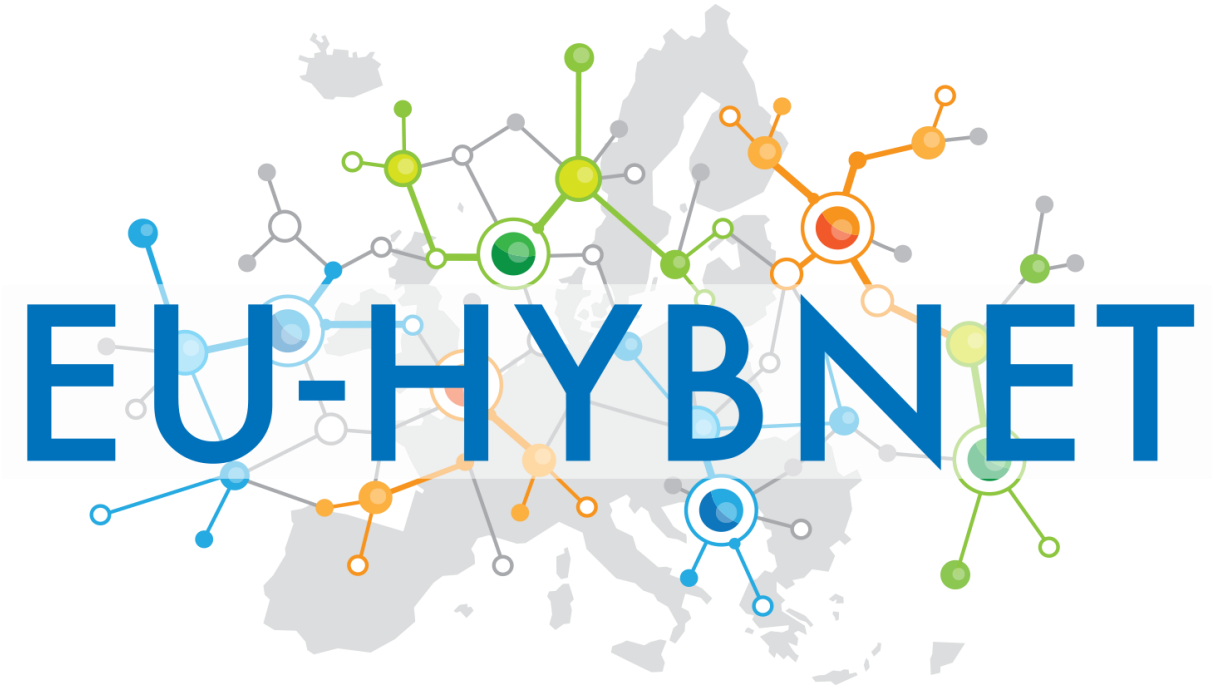


FIFTH SIX MONTH ACTION REPORT

DELIVERABLE 1.10

Lead Author: Laurea

Contributors: L3CE, ZITiS
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

D1.10 FIFTH SIX MONTH ACTION REPORT

Deliverable number:	**1.10**	
Version:	**1.0**	
Delivery date:	**26/10/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main author:	Päivi Mattila	**Laurea**
Contributors:	Edmundas Piersarskas, Egidija Versinskiene Review: Michael Meisinger, Lukas Hardi Review: Jari Räsänen	**L3CE** **ZITiS** **Laurea**
	Input to the report from all consortium partners due to their project work in various Tasks and events as contributors	**MTES, URJC, Hybrid CoE, PPHS, UiT, RISE, KEMEA, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, Maldita, Espoo, COMTESSA**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	22/9/2022	Päivi Mattila/ Laurea	First draft.
0.2	11/10/2022	Päivi Mattila/ Laurea	Description of activities conducted during the reporting period.
0.3	13/10/2022	Päivi Mattila/ Laurea	Description of activities conducted during the reporting period.
0.4	16/10/2022	Päivi Mattila/ Laurea	Finalizing descriptions in the report. Report delivery for the review.
0.5	24/10/2022	Jari Räsänen/ Laurea	Review and comments for improvements
0.6	10/2022	Michael Meisinger, Lukas Hardi/ ZiTIS	Review and comments for improvements
0.7		Edmundas Piersarskas, Egidija Versinskiene/L3CE	Text delivery form T2.4 to the document
0.8		Päivi Mattila/ Laurea	Final text editing
1.0		Päivi Mattila/ Laurea	Document to be submitted for the EC

DISCLAIMER

TABLE OF CONTENT

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The goal of the *Empowering a Pan-European Network to Counter Hybrid Threats* (EU-HYBNET) project deliverable (D) 1.10 "*Fifth Six Month Action Report*" in project month (M) 30/October 2022 is to describe how the project has proceeded from M24 until end of M30 of the project (May 2022 – October 2022) according to the European Commission (EC) defined, *"three lines of action*" which are mandatory to report according to the Horizon2020 Secure Societies Programme/General Matters-01-2019 funded projects. The *"three lines of action*", also mentioned in the EU-HYBNET Description of Action (DoA) are:

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

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

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

Furthermore, D1.10 also highlights what actions and results are expected from EU-HYBNET during the next six-month period (Nov 2022- April 2023).

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1. Provides an overview to the document content.
- Section 2. Describes the importance of deliverable D1.10 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 24-30 (May – October 2022) have contributed to the EC's requested "three lines of action" activities.
- Section 4. Conclusion and next steps for the upcoming six-month period of the project (November 2022 – April 2023).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.10 "*Fifth 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 D1.10, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.10 is to provide a general update on how the project reaches the results mentioned in the project objectives and KPIs. We have highlighted this in the figure below, showing the role of WP1 to support and guide project WPs 2-4 where the main project activities take place and the core project results are achieved.

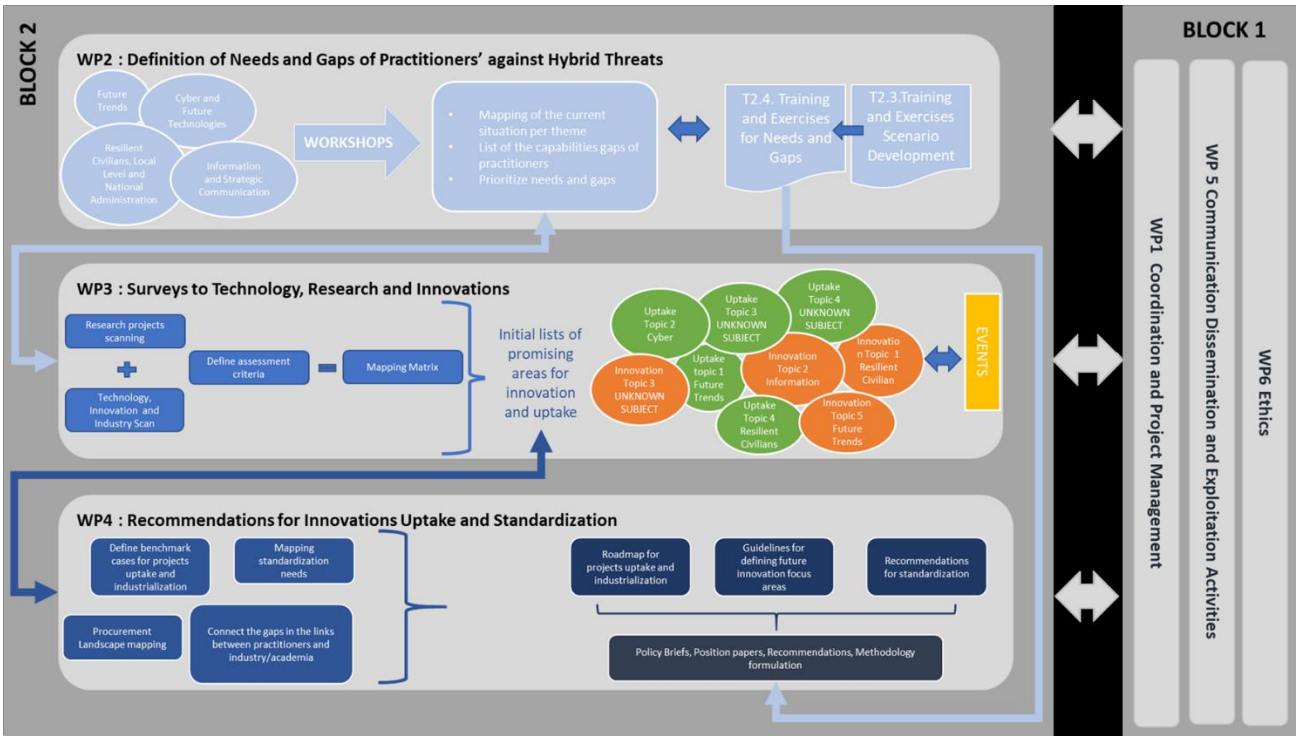


Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in D1.10 are linked to the project milestones (MS) achieved during the last six month period. The milestones relevant to D1.10 are following:

Milestone No.	Milestone (MS) name	MS related Task	Due project month
17	2nd Cycle of mapping gaps and needs on the innovations and research completed and shortlist of solutions handed over to WP4	All	28

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The fifth Six-Month Action Report (D1.10) main author is Laurea, the organization responsible for the delivery of D1.10. However, EU-HYBNET work package (WP) and task (T) leaders have also provided information on the tasks they are responsible for and have been working on during the fourth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager have contributed to D1.10 by providing general remarks on the project's general progress and innovation uptake.

3. THREE LINES OF ACTION REPORTING

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

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

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

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

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

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

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

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

During this reporting period the innovation analysis work relevant to the first Three Lines of Action reporting has mainly been conducted in Work Package (WP) 3 "*Surveys to Technology, Research and Innovations*"/ T3.2 "*Technology and Innovations Watch*" (lead by Satways) and T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE), and T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO). However, activities in WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.3 "*Training and Exercises Scenario Development*" (lead by KEMEA) and in T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE) have also provided input to the results and further proceeding. Moreover, WP4 "*Recommendations for Innovations Uptake and Standardization*" T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE) has also started to contribute to this three lines of action.

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

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

Work Package (WP) 3 "Surveys to Technology, Research and Innovations" includes T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) that delivers basis together with T3.2 "*Technology and Innovations Watch*" to **research and innovation projects with a view to recommending the uptake or the industrialisation of results**. In short, EU-HYBNET T3.3 monitors research and innovation (R&I) projects that may deliver sound innovations and solutions to present most critical EU-HYBNET's identified pan-European security practitioners' and other relevant actors' gaps and needs, threats to counter Hybrid Threats.

During the reporting period T3.3 contributing partners selected the main threats to focus on, and mapped EU MSs' and especially European Commission (EC) funded relevant security projects that to deliver sound innovation(s) and solution(s) to the threats. During the T3.3 assessment EC funded projects (ALIGNER, 7SHIELD, PRECINCT, MEDEA) that were invited to present their innovations and solutions in the 2nd EU-HYBNET Annual Workshop (hybrid format on the 6th of April 2022 in Rome) were more thoroughly analyzed. In addition, especially the EC CORDIS platform was much used to find primary information on the most promising projects. This was followed by more detailed investigation of the discovered project(s) contents and results. During the work it was observed that there is an abundance of research and innovation (R&I) projects and other research material (e.g. articles, journals, studies, research publications). The results can be used for the most relevant solutions to satisfy the identified gaps and needs, and which can be recommend for further analysis and possibly innovation uptake or industrialization into further analysis in T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) and in T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE). T3.3 research results have been thoroughly described in D3.8 "*First Mid-Term report on Innovation and Research Project monitoring*", (L3CE) in M24 (April 2022, submitted May 2022) and according to the research results following **research and innovation projects** are such that include elements for further EU-HYBNET work analysis so as to deliver **view to recommending the uptake or the industrialisation of results.**

The T3.3 identified 15 (fifteen) projects that may deliver promising innovations from research projects to the EU-HYBNET project Core Themes' identified gaps and needs/threats are:

Core theme - Future Trends of Hybrid Threats:

- **PersoNews/ "***Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy***"** https://cordis.europa.eu/article/id/434332-algorithms-are-reshaping-our-newsreading-habits-should-we-worry
- **CONCORDIA/ "**Cyber Security Competence for Research and Innovation**"** https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-04-Reseach-and-Innovation.pdf
- **EU-LISTCO/ "***Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders***"** https://cordis.europa.eu/project/id/769886/reporting

Core theme - Cyber and future Technologies:

- **INSPIRE-5GPlus/ "***INtelligent Security and PervasIve tRust for 5G and Beyond***"** https://cordis.europa.eu/project/id/871808
- **7SHIELD**/ "*Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats*" https://cordis.europa.eu/project/id/883284
- **ISOCRYPT/** "*Isogeny-based Toolbox for Post-quantum Cryptography***"** https://cordis.europa.eu/project/id/101020788
- **PROGRESS/** "*Protection and Resilience Of Ground-based infRastructures for European Space Systems"* https://cordis.europa.eu/project/id/607679
- **CyberCult/ "***Strategic Cultures of Cyber Warfare***"** https://cordis.europa.eu/project/id/844129

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

- **PRECINCT**/ "*Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection*" https://cordis.europa.eu/project/id/101021668
- **WeVerify/ "***In the Wider and Enhanced Verification for You***"** https://weverify.eu/about/
- **IMEDMC/** "*Information and Misinformation Economics: Design, Manipulations and Coutermeasures"* https://cordis.europa.eu/project/id/101001694

Core theme - Information and Strategic Communication:

- **RUSINFORM/ "The Consequences of the Internet for Russia's Informational Influence Abroad**" https://cordis.europa.eu/project/id/819025
- **Open Your Eyes: Fake News for Dummies** http://dlearn.eu/projects/online-and-offline-security/open-your-eyes/

- **COMPROP/** "*Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe*" https://cordis.europa.eu/project/id/648311
- **ALIGNER/** "*Artificial Intelligence Roadmap for Policing and Law Enforcement*" https://cordis.europa.eu/project/id/101020574

At the moment T3.3/D3.8 results have been handed over to T3.1 "*Definition of Target Areas for Improvements and Innovations*" to conduct more thorough analysis of their soundness to 2nd cycle pan-European security practitioners gaps and needs. The soundness of the innovations were also partly analyzed in T2.3 "*Training and Exercises Scenario Development*" and T2.4 "*Training and Exercises for Needs and Gaps*" in order to test the most promising innovations in the 2nd EU-HYBNET training event according to the training scenario.

3.1.2 EU-HYBNET T3.2 TECHNOLOGY AND INNOVATIONS WATCH

On May 2022 Task 3.2 "*Technology and Innovations Watch*" finalized research and analysis on possible promising innovations that could be seen as solutions to the identified gaps and needs, threats in T2.2 "*Research to Support Increase of Knowledge and Performance*" deliverable (D) 2.10 "Deeper analysis, delivery of short list of gaps and needs" (M22/ February 2022) according to the EU-HYBNET four project Core Themes. T3.2 focused mainly on technical innovations delivered by industry. The innovations are described in detail in D3.4 "First Mid-Term Report on Improvement and innovations" (M24/ April 2022, submitted may 2022). In T3.2, a total of 23 promising innovations were identified as follows:

CORE THEME		PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED
1. FUTURE TRENDS OF HYBRID THREATS	1.1	Geopolitical heavyweight of domestic policy	End To End Supply Chain Visibility Labels
			Multi-stage supply chain disruption mitigation strategy and Digital Twins for Supply Chain Resilience
	1.2	Digital escalation and AI-based exploitation	Digital connected security in response to hybrid tactics
			Commitment to Validating and Verifying AI
	1.3	Rise of populism	Establishment and reinforcement of political education of democratic values
			Installation of rules for mandatory declarations
2. CYBER AND FUTURE TECHNOLOGIES	2.1	Space interference and counterspace weapons	7SHIELD: a holistic framework for European Ground Segment facilities
	2.2	Offensive cyber capabilities	The Development of a Proactive Defensive Framework based on ML and cloud
			A fully automated incident response solution based on CT Intelligence

	2.3	Disruptive innovation	The Development of a Deepfake Detection System
			Counter-Unmanned Aircraft Systems
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1	Exploitation of existing political cleavages	Detection of Disinformation Delivery Proxy Actors
			Development of Real-time Rapid Alert System on Disinformation
	3.2	Exploitation of critical infrastructure weaknesses and economic dependencies	Impact and Risk assessment of critical infrastructures in a complex interdependentscenario
			ResilienceTool (incl. RiskRadar)
	3.3	Exploitation or investment in companies by foreign actors	A crawler for correlation of screened FDI with suspicious financial activity
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1	Information manipulation with the aim of destabilization	Increasing capabilities to systematically assess information validity throughout the lifecycle
			Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications
			DDS-alpha (EEAS)
	4.2	Foreign interference in key information institutions	Integrated Monitoring System Against Malware-Based Cyber Operations
			Integrated Monitoring System Against Cyber-enabled Information Operations
	4.3	Promoted ideological extremism and violence	Collection and sentiment analysis of targeted communication
			Identify and safeguarding vulnerable individuals

Because research and innovation projects also include innovative solutions provided by industry and SMEs, T3.2 also discovered some EC funded projects that may deliver promising innovations to some of the EU-HYBNET's identified pan-European security practitioners' gaps and needs. The projects are listed below according to the relevant, identified EU-HYBNET Core Themes and Innovations proposed (the innovations are also marked in light blue in the table above):

Core theme - Cyber and future Technologies:

Innovation Proposed:

- **7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats**.
    - **7SHIELD** project https://www.7shield.eu/ delivers variety of innovative solutions that can be recommended for the uptake or industrialization
- **Counter-Unmanned Aircraft Systems**

- **PESCO** project https://www.pesco.europa.eu/project/counter-unmanned-aerial-system-c-uas/ develops an advanced and efficient system of systems with C2 dedicated architecture, modular, integrated and interoperable with C2 info-structure, able to counter the threat posed by mini and micro Unmanned Aerial Systems

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

Innovations proposed:

- **Impact and Risk assessment of critical infrastructures in a complex interdependent scenario**
  - **EU-CIRCLE** project https://www.eu-circle.eu/ includes IPR platform that has been successfully used and hence seen as aproming innovation for future uptake and industrialization
  - **InfraStress** https://www.infrastress.eu/ project includes IPR platform that has been successfully used and hence seen as aproming innovation for future uptake and industrialization
  - **7SHIELD** project https://www.7shield.eu/ has promising solutions for modelling the impact of climate change

Core theme – Strategic Communication:

- **Increasing capabilities to systematically assess information validity throughout the lifecycle**
  - **WeVerify** project Tools - WeVerify and **InVid project** Description - InVID project (invid-project.eu) developed solutions that are examples how separate components can be developed. InVid project also provides the concept of complete content verification workflow that can be developed further for the EU wide implementation.
  - **FANDANGO** project (fandango-project.eu) breaks data interoperability barriers providing unified techniques and an integrated big data platform to support traditional media industries to face the new "data" news economy with a better transparency to the citizens under a Responsible, Research and Innovation prism. Some relevant tools are collected within the scope of the project (Tools | FANDANGO (fandango-project.eu)).
  - **defalsif-AI** project defalsif-AI - AIT Austrian Institute of Technology employes AI aiming to media content for credibility and/or authenticity. Project also links content analysis to legal and ethical perspective.
  - **AI4media** project AI4media project focuses on AI technologies to improve support tools used by journalists and fact-checking experts for digital content verification and disinformation detection. New AI-based features will be made available within two existing journalism tools: Truly Media (a web-based platform for collaborative verification) and TruthNest (a Twitter analytics and bot detection tool).
- **Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications.**
  - **PHEME** project https://www.pheme.eu combines big data analytics with advanced linguistic and visual methods. The results are suitable for direct application in medical

IS and digital journalism. Set of tools aimed to empower users and journalist to tackle disinformation developed and tested in real world conditions:

- **Collection and sentiment analysis of targeted communication.**
    - **RAIDAR** project RAIDAR - Rapid Artificial Intelligence based Detection of Aggressive or Radical content on the Web | KIRAS Sicherheitsforschung innovations include the development and definition of metrics, measures and methods for quantitative and qualitative evaluation of online hate and radicalization.

At the moment T3.2 results presented in D3.4 "First mid-term report Improvement and innovations" (May 2022) have been handed over to T3.1 "*Definition of Target Areas for Improvements and Innovations*" to conduct more thorough analysis of their soundness to 2nd cycle pan-European security practitioners gaps and needs. The soundness of the innovations was also partly analyzed in T2.3 "*Training and Exercises Scenario Development*" and T2.4 "*Training and Exercises for Needs and Gaps*" in order to test the most promising innovations in the 2nd EU-HYBNET training event according to the training scenario.

3.1.3 EU-HYBNET T2.3 TRAINING AND EXERCISES SCENARIO DEVELOPMENT

EU-HYBNET's three Lines of Action "**monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results"** is also well contributed by WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.3 "*Training and Exercises Scenario Development*" (lead by KEMEA) too due to the delivery of EU-HYBNET training scenario.

During the reporting period, T2.3 created a training scenario for the 2nd EU-HYBNET Training event (hybrid format on the 29th -30th of Sept 2022 in Vilnius). The training scenario included variety of injects according to the EU-HYBNET four core themes. Each of the injects focused on training the event participant to plan measures of the identified gaps and needs to counter hybrid threats, and to test promising innovations identified in T3.3/D3.8 and T3.2/ D3.4 which were seen relevant as counter measures. The training scenario and injects are described in detail in D2.21 "Training and Exercise, Scenario delivery" M27 (July 2022).

T2.3 selected the innovations for each inject among the most promising innovations identified by T3.3 and T3.2. The selected innovations presented both technological and non-technological (human science based) solutions. Many of the innovations resulted from security research and often EC funded project. These kinds of innovations are following according to the EU-HYBNET project four core themes and the training scenario and vignettes:

Core theme "Future Trends of Hybrid Threats"

Vignette 2. *While preparations for the elections in Bhic are ongoing, the minority in Duzec declares the desire to call a referendum for independence, whereas social media in Bhic strongly support this issue.*

Threat, primary context "Rise of Populism"		
Deliverable (D)	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Innovation coming from EC funded project PersoNews ("Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy")** duration : 1/8/2015-31/5/2021, GA No.638514 https://cordis.europa.eu/article/id/434332-algorithms-are-reshaping-our-newsreading-habits-should-we-worry	No specific technologies were developed during this project but methodological approaches. EU-HYBNET training could focus PersoNews recommender models explained in a PersoNews' publication "On the Democratic Role of News Recommenders"[1]. The article consolidates ideas around the ultimate question "how would news recommenders need to be designed to advance values and goals that we consider essential in a democratic society?". In addtion, EU-HYBNET could have discussion how to add hybrid threats dimension to the recommender model(s) alike alerts on information that seems to support populisitc ideas and foster polarization among citizens or between certain type of groups. **Practitioners in focus**: intelligence https://www.tandfonline.com/doi/full/10.1080/21670811.2019.1623700

Vignette 5. *The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full with migrant on Duzec shores*.

&

Vignette 8. *A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions*.

Threat, primary context "Geopolitical heavyweight of domestic policy"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)** EC funded H2020 project, duration : 3/2018-5/May 2021. https://cordis.europa.eu/project/id/769886/reporting	The project may be discussed under this vignette but the solution might not be able to deliver most sound solution to the challenge in question. The project developed innovative quantitative and qualitative empirical methods for risk-scanning, foresight and forecasting. This included large-scale *statistical prediction of conflict* as well as development of in-depth qualitative *risk scenarios*. EU-LISTCO identified six risk clusters: (1) geopolitical rivalry and risks of major armed conflict; (2) unconventional security risks; (3) biological and environmental risks; (4) demography and uncontrolled migration; (5) global financial and other systemic economic risks, and; (6) technology-driven disruption.

		In EU-HYBNET training in could be tested if risk scenarios may support coherent response to migration flow especially in hybrid threats context. **Practitioners in focus**: border and coast guards, civil protection and first responders, authorities and ministries respsonsible for internal and external security and foreign affairs.

Vignette 6. *Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanizedinfantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia*.

Threat, primary context "Digital escalation and AI-based exploitation"		
D	**Name of the innovation**	**Short description on the soundness to be tested**
3.8	**Concordia**, EC funded H2020 project. https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-04-Reseach-and-Innovation.pdf	Artifical Intelligence (AI) is a key technology in the security and defense sectors. Often AI is used to strengthen cyber defense capabilities as well as enhance attack proficiency. In EU-HYBNET training CONCORDIA's key results on adversarial AI attacks and countermeasures can be shortly presented. This is to follow discussion on overarching and detailed view of the role AI in hybrid threat counter measures in defence context (e.g use of AI in cyber attacks against air forces). The discussion is also to highlight which features of AI solutions needs to be exhibit to make them trusted and secure. **Practitioners in focus:** Cyber security experts, defence authorities.

Core theme "Cyber and Future Technologies"

Vignette 3. *Cyber-attacks on Balan, Berkhudia and Bhic cause major power outages. This causes serious problems on households as well as industrial control systems on a frequent basis, having severe financial impact on trade exports*.

Threat, primary context "Offensive Cyber Capabilities"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Strategic Cultures of Cyber Warfare** (CYBERCULT) which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021. https://cordis.europa.eu/project/id/844129	This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and

		cultural factors which motivates development of offensive cyber capabilities, and framework for achieving less destructive global cyberenvironment. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Threat, primary context "Disruptive Innovations"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**INtelligent Security and PervasIve tRust for 5G and Beyond (INSPIRE-5Gplus)** https://cordis.europa.eu/project/id/871808	**INSPIRE-5Gplus** explores ways to improve control of systems and eliminate vulnerabilities for the infrastructure owners and tenants, employing machine learning, AI, and blockchain technologies. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Isogeny-based Toolbox for Post-quantum Cryptography** (ISOCRYPT) https://cordis.europa.eu/project/id/101020788	**ISOCRYPT** is one of the projects exploring cryptography which would be usable in today's technological context, as well as remain secure when quantum computing capabilities are deployed. Project is exploiting mathematical maps called isogenies in new algorithms for security in a pioneering cryptographic paradigm. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Vignette 4. *Telecoms in Berkhudia are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations*.

Threat, primary context "Space interference and counterspace weapons"		
D	**name of the innovation**	Short description on the soundness to be tested
3.4 & 3.8	**7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases** https://www.7shield.eu/project/	The 7Shield framework is being developed to be able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely the pre-crisis, crisis and post-crises phases. The integrated framework is flexible and adaptable enabling the deployment of innovative services for cyber-physical protection of ground segments. The framework will integrate advanced technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection. *Pre-crisis* phase: An early warning mechanism is being used to estimate the level of risk before the

		occurrence of the attack. *Crisis* phase: During the attack, detection and response is effective and efficient, considering also budgetary constraints. A mitigation plan is designed and automatically updated to offer a quick recovery after an intentional attack or a system failure. Business continuity scenarios are also supporting the security and resilience of private installations. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Protection and Resilience Of Ground-based infRastructures for European Space Systems** (PROGRESS). This project was funded under FP7-Security in the period from 01.05.2014 to 31.10.2017. https://cordis.europa.eu/project/id/607679	PROGRESS focused on detecting and mitigating intrusions to GNSS from highly educated attackers whose numbers may increase soon. The goal of the project is to enable expanded intelligence in GNSS architectures to ensure the uninterrupted performance of services. The potential impact of attacks is to be reduced through protective solutions; attacks are to be detected and analyzed for impact, and where necessary, affected elements of the GNSS are to be reconfigured. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Vignette 5. *The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full with migrant on Duzec shores.*

&

Vignette 6. *Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanizedinfantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia.*

&

Vignette 8. *A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions*.

Threat, primary context "Offensive Cyber Capabilities"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Strategic Cultures of Cyber Warfare** (CYBERCULT) which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021. https://cordis.europa.eu/project/id/844129	This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and cultural factors which motivates development

		of offensive cyber capabilities, and framework for achieving less destructive global cyberenvironment. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Core theme "Resilient Civilians, Local Level National Administration"

Vignette 1. *Gas Flow to Bhic from Sharn is paused after a gas pipeline explosion. Initial findings (IED) support the assumption that probably it is about a sabotage and not an accident. Speculation that the Federation is behind the incident is strong.*

&

Vignette 3. *Cyber-attacks on Balan, Berkhudia and Bhic cause major power outages.This causes serious problems on households as well as industrial control systems on a frequent basis, having severe financial impact on trade exports.*

Threat, primary context "Exploitation of critical infrastructure weaknesses and economic dependencies"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with a focus on district or regional protection (PRECINCT)** duration : 06/10/2021-30/10/2023, GA No. 101021668 https://www.precinct.info/	The project "aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures." PRECINCT will develop an ecosystem platform for improving the security and resilience of interdependent critical infrastructures, specifically combining physical and cyber areas for wider situational awareness. It will develop tools and models for collaborative response action to identified threats. It will also develop a vulnerability assessment tool, based on serious games. It will aim to identify vulnerabilities to cascading effects and to assess measures for enhancing resilience. From EU-HYBNET's point of view, PRECINCT's approach is noteworthy because of its ambition to integrate private and public stakeholders under the same CI security framework. PRECINCT will bring together prior results from three EU-funded projects and capitalize on legacy structures. **Practitioners in focus:** Critical Infrastructure operators and those responsible for CI protection need to acquire technologies and skills to identify such complex attacks so that they may respond timely and adequately.

Vignette 5. *The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full with migrant on Duzec shores*.

&

Vignette 6. *Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanizedinfantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia.*

Threat, primary context "Exploitation of existing political cleavages"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**In the Wider and Enhanced Verification for You (WeVerify)** duration : 01/12/2018 – 30/11/2021 GA No. 825297 https://weverify.eu/about/	The aim of the project was to address the advanced content verification challenges through a participatory verification approach, open-source algorithms, low-overhead human-in-the-loop machine learning and intuitive visualizations. The project has developed the InVID-WeVerify browser plug-in that will help its user to verify online information. Furthermore, the WeVerify project assembled a companion to help citizens and fact-checking professionals to take advantage of the features of the plug-in. The companion also includes links for citizens to find online advice concerning disinformation threats. **Practitioners in focus:** NGO's, governmental institutions, private bodies, human rights activists, media outlets.

Core theme "Information and Strategic Communication"

Vignette 2. *While preparations for the elections in Bhic are ongoing, the minority in Duzec declares the desire to call a referendum for independence, whereas social media in Bhic strongly support this issue.*

Threat, primary context "Information manipulation with the aim of destabilization"		
D	**Name of the innovation**	**Short description on the soundness to be tested**
3.8	**Information and Misinformation Economics: Design, Manipulations and Coutermeasures** (IMEDMC) EC funded project. Duration: 1/5/2021 – 30/4/2026. GA No. 101001694. https://cordis.europa.eu/project/id/101001694	IMEDMC will analyze the unexplored designer-agent-receiver class of games considering fake news production – state falsification, pure agency and state shifting, taking a systems approach. For simulations, IMEDMC will employ underutilized designer-agent-receiver class of games, in which the designer picks an information generation system, the agent takes an upstream decision affecting the states of the world, or manipulates the production of information, and receivers choose downstream actions based on realized signals. For EU-HYBNET training the IMEDMC approach, methods and games may render

		specific interest. It may be appropriate to observe successes and drawbacks of IMEDMC approaches and methods applied ,and to discuss their applicability to model and analysis of hybrid threats. In EU-HYBNET training the special focus would be means to influence general opinion via fake news. **Practitioners in focus:** Intelligence, authorities responsible for internal security.

Threat, primary context "Foreign interference in key information institutions"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**The Consequences of the Internet for Russia's Informational Influence Abroad** (RUSINFORM) project - a closer look at Russia's digital disinformation. Funded by EC, H2020. Duration : 11/2019 – 12/2024. https://cordis.europa.eu/project/id/819025	RUSINFORM does not deliver any technical solution but introduces datamining techniques and automated text analysis in combination with traditional methods (surveys, in-depth interviews, grounded theory). The innovative combination of these techniques is to deepen understanding of the phenomena and build a better methodological basis for further analysis efforts. RUSINFORM results area important in advancing our knowledge of the mechanisms of foreign influence. In EU-HYBNET training RUSINFORM solution, namely combination of tools and techniques, and this approaches usability and benefits to security authorities analysis on malicious actors information interference and influence to SOME could be addressed. **Practitioners in focus**: Intelligence, authorities responsible for internal security ; LEAs.

Vignette 7. *A Fake news campaign on Bhic official media, that the electoral process is staged and premeditated is observed. Sandmouthian probes and outlets as for journalists and "independent" analysts are amplifying this narrative, provoking distrust sentiments to the citizens.*

Threat, primary context "Information manipulation with the aim of destabilization"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Open Your Eyes: Fake News for Dummies** Project. Funded by EC, Erasmus+ instrument. http://dlearn.eu/projects/online-and-offline-security/open-your-eyes/	The project is dedicated to improve the digital literacy of adult learners by providing them with tools to identify fake news and fight the spread of disinformation online. It is important to continue and extend of such project beyond "supply side" verification – how we recognize fakes, to understand more "demand side" of fakes.

		In EU-HYBNET training « Open Your Eyes » project's tools could be analysed in order to test their soundness to recognize hybrid threats fake news campaigns. **Practitioners in focus**: Intelligence.

Threat, primary context "Foreign interference in key information institutions"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (COMPROP).** Funded by EC, H2020. Duration 1/2016 – 12/2020. https://cordis.europa.eu/project/id/648311	COMPRPO researched specific aspects of "computational propaganda" involves the use of algorithms, automation, and big data analytics to purposefully disseminate manipulative and misleading messages over these social media networks. The project seeks to answer e.g. to a research questions: How are algorithms and automation used to manipulate public opinion during elections or political crises? What are the technological, social, and psychological mechanisms by which we can encourage political expression but discourage opinion herding or the unnatural spread of extremist, sensationalist, or conspiratorial news? What new scholarly research systems can deliver real time social science about political interference, algorithmic bias, or external threats to democracy? In EU-HYBNET training COMPROP's approach on needed solutions (e.g. big data analytics to LEAs) to real time reaction and analysis on information manipulation in SOME could be under discussion. **Practitioners in focus:** Intelligence, LEAs.

Threat, primary context "Promoted ideological extremism and violence"		
D	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Artificial Intelligence Roadmap for Policing and Law Enforcement** (ALIGNER) EC funded projcet. Duration: 10/2021 – 10/2024. GA No. 101020574. https://cordis.europa.eu/project/id/101020574	ALIGNER, is dedicated to broader set of technologies for law enforcement and policing. It aims to jointly identify and discuss how to enhance Europe's security by employing AI and advanced technologies, it will pave the way for an AI research roadmap. Special focus is on Law Enforcement Authorities (LEAs). In EU-HYBNET training ALIGNER's identified needs of LEA's for most wanted AI technologies and solutions could be under discussion, especially focusing to the context of identifying

		information manipulation and interference by foreign actors. **Practitioners in focus:** Intelligence, LEAs.

In the end T2.3 recommended in total 15 (fifteen) different, mainly European Commission (EC) funded, research and innovation projects' innovations to be tested during the 2nd EU-HYBNET training event arranged by T2.4. Therefore T2.3 provided sound an input for the EU-HYBNET to deliver results in monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results.

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

Similar to Task 2.3, also T2.4 "*Training and Exercises for Needs and Gaps*" (lead by KEMEA) provides input to the Three Lines of Action **monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results** from the EU-HYBNET training activities side. In short, T2.4 arranges testing environment for some selected promising innovations according to T2.3 training scenario suggestions. The testing is important in order to gain EU-HYBNET's Network members' (pan-European security practitioners, academia, industry, SMEs and NGOs) views on the soundness of the proposed innovations.

In the 2nd EU-HYBNET training event (hybrid format on the 29th -30th of Sept 2022 in Vilnus) almost all research and innovation projects with their key innovations as recommend in T2.3 training scenario were tested. The results of the soundness of the selected projects' and their innovations to counter hybrid threats and to **recommend the uptake or the industrialisation of results** are described in next main chapter because the findings are much linked also to the second Three Lines of Action namely **common requirements as regards innovations that could fill in gaps and needs.**

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

During the reporting period the many innovations identified in T3.3 and T3.2 have been set under thorough analyses of T3.1 "*Definition of Target Areas for Improvements and Innovations*" (Lead by TNO) because T3.1 is to deliver the final analysis of the most promising innovations to identified, present pan-European security practitioners and other relevant actors gaps and needs, threats to counter hybrid threats. The work in T3.1/ D3.2 "*Second interim-report mapped on gaps and needs*" (M32/ Jan 2023) is still on-going a hence the results will be reported in the next six month Action report, D1.9 "*6th Six Monthly Action Reports to EC*" (M36/ April 2023).

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

As mentioned in chapter 3.1, EU-HYBNET project activities were launched by identification of practitioners'[2] and other relevant actors' (industry, SMEs, academia, NGOS) gaps and needs and vulnerabilities to counter hybrid threats, in EU-HYBNET Tasks (T) 2.1 "*Needs and Gaps Analysis in Knowledge and Performance*" (lead by Hybrid CoE) and T2.2 "*Research to Support Increase of Knowledge and Performance*" (lead by JRC). The work conducted in T2.1 and T2.2 resulted in D2.9 "Deeper analysis, delivery of short list of gaps and needs" (M5/ September 2020), and now during the second project cycle (M18-M34/ October 2021-February 2023) to D2.10 "Deeper analysis, delivery of short list of gaps and needs" (M23/ February 2022) where the most important pan-European practitioners' and other relevant actors' (industry, SMEs, academia, NGOs) gaps and needs to counter hybrid threats were listed for the 2nd project cycle for the project to focus on.

The identified gaps and needs, threats in D2.10 provide the basis for other EU-HYBNET Tasks to proceed in their work related to innovation mapping to gaps and needs, finding most promising innovations and to compile recommendations for innovation uptake and standardization.

What comes to the second Three Lines of Actions focus area "**common requirements as regards innovations that could fill in gaps and needs",** the research activities and results in this Six Month Action Report reporting period are delivered by T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE) and T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS). Furthermore, T4.3 "*Recommendations for Standardization*" (lead by PPHS) results are also linked to the Second Three Lines of Action but because the results serve more the Third Three Lines of Action, they are described under the Third Three Lines of Action. More information about T.2.4 and T3.4 results to the Second Three Lines of Action in the following subchapters.

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

The 2nd EU-HYBNET Training and Exercises event was arranged by T2.4/ L3CE in hybrid format on the 29th – 30rd of September 2022 (Agenda in Annex III). In the training event DTAG game was used because the game was seen fruitful during the 1st EU-HYBNET training event (April 2021) to enable pan-European practitioners and other relevant actors (industry, academia, NGOs) from the EU-HYBNET

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

consortium and Network to test and assess the pre-selected innovations in a realistic scenario and inject setting.

The training and exercises were built around the scenario and injects from T2.3/D2.18. However, though a majority of the innovations listed in T2.3/D2.18 injects, not all were eventually introduced to the training participants but most promising selected. In addition, during the first training day also four innovation provides were asked to provide a live innovation presentation (demo) on their solution(s) that were analyzed as a promising innovation to counter the EU-HYBNET's identified present main gaps and needs, vulnerabilities of pan-European security practitioners and other relevant actors to counter Hybrid Threats. The live innovation presentations were given by following organizations:

- Lithuanian Armed Forces Strategic Communication on innovative tools and methodology application to information analysis
- HENSOLDT on open-source intelligence solution
- MALTEGO on open source intelligence solution
- European External Action Service/ Strategic Communication Division on a *DDS-Alpha/ The FIMI Data Space (A common framework and methodology for collecting systematic evidence on disinformation (FIMI)"/ Open CTI* tool

During the training the participants did test some of the introduced innovations according to the selected vignettes. The section of the innovations was to ensure more profound discussion on the innovations usability within the inject context, and to conduct a more thorough analysis on the selected innovations usability. The next subchapters describes the innovation analysis according to the project four Core Themes and as presented in D2.21 "Training and Exercises Delivery on up-to-date topics" (by L3CE) - The results of the innovation evaluation are described in detail in D2.21 (Submission on Oct 2022).

Core Theme – Future Trends of Hybrid Threats

Discussion	Priority	Innovation	Comments
Day 1	1	OSINT	Mostly discussed. Some points for further considerations were identified: - Visual representation of key results of the request is very important. - Verification and traceability of information included is essential. - Some ML (AI) features can be added in the future for improved request execution.
	2-3	Digital Twins	Requires more information, but might be considered interesting solution for industry and critical supplies. Can be considered for the future as potential subject for regulation.
	2-3	DDS-alpha	Too early to evaluate at operational level. Considered interesting and valuable.
	4	Multi-source integr.	Needs significant preparation to be deployed.
	5	EU-LISTCO	
Day 2	General comment: the most valuable innovations were considered those, providing capabilities of collaborative response. OSINT, multi-source and DDS-alpha support such actions from the list provided. More attention was given for the innovations not discussed in previous round:		

		PersoNews	Ethical issues to be considered, as it can be interpreted as micro-targeting.
		Education	Rather long discussion emerged around the education issue. It was evaluated as rather low priority as if it is described at the moment, concluding that it should be changed, but providing no recommendations on "how".

No additional remarks were delivered from the innovations.

Core theme - Cyber and future Technologies

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	1	7 Shields	- It does not contribute to the prevention of crisis or attack but rather works for during and post crisis stages. - Works good for higher coordination and management capabilities involved in mid and high-level decision making processes. - Especially useful for information sharing cross institution and cross-borders among alliance partners. - Allows better to organize responsible capabilities for different actions. - Data correctness is key factor for platform to be trusted. - It should be developed further from security and high availability perspective as such a solution immediately becomes strategic target (decentralization should be a solution).
	2	Defence Framework	- How to ensure that it is correct? - In case on attack situation is changing too fast for system to learn and train on the data to address it correctly. - Typically, attacks are uniquely designed and there is high probability that it will miss the new major attacks. - Very dependent on data quality and there is not clear presentation how data quality will be addressed. - New technologies and software upgrades are released on daily basis that it is hardly imaginable how to maintain such a framework actuality.
	Key considerable factors for success: - it is important to address cascading effects therefore timely, precise communication with citizens in critical feature. All institutions having precise situational awareness information is a key. - In large scale crisis it is mandatory to enable local/regional autonomous handling of life critical functions, therefore localized situational awareness and coordination should be considered as improvement. - For cyber incidents quick analysis features can be considered additionally (who is behind analysis, attack scale assessment). - Integration of automated response protocols would be considered as one of features helping a lot to efficiently handle first stage after crisis incident report.		

No additional remarks from the innovations in the discussions.

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

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	General comment: rationale for selecting these innovations when having the above-mentioned vignette in mind was their perceived level of readiness to be deployed in this case, as well as suitability to deal with such type of hybrid threats. One important downside of these innovations is their apparent focus on information exchange, but not on collection.		
	1	PRECINCT	- Assets used to support the national electoral process can be considered as CI and calls for independence from minority groups in this period may disrupt the established democratic procedures. - Innovation may be adapted for contingencies such as the one described in the respective vignette.
	2	Screened FDI	- Innovation could help with unveiling connections between organisations representing, (or claiming to be representing), minority groups and their financial backers, especially if the latter are operating covertly. - There are therefore specific concerns about the use and security of the data collected.
	3	Real-time Rapid Alert System	- Linking of information exchange systems on national level with those of the EU, (and potentially between both private and public entities). - Might produce 'false positives' and potentially lead to privacy issues, especially when it comes to the EU environment with its strict personal data exchange and processing policies.

According to the additional remarks, the conclusion from discussions was that innovations proposed for discussion and review mostly focus on technology as a potential answer to hybrid threats. As good as such technological solutions may be, they may not be enough to deal with the whole spectrum of threats. Perhaps, such measures as strengthening democratic institutions could be used in combination with the proposed tools to combat minority jingoism and separatist tendencies in times of national elections.

Core theme – Information and Strategic Communication:

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	1	DDS-Alpha (EEAS)	- Were considered helpful with regard to data collection and management but was also highlighted their limitations from the perspective of how to counter the threats.
	2	Systematically assess information validity	- Were considered helpful with regard to data collection and management but was also highlighted their limitations from the perspective of how to counter the threats.
	3	Integrated Monitoring System against cyber-enabled IO	- Making sense against deepfakes

		IMEDMC	- Raised doubts about its nature since this is a project at an early stage.
		RUSINFORM	- Was considered interesting from the perspective of understanding and methodology although having an external perspective and ignoring the hybrid dimension.

According to the additional remarks, during the discussion there were some additional ideas on relevant innovations raised. One such example of non-technological innovation was enabling cross-government crisis management and organization cultural practices development.

Discussions resulted in a very different selection of innovations. Priorities can be grouped into several groups that can be summarized as most relevant directions for innovation up-take:

- Open source intelligence (OSINT) related tools (example: HENSOLD), that provide fasted information on the maximized scope of the event, including significantly different information space. Focus made on information collection and visual presentation.
- Support of critical infrastructure in securing their services provision in case of direct attacks or supply chain breakdowns (example: Digital Twins, 7 Shield). Focusing on CI resilience.
- Information about hybrid treats and relevant operations exchange and structurisation providing faster and more focused response (example: DDS-Alpha). Focusing on information exchange and systematization.
- Innovations, that provide possibilities for collective response to hybrid treats. Focusing on involvement at different levels, from crowd sourcing to international collective actions.
- Means for verification in different processes, starting from fact checking, debunking and going to decision making protection, ensuring ML credibility.

The general comment from discussion was, that it is still very difficult to asses innovations, even at the prioritization stage. Early stage TRL innovation presented raised even more questions, most of them seem interesting, but estimation of their value in a given situation, described by Vignette, was very difficult.

On the whole, the evaluation of the innovations in T2.4 has been very important to the EU-HYBNET 2nd cycle activities because the results are imbedded into the T3.1 final analysis of the most promising innovations that will be delivered in D3.2 “Second Interim-Report Mapped on Gaps and Needs” (M33/ Jan 2023).

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

During the reporting period EU-HYBNET T3.4 “*Innovation and Knowledge Exchange Events*” (lead by EOS) delivered comprehensive findings to **common requirements as regards innovations that could fill in gaps and needs** in the *2nd Innovation Knowledge Exchange Workshop* (IKEW) that was arranged on the 14th of June 2022 in Hague and online by TNO. Program in Annex IV, and the comprehensive

description on IKEW is delivered in D.3.12 "*2nd Innovation and Knowledge exchange events report*" (by MoD NL, M 27/July 2022). The chapters below summarizes key findings of IKEW from D3.12.

The IKEW provided an opportunity for practitioners, industry, SMEs, and academia to exchange information on challenges to counter hybrid threats and possible innovations to answer them. Therefore, IKEW focused on facilitating the continuous mapping of needs, monitoring of solutions and innovations, and provided a forum where security practitioners could engage with innovation providers. This was to provide exchange of knowledge and information about innovations to increase the likelihood of future uptake of the most sound innovations and solutions to counter Hybrid Threats. IKEW was open to open to project partners, EU-HYBNET network members and external participants upon registration because the event aimed also to boost cross-fertilization between the EU-HYBNET and other EU projects, institutional and industry actors and variety of stakeholders. More than 100 participants registered to IKEW and hence the event delivered comprehensive views on **common requirements as regards innovations that could fill in gaps and needs**.

The 2nd IKEW started with two key-note speeches. The first key-note was provided by MS Hester Somsen, Deputy National Coordinator for Counterterrorism and Security (NCTV) and director for Cyber Security and State threats in the Netherlands. The keynote was about Dutch developments in hybrid threats, and also views on needed future innovations and solutions was partly highlighted. After all according to MS Somsen not only awareness of hybrid threats is needed but also innovations on how to defend ourselves in many domains e.g. disinformation, cyber, better legalisation, etc. The second keynote speech was given by Geert Kuiper, the Director for Strategy and Knowledge at the Dutch Ministry of Defence. Mr Kuiper spoke about connecting the dots to counter hybrid threats and the role of the Dutch Defence. In addition, he highlighted that enhanced capabilities in information guided operations, automatization, robotization, cyber, electronic warfare and space are central to a more future proof armed forces. This comment also provided insight of future needs of new innovations in the area.

After the two opening speeches EU-HYBNET partner TNO/Mr. Okke Lucassen presented shortly what are the first EU-HYBNET project cycle discoveries of most promising innovations, and how innovation analysis is done in order to define from the various promising innovations especially those that seems to answer to EU-HYBNET's identified gaps and needs, threats and vulnerabilities to counter hybrid threats. This provided good basis to start the second part of the IKEW workshop that was dedicated to hosted smaller workshop group discussions (Break out session, "BOS") on relevant innovations to the EU-HYBNET's 2nd project working cycle's identified gaps and needs to counter hybrid threats. Each BOS included variety of innovations and the discussion was formulated according to the EU-HYBNET project Four Core Themes:

1. Future trends of Hybrid Threats
2. Cyber and future technologies
3. Resilient civilians, local level, and administration
4. Information and strategic communications

The results of the Break-Out Sessions (BOS) and innovations under discussion were following.

Core Theme: "Future trends of Hybrid Threats"

BOS1.1. "Dilemman Gaming"/ **Innovation**: *Hybrid online dilemma Game*

The starting point to the discussion of the innovation is to understand that strategic decision making in countering hybrid threats is highly situational, cognitively complex and performed under demanding circumstances. Moreover, the higher the level of decision making, the more political considerations play a role as strategic decision making in essence is about reconciling divergent interests. Hence, hybrid threats confront decision makers with complex dilemma's that require trade-off decisions such as choosing between economics and security or between external and internal frictions. To make policy and decision makers aware of such dilemmas and subsequently train them for decision making under such complex circumstances Hybrid online dilemma Game had been developed by TNO and Hybrid CoE. The game aims to expose for decision makers a rapidly unfolding scenario where they are confronted with dilemmas that need decisions.

According to the discussion the dilemma game was seen to serve practitioners and policy makers by supporting them to realize the complexity of hybrid threats and response to hybrid attacks. However, a question was raised about the scalability of the game, how to make the game more scalable to larger audiences. During the discussion several possible solutions were presented by different participants, but it was underlined quality should not be harmed by the need to expand.

BOS1.2. "Hybrid Threats impact on critical infrastructure Disruption: Existing Measures and Solution Needs"/ **Innovations**: *"Supply chain label "Made in EU", Fully automated incident response solution", "Counter-Unmanned aircraft systems, "Critical infrastructure resilience tool", "Digital twins for supply chain disruption",* and *"Holistic framework for European ground segment facilities"*

This online break-out session focused on how to best strengthen critical infrastructure resilience against hybrid threats. The session discussed on solutions, innovations and other measures - either technological or non-technological - to counter the impact of hybrid threats on critical infrastructure disruption, including economic dependencies and cascading effects across sectors. According to the discussion the innovation of *fully automated incident response solution* was seen as a very promising innovation by all of the participants. The *critical infrastructure resilience tool* and the *digital twins for supply chain disruption* were also seen as promising. It was concluded that tooling can create awareness/ detection on disruption which is the first necessary and critical step before countering the disruption. Therefore, there is clear need to work on awareness (non-technical) and have (technical) tools to forecast the impact when critical infrastructure is disrupted. However, at present there is no systematic approach available with interdependencies between the different sectors, and hence there is a need for a good registration of critical infrastructure in Europe in order identify what and where to defend. This being said, it was seen that the EU could play a large role in setting the requirements, in the form of legislation, for developing critical infrastructure (e.g redundant communication systems).

Core Theme: "Cyber and future technologies"

BOS2.1 "Cyber and Future Technologies – How to Advance?" **Innovations(s)**: *Establish Data Embassies or E-embassies*, and *A Quantum-Resistant Trusted Platform Module*

The starting point for the discussion was that we have been experiencing exponential growth of the technology driven social processes throughout the last decade(s). New levels of information manipulation, misinformation, disinformation, fake information, propaganda are taking place. Information warfare is new reality, and there are many proven cyber capabilities so that public can be manipulated and their information is misused. Therefore, the key questions were "What risks must countries prepare for?" and "What technological and social innovations will be needed to mitigate them?".

The first introduced innovation that could be seen as a part of a solution to the acknowledged challenges was *Establish Data Embassies or E-embassies*. The Lithuanian experience of E-embassies was introduced, and the key element is that Lithuania has established an E-Embassy/data Embassy on the territory of another country, Luxemburg. During the discussion the idea of establishing E-embassies was criticized for creating a different target but then in another country. Also, there is the question that data needs to be updated all the time and by destruction the most recent data will be lost anyhow. Suggestions were made for improving the innovation by compartmentalization of the data on various locations or on various digital storages (clouds). More and safer storage possibilities were suggested in space or at the bottom of the sea.

The second innovation under discussion was *A Quantum-Resistant Trusted Platform Module*. It was greed that there is need to create a quantum testbed, where to test cryptography, test quantum algorithms and demystify cryptograded-digital hacking, preferably in Europe. In short, it was seen necessary for the EU to set up their own test bed in order to stay innovative. It was the organiser's belief that whoever develops quantum computing to its fullest capabilities would have a strong disruption potential, especially in the field of countering hybrid threats. The testbed is also needed to demystify to what extent quantum can be mass adopted. Quantum in the wrong hands can have a lot of impact, so there is a need for technological literacy.

BOS2.2 "Emerging Technologies: From Reactive to Proactive Use of Innovations to Counter Hybrid Threats " **Innovations(s)**: *Swarm wolf scenarios,* and *AI computer vision*

This online break-out session facilitated discussions on the need to exploit specific innovations and tailor adequate solutions as an important part of increasing threat awareness and resilience of EU target democracies against the exploitation and manipulation of political cleavages, social tensions and polarization by hybrid campaigns.

It was underlined that individual data aggregation and computing gives unprecedented transparency of societal fault lines, and cognitive processes at individual and collective levels can be leveraged to drive cognitive radicalization online into physical violence in the real world. Furthermore, it was acknowledged that disruptive technologies can harness behavioural data. Those disruptive technologies are democratizing and can be available to more individual or smaller group levels, and they can be used both in hybrid attacks and to prevent the hybrid attacks. It was concluded that more research of the possible innovations in the field is needed.

Core Theme: "Resilient civilians, local level, and administration"

BOS3.1 "Who do You Trust?". **Innovations(s)**: *Journalism trust initiative*, and *Government and social media cooperation framework to counter election interference*

This session focused on the trust between civilians themselves, between civilians and technology, civilians and the private sector, and between civilians and their authorities/governments. The group brainstormed about how trust operates in society and amongst civilians. On the basis of the brainstorming, the group gathered indicators of trust/distrust and used these to further analyse two innovations: the journalism trust initiative and the government & social media cooperation framework.

It was highlighted that the two innovations are very information centred, rather than people centred. The focus is very much on the way information is being transmitted; how the information is received should also be taken into account. The innovations mainly focus on controlling institutional and organizational filters in information; however, it is much more difficult to do the same for people. It is difficult to really influence the public to larger degrees, because personal filters often rely on security/insecurity, values and who people trust. However, more awareness could be raised about personal filters. During the brainstorm, the participants discovered that trust is context based. The concept of trust can change while it adapts to the context. Uncertainty, for example, influences the extent of trust in a person or institution. The outcomes of this brainstorm were applied to the further analysis of the two innovations

BOS3.2 "Grazy Ideas Gaming Session". **Innovations(s)**: *Hybrid Threats Scenario game*

This break-out session was a brainstorm-game to gather many new, original ideas about possible hybrid threats. The participants were divided into duos in order to play the game, and the duos had to continually think of logical follow-up events. In addition, the game included 2-3 scenarios, in which hybrid threats and tactics are common place. It was encouraged to think of emerging and disruptive technologies that lead to new manifestations of hybrid threats, and new actors on the pitch or new vulnerabilities that could be targeted. In addition, weird tactics, probably beyond the current legal and ethical playground, were under discussion. The conclusion from the session was that the actions to create fake news about the counter part was seen very fruitful and hence technology in this field to support to counter disinformation in hybrid attacks were acknowledged. In addition, the game format itself was seen as a fruitful non-technological innovation to support security practitioners to be more prepared for hybrid attacks.

Core Theme: "Information and strategic communications"

BOS4.1 "Identifying and Countering Information Manipulations: Professional Tools and Networks of Fact-checking and OSINT Practitioners" **Innovations(s)**: *Journalism trust initiative,* and *Government and social media cooperation framework to counter election interference*

In this interactive break-out session, participants discussed the role of professional solutions and innovations supporting the practice of open-source intelligence (OSINT) and fact-checking/debunking against information manipulations. It was underlined that disinformation is globalized, and sometimes the same contents and tactics are used but translated to different contexts. Therefore, connection with other fact-checkers is essential, and need to create cooperation mechanisms for fact-checker communities was introduced as an innovation. However, for this noticed need an innovation was also introduced and seen to provide a welcomed solution. In short, the European External Action Service (EEAS) FIMI (Foreign Information Manipulation and Interference)-division presented their detection and analysis tool to inform measures against misinformation, so- called *An Open CTI*. An Open CTI has been created and funded by the EU, for forensic secure and court ready information generation. It is used for OSINT-analysis and serves as a tool for fact-checkers. However, there is still need to increase the awareness of the usability of the *Open CTI*, or as it is also called "*DDS-Alpha/ The FIMI Data Space (A common framework and methodology for collecting systematic evidence on disinformation (FIMI)*" for fact-checkers so that the communities may enhance their cooperation.

BOS4.2 "Political Cleavages and Hybrid Threats: Exploiting the New Drivers" **Innovations(s)**: *Detection of proxy actors spreading disinformation, Development of real-time rapid alert system on disinformation, The development of deep fake detection system, Establishment and reinforcement of political education of democratic values, Increasing capabilities to systematically assess information validity throughout the lifecycle, Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications,* and *Installation of rules for mandatory declarations.*

The on-line break-out session investigated on how good governance, communication tools and technical strategies may be crucial to counter hybrid threats. In addition, the session facilitated discussion among stakeholders on the need to exploit specific innovations and to tailor adequate solutions as an important part of increasing threat awareness and resilience of EU target democracies against the exploitation and manipulation of political cleavages, social tensions and polarization by hybrid campaigns. According to the discussion and feedback following three innovations were seen as a promising to the acknowledged challenges – the innovations are: (1) the detection of proxy actors spreading disinformation (2) the establishment and reinforcement of political education of democratic values, and (3) the development of a deep fake detection system. However, a general view was that perhaps technological innovations are not always providing comprehensive solution to resolve political cleavages but can play a part of the solution. Talking about economic terms of innovation, some tools even promising require a lot of investment. Still, the general thought was that when an innovation is labelled as important enough, there are always ways of funding.

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

During the reporting period the main EU-HYBNET task which contributed to the Three Lines of Action "**Priorities as Regards of Increasing of Knowledge and Performance Requiring Standardisation**" was Task (T) 4.3 "*Recommendations for Standardization*" (lead by the Polish Platform for Homeland Security/ PPHS) due to their arrangement of the *1st EU-HYBNET Innovation and Standardisation Workshop* (ISW) on the 15th of June 2022 in Hague (in person and on-line). The key results of the ISW to the third three lines of action is described in the following subchapter. The results base on the ISW report published in EU-HYBNET webpage: https://euhybnet.eu/other-publications/ , ANNEX V includes ISW program.

3.3.1 EU-HYBNET T4.3 RECOMMENDATIONS FOR STANDARDIZATION

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

In every EU-HYBNET working cycle (M1-M17/ cycle I, M18-34/ cycle II, M35-51/ cycle III, M52-M60/ cycle IV), T4.3 is the final project Task that will highlight the key selected project innovations that are seen as a sound solution for the identified working cycle gaps and needs and answering to the pan-European security practitioners and other relevant actors' needs. Therefore during the reporting period, T4.3 arranged the *1st EU-HYBNET Innovation and Standardisation Workshop* (ISW, the 15th of June 2022, Hague) in order to have a workshop where consortium partners and external participants (practitioners, industry, academia and NGOs) discussed standardisation recommendations for EU-HYBNET's most promising, EU-HYBNET T4.2 selected innovations to counter hybrid threats in two thematic areas. The thematic areas were:

- **Thematic Area 1.** *Standardisation measures in the context of critical infrastructure protection and innovations to enhance information sharing*
- **Thematic Area 2.** *Innovations in disinformation and media literacy*

The two thematic areas formed own parallel working groups during the ISW and each of the working group focused on EU-HYBNET's recommended innovation for the thematic area. The Innovations were following:

1. **Thematic Area**: *Critical Infrastructure protection*

   An innovation:

- A technological Innovation called "Public-private information-sharing networks for developing collaborative investigations and collective actions - A Common Information Sharing and Analysis Environment" (**CISAE**)

2. **Thematic Area**: *Disinformation and media literacy*

   Two innovations:

   - A technological innovation from EEAS called as "**Open CTI**", or as it is also called **DDS-Alpha/ The FIMI Data Space** ("*A common framework and methodology for collecting systematic evidence on disinformation"*)
   - Non-technological innovation focusing on **measure to enhance citizens media literature skills**

Next to the working group discussions on the named innovations, also other ISW presentations in the working groups and in the beginning of the event provided larger understanding on the context of the innovations and their need, also in the frames of standardization.

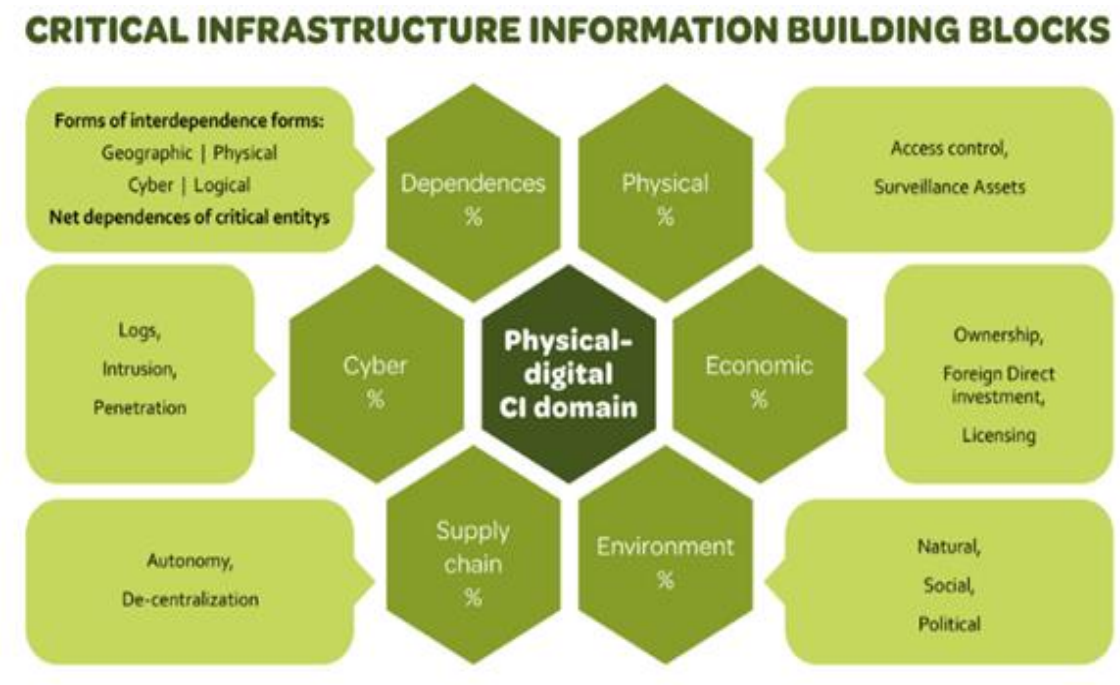
The two working groups resulted to highlight priorities in increasing knowledge of the suggested EU-HYBNET innovations and measures that are needed in performance and as a standard so as to have the named innovations in use. The result are described from each working groups below.

Thematic Area: *Critical Infrastructure protection*

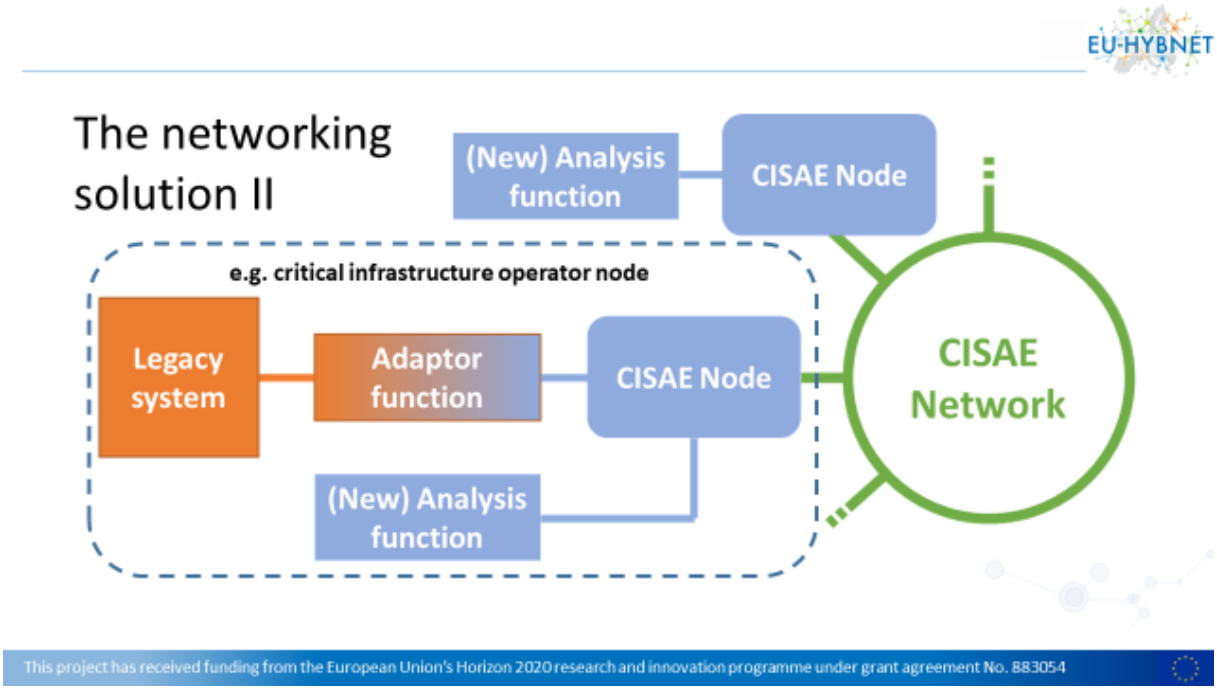
An innovation: A technological Innovation called "Public-private information-sharing networks for developing collaborative investigations and collective actions - A Common Information Sharing and Analysis Environment" (**CISAE**)

In the beginning of the working groups sessions, EU-HYBNET T4.2 "*Strategy for Innovation uptake and industrialization*" leader RISE/ Dr. Rolf Blom and EU-HYBNET Innovation Manager/ Mr. Isto Mattila (Laurea) presented the selected CISAE innovation and highlighted key elements in **priorities as regards of increasing knowledge and performance** of the CISAE and what it requires in **standardization**.

The CISAE is meant for critical infrastructure (CI) practitioners and organizations (public & private) to share and to analyse situational information in order to empower their situational awareness related to hybrid threats and attacks, and to support to possible joint mitigation actions. The use of CISAE should take place on voluntary basis between CI operators. A starting point is to develop CI sector/domain specific CISAEs (A Common Information Sharing and Analysis Environment). This requires development of key analysis tools and to establish a governance body for the information exchange. Furthermore, a framework agreement in each CI domain comprising information sharing principles needs to be developed alike agree on how and where joint analysis tools should be implemented and operated in the named domain between the entities/operators. Furthermore, to establish CISEA there is need to define and to develop interoperability protocols and principles, also data exchange formats and procedures per type of critical infrastructure. The pictures below describes building blocks and plans to establish CISAE in a CI domain:



The CI domain CISAE would be connected to other CI domains CISAE with a node and eventually this would for holistic CI CISAE network for information sharing on hybrid attacks and threats in the CI domain pan-European wide. The picture below describes the networking solution elements.



In order to proceed in the CISAE development and uptake, following tentative barriers are to overcome

- Explain the benefit of the CISAE pan-European wide especially for public and private CI entities, security practitioners, EC and EU MS relevant actors and organizations in order to proceed in establishment of CISAE. Without engaging key actors the development may not start.

- Agreement on what type of information will be shared with whom is central not only to CISAE function but also to develop mutual partners trust both at EU and Member State level in the context of information-sharing.

- Analyse possibly missing or restrictive legal framework for CI entities for information sharing in CISAE

However, to support the CISEA development and uptake, the European Maritime Security Agency's (EMSA) "Common Information Sharing Environment" (CISE) to maritime domain security practitioners pan-European wide serves as a well working and established, up and running example how CISAE may work and how the users may benefit on it. As in the development of CISE also following required standardization activities to establish CISAE were noted:

- **Network architecture.** Learn from EMSA CISE Architecture.
- **Taxonomies and encodings per CI domain.** Connected with ETSI. ETSI is an independent, not-for-profit, standardization organization in the field of information and communications. ETSI supports the development and testing of global technical standards for ICT-enabled systems, applications and services
- **Legal framework.** Learn from EMSA CISE Architecture.

In the working group session many additional remarks were also given to priorities as regards of increasing knowledge and performance of the CISAE and what it requires in the context of standardization. First of all European Reference Network for Critical Infrastructure Protection (ERNCIP) was identified as an important step to enhance technical collaboration among all relevant stakeholders, share best practices and guidelines and overall improve the protection and resilience of critical infrastructures in Europe. Therefore ERNCIP's views and support to CISEA development is seen important. Furthermore, Dr. Aikaterini Poustourli, Standardisation Expert, Member of EURAS, identified as a first step the need to examine which of the existing standards in the field could correspond to future needs. Mr. Yves Rougier from the French Ministry for an Ecological Transition and Territory Cohesion presented his perspective on resilience against hybrid threats and highlighted the importance of clear definitions. Participants concluded that hybrid threats are not clearly defined in a way that would allow for an EU-wide regulation on standardisation, also in the context of Critical Infrastructure protection against hybrid threats and attacks. Moreover, two European Commission Horizon projects PRAETORIAN and 7SHIELD from the CI domain presented their LL of standardisation activities and highlighted why standards are needed to align the activities and to deliver the needed security measures.

Thematic Area: *Disinformation and media literacy*

In the beginning of the working group sessions, EEAS Strategic Communication Division/Mr. Daniel Fritz presented the selected Open CTI innovation and some priorities as regards of increasing knowledge and performance of the OpenCTI and what it requires in standardization.

The starting point for the Open CTI is to apply threat informed defence principles to detect and measure Disinformation. EEAS is providing a framework for identifying disinformation, including taxonomy and relevant standards. What is needed in this respect is to have a common definition, a

common taxonomy, a common methodology, a common data exchange format, and a common Interface & Tool (optl.) Especially the common data exchange format Open CTI delivers while it also delivers solution for the other named common needs. The Open CTI is much welcomed because in fact checking, shared methods to detect (e.g. deep fake) and to report on findings among relevant pan-European actors and stakeholder has been needed. Furthermore, there has also been need to create database(s) for presenting the narratives most often used in disinformation, and again Open CTI answers to this need too. The importance of the data base is that the information in the database at the same time creates a list of European vulnerabilities that will support to consider counter measures do diminish these vulnerabilities. Therefore, it was also recognized a need for countermeasure standards to disinformation that would include key elements for cooperation between various actors in different key domains (public sector, education system, civil society organizations, the media, business). Multi-stakeholder cooperation is central part of the use of to the Open CTI alike alerts on disinformation campaigns. In the working group the alerts on disinformation campaigns much called for as a standard activity in societies, in similar fashion as it is nowadays the case with extreme weather forecasts.

Another innovation, a non-technological innovation focusing on measure to enhance citizens media literature skills was also widely analysed in the working group in the context of **priorities as regards of increasing knowledge and performance requiring standardization.**

The discussion was started by MS Emma Goodman, European Digital Media Observatory (EDMO), who stressed the importance of media literacy as a tool that can help populations counter disinformation. Furthermoe, MS Solvita Denisa-Liepniece added that through media literacy we can increase cognitive resilience in society. Once cognitive resilience is built within a population, then this population is much less susceptible to disinformation campaigns. Therefore, it was underlined that cognitive resilience must also be introduced and built as early as possible. This was agreed by MS Liisa Talonpoika, Ambassador for Hybrid Affairs at the Ministry for Foreign Affairs of Finland, who introduced Finnish best practices to increase media literacy and counter disinformation. This was followed by the working group discussion on the needs for standardisation in enhancing citizens' media literature skills. The main conclusion was that special attention should be paid to practical skills that should be transferred to various groups of recipients as standards. It is primarily about the ability to verify the source of information, critical analysis of information, as well as basic behaviours, e.g. not sharing unverified content, not duplicating unverified information, etc. In this context it was noted that the use of modern technologies, esp. AI requires standardization in the context of media environment.

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 2022 – October 2022) contributed to the Three Lines of Action. In addition, chapters have described how the work in the project Tasks has been conducted now when the 2nd project cycle has started to deliver results from this cycle as well, and how some results especially in the case of T4.3, still serve and continue the project work conducted during the first project cycle (M1-M17/ May 2020 – September 2021). Furthermore, the goal of the document has 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 addition, we gave a short description of the contributors to the Six Month Action Report.

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

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

4.2 FUTURE WORK

The EU-HYBNET project results to the Three Lines of Actions from the beginning and mid of the second project cycle (2nd cycle duration: M18-M34/ October 2021 – February 2023) have been now explained to the EC. However, the next Six Month Action Report (in April 2023) will describe the second cycle results and findings to the Three Lines of Actions, and how the project has been able to implement the findings even more to the benefit of pan-European practitioners to counter hybrid threats. In addition, the next report will describe the project activities in the beginning of the 3rd project cycle (March 2023 – August 2024). Definitely, best practices and lessons learned and key findings will be taken into further work in the second cycle and Three Lines of Action related work in different EU-HYBNET project work packages and Tasks. During the next project six month period, the following fourteen (14) deliverables and four (4) milestone will be delivered:

Deliverables (D):

T4.1 Mapping on the EU Procurement Landscape

- D4.2 Second Report on the Procurement Environment (KEMEA), M31

T2.4 Training and Exercises for Needs and Gaps

- D2.24 Training and Exercises Lessons Learned Report (Hybrid CoE), M31

T3.1 Definition of Target Areas for Improvements and Innovations

- D3.2 Second Interim Report Mapped on Gaps and Needs (TNO), M33

T2.4 Training and Exercises for Needs and Gaps

- D2.27 Training and exercises Scenario& Training Material (KEMEA), M34

T4.2 Strategy for Innovation Update and Industrialization

- D4.5 "2nd Innovation Uptake, Industrialization Research Strategy (RISE), M34

T5.1 Dissemination and Communication Strategy and Plan

- D5.6 Midterm Project Dissemination Impact Assessment Report2 (URJC), M34

T1.3 EU-HYBNET Community Extension

- D1.21 List of Actors to the extended EU-HYBNET Network (Hybrid CoE), M35

T2.1 Needs and Gaps Analysis for Knowledge and Performance

- D2.3 3rd Gaps and Needs Event (Hybrid CoE) M35

T1.1 Administrative and Financial Planning and Coordination

- D1.9 6th Six Month Action Report (Laurea), M36

T2.1 Needs and Gaps Analysis for Knowledge and Performance

- D2.7 Long List of Defined Gaps and Needs (Hybrid CoE) M36

T2.2 Research to Support Increase of Knowledge and Performance

- D2.14 Articles and Publications on Themes and Measures (UiT) M36

T4.3 Recommendations for Standardization

- D4.9 2nd Report for Standardization Recommendations (PPHS), M36

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

- D4.13 2nd Policy Briefs, Position Papers, Recommendations Report (Hybrid CoE), M36

T5.1 Dissemination and Communication Strategy and Plan

- D5.4 Updated DCE Plan 2 (EOS), M36

Milestones (MS):

- MS14/ Cycle III. Due by project month M35 (March 2023)

- MS27/ 2nd Policy briefs, Position Papers, or Recommendations documents are published. Due by project month M36 (April 2023)
- MS7/ 3rd EU HYBNET Project Management Board Meeting. Due by project month M36 (April 2023)

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

Furthermore, new project results to the Three Lines of Action will be reported especially because deliverables focusing on most promising innovations analysis and selection, and the strategy for their uptake will be ready. This is followed by research results on procurement landscape for new innovations and how does the standardization environment look for the innovations. The next sixth month deliverables will also describe EU-HYBNET raining results and deliver trianing materila for uptake. In addition, the third project cycle will be kicked of in Mach 2023 and as a results of this new, third selection of identified critical pan-European security practioners gaps and needs, threats to counter Hybrid Threats will be delivered. Moreover, an important part of the next Six Month Action report will be results from the forthcoming two EU-HYBNET events, namely “Future Trends Workshop” (ISW) and “Annual Workshop” (AW) during April 2023 in Bucharest. 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 “Open CTI tool” development will continue. This all is to benefit the pan-European stakeholders from the EU-HYBNET results and to enhance joint measures to counter Hybrid Threats.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threat –project, No. 883054
EC	European Commission
GA	Grant Agreement
DoA	Description of Action Part A and B
H2020	Horizon2020, EC funding Program for EU projects' funding
FP7	The EC's 7th Framework Program to EU project funding
D	Deliverable
CO	Consortium only deliverable
WP	Work Package
T	Task
M	Month
MS	Milestone
OB	Objective
KPI	Key Performance Indicator
NoP	Network of Practitioners project
R&I	Research and innovations
EU MS	European Union Member State
G&N	gaps and needs
ISO	ISO Standard is a formula that describes the best way of doing something. It could be about making a product, managing a process, delivering a service or supplying materials – standards cover a huge range of activities. Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators
IKEW	Innovation and Knowledge Exchange Event
BOS	Break Out Session
ISW	Innovation Standardization Workshop
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
Open CTI	OpenCTI is a comprehensive tool allowing users to capitalize technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of analysed information to its primary source (a report, new article, etc.) when solving the traits of disinformation
PRECINCT	Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber physical Threats and effects with focus on district or regional protection -Project
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges -Project

7Shield	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats –Project
ALIGNER	Artificial Intelligence Roadmap for Policing and Law Enforcement –Project
PersoNews	Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy –Project
EU-LISTCO	Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders –Project
CYBERCULT	Strategic Cultures of Cyber Warfare -Project
INSPIRE-5GPlus	INtelligent Security and PervasIve tRust for 5G and Beyond -Project
ISOCRYPT	Isogeny-based Toolbox for Post-quantum Cryptography -Project
PROGRESS	Protection and Resilience Of Ground-based infRastructures for European Space Systems -Project
WeVerify	In the Wider and Enhanced Verification for You -Project
IMEDMC	Information and Misinformation Economics: Design, Manipulations and Coutermeasures -Project
RUSINFORM	The Consequences of the Internet for Russia's Informational Influence Abroad –Project
Open Your Eyes	Open Your Eyes: Fake News for Dummies –Project
COMPROP	Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe -Project
CONCORDIA	Cyber Security Competence for Research and Innovation -Project
ECSCI	European Cluster for Securing Critical Infrastructures
DDS-aplha	DDS-alpha is the Disinformation Data Space
STIX	STIX standard: Standard Threat Information Expression
CI	Critical Infrastructure
CISAE	Common Information Sharing and Analysis Environment. Similar innovation as CISE while focusing to other domain than maritime CISE.
CISE	
EMSA	European Maritime Security Agence
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
RAS	Rapid Alert System in EEAS
EDMO	European Digital Media Observatory
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria

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

.

ANNEX II. REFERENCES

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

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

ANNEX III. THE 2ND TRAINING AND EXERCISES EVENT

EU-HYBNET 2nd Training and Exercise Event

29-30 September, 2022, Vilnius Didlaukio g. 55, Lithuania

Agenda

Day 1, September 29 (Thursday)

Link for on-line participants in MS Teams platform: Click here to join the meeting
Meeting ID: 355 594 774 007
Passcode: PfkpnD

Time	Item	Room
12:00-12:10	Welcome and Introduction	102
12:10-12:30	Description of the training flow	
12:30-12:50	Introduction to Scenario	
12:50-13:00	Q & A	
13:00-13:15	**Break**	
	Breakout rooms: 1. "Future trends of Hybrid Threats" 2. "Cyber & Future Technologies" 3. "Information and Strategic Communication" 4. "Resilient Civilians, Local Level National Administration"	 104 102 101 407
13:15-14:30	Breakout rooms: • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
14:30-15:00	**Break**	
15:00-15:30	Presentation of results of Core Themes	
15:30-17:00	Live innovation presentations: • LT Armed Forces StratCom (innovative tools and methodology application) • HENSOLDT (open-source intelligence) • MALTEGO (solution) • European External Action Service (EEAS) (tool for strategic communication)	102
17:00-17:15	Closing remarks	102

.

Day 2, September 30 (Friday)

Link for on-line participants in MS Teams platform: Click here to join the meeting
Meeting ID: 355 361 106 128
Passcode: jtvEi9

Time	Item	Room
10:00-10:15	Welcome and Introduction	102
	Breakout rooms: 1. "Future trends of Hybrid Threats" 2. "Cyber & Future Technologies" 3. "Information and Strategic Communication" 4. "Resilient Civilians, Local Level National Administration"	 104 102 101 407
10:15-12:15	Breakout rooms: • Introduction to innovations • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
12:15-13:00	**Break**	
13:00-14:00	Breakout rooms: • Introduction to innovations • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
14:00-14:15	**Break**	
14:15-14:45	Presentation of results of Core Themes	102
14:45-15:00	Closing remarks	

ANNEX IV. THE 2ND INNOVATION AND KNOWLEDGE EXCHANGE EVENT (IKEW)

EU-HYBNET

EU-HYBNET 2nd Innovation and Knowledge Exchange Workshop, Hybrid #IKEW

14 JUNE

In the Hague and online

09.00-17.00 CEST

The purpose of IKEW is to provide practitioners, industry, SMEs, and academia an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to answer them.

The EU-HYBNET consortium will hold its 2nd Innovation Knowledge Exchange Workshop (#IKEW) in hybrid format on 14 June 2022 in the Hague and online!

The IKEW will maintain adherence to the project's four core themes, which are:

- Future trends of Hybrid Threats
- Cyber and future technologies
- Resilient civilians, local level, and administration
- Information and strategic communications

It will facilitate the continuous mapping of needs, monitoring of solutions, and providing a forum where practitioners can engage with innovation providers. It will ensure the exchange of knowledge and information about innovations to increase the likelihood of future uptake.

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

When? 14th of June 2022 at 09.00-17.00 CEST

Where? The Babylon Hotel Den Haag, the Hague, Netherlands

More information: Event organizer at TNO: Ms Angela Kwaijtaal at angela.kwaijtaal@tno.nl and Ms Kimberley Kruijver at kimberley.kruijver@tno.nl.

.

Agenda

The 2nd IKEW will start with a plenary session held live in the Hague and live-streamed to participants attending digitally.

Two tracks of workshops will be organised in two rounds: live in the Hague or online for participants attending remotely. In each round, participants can express their preference between two live or online sessions.

The day will end in the plenary with pitches from the workshops and a closing keynote speech.

Time CEST	Topic	Speakers	
Welcome and registration			
Plenary session (live in the Hague and online) *Room: Lange Voorhout*			
9:00-9:15	Opening	Moderator: Michel Rademaker (HCSS)	
09:15-09:45	Keynote on Dutch developments in hybrid threats	Keynote speaker: Hester Somsen (Dutch National Coordinator for Security and Counterterrorism)	
09:45-10:15	Keynote speech on 'Connecting the Dots to Counter Hybrid Threats – the Role of Dutch Defence'	EU-HYBNET Speaker: Geert Kuiper (Dutch Ministry of Defence)	
10:15-10:45	Results of Innovation Assessment 1st EU-HYBNET Cycle	EU-HYBNET speaker: Okke Lucassen (TNO)	
10:45-11:00	*Coffee break*		
Break-out sessions LIVE in The Hague *In each round, in-person participants will be split in two parallel working groups.*			
	***Room:** Vijverberg*		***Room:** Noord-einde*
11:00-12:30	***BOS 1: Dilemma gaming*** Innovation: Hybrid online dilemma game	Anja van der Hulst (TNO) & Willem Verdaasdonk (TNO)	***BOS 2: Cyber and future technologies – how to advance?*** Innovation: A Quantum-Resistant Trusted Platform Module Establish Data Embassies or E-embassies	Evaldas Bruze (L3CE), Rimantas Zylius (L3CE)
12:30-13:30	*Lunch break*		

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

.

EU-HYBNET

	Room: Vijverberg		Room: Noord-einde	
13:30-15:00	***BOS 3: Who do you trust?*** Innovation: Journalism trust initiative Government & social media cooperation framework to counter election interference	Gunhild Hoogensen Gjørv (The Arctic University of Norway	***BOS 4: Identifying and countering information manipulations: professional tools and networks of fact-checkers and OSINT practitioners*** Innovation: Automated detection of hate speech in social media	Rubén Arcos (URJC) and Manuel Gértrudix (URJC) In cooperation with Daniel Fritz (EEAS)
Break-out sessions ONLINE *In each round, online participants will be split in two parallel working groups.*				
11:00-12:30	***BOS1: Hybrid threats impact on critical infrastructure disruption: existing measures and solutions needs*** Topic: Output from Gaps & needs 2nd cycle= Critical infrastructure	Monica Cardarilli (JRC)	***BOS 2: Emerging technologies: from reactive to proactive use of innovations to counter hybrid threats*** Topic: Output from Gaps & needs 2nd cycle = disruptive technologies; what to pay attention to?	Maxime Lebrun (HCoE)
12:30-13:30	*Lunch break*			
13:30-15:00	***BOS 3: Crazy ideas gaming session*** Topic: Open brainstorm in the format of an online gaming session based on hybrid threats scenario's	Rick Meessen (TNO) & Jesper van Putten (TNO)	***BOS 4: Political cleavages and hybrid threats: exploiting the new drivers*** Topic: Output from Gaps & needs 2nd cycle = Political cleavages – foreign interference	Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)
15:00-15:30	*Coffee break*			
Plenary session (live in the Hague and online) ***Room**: Lange Voorhout*				
15:30-16:15	Keynote speech on 'Disinformation; The BadNews and resilience'		Key note speaker: Gwenda Nielen (TILT)	
16:15-16:45	Pitch outcomes workshops		Organisers & Moderator	
16:45-17:00	Summary of the day & closing remarks		Moderator: Michel Rademaker (HCSS)	

.

ANNEX V. THE 1ST INNOVATION STANDARDIZATION WORKSHOP (ISW)

.

EU-HYBNET
Innovation and Standardization Workshop
#ISW

15 JUNE

In the Hague and online

09.00-16.15 CEST

The purpose of ISW is to develop recommendations for activities regarding the development and implementation of most promising EU-HYBNET's identified four innovations to counter hybrid threats.

The EU-HYBNET consortium will hold its 1st Innovation Standardization Workshop (ISW) which will take place on 15 June 2022 in the Hague, the Netherlands!

The Innovation Standardization Workshop (ISW) focuses on EU-HYBNET's identified most promising technological and non-technological innovative solutions and tools to counter Hybrid Threats and their standardization landscape in two fields:

- Countering disinformation and fake news, increasing the level of media literacy and social resilience.
- Critical infrastructure protection and information sharing.

In the context of Hybrid Threats and focus areas of the ISW, participants will be split in two working groups aiming to formulate recommendations concerning standardization and present standards.

Who? The workshop is invitation based and open to project partners and network members. If interested in joining or wish to recommend an expert in the ISW area to join, please contact the organisers.

When? 15th of June 2022 at 09.00-16.15 CEST

Where? The Babylon Hotel Den Haag, Bezuidenhoutseweg 53, 2594 AC, the Hague, Netherlands

Links for accepted online participants will be provided few days before the event.

More information: Event organizer at PPHS: Bartłomiej Ostrowski bartlomiej.ostrowski@ppbw.pl.

.

Workshop format

The 1st ISW will start with keynote speeches held live in the Hague and live-streamed to participants attending digitally.

Two parallel working groups will be organised live in the Hague and livestreamed for online participants:

- WG1. on "Standardization measures in the context of critical infrastructure protection and innovations to enhance information sharing" will focus on standardization experts and pan-European security practitioners' views on present standards, needs and possibilities for standardization in the future noticing the challenges deriving form hybrid threats.

- WG2. on "Innovations in disinformation and media literacy" is dedicated on standardization best practices and innovative solutions answering security practitioners' needs to counter information manipulation and interference, disinformation and media literacy.

The working groups will begin with keynote speeches and presentations and will also include hosted discussion between the speakers and other workshop participants, as well as comments from on-line participants.

"In the context of Hybrid Threats and focus areas of the ISW, the WGs aim to formulate recommendations concerning standardization and present standards. Their goal is also to support EU-HYBNET's most promising proposed innovations uptake for pan-European security practitioners to counter Hybrid Threats.

.

Agenda

08:00 –09:00	**Registration**
Plenary session ***Room:*** *Lange Voorhout*	
09:00 – 09:15	**Opening of the workshop** **Dr. Päivi Mattila,** Director of Security Research Program & EU-HYBNET Project Coordinator, Laurea University of Applied Sciences, Finland **Mr. Rashel Talukder,** Managing Director of the Polish Platform for Homeland Security, Poland
09:15 – 09:30	**Keynote speech: Countering Russian disinformation during the war against Ukraine** **MS Maria Avdeeva,** Research Director at the European Expert Association, Kharkiv – Ukraine
09:30 – 09:45	**Keynote speech "Standardization Landscape and Critical Infrastructure Protection"** **Prof. Dr. Aleksandar Jovanović,** Chief Executive Officer Steinbeis European Risk & Resilience Institute
09:45 – 10:00	***Questions & Answers session*** **Moderator: Mr. Isto Mattila,** EU-HYBNET Innovation Manager, Laurea University of Applied Sciences, Finland
10:00 – 10:30	**Coffee break**

10:30 – 12:30	**Parallel Working Group Sessions** - **Keynote Speeches and Introduction to the Standardization Measure and Needs**	
	Standardization in the scope of Hybrid Threats and Critical Infrastructure Protection **Room:** *Lange Noord-Einde*	**Innovations in disinformation and media literacy** **Room:** *Lange Voorhout*
	Focus: Standardization in the context of Hybrid Threats and Critical Infrastructure Protection and innovations to enhance information sharing **Moderator:** *Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea University of Applied Sciences*	**Focus: Debunking of fake news, Training application for media literacy, Guides to identify fakes news.** ***Moderator:*** *Mr. Bartek Ostrowski, Senior Project Officer, Polish Platform for Homeland Security*

.

	10:30-10:50 Hybrid Threats and Critical Infrastructure - EU policy framework and JRC support • Dr. Monica Cardarilli, Project Officer, Joint Research Centre **10:50-11:10 EU-HYBNET's Identified CI Innovation for Uptake** • Dr. Rolf Blom, Senior Expert, Research Institutes of Sweden • Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea **11:10-11:30 Present standards, needs and possibilities for standardization in the future noticing the challenges deriving form hybrid threats** • Prof. Dr., Chief Executive Officer Aleksandar Jovanović, EU-Vri - Steinbeis European Risk & Resilience Institute **11:30-12:30 Panel discussion focusing on previous presentations and focus of the WG** • Dr. Evita Agrafioti, R&D Project Manager at Gap Analysis SA and External Expert at ERNCIP • Mr. George Karagiannis, Deputy Secretary General for Civil Protection in Greece, PhD CEM • Dr. Aikaterini Poustourli, Standardisation Expert, Member of EURAS	**10:30-10:50 Anti-disinformation campaigns as the element of building social resilience - case study** • LTC Tomasz Gergelewicz, Academic Centre for Strategic Communication, Poland **10:50-11:10 [Title TBD]** • Mr. Daniel Fritz, European External Action Service (EEAS) **11:10-11:30 [Title TBD]** • Ms. Emma Goodman, European Digital Media Observatory **11:30-11:50 Artificial Intelligence's impact on disinformation: generating and combating deepfakes** • Prof. Aleksandra Przegalinska - Associate Professor and Vice-President of Kozminski University **11:50-12:10 Use of media literacy to increase cognitive resilience, based on the results of the research in Estonia, Lithuania, Latvia, Georgia, Moldova and Ukraine in 2021-2022** • Dr. Solvita Denisa-Liepniece, Baltic Centre for Media Excellence, Latvia **12:10-12:30 Countering disinformation and the Finnish best practices of increasing media literacy** • Ms. Liisa Talonpoika, Ambassador for Hybrid Affairs at the Ministry for Foreign Affairs of Finland
12:30 – 13:30	**Lunch break**	

13:30 – 15:30	**Parallel Working Group Sessions** **Keynote Speeches and Introduction to the Standardization Measure and Needs**	
	Standardization in the scope of Hybrid Threats and Critical Infrastructure Protection **Room:** *Lange Noord-Einde*	**Innovations in disinformation and media literacy** **Room:** *Lange Voorhout*

.

	Moderator: *Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea University of Applied Sciences* **13:30-14:00 Insights from EU-HYBNET Critical Infrastructure and security practitioners to standardization** • General Engineer Yves Rougier, French Ministry for an Ecological and Solidarity Transition • Prof. Stefan Pickl, Bundeswher Universität • Universita Cattolica del Sacro Cuore (TBC) **14:00-14:45 Standardization Framework and Best Practices in the Innovation Uptake Enhancing Information Sharing between CI Entities pan-European Wide. Organizations and experts and projects in the field** • "Protection of Critical Infrastructures from Advanced Combined Cyber and Physical Threats" (PRAETORIAN) project • Dr. Gabriele Giunta (Engineering), Project Coordinator for "Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats" (7SHIELD) **14:45-15:30 Concluding discussion with Session Participants – "Way forward"**	**Moderator:** *Mr. Bartek Ostrowski, Senior Project Officer, Polish Platform for Homeland Security* **13:30-14:45 Discussion:** *Standards for the uptake of innovative products, services and solutions. Cooperation of institutions from various sectors on countering disinformation and fake news. Instruments to support raising the level of media literacy, with a special focus on senior, youth and socially disadvantaged groups of the society.* **14:45-15:30 Concluding discussion with Session Participants – "Way forward"**
Plenary session ***Room:*** *Lange Voorhout*		
15:30 – 16:00	**Summary of the two parallel sessions** Working Group Moderators	
16:00–16:15	**Closing Remarks** **Dr. Päivi Mattila,** Director of Security Research Program & EU-HYBNET Project Coordinator, Laurea University of Applied Sciences, Finland **Mr. Rashel Talukder,** Managing Director of the Polish Platform for Homeland Security, Poland	

.