reinforced?
- How can we build algorithms that respect fairness constraints by design through understanding causal influences among variables for dealing with bias-related issues?
- How to uncover accountability gaps w.r.t. the attribution of AI-related harming of humans?
- Can we guarantee privacy while preserving the desired utility functions?
- Is there any chance to reduce energy consumption for a more sustainable AI and how can AI contribute to solving some of the big sustainability challenges that face humanity today (e.g. climate change)?
- How to deal with properties and tensions of the interaction among multiple dimensions? For instance, accuracy vs. fairness, privacy vs. transparency, convenience vs. dignity, personalization vs. solidarity, efficiency vs. safety and sustainability.

SHERPA - Shaping the Ethical Dimensions of Smart Information Systems

Timeline: 01/08/2018 - 31/10/2021
Website: https://www.project-sherpa.eu

HERPA project looked into, examined, and synthesized our knowledge of how ethics and human rights issues are affected by smart information systems (SIS; the fusion of artificial intelligence and big data analytics), working with a broad spectrum of stakeholders. The project:

- Described and represented the moral and human rights issues raised by intelligent information systems via case studies, scenarios, and creative representations.
- Collaborated with various stakeholders to determine their issues and ideal fixes (via stakeholder boards, Delphi studies, extensive internet surveys, and interviews).
- Created and published a workbook on the responsible development of smart information systems.
- Provided technical and regulatory options (such as a regulator's terms of reference).

- Used multi-stakeholder focus groups to validate and rank the proposals. Then, targeted dissemination and communication efforts to advocate for, promote, and implement the most promising solutions.

The project outputs are relevant to the addressed threat since they tackled the problem of protecting ethical aspects and human rights while developing smart information systems (AI and Big data). On their homepage, the two highly relevant guidelines are provided:

- Guidelines for the Ethical Use of AI and Big Data Systems[9]
- Guidelines for the Ethical Development of AI and Big Data Systems: An Ethics by Design approach[10]

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

Threat: Political deficiency

Supporting vulnerable populations in combating disinformation and improving social participation, DesinfoEND

project duration: 1/02/2022-1/02/2024
web: https://desinfoend.eu/

The main purpose of this project is to promote the social inclusion of adults in a vulnerable situation through the acquisition of critical thinking and digital and media literacy skills. The approach adopted by the project, which can be inspirational for other projects and actions connected with countering disinformation, is to define the groups of vulnerable individuals and boost critical thinking in those groups (Vulnerable populations defined in DesinfoEND: Unemployed adults, people with lower level of education, people aged 55+)

IMMUNE 2 INFODEMIC

project duration: 1/01/2023 – 31/12/2024
web: https://immune2infodemic.eu/

IMMUNE 2 INFODEMIC aims to immunise EU citizens against the disinformation and misinformation on selected themes by empowering and equipping them with several methods using eye-catching material and easy-to-use tools. The project consortium formulates and co-produces 3 instruments (vaccines): digital literacy, media literacy, critical thinking; and applies these instruments on 3 selected hot themes (boosters): elections, COVID-19 and migration. The aspect that is especially interesting is the idea of being proactive (rather than reactive) and informing about disinformation action/campaign before it actually happens so that citizens are prepared before it starts.

Threat: New agit-prop

vera.ai / VERification Assisted by Artificial Intelligence, Grant agreement no: 101070093

[9] https://www.project-sherpa.eu/wp-content/uploads/2019/12/use-final.pdf
[10] https://www.project-sherpa.eu/wp-content/uploads/2019/12/development-final.pdf

Cordis: https://cordis.europa.eu/project/id/101070093
Project duration: 15 September 2022 - 14 September 2025

The main goal is to fighting online disinformation with trustworthy AI solutions. Online disinformation and fake media content has become a serious threat to democracy, the economy and society. Assessing the veracity/reliability of online content and uncovering highly complex disinformation campaigns is a huge challenge for researchers and media professionals. Vera.ai aims to build professional, trustworthy AI solutions against high-level disinformation technics, to be co-created with and for media experts and researchers, and to lay the groundwork for future research in AI counter disinformation. Key innovative features of artificial intelligence models will be fairness, transparency (including explainability), resistance to concept drift, continuous adaptation to the evolution of disinformation through a fact-checker-in-the-loop approach, and the ability to handle multimodal and multilingual sources. Recognizing the dangers of AI-generated content, the project will develop tools for deep detection of false information (audio, video, image, text). Artificial intelligence models will continuously collect fact-checking data collected from real-world content verified using the InVID-WeVerify plugin and the Truly Media/EDMO platform.

What is most interesting about vera.ai tool (Verification Plugin) is that social media and online content will be rapidly analysed and contextualised to reveal disinformation campaigns and measure their impact.

SMIDGE: Social Media narratives: addressing extremism in middle age, Grant agreement no. 101095290

Cordis: https://cordis.europa.eu/project/id/825469
Project duration: 1 March 2023 – 28 February 2026

Conspiracy theories, misinformation and extremism online having a direct impact on perceptions of democratic institutions, trust in science, and leads to calls for direct action to overthrow or disrupt democratically elected governments. Those in middle age (45-65) may be both susceptible to extremist narratives and also influential as decision-makers. SMIDGE will analyse the various forms of extremist discourses and narratives across Europe through social network analysis, textual and content analysis of extremist discourse, and will consider national and demographic specifics through survey, focus groups and interviews in 6 countries (UK, Italy, Belgium, Denmark, Kosovo, Cyprus). From this in-depth examination of the current state of the art, SMIDGE will:

- develop counter-narratives and educational resources to promote reflexivity and provide evidence-based tools and training for journalists and security professionals;
- provide guidelines & recommendations for policy and decision-makers based on the project findings, and present these findings to security professionals, policy makers, and journalists through roundtables and conference.

SMIDGE will provide effective and innovative countermeasures for policymakers with valuable insights and recommendations on how to tackle extremist narratives related to disinformation and conspiracy theories that affect the society (with special emphasies middle-aged adults).

FERMI: Fake nEws Risk MItigator, Grant agreement no: 101073980

Cordis: https://cordis.europa.eu/project/id/101073980
Project duration: 1 October 2022 – 30 September 2025

FERMI develops a framework to detect and monitor the way that disinformation spreads, both in terms of locations and within different segments of the society, and to put in place relevant security countermeasures. The main goal is to analyse and assess direct risks posed by disinformation to the offline environment and minimise the impact. The FERMI project result will be relevant for European Police Authorities, other professionals and stakeholders, and EU citizens Facilitate the EU LEAs and (social) media organizations in the combat against disinformation by providing training and education material.

RECLAIM: Reclaiming Liberal Democracy in Europe, Grant agreement no: 101061330

Cordis: https://cordis.europa.eu/project/id/101061330
Project duration: 1 October 2022 – 30 September 2025

New tools to address post-truth politics in Europe. RECLAIM project will address the implications of post-truth phenomena in three distinct phases by generating a conceptual definition, operationalisation and empirical indicators to analyse post-truth/post-factual politics; analysing the current state of play as regards the various dimensions of post-truth politics in Europe; using its own empirical findings regarding the state of play of post-truth politics to develop policy recommendations, methods and toolkits to effectively address the various expressions of the phenomenon. One of the Work Package is dedicated to trust in and demand for quality journalism. Moreover, project will map and assess the demands and supply of quality news and journalistic standards in terms of impartiality and truth from the perspective of three key players in news production and dissemination: a) digital platform/social media providers; b) professional journalists and news media organizations; c) governments. A key element of the RECLAIM project is to analyse disinformation in Europe and use the results to advise policy-making, education and action to respond to the negative impact of disinformation on democratic discourse and the basic structure of modern liberal democracy.

ReMeD: RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE, Grant agreement no: 101094742

Cordis: https://cordis.europa.eu/project/id/101094742

Project duration: 1 march 2023 – 28 February 2026

The project will address existing challenges to a healthy relationship between media and democracy by taking an approach to improving the relationship between citizens, media and digital technologies. Through an interdisciplinary approach and innovative methodology that combines qualitative and quantitative methods, ReMeD will collect, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in today's media landscape. This project's timing is especially pertinent, as the outcomes and policy suggestions from ReMeD will directly contribute to the ongoing discussions regarding the development and execution of the Digital Services Act and Digital Markets Act.

MeDeMAP: Mapping Media for Future Democracies, Grant agreement no: 101094984

Cordis: https://cordis.europa.eu/project/id/101094984
Project duration: 1 march 2023 – 28 February 2026

Project aims to establish forward-looking pathways to strengthen democracy by improving accountability, transparency and efficiency in media production and expanding active and inclusive citizenship. Based on the research results, an interactive multi-layer map of European political information environments will be created, whose layers reflect the legal and regulatory framework and the democratically relevant features of media supply and demand. Moreover, the obtained map is to be compared with a map of how European citizens envision the future media landscapes. By comparing these maps, it is possible to learn from the compatibility and differences between them, identify good practices and develop guidelines to support development that promotes democracy and counteracts phenomena (disinformation) that may threaten it. These guidelines will be aimed at policymakers, regulators, self-regulatory bodies, media houses, journalists, NGOs and citizens.

Threat: Substitutive reality

XRHuman: Establishing the European standards for extended reality

Timeline: 01/11/2022 - 31/10/2025
Project Website: https://xr4human.eu

The XR4Human project, financed by the EU, intends to create living standards for XR technology ethics and related legislative, regulatory, governance, and interoperability concerns within a European community of practice. The work on this project will prepare the path for a robust and competitive ecosystem, headed by European businesses, for the widespread deployment, use, and acceptance of XR technology[11]. The project addresses directly the need mentioned above by creating guidance documents and standards for XP development. The main outputs of the projects are:

- A European code of conduct for responsible XR technologies
- Test cases for demonstration and validation of XR development
- An Interoperability guidance document
- And a rating system and education sandbox for XR development.

GuestXR: A Machine Learning Agent for Social Harmony in eXtended Reality

Timeline: 01/01/2022 - 31/12/2025
Project Website: https://guestxr.eu/

GuestXR has been created to be a socially interactive multisensory platform system that leverages Extended Reality (virtual and augmented reality) as the medium to bring people together for immersive, real-time face-to-face engagement with valuable social outcomes. The crucial innovation is the involvement of artificial agents that assist online social gatherings in realizing their objectives through gradual learning. These agents use machine learning to figure out how to steer a meeting toward a particular goal [12]. The participants' individual and social behaviour will be analysed by a machine learning agent named "The Guest" using current theoretical frameworks from the perspectives of neuroscience and social psychology. The results of GuestXR are highly relevant to the threat discussed above. We would like to see how the online social available information can be gathered and later used to train the agent and how the agent will influence human behaviour and human brain.

iv4XR - Intelligent Verification/Validation for Extended Reality Based Systems

Timeline: 1/10/2019 - 31/12/2022
Project Website: https://iv4xr-project.eu/

iv4XR provides the XR developers with a novel AI-based content verification and validation environment. The developers will have a tool to test their developed virtual world automatically. Besides, to enable test agents to automatically evaluate the quality of the user experience and parameterize it by various demographic and socioeconomic kinds, such as male, female, young, and elderly, iv4XR also creates a socio-emotional AI[13].

[11] https://xr4human.eu
[12] https://guestxr.eu/
[13] https://iv4xr-project.eu/

> The core idea and objectives of the project are interesting for the threat described above. The content of XR can be validated with AI agents. Besides improving user experience, we can extend the platform to validate the correctness of the virtual world or to experiment how the XR content can impact the human brain.

Alike with the results coming from T3.2, also the results from T3.3 will next go through more thorough analysis in T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) in order to find most promising innovations to present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats.

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

EU-HYBNET Task (T) 5.3 "*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, and a thorough report on the event is delivered in D5.12 "*Annual workshop Report 3*" (M37/ May 2023 by MVNIA). 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 is also to 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 results alike increase amount of new relevant members in the 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 were 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**. In the Annual workshop, after the pitches and project presentations, Annual Workshop participants had an opportunity to address questions to the innovation providers to learn more on the innovations and their promising nature. The participants were also requested to assess and rate the innovations innovations' uptake possibilities via questionnaire which was sent to them. The assessment criteria in the questionnaire originated from EU-HYBNET T3.1 "*Definition of Target Areas for Improvements and Innovations*" and focused on the following three elements: 1) Excellence, 2) Impact and 3) Implementation; scale 1-5 (1: lowest, 5: highest). The use of the T3.1 assessment criteria in the questionnaire was to ensure that the results could be easily imbedded into

T3.1 analysis work on most promising innovations. According to the questionnaires results reported in T5.3/D5.12, the ratings were as follows:

Name of the innovation	Excellence	Impact	Implementation
Maltego	*4,7*	*4,2*	*4,0*
TrustServista	*4,56*	*4,33*	*4,22*
CRiTERIA -project	**4,4**	**4,4**	**4,10**
CYCLOPES -project	3,8	3,89	3,8
CRESCENT -project	4,10	4,0	4,00
DOMINOES -project	4,10	4,0	4,00

The Annual Workshop innovation presentations and assessment from the audience pointed out that developed innovations from projects CriTERIA and CRESCENT and DOMINOES and innovation development actions in the case Maltego do offer very promising solutions to the identified gaps and needs to counter hybrid threats. Therefore, the identified and recommended solutions are also to be further promoted by EU-HYBNET and to have a more thorough analysis in EU-HYBNET Task 3.1/ Deliverables D3.19 "*Final Report with Overview Mapped on Gaps and Needs*" M50 (June 2024). The CRiTERIA project was welcome add to the innovation discussion because it is seen that sound solutions to counter hybrid threats in European borders are much needed.

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, especially EU-HYBNET's Task (T) 2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC) results are playing a key role because T2.2 delivers the knowledge of the latest, most critical pan-European security practitioners' and other relevant actors' gaps and needs to counter hybrid threats. However, while T2.2 delivers the knowledge of gaps and needs, the knowledge of **common requirements as regards innovations that could fill in gaps and needs** is delivered by T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) in their latest and also forthcoming event. In addition, latest EU-HYBNET report on recommendations for a promising innovation uptake delivered by T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE) together with WP5 "*Communication, Dissemination and Exploitation Activities*" (lead by EOS) is also central to highlight the **common requirements as regards innovations that could fill in gaps and needs**. More detailed descriptions of the named Tasks and their results are described in the forthcoming sub-chapters.

Next to the named task it is also important to highlight that also results from T3.2 and T3.3 innovation mapping to gaps and needs have provided some insight on **common requirements as regards innovations that could fill in gaps and needs.** Because T3.1 will deliver deeper analysis on EU-HYBNET's T3.2 and T3.3 identified innovations to the EU-HYBNET's 3rd project cycle gaps and needs, the results will be described in the forthcoming EU-HYBNET Six Month Action Reports.

3.2.1 EU-HYBNET T2.2 RESEARCH TO SUPPORT INCREASE OF KNOWLEDGE AND PERFORMANCE

EU-HYBNET's work to deliver results to **common requirements as regards innovations that could fill in gaps and needs** is especially part of EU-HYBNET's T2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC) because T2.2 delivers the knowledge of the latest, most critical pan-European security practitioners' and other relevant actors' gaps and needs to counter hybrid threats. The key gaps and needs, threats has been described in T2.2 latest deliverables D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (M39/ July 2023) that is "consortium only" labelled document. Therefore, following summary of the D2.11 key findings of gaps and needs are described in the form of "threats" relevant to the second Three Lines of Action and reported according to the EU-HYBNET project's four Core Themes. As it is stated in D2.11 the result could certainly not claim to be an exhaustive collection of all threats that face Europe. It is, nonetheless, an attempt to a better understanding, and a step to improve the continent's security environment through EU-HYBNET project's collective work.

<u>EU-HYBNET Project Core Theme: Resilient Civilians, Local Level and National Administration</u>

It is seen especially important to addresses threats related to the links between the society and its institutions, also paying attention to long term perspective in the malicious actions. There is especially need to focus on three following threats:

- Diffusion of violence among the society
- Attacks against the institutions providing social services to the population
- Pressures on institutional systemic issues

EU-HYBNET Project Core Theme: Cyber and Future Technologies

The main concerns of threats focus on mobilising innovative technical means to breach security environments. Special attention needs to be put in capabilities in an always evolving environment.

There is especially need to focus on three following threats:

- Risk citizen's face through digitalized personal information
- Misleading influence on the Internet
- Preventing the access for the citizens to services

EU-HYBNET Project Core Theme: Information and Strategic Communications

The main attention is given on broadcasting contents and processes, and the main challenges that information is a strategic area that is able to produce diverse but heavy repercussions. Therefore, the information domain is and remains to be object of many offensives.

There is especially need to focus on three following threats:

- Pitfalls for information providers
- Societies' cohesive issues
- Attempts to derail facts

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

The key concerns are related to the various ways threatening agents try to shape the future of European societies by weaponizing current trends. The seems to be interest to inflame society and direct them in the future direction that serve adversaries interests.

There is especially need to focus on three following threats:

- Combination of the difficulties inherent to democracy
- Efforts to unsettle democratic regimes
- Aim to replace truth by alternative narratives

On the whole, as it is underlined in T2.2 research, threats are ontologically imprecise, changing, and adaptive phenomena. It is therefore fundamental to address them dynamically to comprehend their permanent evolution. However, beyond theoretical scientific interests, designing security policies for practitioners requires to write down what are the threats, who are potential emitting agents, what are the breaches and what should be done to occlude them. It is therefore extremely important, to stick to threats' behaviours, and therefore to keep the approach innovative and the analysis dynamic, moving with its object.

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

The key activity in Task (T) 4.2 ”*Strategy for Innovation uptake and industrialization*” (lead by RISE) is to define a concrete strategic approach for innovation uptake and industrialization and to the innovations seen as most promising ones in WP3 “*Surveys to Technology, Research and Innovations*” to the identified present pan-European actors' gaps and needs to counter hybrid threats identified in WP2 “*Gaps and Needs of European Actors against Hybrid Threats*”. 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**“.

T4.2 had finalized its' work and reported about the key findings on most promising four innovations to the second project cycle gaps and needs (Oct 2021 - Feb 2023) in D4.5 “*2nd Innovation uptake, industrialisation and research strategy*” in Feb 2023 (M34) and the next step was to provide a policy brief or a report that would support the most promising innovations uptake and to describe for EU-HYBNET stakeholders **common requirements as regards innovations that could fill in gaps and needs**“. The T4.2 selected to write a Report on its' most promising innovation called *MIMI (“A Market place for Information Manipulation and Interference Information”)* that entails not only an idea of having a platform but also an approach that supports pan-European security practitioners and private sector actors to share their knowledge on on-going disinformation campaigns also used as part of hybrid threats campaign. The MIMI innovation that has been inspired from the structure of the *European External Actions Service (EEAS)/Strategic Communication division's (Strat.comm*.) work on FIMI Data Space, can practically support FIMI Data Space initiative as a concrete tool to connect information providers and requesters from different fields across the society and hence enhance the societal responsiveness to IMI (information manipulation and interference).

The common requirements as regards of MIMI innovation to fill the gaps and need in disinformation sharing analysis cooperation between public and private sector are following according to the report of MIMI created by T4.2 (RISE) together with EEAS/Strat.Comm. The Report “*MIMI an EU-HYBNET Innovation. Boost Sharing of IMI (Information Manipulation and Interference) Information. Create MIMI, a Marketplace*” is published with support of EU-HYBNET WP5 “*Communication, Dissemination and Exploitation Activities*” (lead by EOS) and the Report can be found in EU-HYBNET website: https://euhybnet.eu/policy-briefs-and-reports/ - see Report No.2. https://euhybnet.eu/wp-content/uploads/2023/06/EU-HYBNET_Report_2_MIMI_Oct-2023_Final.pdf

Main features in MIMI:

MIMI, a marketplace for IMII would stimulate the establishment of multiple actors that specialize and compete in different segments of the supply chain of (F)IMI ((Foreign) Information Manipulation and Interference). There may be actors that mine the Internet, others monitor media outlets, domains, social media 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 identifying specific tactics, techniques and procedures (TTPs) used by threat actors, in diverse 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 marketplace is established, it would lead to a situation with highly competent and specialized competing actors, and in the end, this would provide high quality results and end products.

An IMII sharing environment and supply chain can be depicted in a value chain. At least five categories of stakeholders can be envisioned in an IMII sharing value chain:

1. Data providers that do different types of monitoring and generate data for IMI incidents and related information.
2. Aggregators that collect descriptions from different data providers and sort and relate them.
3. Analysts that perform analysis of incidents on IMI activities, campaigns and mitigating actions.
4. Distributors that collect analysts results and make them available for interested end-users.
5. End-users that based on distributors’ reports perform mitigating actions.

Already now, numerous companies and organizations work in the field of IMII analysis. On a commercial basis they sell their results to different types of end-users. Oftentimes, these results take the form of written reports presenting finalised analysis and therefore their usability remains limited in time. The possibility to obtain IMI data and reuse it, thereby aggregating different types of knowledge obtained from different providers, is currently a service that few actors in the market are able to offer, but which remains in high demand. Furthermore, IMII often has a direct business value (similar to CTI[i]) and may also be business sensitive giving, for example, clues about ongoing market events. The willingness to share IMII without compensation may thus be limited in private business ventures. Hence **there is a need and a common requirement for the establishment** of **an open commercial IMII marketplace (MIMI)** in which the value of IMII is recognized.

Requirements for the establishment of an IMII marketplace (MIMI):

1) **Standardized taxonomies, procedures and protocols** for descriptions, interpretation of and distribution of IMII. The development of the **MIMI** should build on ongoing standardization activities around IMII sharing, in particular the ongoing work at the EU-level by the EEAS to establish what is called the FIMI (Foreign Information Manipulation and Interference) Dataspace. This work includes a commonly accepted and used

taxonomy for IMII and TTPs (Tactics, Techniques and Procedures), the extension of STIX[ii] and TAXII[iii] to cover IMII sharing needs and the use of the DISARM framework[iv] as TTPs categorization methods. The work is presented in the *1st EEAS Report on Foreign Information Manipulation and Interference Threats*[v]. The EEAS currently uses OpenCTI[vi] as knowledge management and sharing platform, but other possibilities, like MISP [vii] platforms exist. The EEAS's framework for establishing a standardized IMII sharing environment has been agreed with the US[viii] and will be a joint development effort. Likewise, some EU Member States are on their path to establish services that apply said methodologies in their analytical work.

2) **Sharing platforms that are secure and trusted by stakeholders** which means that stringent security guarantees must be incorporated in the specifications of utilized implementations and platforms. In some cases, IMII is considered to be a security threat and thus is restricted with respect to sharing. Thus, there is a need to ensure that the process of sharing IMII can be trusted by all the users of MIMI and that sharing can be securely controlled with respect to how and with whom the information is shared and how the aggregated and analysis results are shared. The set-up of MIMI must implement safeguards against malicious actors becoming part of the market place.
3) **A business model for IMII sharing** which is accepted by all stakeholders needs to be developed. There can be different options for access and sharing like subscriptions or "pay-per-view". The relevance of the options partly depends on the distribution mechanism used. Anyhow, there should be standardized procedures and interfaces for ordering, specifying and paying for IMII. These procedures and interfaces should be integrated into the sharing platform and follow standard procedures for business agreements, contracts and payments

Recommendations on actions and common requirements to create MIMI

Based on the findings described above, the EU-HYBNET project recommends that the following actions are implemented:

- **Convene IMII sharing stakeholders to discuss and agree baseline requirements for the establishment of an IMII marketplace (MIMI)**. The baseline requirements should at least cover a business model, access methods and controls, service level agreements, payment and charging solutions, and stakeholder mutual trust establishment.
- **The stakeholders should also agree policies for the use of the IMII,** this to ensure that its use doesn't lead to political censorship but allows freedom and speech and legitimate political expressions.
- **Drive the development and adoption of common data sharing standards and taxonomies based on open and interoperable standards like STIX or TAXII** to achieve wide adoption and interoperability of IMII sharing solutions. IMII sharing standards should be based on standardized, collaborative and open frameworks, taxonomies, and data standards, enabling users to build upon shared threat models and information. It should also strive for interoperability with other information sharing solutions in other communities e.g., cybersecurity, OSINT, etc, to provide access to as much (relevant) information as possible.

- **Standardize required security solutions for trusted and controlled sharing of IMII.** The authenticity and integrity of the IMII must be verifiable as well as its origin so that contaminated information will be detected and not entered into the sharing environment. Furthermore, sharing must be controlled so that IMII items only are shared with intended recipients and not forwarded/leaked to "external agents" and unauthorized parties
- **Develop and integrate the required interfaces and APIs (**Application Programming Interfaces) **for support of the IMII marketplace in the sharing and analysis framework.**
- **Review if there are any EU or national rules and regulations that would be hindering IMII sharing.**
- **Create demand for services that provide IMII in accordance with common frameworks**

MIMI answering to Gaps and Needs

Lastly, Within the European Union, several policy documents present different strategies, actions and regulations with respect to how to handle IMI activities and campaigns (of which disinformation is just one dimension). In 2020 the *European Democracy Action Plan*[ix] *(EDAP)* was published and now a new initiative "Defence of Democracy Package" [x] is under preparations. In the context of MIMI innovation, the following actions listed in the EDAP are deemed relevant to counter disinformation and IMI:

- Put in place a new protocol to **strengthen existing cooperation structures** to fight disinformation, both in the EU and internationally
- Develop a common framework and methodology for **collecting systematic evidence** on foreign interference and a structural **dialogue with civil society, private industry actors and other relevant stakeholders** to regularly review the threat situation.
- **Increase support for capacity-building** of national authorities, independent media and civil society in third countries **to detect and respond to disinformation and foreign influence operations**.

In 2022 ***A Strategic Compass for Security and Defence***[xi] **was published, which together with its annex** ***Foreign Information Manipulation and Interference (FIMI) Toolbox*** **highlights the necessity of developing a European Hybrid Toolbox. The annex underlines a set of preventive and counter measures to be applied at EU level in order to counter FIMI, including a FIMI Data space built on a** common analytical framework and methodology to collect systematic evidence of FIMI incidents**. This is what MIMI is to serve as well**.

MIMI, a recommendation that will contribute to the implementation of the referenced policy actions, and suggest a solution for the toolbox, thereby building on ongoing research regarding the development of a common framework and methodology for collecting systematic evidence on IMI activities. The MIMI's aim is to strengthen and widen cooperation structures in the fight against IMI and enhance the ability of national authorities, independent media and civil society to detect and respond to IMI operations.

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 insights to the second Three Lines of Action in the 3rd Future Trends Workshop (FTW) arranged by EOS and MVNIA in Bucharest during 19th of April 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**". The reporting highlights what is especially expected from innovations in general to counter Hybrid Threats.

EU-HYBNET 3rd Future Trends Workshop (FTW) keynote 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 a chance to interact and debate in break-out sessions (BOS) on existing and future trends of hybrid threats. Following key take aways as **common requirements as regards innovations that could fill in gaps and needs** were highlighted:

- only major way forward is to enhance cybersecurity awareness, the resilience of citizens and institutions etc.
- the next crisis will by all means imply a significant cyber component, which is low cost, high impact; however, it must be mentioned that a cyber-attack will never come alone and most likely will be accompanied by and coordinated with other types of attacks – especially in the information domain. Therefore, foresight capabilities and tools to support the foresight are much needed and important.
- there is much need for innovations that serve critical infrastructure protection and changes brought forth by climate change.
- Innovations to detect and o report on disinformation are much needed because adversaries are creating disinformation campaigns in increasing amounts to lower citizen trust in state institutions, weakening purchasing chains for strategic goods and cyber operations.
- In order to counter hybrid threats, we need an approach (non-technological innovation) based on a whole of society involvement, incorporating industry, international partners and civil society, but also to develop a rapid response capacity at EU level and implementation of EU regulation at national level.
- The use of soft power methods (e.g. political messages advanced on sports arena) to diminish trust in the Ukrainian cause, the cereal blockade enforced by Russian ships against Ukraine, the emerging disinformation campaigns in Africa (blaming the West for the lack of food stocks and prospects of famine) were other threats signalled in the hybrid spectrum against which one can only succeed in wining if and only if the response is a shared, joint and convergent one at EU level.
- Biological attacks may become a major threat, especially when combined with online disinformation. Therefore, innovations that may prevent or discover this type of hybrid campaigns in planning or ongoing are seen as a necessity.

- There is demand for innovations that will support to discover and to analyze differences and special features in hybrid threats in different regions of Europe (e.g. south, east, west, north, central Europe alike Nordic Countries, Baltic States, Balkan region etc).
- It seen highly important to develop special AI generated algorithms that can detect recurrent aspects in seemingly unrelated events.

During the reporting period T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) has also being working on preparations to the forthcoming 3rd Innovation and Knowledge Exchange Workshop (IKEW) arranged by EOS and PLV in Valencia during 7th of November 2023. The IKEW will present innovations identified during the project's ongoing third cycle which correspond to the gaps and needs pan-European security practitioners face when countering hybrid threats. These innovations include: a European CISE for customs, a Disinformation Toolbox, AI tools for LEAs, AI developments and future trends. In addition, the event will feature high-level speakers from DG HOME, Europol, EACTDA and the Spanish Ministry of Interior who will share their perspective on innovation uptake. The results on the IKEW to the second Three Lines of Action "**common requirements as regards innovations that could fill in gaps and needs**" will be reported in the next Sixth Month Action Report. IKEW Agenda in ANNEX III.

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

In EU-HYBNET the WP4 *"Recommendations for Innovations Uptake and Standardization*" has delivered contribution during the reporting period to the third Three Lines of Action "**Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation**". The WP4 Tasks in questions are T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE) who has provided valuable recommendations in the form of a report on a promising innovation, MIMI, uptake. The recommendation work is done together with WP5 "*Communication, Dissemination and Exploitation Activities*" (lead by EOS). In addition, T4.3 "*Recommendations for Standardization*" (lead by PPHS) has been conducting preparations to the *2nd Innovation and Standardization Workshop* (ISW; arranged together with PLV in Valencia during 8th of November 2023) that will deliver insights especially from the standards development pint of view to the second Three Lines of Action. Furthermore, T5.3 "*Annual Workshop for Stakeholders*" (lead by Laurea) included insights on priorities as regards of increasing knowledge and performance requiring standardization. The following subchapters describe the contribution from each of the named tasks with more details.

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

As already described in chapter 3.2.2, T4.2 "*Strategy for Innovation Uptake and Industrialization*" (lead RISE) had finalized its' work and reported about the key findings on most promising four innovations to the second project cycle gaps and needs (Oct 2021 - Feb 2023) in D4.5 "*2nd Innovation uptake, industrialisation and research strategy*" in Feb 2023 (M34); the next step in T4.2 was to provide a policy brief or a report that would support the most promising innovations uptake. The T4.2 selected to write a Report on its' most promising innovation called *MIMI ("A Market place for Information Manipulation and Interference Information")* in order to promote the MIMI innovation uptake. The report on MIMI is published in EU-HYBNET website (https://euhybnet.eu/policy-briefs-and-reports/ - see Report No.2. https://euhybnet.eu/wp-content/uploads/2023/06/EU-HYBNET_Report_2_MIMI_Oct-2023_Final.pdf) and the Report highlights priorities as regards of increasing knowledge and performance requiring standardization as follows:

<u>MIMI/ "A Market place for Information Manipulation and Interference Information" – a platform and an approach</u>

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 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. Following standardized approaches would be welcomed to improve the present situation.

First of 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 MIMI 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).

Because MIMI is to increase knowledge and performance in a described standardized format the innovation is seen as a priority when novel solutions for efficient sharing of IMI (information manipulation and interference) Information (IMII) between concerned stakeholders are considered.

3.3.2 EU-HYBNET T4.3 RECOMMENDATIONS FOR STANDARDIZATION

T4.3 “*Recommendations for Standardization*” (lead by PPHS) has been conducting preparations to the *2nd Innovation and Standardization Workshop* (ISW; arranged together with PLV in Valencia during 8th of November 2023) where the goal is to bring together EU-HYBNET consortium partners and hybrid threats stakeholders to map the current status of standardisation efforts in the field of FIMI (Foreign Information Manipulation and Interference) and critical infrastructure (CI) protection in the context of hybrid threats. In addition the goal is to identify needs and possibilities for best practices and standards for innovation uptake in the FIMI and CI context for the future so as to enhance pan-European response to Hybrid threats. The ISW focus to information and infrastructure domain was selected because EU-HYBNET’s most promising innovations for uptake recommendations were presented in these domains during the 2nd EU-HYBNET working cycle. On the whole, ISW is delivering the final analysis and recommendation for the innovations uptake and future development for pan-European security practitioners needs. The ISW program, incl. speakers, has been tailored in a manner that it will support the project to gain wider knowledge on **priorities increasing knowledge and performance requiring standardization in FIMI and CI protection.** The ISW results to the third Three Lines of Action" will be reported in the next Sixth Month Action Report. ISW Agenda in ANNEX IV.

3.3.3 EU-HYBNET T5.3 ANNUAL WORKSHOP FOR STAKEHOLDERS

The EU-HYBNET partners MVNIA, EOS and LAUREA organized the 3rd EU-HYBNET Annual Workshop (AW) on April 20th, 2023 in Bucharest according to T5.3 "Project Annual Workshops for Stakeholders" (lead by Laurea) activities. During the AW the project's 3rd year key research findings and results were presented, and the event also focused on new innovation analysis and networking, knowledge exchange in order to empower pan-European measures to counter hybrid threats. The event was addressed to the EU-HYBNET network members and pan-European stakeholders; it hosted lectures from policy makers, security practitioners, industry, SMEs, academia, and NGOs. Additionally, the workshop hosts a handful of presenters and European projects, introducing their unique innovation ideas to counter hybrid threats.

During the Annual Workshop the European External Action Service (EEAS)/ Strategic Communication Division (Strat.Comm.) presented the EEAS concept of FIMI Data space/ FIMI toolbox that they have been developing in order to enhance pan-European measures to tackle challenges in FIMI. The presentation was included a demo on the FIMI tool and highlighted core elements mentioned in the First EEAS Report on Foreign Information Manipulation and Interference Threats: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

In short, the EEAS presentation highlighted that the key actions to prevent FIMI attacks to escalate are threefold: i) to collect the information on the attack, ii) to analyze the tactics, techniques and procedures used in the attack, iii) plan counter measures. It was also highlighted that similarly to cyber attacks, FIMI operations should focus on "kill chain" - if a certain stage is disrupted, then then whole attack can be disrupted.

Because the EEAS/Strat.Comm. FIMI data space provides coherent and solid approach to tackle FIMI pan-European wide, the solutions is seen as a priority as regards of increasing knowledge and performance of pan-European security practitioners to counter hybrid threats in the information domain. The required standardization efforts related to the use of FIMI are described with more details in this document sub-chapters: 3.3.1 and 3.2.2.

4. CONCLUSION

4.1 SUMMARY

In the chapter above it is described how the EU-HYBNET project activities from the past six project months (May 2023 – Oct 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 3rd 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 beginning of the 3rd project cycle (duration: M35-M52/ March 2023 – August 2024) have been now explained to the EC from the reporting period of this deliverables. The next Six Month Action Report (in May 2024) will continue to describe 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. 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 eight (8) deliverables will be delivered during next six-month period. Three milestones take place M43-M49.

Deliverables (D):

T2.3 Training and Exercises for Needs and Gaps

- ➢ Training and Exercise, Scenario delivery (KEMEA), M44/ DEC 2023

T3.4 Innovation and Knowledge Exchange Events

- ➢ 3rd Innovation and Knowledge exchange events report (EOS), M44/ DEC 2023

T2.4 Training and Exercises for Needs and Gaps

- ➢ D2.22 Training and exercises delivery on up-to-date topic (L3CE), M46/ Feb 2024

- D2.25 Training and exercises Lessons Learned report (Hybrid CoE), M48/ April 2024

T1.3

- D1.22 List of actors to the extended EU-HYBNET Network (Hybrid CoE), M47/ March 2024

T1.1 Administrative and Financial Planning and Coordination

- D1.12 8th Six Month Action Report (LAU), M48/April 2024

T2.2 Research to Support Increase of Capacity and Knowledge

- D2.15 Articles and publications on themes and measures (UIT), M48/ April 2024

T4.1

- D4.3 3rd Report on the Procurement Environment (KEMEA), M48/ April 2024

Milestones (MS):

- MS18 3rd cycle of mapping gaps and needs on the innovations and research completed and shortlist of solutions handed over to WP 4, M45 (January 2024)
- MS37 4th Annual Workshop, M48 (April 2024)
- MS8 4th EU HYBNET Project Management Board meeting, M48 (April 2024)

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 promising innovations to present pan-European security practitioners gaps and needs to counter hybrid threats (by T2.1, T2.2) will be available alike take aways from innovation analysis in EU-HYBNET events. 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 is in the plans to continue alike fruitful information exchange with EUROPOL Innovation Lab. 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
IKEW	Innovation and Knowledge Exchange Event
BOS	Break Out Session
ISW	Innovation Standardization Workshop
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
AI	Artificial Intelligence
VR	Virtual Reality
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras

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

.

ANNEX II. REFERENCES

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

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

.

ANNEX III. IKEW AGENDA

.

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	Mr. José L. Diego, Inspector, Head of the Innovation & Project Management Division, Valencia Local Police
09:15-09:30	**Keynote Speech #1:** Considerations on "Innovation Uptake"	Mr. Giannis Skiadaresis, Area Coordinator for Strengthened Security Research and Innovation, DG HOME, European Commission
09:30-09:45	**Keynote Speech #2**	Mr. Francisco Alonso Batuecas, Head of ICT Infrastructure and Security at the Security Technology Centre (CETSE) of the Secretary of State for Security
09:45-10:15	Results of Innovations Mapping and Assessment (3rd EU-HYBNET Cycle)	Dr. Souzanna Sofou, SATWAYS Mr. Okke Lucassen, TNO
10:15-10:30	Audience Q&A	***Moderator:*** Mr. José L. Diego, Inspector – Head of the Innovation & Project Management Division, Valencia Local Police Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police
10:30-10:45	Coffee Break	
Parallel Breakout Sessions		
10:45-12:15	**Breakout Session #1:** Cyber and future technologies **Innovation:** STARLIGHT EU Project – way forward with AI transformative impact on security domain	**Moderator & Presenter:** Mr. Evaldas Bružė, Deputy Director, Head Innovations' Architect, Lithuanian Cybercrime Center of Excellence for Training, Research & Education (L3CE)

	Breakout Session #2: Information and strategic communications **Innovation:** VIGILANT EU Project	Ms. Eva Power, VIGILANT Project Manager, ADAPT Centre, Trinity College Dublin Mr. Oisin Carroll, VIGILANT Technical Coordinator, ADAPT Centre, Trinity College Dublin **Moderator:** Dr. Päivi Mattila, EU-HYBNET Project Coordinator, Laurea UAS
12:15 – 13:15	Lunch Break	
Parallel Breakout Sessions		
13:15-14:45	**Breakout Session #3:** Resilient civilians, local level, and administration **Innovation:** CONNECTOR EU Project	Mr. Javier Moreno García, Maritime Officer in Spanish Customs and Coast Guard (DAVA-AEAT) **Moderator:** Dr. Gunhild Hoogensen Gjørv, UiT – The Arctic University of Norway Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea UAS
	Breakout Session #4: Future trends of Hybrid Threats **Innovation:** AI transformative implications on security research and emerging security practitioners' needs	**Moderator & Presenter:** Mr. Evaldas Bružė, Deputy Director, Head Innovations' Architect, Lithuanian Cybercrime Center of Excellence for Training, Research & Education (L3CE)
14:45-15:00	Coffee Break	
15:00-16:00	**Break-out session outcomes**	Break-out session moderators in conversation with: • Europol Innovation Lab Representative • Mr. Rashel Talukder, Managing Director of the Polish Platform for Homeland Security • Mr. José L. Diego, Inspector – Head of the Innovation & Project Management Division, Valencia Local Police
16:00-16:10	Audience Q&A	

16:10-16:25	Linking innovation providers and practitioners	Ms. Eva Škruba, Capability Manager of European Anti-Cybercrime Technology Development Association (EACTDA)
16:25-16:30	Closing remarks	Mr. José L. Diego, Inspector – Head of the Innovation & Project Management Division, Valencia Local Police Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police
16:30-18:00	**Round table discussion:** EU-HYBNET post-project topics	Dr. Päivi Mattila, LAUREA Mr. Christian Despres, MTES Prof. Gunhild Hoogensen-Gjorv, UIT Dr. Souzanna Sofou, SATWAYS Dr. Julian Theron, JRC

.

ANNEX IV. ISW AGENDA

.

Time CET	Topic	Speaker
08:30-09:00	Registration	
Plenary session		
09:00-09:15	Welcome & Opening remarks	Iván Luis Martínez Villanueva, Valencia Local Police
09:15-09:30	Keynote Speech #1 Protecting Critical Infrastructure in a changing world – a government perspective	Kimini Delfos, Kiki van Setten, Dutch Ministry of Infrastructure and Water Management
09:30-09:45	Keynote Speech #2 Unlocking sustainable networked defence against FIMI: The key role of standards	Daniel Fritz, European External Action Service
09:45-10:00	Keynote Speech #3 Whole of government approach to countering hybrid threats: lessons learned and challenges from Slovakia (focus on non-technical innovation in terms of coordination of actors, setting up structures, joint analytical outputs and monitoring of information space)	JUDr. Daniel Milo, Centre for Countering Hybrid Threats, Institute for administrative and security analysis, Ministry of Interior of the Slovak Republic
10:00-10:15	Audience Q&A	*Moderator:* Iván Luis Martínez Villanueva, Valencia Local Police
10:15-10:45	Coffee Break	

Parallel Breakout Sessions				
	Breakout Session #1: Foreign Information Manipulation and Interference (FIMI)		**Breakout Session #2:** Protection of Critical Infrastructure	
10:45 - 11:15	Keynote speech: Foreign Information Manipulation and Interference: Strategic Threats on the Rear Dr. Julien Théron, Joint Research Centre (JRC)	*Moderator:* Rashel Talukder, Polish Platform for Homeland	Keynote speech: From Paper to Practice: Entangled Critical Infrastructures & Hybrid Exploitation Dr. Georgios Kolliarakis,	*Moderator* Isto Mattila, Laurea

	Audience Q&A 11:00 – 11:15	Security (PPHS)	German Council on Foreign Relations (DGAP) Audience Q&A 11:00 – 11:15	
11:15 – 12:30	**#1 case study presentation & discussion** Antagonising Poles and Ukrainians through disinformation – challenges and responses Paula Rejkiewicz, Ministry of Foreign Affairs Republic of Poland, Strategic Communication and Countering Disinformation Unit		**#1 case study presentation & discussion** Hybrid activities aimed at Polish Critical Infrastructure (CI). Case study based on a transportation system Dr. Karolina Wojtasik, Government Centre for Security (RCB), Polish Association for National Security (PTBN)	
12:30 – 13:30	Lunch Break			
13:30 – 14:30	**#2 case study presentation & discussion** (F)IMI & Innovative solutions for detection: A case study of online coordinated inauthentic campaigns from 'pro-Iranian' and 'pro-Palestinian' accounts on Twitter / X Esther Jacobs, TILT Insights	*Moderator*: Rashel Talukder, PPHS	**#2 case study presentation & discussion** Hybrid threats against Critical infrastructures and the case of Italy Paola Tessari, IAI Istituto Affari Internazionali	*Moderator* Isto Mattila, Laurea
14:30 – 15:30	**#3 case study presentation & discussion** Addressing the challenges of the early detection of advanced manipulation campaigns Dr. David Arroyo, Spanish National Research Council (CSIC)			
15:00 - 15:15	Coffee Break			

15:15 - 15:45	Breakout sessions outcomes Audience Q&A	***Moderator*** Isto Mattila, Laurea and Rashel Talukder, PPHS
15:45 – 16:00	**Closing remarks**	Iván Luis Martínez Villanueva, Valencia Local Police

[i] CTI (Cyber Threat Intelligence) is a branch of cybersecurity that deals with the collection, analysis, and dissemination of information about current and potential cyberattacks that pose a threat to an organization's assets.

[ii] STIX (Structured Threat Information Expression) is a structured language for describing cyber threat information and how it can be shared, stored, and analysed in a consistent manner. http://stixproject.github.io/about/

[iii] TAXII (Trusted Automated eXchange of Intelligence Information) defines how cyber threat information (e.g., in STIX) can be shared via services and message exchanges. https://oasis-open.github.io/cti-documentation/taxii/intro.html

[iv] DISARM is the open-source, master FRAMEWORK for categorizing Tactics techniques and Procedures of information manipulation, as well as related counter-actionshttps://www.disarm.foundation/framework

[v] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

[vi] OpenCTI, an open source platform for managing cyber threat intelligence knowledge and observables. It structures, stores, organizes and visualizes technical and non-technical information about cyber threats. https://github.com/OpenCTI-Platform/opencti#readme

[vii] MISP, an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security. https://www.misp-project.org/

[viii] Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden (section “Foreign information manipulation and interference (FIMI) in third countries”) and the technical annex.

[ix] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790

[x] Commission Work Program 2023, p. 14.

[xi] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en