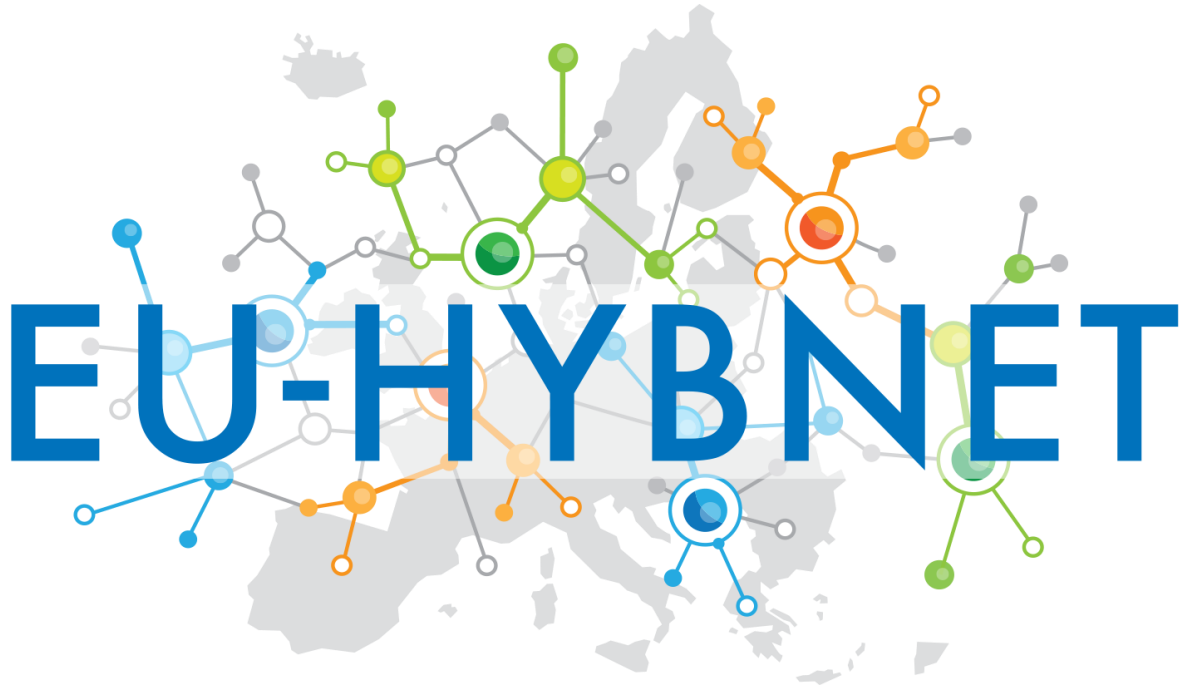


EIGHT SIX MONTH ACTION REPORT

DELIVERABLE 1.12

Lead Author: Laurea

Contributors: All partners
Deliverable classification: Public (PU)

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

D1.12 EIGHT SIX MONTH ACTION REPORT

Deliverable number:	**1.12**	
Version:	**1.0**	
Delivery date:	**28/8/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status:	**Ready**	
Nature:	**Report**	
Main authors:	Päivi Mattila, Tiina Haapanen	**Laurea**
Contributors:	Stefan Pickl	**COMTESSA**
	Input to the report from all consortium partners due to their project work in various Tasks and events as contributors	**MTES, URJC, Hybrid CoE, PPHS, KEMEA, TNO, Satways, UCSC, JRC, MVNIA, Hybrid CoE, MoD NL, ICDS, PLV, ABW, DSB, RIA, RISE, UCSC, Maldita, Espoo, ZITiS, L3CE, UiT**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	6/5/2024	Päivi Mattila/ Laurea	1st draft of text
0.2	14/5/2024	Päivi Mattila/ Laurea	Text editing
0.3	1/6/2024	Päivi Mattila/ Laurea	Text editing
0.4	15/6/2024	Päivi Mattila/ Laurea	Text editing
0.5	1/7/2024	Päivi Mattila/ Laurea	Text editing
0.6	6/8/2024	Päivi Mattila/ Laurea	Text editing
0.7	13/8/2024	Päivi Mattila/ Laurea	Text editing
0.8	16/8/2024	Päivi Mattila/ Laurea	Text editing
0.9	19/8/2024	Päivi Mattila/ Laurea	Text editing
0.91	20/8/2024	Päivi Mattila/ Laurea	Text Editing and document for review
0.92	27/8/2024	Stefan Pickl/ COMTESSA	Review
1.0	28/8/2024	Päivi Mattila/ Laurea	final review and document submitted to the EC

DISCLAIMER

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

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

TABLE OF CONTENT

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The goal of the *Empowering a Pan-European Network to Counter Hybrid Threats* (EU-HYBNET) project deliverable (D) 1.12 "*Eighth Six Month Action Report*" in project month (M) 48/April 2024 is to describe how the project has proceeded from M42 until end of M48 of the project (October 2023 – April 2024) 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, D1.12 also highlights what actions and results are expected from EU-HYBNET during the next six-month period (May 2024 - October 2024).

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1. Provides an overview to the document content.
- Section 2. Describes the importance of deliverable D1.12 to the whole project and its proceeding will be explained.
- Section 3. Describes how the project activities from the project months 42 - 48 (October 2023 – April 2024) have contributed to the EC's requested "three lines of action" activities.
- Section 4. Conclusion and next steps for the upcoming six-month period of the project (May 2024 - October 2024).

2. SIX MONTH ACTION REPORT AND IMPACT TO THE PROJECT

2.1 CONTRIBUTION TO THE PROJECT

The EU-HYBNET deliverable (D)1.12 "*Eighth 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 D1.12, have no specific project objective or key performance indicator(s) (KPI) to answer. However, the importance of D1.12 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.

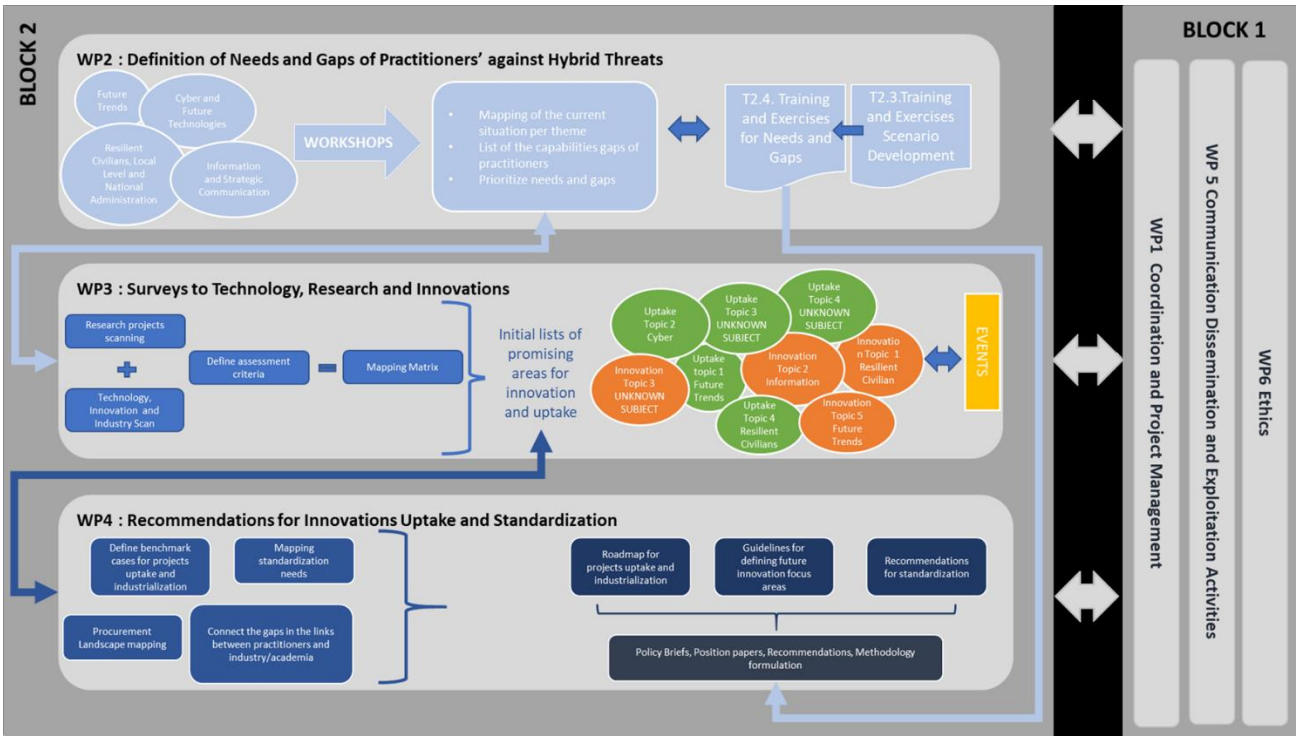


Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

In addition, the project results and findings described in EU-HYBNET Six Moth Action Reports are often linked to the project milestones (MS) achieved during the last six-month period. During D1.12 reporting period project Milestone(s) set to the project were following and they were well reached. Milestones are:

MS number.	MS action description

18	3rd cycle of mapping gaps and needs on the innovations and research completed and shortlist of solutions handed over to WP4
37	4th Annual workshop is organised
8	4th yearly EU HYBNET Project Management Board meeting where new extended EU HYBNET actors will be accepted

.

2.2 SIX MONTH ACTION REPORT CONTRIBUTORS

The seventh Six-Month Action Report (D1.12) main author is Laurea, the organization responsible for the delivery of D1.12. However, EU-HYBNET work package (WP) and task (T) leaders have also provided information on the tasks they are responsible for and have been working on during the sixth six-month period of the EU-HYBNET project. In addition, the EU-HYBNET Project Manager and Innovation Manager and Network Manager have contributed to D1.12 by providing general remarks on the project's general progress and innovation uptake.

3. THREE LINES OF ACTION REPORTING

This chapter describes EU-HYBNET's activities, especially in Work Packages (WPs) and Tasks (T) relevant to the Three Lines of Action during the project past six months, namely period May - October 2023. According to the EC's request, EU-HYBNET should report according to the following Three Lines of Action:

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

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

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

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

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

The starting point for the first "Three Lines of Action" reporting is coming from the EU-HYBNET WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ Task (T)2.3 "*Training and Exercises Scenario Development*" (lead by KEMEA) and T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE) who provided material and arranged the 3rd and final EU-HYBNET training event for pan-European security practitioners and other relevant actors (academia, industry, SMEs, NGOs). The work conducted in T2.3 delivered training scenario and methodology and suggestions on innovative solutions (technological and non-technological) to be tested according to EU-HYBNET's T3.2 "*Technology and Innovations Watch*" (lead by Satways) and T3.3 "*Ongoing Research Projects Initiatives Watch*" (lead by L3CE) promising innovation mapping in T2.4 training event. Especially in T3.3 focus was also in project's that had promising innovations to be tested in the T2.4 Training event and hence more about the most promising research and innovation projects whose solutions EU-HYBNET recommends to the uptake or industrialization in the subchapter below.

In addition, during the reporting period EU-HYBNET T3.4 "*Innovation and Knowledge Exchange Events*" (lead by EOS) delivered insights to the First Three Lines of Action in the 3rd Innovation and Knowledge Exchange Workshop (IKEW) arranged by EOS and Valencia Local Police (PLV) in Valencia during 7th of November 2023. Comprehensive description on IKEW is delivered in D.3.13 "3rd *Innovation and Knowledge Exchange Workshop*" (by EOS, M44/Dec 2023). The chapters below summarizes key findings of IKEW from D3.13 what comes to First Three Lines of Action "**Monitoring of research and innovation projects with a view to recommending the uptake or the industrialization of results**". The reporting highlights especially EC funded projects that seem to deliver solutions important to uptake and industrialization in order to empower pan-European actors' measures to counter hybrid threats.

Lastly, also in WP5 "*Communication, Dissemination and Exploitation Activities*"/ T5.3 "*Project Annual Workshops for Stakeholders*" (Lead by Laurea) important innovation mapping relevant to the first Three Lines of Action reporting has been conducted. In T5.3 EU-HYBNET 4th Annual Workshop (AW) was arranged on 24th of April 2024 in Valencia where sound projects to identified pan-European security practitioners' gaps and needs were provided pitching opportunities. More on the selected projects in the AW in the next Six Month Action report because the deliverable of the 4th AW has been delivered after this Six Month reporting period.

3.1.1 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 well contributed 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 final, 3rd EU-HYBNET Training event (hybrid format on the 18th -19th of Jan 2024 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/D3.9 "*Second mid-term report Innovation and monitoring*" and T3.2/ D3.5 "*Second mid-term report Improvement and innovations*" which were seen relevant as counter measures. The training scenario and injects are described in detail in D2.19 "Training and Exercise, Scenario delivery" M44 (Dec 2023).

T2.3 selected the innovations for each training scenario 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 1. *Wide spread of online harassment and acts of violence in LATARUM against POLDONIAN ethnic groups related to STEPLAND escalates to riots. Police and rescue agencies are trying to control and use their resources more efficiently while managing the situation.*

- focusing on Core Theme's Threat No 1.1 "Political Deficiency"

Proposed project innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested

3.9	**SMIDGE** **https://www.smidgeproject.eu/**	**Horizon funded SMIDGE/ "*Social Media Narratives Addressing Extremism in Middle Age*" project.** Online extremism can result being extremely destabilizing, even if a short amount of activists are propelled into action. Attempts to overthrow democratic government regularly occur from reduced and clandestine cells praising extremist ideologies. The solution proposes to provide a dual effect. The first one concerns the promotion of a sane information through counter-narrative and reliable resources for professionals dealing with information. The second one deals with policy- and decision-makers through guidelines and recommendation.

Vignette 2. *The President of LATARUM has allegedly declare in videos that a referendum will be called regarding the self determination and autonomy of Poldovian residents in the North area of the country. These videos are considered fake.*

- focusing on Core Theme's Threat No 1.3 "Substitutive Reality"

Proposed project innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**We Verify, a video plugin to debunk fake videos on social media that spread conspiracy theories https://weverify.eu/#**	**Horizon funded We Verify/ "Wider and Enhanced Verification for You" project.** Debunking became an imperative necessity in all democracy as spiral of violence could be easily triggered from disinformation. Dividing society, groups against group is a way to undermine the unity of a country, and social media contribute even more to the polarisation, isolation and antagonisation of social groups. General conspiracy theories and fake news spread more easily than the solutions to counter them. It seems therefore compulsory to spread debunking solutions that are able to tackle the phenomenon. Easily usable through plug-in and applicable to social networks, this solution aims at preventing viral fake videos to intoxicate the citizens by reaching metadata, copyright, transformations to analyse the authenticity of the video. As videos are easily shared, this tool can participate to contain the phenomenon.
3.9	**DesinfoEND** **https://desinfoend.eu/**	**Horizon funded DesinfoEND/ "Developing Critical Thinking to Counteract Disinformation across Europe" project.** As people can be vortexed into a spiral of online disinformation, it is necessary to both prevent such actions and protect from its negative effects. Cutting short the conspiracies disinformation permits to protect the informational scene and favour a safe access to reliable news to the population. The tool proposed here aims to focus on vulnerable groups, promoting critical

		thinking against antagonizing disinformation. Immediate critical thinking is also accompany through this solution with a more long-term education to responsible behaviour regarding information and online communication.

Core Theme "Cyber and future Technologies"

Vignette 3. *Hospitals and emergency services are targeted, physical attacks with IED on their premises affect their ability to provide rapid and efficient assistance in the event of an emergency in BAKVERIA.*

- focusing on Core Theme's Threat No 2.3 "Attack on Services" and Threat No. 2.1 "Stealing Data, Attacking individuals"

Proposed project innovation to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.9	**ENGAGE** https://www.project-engage.eu/	**Horizon funded ENGAGE/ "Engage Society for Risk Awareness and Resilience" project.** Civil society has an important role to play in the societal preparedness against natural and man-made disasters. This innovative project aims are to find ways how individuals and local practices could interrelate with planned preparedness and response, practitioners, and technology. The project focuses on aspects that can be directly enhanced such as risk awareness, communication, social media, citizens' as well as authorities' and first responders' involvement. Solutions will aim at bridging the gap between formal and informal approaches to risk and emergency management, increasing the ability of communities to adapt before, during and after disaster. In this project, the prototyped solutions are validated via 3 social emergency simulations that threaten the security of EU societies. The outcomes of this project can be used to enhance and strengthen the collaborative efforts between citizens, first aid responders and emergency workers during a period of a crisis. Strengthened collaboration would at best increase the risk awareness and societal resilience.

Vignette 8. *No specific regulatory framework exists in FREEWICK regarding Disinformation by major online platforms. Social media giants present a manipulative danger combined with the media ownership status, at the same time the situation remains hardly reachable from regulatory perspective.*

- focusing on Core Theme's Threat No 2.2 "On-line Manipulation/ Attacking democrazy"

Proposed project innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Starlight Disinformation-Misinformation Toolset** https://www.starlight-h2020.eu/	**Horizon funded STARLIGHT/ "Sustainable Autonomy and Resilience for LEAs using AI against High Priority Risks" project** STARLIGHT project is one of the flagship projects dedicated to deliver easy deployable toolset to address various need of LEA and other security practitioners driven by constantly changing tech driven crimes modus operandi. In particular, STARLIGHT has one direction dedicated for disinformation and misinformation related threats. This direction is composed of several organisations developing different tooling enabling deep access of information in social platforms and tools to detect different misleading aspects of the information. There are tools dedicated to access information on general internet, communication platforms such as Telegram or X (Twitter) platforms, but majority are focused on detection of fault or forbidden content. Majority of them can work on different languages. All of Starlight tools listed are planned to be integrated in one interface, making them easier to use. At this point of time Starlight project is developing solutions for LEA, but it can be developed further for different target groups and serves as a good example of what is needed to handle artificial amplification complexity. In the context of the vignette Starlight could provide support for LEAs to discover manipulation in information and also have material to prove the manipulation. This could ease the citizens to gain trusted informaiton from LEAs that the citizens are under influencing. Furthermore, this could support the regime to develop new legistlation that will ask media giants to check

		the possible false information and to prevent spreading the information.
3.9	**INCLUDING** https://cordis.europa.eu/project/id/833573	**Horizon funded INCLUDING/ "Innovative Cluster for Radiological and Nuclear Emergencies" project.** The EU-funded INCLUDING project will build a dynamic cluster of 15 partners from 10 EU Member States acting in the INCLUDING Federation. An advanced web platform will shape a map of cooperation between governmental, security and medical institutions, industrial services and others. Partners will provide multidisciplinary knowledge, research, new technologies and infrastructure. Procedures will be formed for joint actions: field exercises, training and simulations. The project will be a base for a modern flexible network for better security in the RN field in Europe. In the context of the vignette, INCLUDING could be an example how information sharing from authorities side will remain crucial in society even though Media Outlets would be bought by malicious actors.

Core Theme "Resilient Civilians, Local Level, National Administration"

Vignette 4. *Telecoms operators in Silveritanian Hospitals are facing a chaos. During the Mega fire crisis the number of emergency calls has proven to be exponential, from 1 per minute to over 100 per minute, becoming impossible to sort out by emergency dispatchers, especially with the average emergency call lasting from 3 to 15 minutes dealt by just a few emergency dispatchers. Creating a massive telephonic congestion, the population is no longer capable to reach by phone the emergency services, report their positions and the evolution of their situation. This lack of communication increases the workload of Search & Rescue, which in the aftermath have to go place by place instead of focusing on population's reported positions.*

- focusing on Core Theme's Threat No 3.2. "Attack on Social Structures"

Proposed project innovation to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.9	**The Countering Foreign Interference (CFI) project** https://www.iss.europa.eu/content/euiss-launches-eu-funded-project-countering-foreign-interference	The FCI project is funded by the **Service for Foreign Policy Instruments (FPI)** at the European Commission. The project focuses on improving understanding of potential threats in

		the information space. It will utilize accumulating knowledge for developing improved tools and methods to identify, monitor and counter those threats. Often adversaries aim to amplify the present crises by increasing disinformation in the information flow. Therefore, in a case of crises, it is important for the authorities that their guidance and information can be well reached so that the crises will not escalate further on the basis of false information. Therefore, it is important for the authorities to have the improved tools and methods to identify, monitor and counter disinformation in early phase.

Vignette 5. *The internal integrity of the Silveritanian Hospitals is under attack by hostile messaging, and disinformation, via Viber and Telegram messaging to the staff, that the higher management is unreliable and incompetent to handle the situation. Not only the employees of the Hospitals but also outside stake holders are targets of hostile messaging and this put additional pressure to the organization and creates serious problems for the organization that causes its integral structure disintegrating.*

- focusing on Core Theme's Threat No 3.3. "Undermining institutions' internal organization"

Proposed project innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.9	**EUCISE2020** https://cordis.europa.eu/project/id/608385	**Horizon funded EUCISE2020/ "European test bed for the maritime Common Information Sharing Environment in the 2020 perspective" project.** It is expected that information sharing platforms for strategic security institutions would provide not only needed tools for information sharing inside the organization but also between the institutions. The platforms are also to increase cooperation between actors and to increase traceability and trust alike motivation for the cooperation due to enhanced results. The gained trust in cooperation builds resilience to adversaries possible attempts to harm the trust and to paralyze joint proceeding in critical cases and in crises. A successful project to increase cooperation in information sharing and cooperation has been

		EUCISE2020 project in European maritime domain. The project has lead to development of Common Information Sharing Environment (CISE) to pan-European and national maritime authorities. On the whole, CISE is not only to support various pan-European security authorities to increase their cooperation, but it also empowers the cooperation in national level due to the development of national nodes. In short, without the cooperation between the national security institutions and authorities in the specific security domain (e.g. in maritime domain/ border guards, navy, police, customs) development of the solution/CISE national node would not have been possible. In short, the pan-European CISE has pushed national security authorities and institutions to find and definite new ways of cooperation and information sharing reducing partly also the culture of secrecy between institutions and inside the institutions. An example of increased cooperation between national *strategic security institutions* is a FINCISE project from Finland **FINCISE 2.0 Project** CISE | The Finnish Border Guard (raja.fi) (Duration: 2022 -2024) where all Finnish Maritime Cooperation (FIMAC) authorities joined to CISE development and finding new ways for future cooperation. On the whole, the takeaway from the above mentioned CISE projects' is that the approach seems to work in various security domains and hence also hybrid threats related security authorities could consider to develop CISE for their purposes. Furthermore, CISE seems to support cooperation between strategic security institutions and diminish culture of secrecy between institutions, also in the institution.
3.9	**STOP-IT** https://cordis.europa.eu/project/id/740610	**Horizon funded STOP-IT/ "Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats" project.** Also solutions that have trained actors in organizations, or between organizations, to work together during crises (e.g. during malicious influencing campaigns to cooperation) are much needed in order to ensure critical institutions solid work flow. With reference to this, STOP-IT project has developed a solution that ensures training for organization to face future severe cases in a manner that trust and knowledge how to proceed without severe challenges will be maintained.

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

Core Theme Information and Strategic Communication

Vignette 6. *The impact of increasing levels of visual misinformation by STEPLAND regarding the illegal actions of its Airforce and Navy changes the social and political climate. It undermines democratic processes, distorts the public and fuels social unrest. False or manipulated images can incite violence, trigger outrage and provoke conflict by exploiting people's emotions. The spread of visual misinformation also poses challenges for media companies and technology platforms responsible for moderating content.*

- focusing on Core Theme's Threat No 4.3. "Attack on information" and Threat No 4.2 "Antagonizing victimization narratives in the informational space"

Vignette 7. *News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual. Evidently questions are raised on the objectivity of these media and the control exercised over them.*

- focusing on Core Theme's Threat No 4.3. "Attack on information"

Proposed project innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.9	**ReMeD** https://resilientmedia.eu/	**Horizon funded REMED/ "Resilient Media for Democracy in the Digital Age (ReMeD)" project.** It tackles existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. ReMeD could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, in the same way project MeDeMAP can. By gathering, analysing, comparing and contrasting data regarding professional journalists, alternative media content producers and citizens which operate in technologically mediated configurations, as well as

		the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape, ReMeD could, as a biproduct identify trends and qualitative indicators which could help better understand the demand of and thus the sustainability of quality journalistic media.

Vignette 7. *News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual. Evidently questions are raised on the objectivity of these media and the control exercised over them.*

- focusing on Core Theme's Threat No 4.1. "Media Conundrum"

Proposed project innovation to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
D3.9	**INJECT** https://cordis.europa.eu/project/id/732278	**Horizon funded INJECT/ "Innovative Journalism: Enhanced Creativity Tools" project.** INJECT's objective was to transfer new digital technologies to news organisations to improve the creativity and the productivity of journalists, to increase the competitiveness of European news and media organisations. To achieve this objective, INJECT extended and aggregated new digital services and tools already developed by consortium members to support journalist creativity and efficiency, and integrated the services and tools with current CMSs and journalist work tools in order to facilitate their uptake and use in newsrooms. The services undertook new forms of automated creative search on behalf of journalists, using public sources (e.g. social media) and private digital resources (e.g. digital libraries of political cartoons) to generate sources of inspiration for journalists who were seeking new angles on stories. The tools provide new interactive support for journalists to think creatively about new stories and reuse news content in new ways to increase productivity. To transfer the new services and tools to Europe's news and

		media organisations, INJECT established a new INJECT spin-off business, built up and expanded multiple vibrant ecosystems of providers and users of new digital technologies, and exploited its position at the heart of Europe's journalism industry to raise market awareness and take-up on the services and tools. With respect to Call ICT21, INJECT increased the competitiveness of one of Europe's most important creative industries – journalism - by stimulating ICT innovation in SMEs, by effectively building up and expanding vibrant EU technological ecosystems that met the emerging needs of Europe's new and existing news and media organisations. In the context of the vignette, INJECT could deliver new ideas on ways how small scale media outlets may compete against giant Media outlets and have their news feed also heard by the citizens.

3.1.2 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 byL3CE) 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 final, 3rd EU-HYBNET training event (hybrid format on the 18th -19th of Jan 2024 in Vilnus) many research and innovation projects with their key innovations as recommend in T2.3 training scenario were tested. The EU-HYBNET T2.4/ D2.22 "*Training and exercises delivery on up-to-date topics*" describes the training event with details while central results from D2.22 on 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 below.

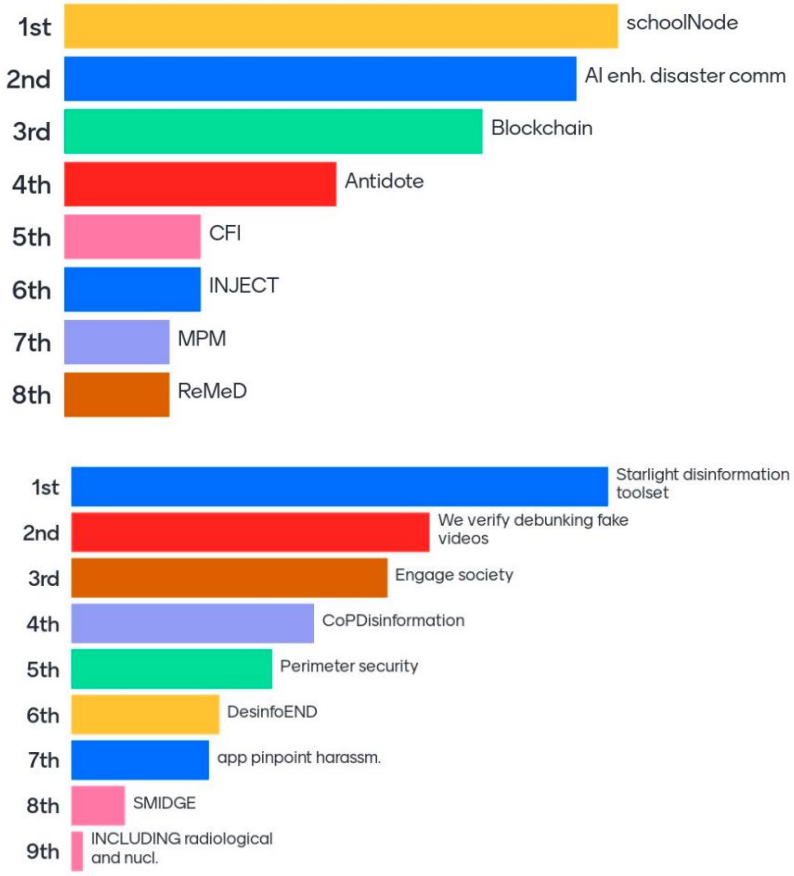
During the 3rd EU-HYBNET Training the innovation testing took place in two groups. They groups were (1) *Future Trends of Hybrid Threats with Cyber with Future Technologies* as more technological oriented and (2) *Resilient Civilians: Local Level and National Administration with Information and Strategic Communication* as more social oriented.

First both of the groups discussed the training scenario and attributed Vignettes and then, after this so-called "situation assessment", relevant innovations were introduced to groups' participants. List of innovations varied according to Scenario Vignette but still in each group participants were asked to discuss all innovations presented and then eventually select the most relevant (1 or 2) for the given situation. Then according to the selected innovations, there was hosted discussion how the groups' selected innovations could improve response to different challenges described in Scenario and Vignettes to hybrid threats. In the end of the training event, innovations were prioritized and ranked according to participants' reflections on the innovations' usability and soundness. Innovations prioritized and ranked at highest included project's such as: STARLIGHT, WeVerify and ENGAGE. The most promising innovations according to the groups' ranking were following:

- *GROUP 1. "Future Trends and Cyber and Future Technologies*" innovations focus:
  - **STARLIGHT project/** Disinformation-Misinformation Toolset
  - **We Verify project/**, a video plugin to debunk fake videos on social media that spread conspiracy theories
  - **ENGAGE project**/ Engage Society for Risk Awareness and Resilience solutions
  - Code of Practice on Disinformation

- *GROUP 2. "Resilient Civilians and Strategic Communication"* innovations focus:
  - SchoolNode (innovative solution that was not initially on the assessment list)
  - AI-enhanced disaster emergency communications
  - Blockchain -based verification
  - 'Antidote' to hostile messaging delivered by private messaging apps

The ranking results of all innovations that were under discussion in the groups during the training event were following:



Still, it is to be noticed that such prioritization does not provide a proper quantitative indication of the innovations' ranking but should be considered as qualitative indication of preference of a given group of participants. Dissemination level of the Training event deliverables D2.22 is public, so details of discussion within groups are not provided. Those can be requested by trusted partners and will be delivered as inputs for the further EU-HYBNET 3rd cycle work especially in EU-HYBNET WP4 "*Recommendations for Innovations Uptake and Standardization*" where the most promising innovations for standardization and industrialization are stated.

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

During the reporting period EU-HYBNET T3.4 "*Innovation and Knowledge Exchange Events*" in the lead of EOS arranged the final, 3rd Innovation and Knowledge Exchange Workshop (IKEW) together with Valencia Local Police (PLV) in Valencia during 7th of November 2023. Agenda of the IKEW in Annex III. Because the IKEW also provided floor for relevant European Commission (EC) funded projects whose solutions are seen also relevant to pan-European security practitioners and other relevant actors to counter hybrid threats, the projects and more thorough analysis on their solutions' soundness for uptake and industrialization is provided below according to the EU-HYBNET Four Core Themes: *Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and*

Strategic Communication. In addition in the IKEW the closing Keynote Speech was given by EU funded project, Tools4LEAs, and hence also its take ways are described below.

BOS for Core theme "Cyber and future technologies" & STARLIGHT Project

Description: *STARLIGHT Project* (https://www.starlight-h2020.eu/) aims to create a community that brings together LEAs, researchers, industry and practitioners in the security ecosystem under a coordinated and strategic effort to bring AI into operational practices across a number of high priority threats, such as counterterrorism, child sexual exploitation, cybersecurity and more. The presentation focused on the tools developed to counter online terrorism, with the set of tools being able to do individual instance assessment, multi-instance assessment and monitor rapidly developing phenomena through online detection analysis. One tool highlighted was the telegram crawler, able to analyse various topics and subtopics and create inter-topic distance mapping. With these AI-enabled tools, LEAs are able to focus on extreme and harmful disinformation, detect symbolism of banned movements, conduct a toxicity analysis to determine those moving towards radicalisation and conduct a more thorough sentiment analysis to understand the effects of online terrorism and disinformation campaigns.

Discussion: The three main takeaways of this discussion were:

1. Legal narratives that could be activated for extremism were not taken into consideration by STARLIGHT; however, they could be easily implemented into the AI tools developed by the project.
2. In turn, one of the needs highlighted was for the tools to not be used to clamp down on legal speech.
3. The conclusion of the discussion was that cyber development will be accelerated, the malicious use of technologies will grow exponentially, and the lawful growth of technology will slow. In this case, the STARLIGHT project will be a useful tool for LEAs to counter hybrid threats.

Innovation(s): AI Toolbox for countering (online) terrorism

BOS for Core theme "Information and strategic communication" & VIGILANT Project

Description: *VIGILANT project* (https://www.vigilantproject.eu/) will provide Police Authorities with the technical capabilities necessary to combat disinformation and other related forms of harmful content (radicalisation, extremism, hate-speech) linked to criminal activities while at the same time building their institutional knowledge to provide them with an understanding of the social drivers and behavioural dynamics behind the phenomena. The project also includes first-of-its-kind disinformation response and investigation training for police officers. Finally, the project includes setting up a specialist European network for officers to share their experiences and knowledge and to promote a unified European approach to a problem that ignores borders.

Central to the platform is the VIGILANT Toolbox, which contains over 30 state-of-the-art textual, image and video, and network analysis tools developed by partner academic institutions.

Text analysis tools are designed to work with data from social media, blogs and online news sources and will enable PAs to evaluate claims, synthetic (machine generated) text, find protests or calls to action, to understand individuals' stances within a discussion and more. Image and video tools can find if an image or video has been seen previously, detecting symbolism, flags and guns in images, detect facial deep-fakes and manipulated images. Network tools increase understanding of the behaviour both within groups and across groups, and enable detection of coordinated behaviour of different individuals, as well as determining key members of public groups.

These tools, when combined with VIGILANT's novel UI and search and filtering capabilities, enable PAs to do the work they already perform in detecting, evaluating and monitoring disinformation groups in a much more efficient way. It also enables PAs to broaden the scope of their work, to find and monitor more groups and to increase their understanding of ongoing trends.

Discussion: The four most important takeaways of this session are:

1. Defining Disinformation: The judgment of what constitutes disinformation varies by country and is adaptable. The toolbox is designed to allow LEAs to tailor their approach based on the specific context and legal frameworks of their respective jurisdictions. The tools only highlight content that has been debunked or cannot be found in other sources, but it is up to the users to determine if a criminal activity has taken place. However, there was a notable recognition of the need to align activities with specific legal frameworks and crimes, including exploring the legal implications of disinformation.
2. Challenges in Deepfake Detection: Recognising the challenges posed by deepfakes, the toolbox addresses them by deploying a dedicated team focused on detecting deepfake content. Acknowledging the evolving nature of deepfake technology, the session highlighted the continuous improvement of AI both in generating fake images and in tracking them.
3. Linguistic Concerns: The Toolbox can analyse content in over 30 languages, but the tools themselves are currently provided in English. A key takeaway was that the tools themselves could also be updated to meet the needs of LEAs across Member States.
4. Future Considerations: Acknowledging resource constraints, especially for smaller law enforcement agencies, the session discussed the ongoing challenge of creating sustainable and ethical tools. The future landscape also presents challenges, including potential resistance from social media companies in providing data access, highlighting the evolving nature of the fight against disinformation.

Innovation(s): VIGILANT Disinformation Toolbox

BOS for Core theme "Resilient civilians, local level, and national administration" & CONNECTOR project

Description: *CONNECTOR project's* (https://connector-project.eu/) vision is to contribute to the European Integrated Border Management (EIBM) and to the EU Customs Action Plan by addressing the need of close cooperation between Customs, Border and Coast Guard Authorities within the

current and upcoming challenging and demanding environment of borders' control by further involving Customs to the Common Information Sharing Environment (CISE) network and Enhanced Common Information Sharing Environment (e-CISE) through the proposed Customs Extended Common Information Sharing Environment (CE-CISE).

CONNECTOR aims for the first time to suggest an integrated, common and shared risk assessment approach for all Border Management Authorities, considering the pan-EU common risk indicators per end user group (Customs, Border and Coast Guards Authorities including FRONTEX), to ensure external EU border and secure EU citizens from cross-border crime and/or secure the seamless flow of travellers, as recommended in the multiannual strategic policy document. Thus, in this sense, CONNECTOR proposal, will design and develop the CONNECTOR system as an interoperable technical environment, ensuring close and practical cooperation and information exchange at all levels. The design and the development of the CONNECTOR system will be based on the analysis of current policy initiatives in EU level (directives, policy and staff documents, guidelines etc.) along with needs, gaps and future views of the end-user groups going beyond previous initiatives (ANDROMEDA, MARISA, EFFECTOR, etc.), complying with the Societal, Ethical and Legal (SoEL) requirements and regulations, following the SoEL-by-design principle.

The CONNECTOR system will be validated in real operational environment, based on well-defined National, Cross-border and Transnational use cases defined commonly by Customs and Border and Coast Guards authorities, during three (3) long lasting trials (Demonstration and Testing) under standardised methodology.

Discussion: the three main takeaways from this system were:

1. You cannot share data by force. It is all voluntary and there needs to be either a trigger or great motivation. Part of what CONNECTOR and customs authorities needs to do is highlight why it is necessary to cooperate and share information and data.
2. The creation of an EU Customs Authority would be an important step to ensuring cooperation between Member States' and closing the gaps between customs regimes. Additionally, an EU Customs Authority would be essential to creating an EU-wide operational picture for customs.
3. Due to custom regimes being fragmented, hybrid threat and criminal actors are currently able to target easier areas of entry to commit acts further in the EU past the original point of entry. The example used was if illegal food enters Spain, it could end up in Norway, affecting them. Therefore, cooperation between EU member states is paramount for customs' contribution in countering hybrid threats.

Innovation(s): CE-CISE

The Closing Keynote Speech by European Anti-Cybercrime Technology Development Association (EACTDA)

The IKEW closing keynote speech was provided by Eva Škruba/ Capability Manager at the European Anti-Cybercrime Technology Development Association (EACTDA) and MS Škruba highlighted the process followed by EACTDA through the *Tools4LEAs project I-II* https://www.tools4leas.eu/ to link innovation providers and practitioners. The goal in Tools4LEAs has been to facilitate the uptake of

security research project results, bridging the gap between prototype and product to develop fully tested and operational-ready software tools with no licence costs and access to the source code for EU public security organisations fighting cybercrime. This has been tested as a successful approach already in Tool4LEAs project I that Tool4LEAs II is now continuing. From the EU-HYBNET point of view Tool4LEAs testing and development approach is seen profoundly to answer security practitioners needs and hence it is much recommended for uptake. In the Tool4LEAs project also following approaches are seen important for uptake in pan-European security RDI community in order to enhance capabilities to answer hybrid threats alike other security concerns:

- to deliver fully tested tools and also to maintain them for users after project
- to provide complementary services, such as training, IT consultancy, and support and maintenance, provided by trusted service providers. Tools4LEAs II has incorporated a pilot offering these services to early adopters, fostering active communities around the tools. Collaboration with other stakeholders like ECTEG and CEPOL is highlighted as essential for comprehensive training and educational materials and services.

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

What comes to the second Three Lines of Actions focus area "**common requirements as regards innovations that could fill in gaps and needs"**, the research activities and results in this Eight Six Month Action Report reporting period are also partly 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). More information about T2.4 and T3.4 results to the Second Three Lines of Action in the following subchapters.

Also EU-HYBNET WP4 *"Recommendations for Innovations Uptake and Standardization"*/ T4.1 "*Mapping on the EU Procurement Landscape*" in its' D4.3 "*3rd Report on the Procurement Environment*" (by KEMEA) has focused on "**common requirements as regards innovations that could fill in gaps and needs**" on its research on procurement landscape for the EU-HYBNET's latest discovered most promising innovations for uptake. Key findings from T4.1/ D4.3 are also presented in the subchapters below.

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

During the reporting period EU-HYBNET T3.4 "*Innovation and Knowledge Exchange Events*" in the lead of EOS arranged the final, 3rd Innovation and Knowledge Exchange Workshop (IKEW) together with Valencia Local Police (PLV) as a local host in Valencia during 7th of November 2023. Because the IKEW's key focus is on innovations that are seen relevant to pan-European security practitioners and other

relevant actors to counter hybrid threats, the IKEW handled innovations from variety of view points. Comprehensive description of IKEW is delivered in D.3.13 "3rd *Innovation and Knowledge Exchange Workshop*" (by EOS, M44/Dec 2023) while the sub-chapters below summarizes the key IKEW findings on "**Common requirements as regards innovations that could fill in gaps and needs**" according to the IKEW Agenda starting from Keynote speeches and ending to panel discussion on days key findings.

The First Keynote Speech by DG HOME

The first IKEW Keynote speech on "Innovation Uptake of Security Research" was given by Mr. Giannis Skiadaresis, SSRI Area Coordinator for DG HOME. Mr Skiadaresis underlined that EU-HYBNET, alike other EC funded similar projects, should see the four following pillars of security research and innovation as starting point when considering common requirements to innovation that could fill in gaps and needs. The pilars are:

1. Tools that has possibility for pre-commercial procurement and they follow standards
2. From impact point of view innovations should be in-line with terms of reference with EU Agencies, synergies with other funds, new technology in Internal Security Fund (ISF)
3. Thorough study on EU Security Market and study on uptake factors are common requirements for successful innovation uptake leading to industrialization
4. Community/communities (CERIS, SRE, Networks, EU Innovation Hub on Internal Security, Users in R&I projects) views on the soundness and need on the innovation is a requirement so that it may fill gaps and needs

In addition, Mr. Skiadaresis stressed the importance of the Study on Uptake Factors as it highlights a series of factors that either hinder or promote the uptake of innovation. Below is a list of promoting factors for innovation uptake that can be taken as a starting point when considering common requirements to innovation that could fill in gaps and needs:

Promoting Factors for Innovation Uptake:

- Funding mechanisms' soundness
- Communication and Dissemination of Information in order to ensure stakeholders awareness of the innovation
- Procurement Mechanisms' needs to be well know and place in order to support the innovation uptake
- End-user involvement is a must when innovation is developed because this will ensure that the innovation will deliver needed answer to the end-users' gaps and needs
- Partnership and collaboration with relevant actors and stakeholder ensures innovation uptake
- Testing and demonstrations are a crucial requirement in order to ensure that the innovation will be in-line with end-users needs and expectations to fill the gaps and needs

Mr. Skiadaresis concluded by noting what the EU is doing to push forward and drive innovation uptake. There was two relevant points in this, also if we consider **common requirements as regards innovations that could fill in gaps and needs**

- Have a proactive approach based on foresight, prevention & anticipation
- Enabling police authorities, border guards and first responders to identify & develop the capabilities they need for the future.
- Use adequate funding instruments to acquire and to implement innovative solutions

The Second Keynote Speech by Infrastructure and Security at the Security Technology Centre (CETSE)

The second keynote speech was given by Mr. Francisco Alonso Batuecas/ Head of ICT Infrastructure and Security at the Security Technology Centre (CETSE) within the Ministry of the Interior in Spain. Mr. Batuecas spoke about the recent attacks of the group as NONAME on the Spanish government due to the Spanish Government's support for Ukraine. After describing NONAME and their tactics, Mr. Batuecas described the attacks Spain has faced from NONAME. Four attacks were described and the key take away to innovations needed to support authorities to prevent similar attacks to happen in the future was summarized clearly. In short, Mr. Batuecas concluded by emphasising the work that is still needed to be done to counter hybrid threats such as the ones faced by Spain, including learning more about those attacking us and how they are doing it. Furthermore, information sharing is seen paramount to achieving this goal.

Break Out Session Outcomes in Panel

The last part of IKEW included session where all IKEW Break Out Session outcomes were presented and further analyzed in a Panel Round Table discussion. The roundtable discussion was opened by the representative of the Europol Innovation Lab with a brief presentation of the Lab's mission: to support innovation for law enforcement, both by mapping new tools for LEAs to use, as well as by looking into threats that are ahead and developing foresight and an anticipatory approach to address them. The EU-HYBNET network and results are particularly important for the Europol Innovation Lab in this regard as they can support their work in determining which tools LEAs could use to address hybrid threats and put forth suggestions for the Europol Tool Repository. Therefore similar projects as EU-HYBNET can be seen as a common requirement for innovations that could fill in gaps and needs. Furthermore, EUROPOL Innovation Lab underlined that a **common requirement for innovations that could fill in LEAs' gaps and needs are following:**

1. Innovations and innovative solutions that tackle threats posed by technologies like Deepfake and ChatGPT in fuelling misinformation, by generating materials on which a fake narrative can be built.
2. Innovations answering possible harmful impact of quantum computing on decryption. The advances in quantum cryptography could enable adversaries to steal confidential information and data today, and eventually decrypt them, once the capabilities exist in the future.

EUROPOL Innovation Lab summarized and underlined that it is important to introduce solutions that would allow LEAs to get ahead of such threats, rather than chase them. LEAs need to have these tools available in advance rather than try to create them when these threats materialise. On

the issue of uptake, **a common requirement as regard of the innovations that could fill in gaps and needs** it was proposed making the source code of the developed solutions open source to facilitate uptake by LEAs. The large number of solutions developed by different projects makes it impossible for LEAs to purchase them all; standardising and integrating the solutions so that they could work together could be a solution in that regard.

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

During the reporting period EU-HYBNET T2.4 "*Training and Exercises for Needs and Gaps*" (lead by L3CE) arranged the final, 3rd EU-HYBNET training event (hybrid format on the 18th -19th of Jan 2024 in Vilnus) where variety of innovations were tested according to the training scenario provided by EU-HYBNET T2.3 (lead by KEMEA). The EU-HYBNET T2.4/ D2.22 "*Training and exercises delivery on up-to-date topics*" describes the training event with details while central results from the document concerning **common requirements as regards of the innovations that could fill in gaps and needs** are described below.

The starting point to test the selected innovations in the 3rd EU-HYBNET training event was formulation of two groups according to participants interests and expertise in the named areas. The two groups were formulated around EU-HYBNET Four Core themes and the first group included Core Themes " *Future Trends of Hybrid Threats"* and *"Cyber with Future Technologies"* as more technological oriented; the second group included Core Themes "*Resilient Civilians: Local Level and National Administration"* and "*Information and Strategic Communication"* as more social oriented. In both of the groups following innovations were tested and their soundness for uptake is described in the analysis results below.

Innovations presented and tested in the context of Future Trends of Hybrid Threats Core Theme

Vignette 2	Vignette 2
Mobile application to pinpoint acts of harassment/violence on the street and online	We Verify, a video plugin to debunk fake videos on social media that spread conspiracy theories
SMIDGE	DesinfoEND

Innovations presented and tested in the context of Cyber and Future Technologies Core Theme

Vignette 2	**Vignette 2**
Advanced Surveillance Systems with Perimeter security	Starlight Disinformation-Misinformation Toolset
Code of Practice on Disinformation	Innovative Cluster for Radiological and Nuclear Emergencies, INCLUDING
ENGAGE (Engage Society for Risk Awareness and Resilience)	

After innovations were presented, prioritization discussion was held in both of the named Core Theme groups. This lead to testing and more thorough analysis of the innovations. Priorities from both groups for the innovations soundness and uptake interest are summarised in the figure below.

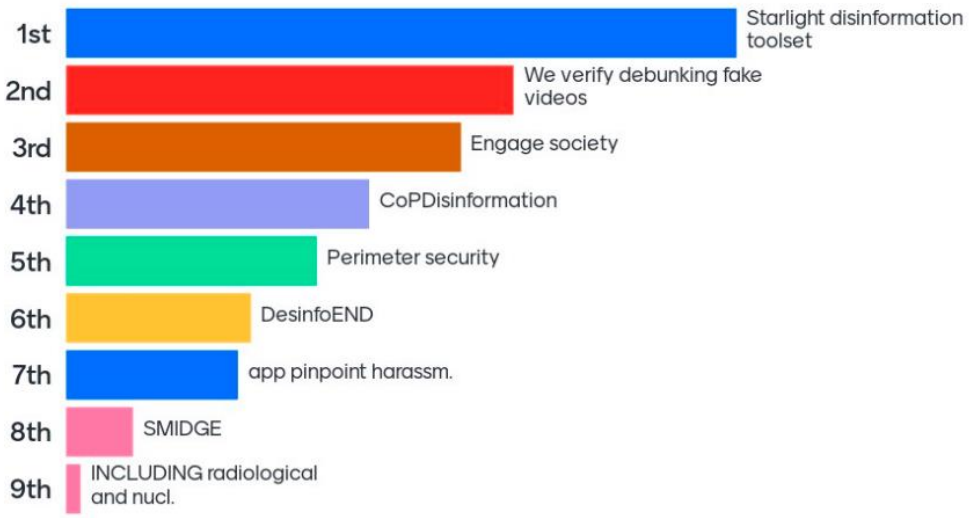


Figure 2 Response to the question "Which innovations were most useful for the given situation?".

Innovations presented and tested in the context of Resilient Civilian, Local Level and National Administration Theme

Vignette 2	Vignette 2
AI-enhanced disaster emergency communications - innovation	'Antidote' to hostile messaging delivered by private messaging apps
The Countering Foreign Interference (CFI) project	EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective
	STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

Innovations presented and tested in the context of Information and Strategic Communication Core Theme

Vignette 2	Vignette 2
Blockchain -based verification -innovation	Media Pluralism Monitor (MPM) tool
Media Pluralism Monitor (MPM) tool	ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE
ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE	INJECT Innovative Journalism: Enhanced Creativity Tools -project

After innovations were presented, prioritization discussion was held in both of the named Core Theme groups. This lead to testing and more thorough analysis of the innovations. Priorities from both groups for the innovations soundness and uptake interest are summarised in the figure below.

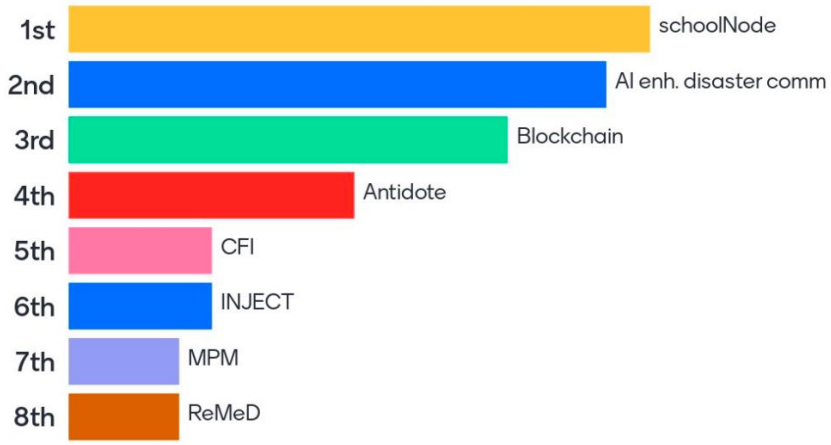


Figure 3 Response to the question "Which innovations were most useful for the given situation?".

According to the training event participants analysis and results of most sound innovations to fill in security practitioners' and other relevant actors' gaps and needs to counter hybrid threats, more thorough analysis of the most promising innovations was launched in WP3 "*Surveys to Technology, Research and Innovations*" (lead by Satways)/ T3.1. "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) and esp. in WP4 "*Recommendations for Innovations Uptake and Standardization*" (lead by KEMEA)/ T4.1 "*Mapping on the EU Procurement Landscape*" (lead by KEMEA) and T4.2 "*Strategy for Innovation uptake and industrialization*" (lead by RISE). According to T4.1 and T4.2 analysis following four innovations were selected to innovation uptake strategy creation in T4.2 and to solve the procurement landscape for them in T4.1 - The innovations are:

- ***STARLIGHT project and Innovation Testing Best Practices*** (https://www.starlight-h2020.eu/)
- ***App to pinpoint harassment -technological solution***
- ***AI enchanced disaster communication – technological solution***
- ***Countering Foreign Interference (CFI) project*** (https://www.iss.europa.eu/content/euiss-launches-eu-funded-project-countering-foreign-interference)

Concerning the named innovations just after this Eight Six Month Action Report reporting period T4.2 has proceed with its analysis of common requirements as regards of the named innovations to fill in gaps and needs. Therefore, T4.2 results will be analyzed in the next Sixth Month Action Report. However in T4.1 the procurement landscape analysis for the named innovations has been finalized during this reporting period and more about these findings in the next subchapter.

3.2.3 EU-HYBNET T4.1 MAPPING ON THE EU PROCUREMENT LANDSCAPE

In EU-HYBNET the WP4 *"Recommendations for Innovations Uptake and Standardization*" has delivered contribution during the reporting period to the second Three Lines of Action "**Common requirements as regards of the innovations that could fill in gaps and needs** " especially in T4.1 "*Mapping on the EU Procurement Landscape*"/ D4.3 "*3rd Report on the Procurement Environment*" (by KEMEA).

The main task in T4.1 has been to focus on procurement landscape of the four most promising innovations that EU-HYBNET has identified according to the innovation (technological and non-technological e.g. training, SOP) mapping to the latest gaps and needs of security practitioners and other relevant actors identified in T2.1/ D2.27 "*Long list of defined gaps and needs*" (by Hybrid CoE, in April 2023) and T2.2/ D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (by JRC, in July 2023) during the 3rd project working cycle (M35/ March 2023 - M52/ August 2024). Variety of promising innovations were mapped to the gaps and needs in T3.2/ D3.5 "*Second mid-term report Improvement and innovations*" (by Satways, in Sept 2023) and T3.3/ D3.9 "*Second mid-term report Innovation and monitoring*" (by L3CE, in Sep 2023) as described in the last Six Month actions report and their analysis in order to find the most fitting and sound innovations to the gaps and needs has been conducted in T2.4 Training event and further onwards in T3.1 "*Definition of Target Areas for Improvements and Innovations*" (lead by TNO) where innovation analysis is getting to its end during this Eight Month Action Report delivery. However, according to the T2.4 Training event where variety of innovations were tested and according to the T3.1 preliminary results, the most promising innovations were identified in T4.1 and hence also more thorough analysis has bene done to the EU-HYBNET's four most promising innovations for uptake and procurement analysis. The four most promising innovations under each of the EU-HYBNET Four Core Themes are following:

1. *Mobile application to pinpoint acts of harassment/violence on the street and online* under Core Theme: Future Trends of Hybrid Threats
2. *AI enhanced Disaster Emergency Communications* under Core Theme: Resilient Civilians, Local Level, National Administration
3. *Media Pluralism Monitor* under Core Theme: Information and Strategic Communication
4. *Starlight Disinformation-Misinformation toolset* under Core Theme: Cyber and Future Technologies

More about the named innovations **Common requirements as regards of the innovations that could fill in gaps and needs** in the following three subchapters.

3.2.3.1 EU-HYBNET T4.1 PROCURRMENT PROCEDURES

According to the T4.1 analysis innovations that could fill in security practitioners' gaps and needs should be such to which funding possibilities and especially procurement does exist. According to T4.1 available procurement procedures that are classified as "innovation friendly" are following to the EU-HYBNET's four most promising innovation uptake. In general, the starting point is that while formulating a procurement procedure, it is crucial to take into account whether the contractual

volumes are above (AT) or under (UT) the EU threshold in order to select the appropriate procedure as analysed below. According to T4.1 there are primarily six distinct options for promising innovations procurement that will support their uptake, and hence innovations soundness to the suggested procurement processes can be seen as **common requirements as regards of the innovations that could fill in gaps and needs**.

Option 1. "Public (UT) and open tender (AT)"

The Public (UT) and open tender (AT) approach is the principal standard procurement procedure. If we talk about innovations that could fill in gaps and needs, the innovations should be such that Public (UT) and open tender (AT) approach would fit to them. If not there are options to support the innovation uptake while Public (UT) and open tender (AT) approach would be the most common. Picture below describes the approach in the context of innovation uptake's **common requirements as regards of the innovations that could fill in gaps and needs**

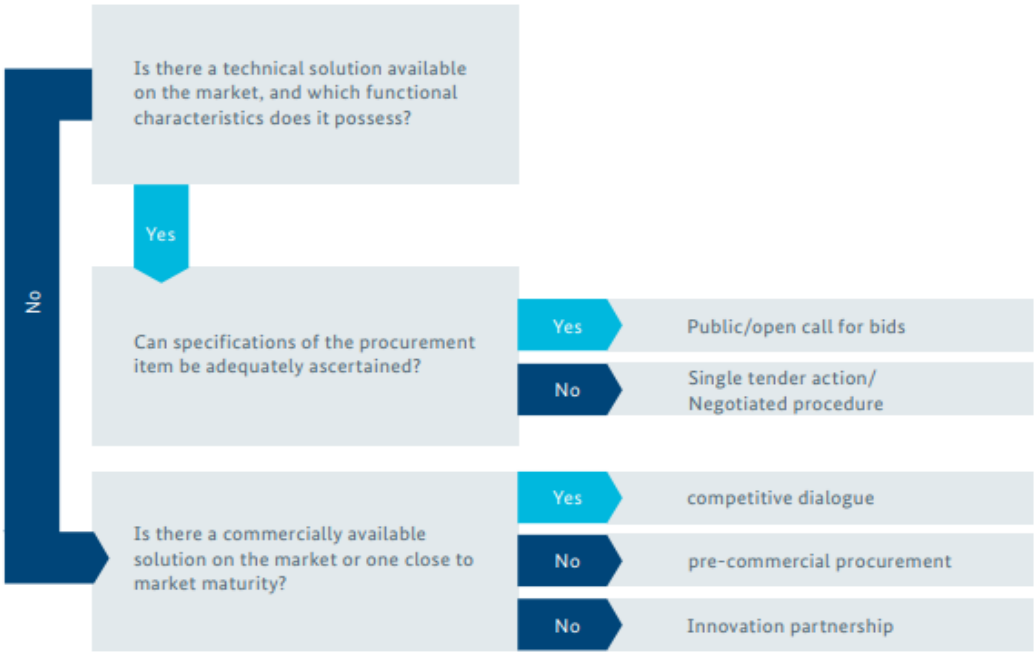


Figure: Decision Tool for selection of Procurement Procedure

Option 2. Negotiated procedure (AT) and negotiated award (AT)

These procedures are characterised by the potential to accommodate the procurement to the specific features. In the process of a pre-ongoing competition open to all bidders, new solutions to procurers could be generate through bidders.

For contracts above the EU threshold values, the negotiated procedure is selected. In more detail, this is a procurement procedure, setting the activity of the contracting authority to approach one or multiple selected companies to negotiate based on a pre-existing defined list of services in the context or not of a call to tender.

The main advantage from implementing such a procedure is that negotiations with the bidder are generating advanced and innovative aspects and hence, negotiated award. Under that aspect, shortfalls and high demands can be improved and high expectations can be met. Furthermore, innovation procurement potential is increasing by the nature of the overall procedure.

Option 3. Competitive dialogue

The competitive dialogue is the process where all the chosen companies are involved in a series of discussions regarding all the aspects of the tender. The aforementioned procedure according to market research, provides a flexible solution when issues arise such as inadequately described technical specifications or when financial and legal framework are not clear. During the analytical discussions with potential bidders, an in-depth understanding of contractual aspects, challenges and the specific demands of the procuring entity take place. The objective of the competitive dialogue is to consolidate all market information into the final description of services in order to respond to the demands of the contracting authority in the most efficient way. In the development of innovative solutions, such procedure between parties provides a methodical and practical approach in the formulation of the procurement documents. During the whole procedure, the following aspects are identified as common requirements in the innovation uptake in order to gain eventually innovations that could fill in gaps and needs:

- This process demands experienced personnel to handle it and more time than conventional procedures. Moreover, the process requires more resources since a dedicated project team or even external support is necessary.
- The dialogue phase demands substantial investment in time from the participating players. In times where it seems appropriate, there should be legitimate coverage for this, nevertheless, this should be set clearly during the implementation of the dialogue.
- To respond to bidders' considerations in relation to confidentiality issues that can arise (intellectual property, disclosure of sensitive data) and equality, mutual non-disclosure agreements could be signed.

Still the process has many advantages. First of all, competitive dialogue can be implemented in complicated markets or in solutions which are challenging to evaluate, where e.g. it is not easily defined what the market provides in terms of technical, financial or legal aspects. Since procurement specialist do not often conduct a comprehensive market research, this process is highly beneficial regardless of its complication.

Option 4. Pre-Commercial Procurement (PCP):

Is implemented for the procurement of solutions that are not available in the market.

Pre-Commercial Procurement (PCP) is the call for bids for R&D services. The objective is the development of innovative products and services which takes place in three stages, during which the competition between the participating companies leads to the identification of several solutions addressing the same need. In this regard, through PCP vendor lock in is avoided.

During the research and development phase, the contracting authority possess the option to choose the ideal solution between various bidders. The research and development phase could possibly happen in multiple stages: for example, there can be six initial bidders competing among them in the concept-building stage and after the end of the said phase the selection only three bidders could evolve to a prototype. Lastly two bidders could pass to the third phase where the prototype will be tested in real operational environment and be financed to conclude with a marketable solution.

The procurement process of a PCP, could generate the decision to purchase the R&D outcome by selecting the most suitable solution. However, there is the possibility to search for a totally different solution outside the PCP procedure. The procurement of the R&D phase and the procurement of the actual products are legally independent. In contradiction, the innovation partnership award a contract to only one bidder or one bidding consortium that is a "partner" in the development phase and the procurement procedure.

PCP is a tool for promoting innovative, adequate, and continuous public sector provision and not a procurement process in a strict way. The principles of transparency, non-discrimination and equality must be taken under consideration (European state-aid rules applicable). Additionally, it is important to highlight that the PCP procedure depicts the typical stages of a product innovation cycle. There is a separation between the R&D activities and the purchase of the subsequent commercial products. Intermediate evaluations are implemented for the each of the three phases. In that way, risks are eliminated, and the most suitable solutions are chosen.

The bidder and the contracting authority are sharing both the risks and the benefits of the PCP on market conditions. The contracting authority does not acquire the rights of use of R&D results since it passes them to the bidders within the framework of the PCP along with the obligation for the commercialisation of the solution. A future call to tender (Procurement on Innovative Solutions – PPI) may take place for the actual procurement and commercial exploitation of the new product solution.

Advantages for the PCP are many fold. All along PCP refers to the procurement procedure where multiple bidders evolve a solution - the contractors are filtered out during several intermediate stages subsequently revealing the best bidder. On the whole, PCP decrease the risks of the procurement in the public sector since the developers hold a substantial proportion of the cost because they have the option to promote their solutions elsewhere if they do not succeed in the competition. Thus, development costs potentially do not exceed the financing

of one developer. Therefore, PCP may be well suitable approach for innovation uptake as regards of the innovations that could fill in gaps and needs.

Option 5. Innovation partnership

This recent procurement procedure associates the award of a development contract with the actual procurement which leads to the establishment of a long- term partnership between the company and procuring authority. Therefore, Innovation partnership can be seen as a **common requirements as regards of the innovations that could fill in gaps and needs**.

The EU public procurement law (Dir/2014/24/EU, Art. 31, introduced a new procurement process identified as the Innovation Partnership. It is specifically designed, for the development and procurement of innovative products, services and works that are not yet available on the market. Thus, there is no need for a distinct process for the purchase, as is the case for pre-commercial procurement (PCP). Between the company and the contracting authority, a continuing partnership is built. Company's objective is to bring a product to the market, introduce it and constantly develop it.

As usually, before the tender process there is a call to tender. A bid is required by the selected companies for the first round of the tender. Following, a negotiation between the bidders and the contracting authority on the initial bids will take place and afterwards the procurer requests the follow-up bids. The objective is to alter and make better the bids in terms of the way they address the tender challenge. When the final bid will be accepted by one or more bidders, the innovation partnership will be implemented. It has to be noted also that award of a tender only taking consideration the lowest price or lowest cost is not foreseen.

An advantage in innovation partnership is clear. In short, for products and services that are not available in the market yet, the innovation partnership assists the contracting authority in their procurement strategy. Hence, research and development actions from a possible bidder may arise because of a current issue or of a non-settled challenge and assisted by the said procedure. Nevertheless, this process is only ideal for complicated products and services because both aspects demand expansion of resources and the various tiers are time-consuming.

Option 6. Public Private Partnerships (PPP)

For the selection of the most suitable form of award in PPPs, principal questions are asked to the industry representatives followed by the market research and consultation. PPPs are contractual arrangements signed among private entities and public institutions and are mainly used for large infrastructure.

A cooperative arrangement between two or more public and private sectors, primarily of continuous nature is defined as a public–private partnership. More precisely, it includes government(s) and business(es) that collaborate in order to complete a project and/or to

provide services to the general public. As funding instruments PPPs have been substantial controversial, mainly because the public return on investment which is considered lower than returns for the private funder. The inadequacy of shared understanding regarding PPP and the confidentiality about its financial details, makes the process for evaluating, whether PPPs have been successful, complex. PPP on the other hand promotes the distribution of risk and the evolvement of innovation, while on the other hand critics highlight its higher costs and issues of accountability. In terms of value for money and efficiency, evidence of PPP performance is complicated and sometimes non available. Still there are some advantages in PPPS, they are:

- Guarantee the effective investments and usage of the public resources into public sector;
- Guarantee high quality;
- More investment projects are taking place in due terms and do not include unforeseen expenditures;
- Private entities can obtain a long-term remuneration;
- Private sector expertise and experience are capitalised from the public sector;
- The PPPs' risks allocation enables the reduction of the associated expenditures.

Due to the advantages PPP can be recommended as a common requirement as regards of the innovations that could fill in gaps and needs.

3.2.3.2 EU-HYBNET T4.1 FINANCIAL TOOLS

Next to different processes and forms that support innovation uptake mentioned above, according to T4.1 findings, there are also some financial tools that can be named as **common requirements as regards of the innovations that could fill in gaps and needs**. These financial tools are such that will support promising innovation uptake - the financial tools are:

Fast Track innovation (FTI)

Close-to-the-market innovation actions open to industry-driven groups which can be consisted of any type of participants are promoted by the Fast Track to Innovation (FTI), a fully-bottom-up innovation support programme which can assist partners to co-create and test breakthrough products, services or business procedures that could possibly alter existing or generate completely new markets, under the helm of the Enhanced European Innovation Council (EIC) pilot. The FTI's goal is to:

- Decrease time from idea to market;
- Encourage the participation of first-time applicants to EU research and innovation funding;
- Escalate private sector investment in research and innovation.

Enhanced European Innovation Council (EIC) pilot

As part of the Enhanced European Innovation Council (EIC) pilot, start-ups and SMEs that are located in one country inside the European Union or are established in a **Horizon 2020** associated country, have the opportunity to receive EU funding and assistance for advanced innovation projects with a market-creating possibility.

The Enhanced EIC pilot provides grant support along with grant in combination with equity investment. The Enhanced EIC funding can rapidly increase company's development and innovations that can create new markets. Further, it will assist the progress of development of innovation entities by giving them access to Business Acceleration Services.

The EIC Accelerator assists high-risk, high-potential innovative SME's which are eager to evolve and commercialise new products, services and business models that have the potential to increase economic growth and generate new markets or disrupt the current ones in Europe and all over the world. Full-cycle business innovation assistance is provided by the EIC Accelerator pilot.

EU Funded PCP/PPI

EC has recognised the importance of innovation procurement and more specifically PCP/PPI and several funding opportunities have been set in place in several funding schemes. In this context the EU's research and innovation programs FP7, CIP, EASME, and Horizon 2020, as well as the Horizon Europe have been funding projects in which groups of procurers from different countries around Europe are jointly implementing Pre-Commercial Procurement (PCP) or Public Procurement of Innovative Solutions (PPIs), as well as coordination and networking projects that prepare the ground for future PCP or PPIs. A limitation in some of the abovementioned funding opportunities may be the innovative procurement selection as it is predefined is several cases.

3.2.3.3 EU-HYBNET T4.1 FOUR MOST PROMISNG INNOVATIONS FOR GAPS AND NEEDS AND THEIR REQUIREMENTS

Finally, T4.1 also created an "Uptake strategy" for the* four most promising innovations are that include some elements as **common requirements as regards of the innovations that could fill in gaps and needs**. The four most promising innovations are as follows alike the key T4.1 findings.

3.2.3.3.1. MOBILE APPLICATION TO PINPOINT ACTS OF HARASSMENT/VIOLENCE ON THE STREET AND ONLINE

Attacks on societal structures and cohesion, both in the form of online harassment and spread of violence, are both a current trend, but also a future trend in hybrid threats that need to be challenged. In order to be challenged successfully, the first signs of such occurrences should be noted in order to provide situational awareness if not to also provide an early warning. In that case, the responsible law enforcement agencies can react in a timely manner in both virtual and physical space and accordingly use their resources wisely for the situation at hand. Should the situation still escalate, the response from rescue services may be needed as a precaution or to assist possible victims.

Involving the public serves multiple purposes. Firstly, it allows to save on expensive resources, such as online monitoring systems or CCTV, as well as on street patrols. Secondly, it diminishes the required time for discovering and locating occurrences of the mentioned threats. Thirdly, it helps in building societal resilience in itself by allowing everyone the option to participate in creating more security – especially the youth.

The aim of this specific innovation is to utilize readily available, widely used technology – i.e. smartphones – to record and geolocate acts of harassment and violence (or calls for violence) in physical space and acts of harassment and calls for violence online. Such acts may occur in the form of physical actions on the street, but also as graffiti and/or leaflets in physical space and/or online.

Smartphones integrate three important technologies for conducting such activities: the clock, which provides a timestamp on the occurrence; the camera, which allows the recording of the action or written text as photographic, video or as audio evidence; the geolocation to pinpoint the occurrence on the virtual map. In addition, integrating the option to report similar occurrences online gives the users – law enforcement agencies – the opportunity to monitor evolving situations in real time and note the correlations in physical space, as well as online. The application would be especially useful in crisis situations like riots, if used by a large number of users.

The relevant EU directives that govern public procurement

Public procurement in the EU is governed by a comprehensive legal framework that aims to ensure transparency, non-discrimination, and equal treatment of suppliers across member states. These directives include:

- Directive 2014/24/EU: This directive governs the procurement procedures for public contracts by entities operating in the fields of water, energy, transport, and postal services. It establishes procedures for the award of contracts, including open, restricted, competitive dialogue, and innovation partnerships.

- Directive 2014/25/EU: This directive regulates procurement procedures for entities operating in the utilities sector, including water, energy, transport, and postal services. It establishes similar procedures to Directive 2014/24/EU but with specific adaptations for the utilities sector.

- Directive 2014/23/EU: This directive governs the award of concession contracts, which are long-term contracts granted by public authorities to private operators for the provision of services or the exploitation of public assets. While less directly relevant to the procurement of a mobile application, it may apply to certain aspects of the project.

- Directive 2014/55/EU: This directive promotes the use of electronic invoicing in public procurement processes to streamline administrative procedures and facilitate cross-border trade.

These directives provide a framework for conducting procurement procedures in the EU, including the procurement of digital services such as mobile applications. Entities within the EU, including government agencies, municipalities, and public utilities, are required to follow these directives when procuring goods, services, or works above specified financial thresholds.

When procuring a mobile application to address acts of harassment/violence on the street and online, relevant EU directives and national procurement laws would apply. Procurement procedures typically involve advertising the opportunity, issuing tender documents, evaluating bids, and awarding contracts in accordance with the principles of transparency, equal treatment, and competition.

It is crucial for procuring entities to familiarize themselves with the specific requirements and procedures outlined in the relevant EU directives and national legislation governing public procurement to ensure compliance and successful execution of the procurement process. Additionally, they may seek guidance from legal experts or procurement specialists to navigate the complexities of EU procurement rules.

Market Consultation.

A thorough market consultation could result in the identification of state-of-the-art and commercial solutions, suitable vendors, gathering valuable insights, and laying the groundwork for a successful procurement process. In the case of procuring the "Mobile application to pinpoint acts of harassment/violence on the street and online", a structured approach to market consultation should ideally entail:

- A clear definition of Objectives and Scope of the mobile application, its intended functionalities, and the problem it aims to address (e.g., reporting harassment/violence incidents). Define the target audience and any specific requirements.

- Identification of potential suppliers, who specialize in developing similar mobile applications or have experience in related fields such as safety apps, community platforms, or crime reporting systems.

- Conducting of information sessions, or workshops where interested vendors can learn about the project requirements, objectives, and scope, as well as the provision of background information on the issue of harassment/violence and explain how the mobile application will contribute to addressing it.

- Collection of feedback from vendors regarding the project concept, including any challenges they foresee and suggestions for improvement, by asking specific questions about their capabilities, experience, and proposed solutions.

- A review of existing solutions from similar projects developed by vendors, to evaluate their features, user interface, success metrics, and user feedback to identify best practices and potential areas for innovation.

- Discussion of technical requirements, such as platform compatibility (iOS, Android), data security, scalability, and integration with existing systems or databases. Ensuring in this way that vendors understand any specific technical constraints or preferences.

- Encourage vendors to propose innovative features or approaches that could enhance the effectiveness of the mobile application. Consider emerging technologies such as artificial intelligence, geolocation, or real-time data analytics.

- Evaluation of costs and timelines, taking into account factors such as development, testing, deployment, maintenance, and ongoing support.

- Assessing legal and ethical considerations: Discuss legal and ethical considerations related to data privacy, consent, anonymity, and responsibility for content moderation. Ensure that vendors comply with relevant regulations and industry standards.

- Document Feedback and Insights: Document all feedback, insights, and recommendations gathered during the market consultation process. Use this information to refine your project requirements, evaluate vendor proposals, and make informed decisions moving forward.

Available templates.

As mentioned above (Section 4), officials responsible for drafting public procurement specifications and documents would be very much facilitated in case they use as a starting point readily available templates. Generally, regular procurement templates can be found in TED[1], whereas for innovation procurement public entities could consult the EAFIP toolkit[2]. In the case of procuring the "Mobile application to pinpoint acts of harassment/violence on the street and online", templates should encompass several key components to effectively communicate the project requirements and expectations to potential vendors. Such templates should include:

- Project Overview: a brief introduction to the project, highlighting the purpose and objectives of developing the mobile application.
- Scope of Work: a clear definition of the scope of the project, outlining the features and functionalities expected in the mobile application. This should include specifics such as reporting capabilities, geolocation services, support resources, and any other essential components.
- Technical Requirements: the technical specifications and requirements for the mobile application, including platform compatibility (iOS, Android), backend infrastructure, data storage, security measures, and any other relevant technical considerations.
- User Interface/Experience (UI/UX) Requirements: the desired user interface and experience, emphasizing ease of use, accessibility, and intuitive design. Provide any design guidelines or preferences to ensure alignment with user expectations.
- Reporting and Incident Management: the functionality required for users to report incidents of harassment/violence, as well as the process for incident management and communication with relevant authorities or support services.
- Support and Resources: the types of support resources and services that should be integrated into the application, such as helplines, counseling services, legal aid, and community support groups.
- Data Privacy and Security: data privacy and security requirements, including compliance with relevant regulations (e.g., GDPR, CCPA), data encryption, user authentication, and measures to protect sensitive information.
- Timeline and Milestones: a proposed timeline for the project, including key milestones such as design completion, development phases, testing, deployment, and ongoing maintenance.
- Budget and Payment Terms: the budget available for the project and any preferred payment terms. This may include fixed-price or time and materials contracts, payment schedules, and cost breakdowns for different project phases.
- Evaluation Criteria: an outline of the criteria that will be used to evaluate proposals from potential vendors. This may include factors such as technical expertise, experience, cost-effectiveness, timeline adherence, and quality of past work.
- Submission Instructions: instructions for vendors to submit their proposals, including the deadline for submissions, preferred format (e.g., electronic submission), and contact information for inquiries or clarifications.

[1] https://simap.ted.europa.eu/standard-forms-for-public-procurement
[2] https://eafip.eu/

- Legal and Contractual Considerations: any legal or contractual requirements that vendors must adhere to, such as non-disclosure agreements, intellectual property rights, indemnification clauses, and termination conditions.

Skilled personnel.

In the case of procuring the “Mobile application to pinpoint acts of harassment/violence on the street and online”, developers of applications for both iOS and Android devices, steeped in the technical requirements and capabilities is highly recommended in the needs identification, the development of the technical specifications, the monitoring of the development of the solutions and their testing to ensure that expertise in cybersecurity aspects is considered. In this context cybersecurity threats should be considered when planning the procurement of a new system or service while threat identification should be continuous in the whole procurement lifecycle.

Adequate vulnerability assessment.

Conducting an adequate vulnerability assessment is crucial to ensure the security, resilience, trustworthiness and integrity of the application for its users. The vulnerability assessment steps to be followed, in the case of procuring the “Mobile application to pinpoint acts of harassment/violence on the street and online”, should involve:

- Threat Modeling: Begin with the identification of potential threats and vulnerabilities that the mobile application may face. Consider both technical threats, such as data breaches or malware attacks, and non-technical threats, such as misuse of the application's features for harassment or stalking.

- Risk Assessment: Evaluation of the likelihood and potential impact of each identified threat. Prioritizing threats based on their severity and likelihood of occurrence. This will help focus efforts on addressing the most critical vulnerabilities first.

- Security Requirements, Security Architecture and Code Review: Definition of security requirements that the mobile application must meet to mitigate identified threats. This may include requirements related to data encryption, authentication mechanisms, access control, secure communication protocols, and secure storage of sensitive information. Also, perform a review of the mobile application architecture to identify any design flaws or vulnerabilities that could compromise its security. Assurance that security best practices are followed throughout the development process, from design to implementation. Additionally, conduct a thorough code review to identify potential security vulnerabilities in the application's source code. Look for common security flaws such as injection attacks, authentication bypass, insecure data storage, and inadequate input validation.

- Penetration Testing: Performance of penetration testing or ethical hacking to simulate real-world attacks on the mobile application. This involves attempting to exploit vulnerabilities in the application's security controls to gain unauthorized access or manipulate sensitive data.

- Data Privacy Assessment: Assessment of the application's handling of user data to ensure compliance with relevant data privacy regulations, such as GDPR or CCPA. Evaluation of how user data is collected, stored, processed, and shared, and implementation of appropriate measures to protect user privacy.

- User Safety Considerations: Consideration of potential risks to user safety, especially in cases where the mobile application involves reporting incidents of harassment or violence. Implementation of features to protect user anonymity, provide clear guidance on safety measures and establish mechanisms for reporting abusive behaviour.

- Third-Party Components Review: Review any third-party libraries or components used in the mobile application to ensure they are up-to-date and free from known security vulnerabilities. Monitor security advisories and updates for these components to address any newly discovered vulnerabilities.

- Continuous Monitoring and Improvement: Security is an ongoing process, so establishment of mechanisms for continuous monitoring and improvement of the mobile application's security posture is vital. Implementation of regular security audits, updating security controls as needed and staying informed about emerging threats and vulnerabilities.

Intellectual property rights (IPR) provisions.

Intellectual property rights (IPR) provisions play a critical role in protecting the interests of both the procuring entity and the developers/vendors involved and also in mitigating the risk of disputes or infringements related to IPR. A comprehensive provision of IPR might be addressed by following the steps below:

- Ownership of Intellectual Property: Clearly define the ownership of intellectual property rights related to the mobile application. Specify whether the procuring entity will retain full ownership of the application and its associated intellectual property, or if there will be shared ownership with the developers/vendors.

- Licensing and Usage Rights: Determine the scope of licensing and usage rights granted to the procuring entity for the mobile application. Specify the permitted uses of the application, including any restrictions on modification, distribution, or sublicensing.

- Protection of Proprietary Information: Include provisions to protect proprietary information and trade secrets shared during the development of the mobile application. Require developers/vendors to sign non-disclosure agreements (NDAs) to safeguard sensitive information from unauthorized disclosure or use.

- Assignment of Rights: Clarify whether developers/vendors are allowed to assign or transfer their rights and obligations under the contract to third parties. Include provisions to ensure that any such assignment is subject to the procuring entity's approval and does not adversely affect its interests.

- Indemnification for Intellectual Property Infringement: Require developers/vendors to indemnify the procuring entity against any claims of intellectual property infringement related to the mobile application. This includes indemnification for copyright infringement, patent infringement, or unauthorized use of third-party intellectual property.

- Open Source Software Compliance: Ensure compliance with open source software licenses and avoid any violations of third-party intellectual property rights. Require developers/vendors to disclose all third-party components and dependencies used in the mobile application, along with their respective licenses.

- Innovation and Inventions: Address ownership and rights related to any new inventions, innovations, or improvements developed during the course of the project. Specify whether such inventions will be owned by the procuring entity or shared with the developers/vendors.

- Dispute Resolution Mechanisms: Include mechanisms for resolving disputes related to intellectual property rights, such as arbitration or mediation. Specify the applicable jurisdiction and governing law for resolving such disputes.

- Termination and Transition: Outline procedures for the termination of the contract and the transition of intellectual property rights upon termination. Specify whether the procuring entity will have continued access to the mobile application and its source code after termination.

- Review by Legal Experts: Finally, ensure that the IPR provisions are reviewed by legal experts familiar with intellectual property law to ensure compliance with relevant regulations and best practices.

Open requirements.

Compatibility with previously purchased proprietary solutions or legacy systems should be straightforward and easily achievable, in the case of procuring the "Mobile application to pinpoint acts of harassment/violence on the street and online", since smartphone technology has been around for a long enough span of time. Moreover, the standards required for the adoption of this innovation are readily available in both operating environments (iOS and Android) and strongly supported by the market. The negative implications for procuring organisations and public authorities associated with ICT lock-in can be mitigated, since the technology and software – application development tools for both operating systems - behind the innovation is a widely known concept. Reducing the compatibility risk further can be achieved through the adoption of open source and open standards, as well as the creation of some guidelines, which the innovation lends itself to. Exit costs can also be included in the procurement of this innovation, to avoid lock-in.

Open procurement procedure is recommended.

When procuring the "Mobile application to pinpoint acts of harassment/violence on the street and online" through open procurement procedures, it's essential to ensure fairness, transparency, and competition among potential vendors, so as to ultimately select a vendor that best meets the requirements and objectives of the application. The following approach could be followed:

1. Preparation Phase:
   i. Define the requirements: Clearly outline the technical, functional, and security requirements of the mobile application.
   ii. Develop procurement documents: Prepare tender documents such as a Request for Proposals (RFP) or Invitation to Tender (ITT), including specifications, terms of reference, evaluation criteria, and contractual terms.
   iii. Determine budget and timeline: Establish a budget for the procurement and define the timeline for the entire process, including submission deadlines and evaluation periods.

2. Advertising and Tendering:
   i. Advertise the opportunity: Publish the procurement notice in relevant publications, websites, and platforms to reach a wide audience of potential vendors.
   ii. Provide access to tender documents: Make the tender documents available to interested vendors, ensuring equal access and transparency.

3. Clarification and Communication:
   i. Address vendor inquiries: Respond promptly and comprehensively to any questions or requests for clarification from potential vendors regarding the procurement documents or requirements.

ii. Conduct pre-bid meetings: Organize meetings or conference calls with interested vendors to provide additional information and clarify any ambiguities.

4. Submission of Bids:
   i. Receive and evaluate bids: Establish a secure mechanism for vendors to submit their bids within the specified deadline. Ensure that all bids are treated confidentially until the evaluation process begins.
   ii. Enforce compliance: Verify that all bids comply with the requirements outlined in the procurement documents. Disqualify any bids that fail to meet the mandatory criteria.

5. Evaluation Phase:
   i. Establish evaluation criteria: Define clear and objective criteria for evaluating the submitted bids, including technical capabilities, proposed solution, experience, pricing, and compliance with requirements.
   ii. Form evaluation committee: Create an evaluation committee comprising qualified individuals with expertise in relevant areas such as technology, security, and procurement.
   iii. Evaluate bids: Review and assess each bid based on the established criteria, scoring them objectively and consistently.
   iv. Shortlist or select vendors: Identify the highest-scoring bids and shortlist or select the most suitable vendors for further consideration or negotiation.

6. Negotiation and Contracting:
   i. Conduct negotiations: Initiate negotiations with shortlisted vendors to finalize contractual terms, pricing, and other details.
   ii. Sign contracts: Execute contracts with selected vendors, clearly outlining the rights, obligations, deliverables, and timelines for the procurement.

7. Implementation and Monitoring:
   i. Monitor implementation: Oversee the development and implementation of the mobile application by the selected vendor, ensuring compliance with the contractual terms and requirements.
   ii. Address issues: Address any issues or concerns that arise during the implementation phase promptly and effectively.
   iii. Monitor performance: Continuously monitor the performance of the mobile application and the vendor's adherence to contractual obligations.

8. Closure and Evaluation:
   i. Close the procurement process: Officially close the procurement process once the mobile application has been successfully developed and deployed.
   ii. Evaluate the procurement process: Conduct a post-procurement review to assess the effectiveness and efficiency of the procurement process, identifying any lessons learned or areas for improvement.

Standards adoption.

The standards required for the adoption of this innovation are readily available in both operating environments (iOS and Android) and the technological features of all contemporary smartphones provide a more than adequate set of technical standards upon which to apply the technical requirements of the innovation.

3.2.3.3.2 AI ENHANCED DISASTER EMERGENCY COMMUNICATIONS

Social structures are fundamental access doors to influence societies on the short and long run. Hospitals and health care services in general is to be considered as one of such structures. During recent years hospitals have experienced several cyber-attacks. At the same time, the increasing number of natural disasters, experience of handling pandemic related matters, clearly indicates vulnerabilities present in health sector. In the context of hybrid threats trust in healthcare systems and proper functioning of service provision during crisis periods is essential. This threat is focused on the abilities of hospitals to provide proper services in the case of patient afflux. Such phenomena can occur in different circumstances:

- It can be natural (objective) consequences of natural (e.g.: earthquake, flood, etc.) or industrial (e.g.: leakage of hazardous substances, explosions, transport accidents, etc.) disasters as well as man maid incidents (e.g.: terrorist attack, riots, etc.).
- It can be purposefully designed (subjective) to direct extensive crowds to hospitals as a stand-alone event or part of a more sophisticated hybrid attack aiming to undermine trust in local or national healthcare system or even democracy in general.

There might be a variety of tools, methodologies and processes that can deal with different aspects of such afflux despite its nature. Those can include simulation tools, contingency planning, communication with local society, early warning, crisis management, fast mobilization of resources and many others.

Our proposed focus is made on enabling hospitals at afflux risk by any nature to make an early assessment of the situation. This can be done by having remote capabilities able to provide relevant information from the scene of action. Having initial triage, even if the afflux is purposefully designed, will allow hospitals or all parties involved in the incident handling understand that kind of incident it is and get better prepared, faster apply for resources in need and reduce direct and cascading effects.

This does not lead to the predisposition that such solution would solve all patient afflux related problems but can add capabilities in real incident handling as well as prevent afflux use in hybrid context.

During major crisis the number of emergency calls has proven to be exponential, from 1 per minute to over 100 per minute, becoming impossible to sort out by emergency dispatchers, especially with the average emergency call lasting from 3 to 15 minutes dealt by just a few emergency dispatchers. Creating a massive telephonic congestion, the population is no longer capable to reach by phone the emergency services, report their positions and the evolution of their situation. This lack of communication increases the workload of Search & Rescue, which in the aftermath have to go place by place instead of focusing on population's reported positions.

The company HighWind has developed and patented the first Artificial Intelligence that can assess a patient's emergency priority level in less 100 millisecond thanks to Computer Vision and Deep learning using a crossed analysis on traumatology (nature of the wounds), emotions (pain, fears, etc.) and contextual elements (fire, smoke, etc.). Applied to major disasters, and encompassed within an smartphone "Disaster Mode" app for the population (downloaded or emulated by text-message link), it gives the emergency responders the ability to immediately visualize who are the persons most at risks on a map, prioritize search & rescue efforts to the most vulnerable persons, avoid the emergency calls congestion and facilitate patient referrals to hospitals based on the severity of their injures, thereby mitigating the potential influx of patients in hospitals.

Instead of taking one by one, lengthy emergency calls due to stressed persons, the emergency dispatch centre can perform several actions at once: send a "Disaster Mode" notification to the population, receive an accurate view on the emergency requests critical levels and positions on a map in few seconds, to better coordinate SAR efforts.

Leveraging on basic smartphone features, the AI is capable to immediately sort out victims, saving hours for the SAR teams and significantly increasing chances of survival. The “Disaster Mode” is also capable to take decisions to optimize communication based on available networks quality (no data, 2G to 5G).

The analysis of the application of the **“9 Specific Recommendations of the EU-HYBNET uptake strategy”** focuses on:

- Identifying those features the Innovation possesses which are relevant for the procurement process.

Introduced within the past year, this cutting-edge technology stands as an unparalleled innovation globally, as attested by assessments from the esteemed ADIT intelligence agency. Leveraging robust foundations in Computer Vision and AI, HighWind's AI undergoes meticulous training utilizing proprietary algorithms applied to extensive medical databases, encompassing both in-hospital and out-of-hospital scenarios. This training regimen is designed to effectively address three pivotal criteria for emergency detection: Traumas, Context, and Emotions.

The potential applications of this innovation are manifold, particularly within the realm of emergency response infrastructure across the European Union. HighWind's AI technology represents a significant departure from traditional practices, a fact duly acknowledged and celebrated at CES 2023, where it garnered acclaim as one of the most disruptive technologies serving the public interest.

Reports from the ADIT intelligence agency and the European Patent Office affirm the singular nature of HighWind's initiative, with no comparable endeavors evident on a global scale, spanning entities ranging from research institutions to startups and major corporations. While the primary cost drivers revolve around human resources, including AI engineers and legal professionals, substantial expenses are also incurred in AI training for the prototype, encompassing CPU/GPU computation time. The anticipated total budget for achieving a market-ready solution is estimated to approach 150,000 EUR.

In light of potential threats posed by complex cyberattacks orchestrated by state actors targeting critical infrastructure, including emergency services, ongoing efforts in advancing security measures aim to continually mitigate such risks.

- Identifying whether public procurement instruments of the EU landscape actually allow procurement of the kind of selected innovation. In this context, one of the important conclusions will be that either the existing procurement and funding instruments are sufficient, otherwise recommendations can be provided.

As reflected in the “Guidance on Innovation Procurement” by the European Commission in 2021, the procurement of innovative solutions in markets where the main buyers are public buyers can help boost the EU’s resilience, competitiveness and strategic autonomy. Additionally, the health sector, which this innovation has the ability to reinforce (along with the security sector) is specifically mentioned as an area that can benefit from public procurement, further aligning the political direction of the public procurement instruments with the innovation. Since the innovation is a disruptive technology with a path to commercialization and a partnership between two European SMEs, the current procurement landscape seems to be fitting.

All prerequisites have been fulfilled, setting the stage for collaboration between two Small and Medium Enterprises (SMEs): HighWind from France and GAGDPR from Greece. Their partnership aims to develop a product ready for use by end users and for market penetration. This strategic partnership entails the fusion of their respective resources, specialized knowledge, and cutting-edge technologies, culminating in the creation of a market-responsive product ready for commercialization.

- Practical recommendations regarding features of the selected innovation.

HighWind should get in touch with public procurement bodies in their respective countries to understand how to use the innovation procurement tools for their advantage and exploit once they have reached a higher TRL level. Additionally, as there is no other tool in the market that provides the same service as them, HighWind should also reach out to practitioners involved in the crisis management or healthcare sectors to provide

demonstrations of their prototype in order get early adopters and potential investment from end-users to finalise development as quickly as possible. Additionally, there are two pieces of legislation that may be of concern for this innovation: the GDPR and the AI Act. As the concerned innovation deals with AI, the recently approved AI Act will lay out certain rules for the use of AI, which will need to be complied with. The GDPR will also be concerned, as personal data, mainly medical data, will be transferred in mere milliseconds to the authorities. Consent and the protection of data will need to be ensured before this innovation can enter into market, so it is advised that the proper legal analysis is done for the innovation.

3.2.3.3.3 MEDIA PLURALISM MONITOR

The Media Pluralism Monitor (MPM) is a European Union initiative aimed at assessing and monitoring the degree of media pluralism within EU member states. Using an indicator-based approach, the MPM evaluates several aspects of the media landscape, including media ownership, independence of journalists, market access and content diversity. The data collected is analyzed to assess the level of media pluralism in each country and in the EU as a whole. The MPM provides crucial information to identify challenges and good practices in the field of media pluralism and to develop policies aimed at promoting a diverse and democratic media landscape. Analysis of the application of the **Specific Recommendations for EU-HYBNET** uptake strategy to the appointed / selected Innovation, specifically:

Market Consultation.

Regarding the market consultation phase in the context of a public procurement process, the Media Pluralism Monitor is recommended to adopt an inclusive and transparent approach to involve relevant stakeholders. Here are some specific tips:

- **Identification of key stakeholders:** Before launching the market consultation, the Media Pluralism Monitor should clearly identify key stakeholders in the media sector, including representatives of the media themselves, civil society organisations, industry experts and public authorities. This will ensure full involvement of stakeholders who may be influenced or involved in the media pluralism monitoring process.

- **Clear communication of objectives:** During the market consultation, the Media Pluralism Monitor should clearly communicate the objectives of monitoring media pluralism and the role of stakeholders in the process. This will allow stakeholders to fully understand the context and importance of monitoring and make meaningful contributions.

- **Flexible ways of participating:** The Media Pluralism Monitor should offer different ways of participation for stakeholders, for example through public consultation meetings, online questionnaires, workshop sessions or individual consultations. This will allow stakeholders to participate based on their needs and preferences, ensuring broad and representative involvement.

- **Actively listening to opinions and feedback:** During the market consultation, the Media Pluralism Monitor should engage in active listening to the opinions, concerns and feedback of stakeholders. This can include creating safe and inclusive spaces for open discussion and the exchange of ideas, allowing stakeholders to freely express their opinions and suggestions.

- **Transparency and accountability:** The Media Pluralism Monitor should ensure the transparency and accountability of the market consultation process, providing clear information on the outcomes of the consultation and the actions taken in response to the feedback received. This will help maintain

stakeholder trust in the process and ensure the integrity and effectiveness of media pluralism monitoring.

Available templates.

Regarding the availability of templates in the context of a public procurement process, it is recommended that the Media Pluralism Monitor develop and implement standardized and customizable templates for the collection and analysis of data relating to media pluralism. Some specific recommendations:

- **Developing clear and adaptable templates:** The Media Pluralism Monitor should develop clear and well-structured templates for collecting data relating to media pluralism, including questionnaires, interview guides and scorecards. These models should be designed to be adaptable to specific national needs and contexts, allowing countries to customize them according to their own media and institutional characteristics.

- **Inclusion of meaningful indicators**: Models should include a full range of meaningful indicators to assess media pluralism accurately and comprehensively. This may include indicators related to media ownership, independence of journalists, content diversity and market access, among others. Ensure that the templates reflect international best practices and recommendations in the field of monitoring media pluralism.

- **Customization of templates:** Templates should be designed to allow easy customization by participating countries, so that they can be adapted to specific national needs and priorities. This may include the ability to add or remove indicators, modify questionnaire questions, and adapt data collection methodologies to suit local circumstances.

- **Technical support and training:** The Media Pluralism Monitor should provide technical support and training to public buyers and national stakeholders on the use and adaptation of available models. This may include online or in-person training sessions, informational webinars, operational guides and dedicated technical assistance to address participating countries' questions and needs.

- **Periodic updating and review:** The templates should be subject to periodic review and updating to ensure that they reflect the latest trends and developments in the field of media pluralism. The Media Pluralism Monitor should establish a formal mechanism to regularly review the models and incorporate any new recommendations or guidelines emerging from relevant international sources.

Skilled personnel.

With regards to qualified personnel in the context of a public procurement process, the Media Pluralism Monitor is recommended to ensure that it has a highly competent and multidisciplinary team to successfully conduct media pluralism monitoring. Some specific recommendations:

- **Multidisciplinary skills:** Ensure that the Media Pluralism Monitor team includes professionals with multidisciplinary skills, including experts in journalism, media law, social sciences, statistics, communications and information technologies. This diversity of expertise will enable the team to comprehensively and thoroughly address the multiple dimensions of media pluralism.

- **In-depth industry knowledge:** Ensure that Media Pluralism Monitor staff have in-depth knowledge of the media industry, including understanding market dynamics, journalistic challenges and emerging

trends in information and communications. This will allow the team to accurately and contextualised the media landscape of each country.

- **Analytical and research skills:** Media Pluralism Monitor staff should possess strong analytical and research skills, including data collection, analysis and interpretation skills. This is critical for conducting quantitative and qualitative assessments of media pluralism and making evidence-based recommendations.

- **Communication skills and stakeholder engagement:** Ensure that Media Pluralism Monitor staff have effective communication and interpersonal skills to engage relevant stakeholders in the media pluralism monitoring process. This may include the ability to clearly and accessiblely communicate research findings and to establish collaborative relationships with journalists, civil society organisations, public authorities and other key actors.

- **Continuous professional development:** Promote continuous professional development of Media Pluralism Monitor staff through participation in conferences, workshops, training courses and professional development activities. This will ensure that the team is always up to date on the latest trends and methodologies in the field of media pluralism monitoring and can keep their skills high.

Adequate vulnerability assessment.

With regards to adequately analyzing vulnerabilities in the context of a public procurement process, it is recommended that the Media Pluralism Monitor integrate a thorough vulnerability assessment into its media pluralism monitoring framework. Some specific recommendations:

- **Identification of vulnerabilities:** The Media Pluralism Monitor should conduct a comprehensive analysis to identify and understand potential vulnerabilities in the context of media pluralism. This could include assessing threats to press freedom, the safety of journalists, concentration of media ownership and manipulation of information, among other factors.

- **Assessment of the impact of vulnerabilities:** Once identified, the Media Pluralism Monitor should assess the impact of the identified vulnerabilities on media pluralism and democracy as a whole. This assessment should take into account both the direct and indirect effects of vulnerabilities on media functioning and freedom of expression.

- **Measuring the severity of vulnerabilities:** The Media Pluralism Monitor should develop indicators and metrics to measure the severity of identified vulnerabilities. This will allow the Media Pluralism Monitor to systematically and comparably assess the level of risk that vulnerabilities pose to media pluralism in different national contexts.

- **Regular monitoring and updating:** The Media Pluralism Monitor should integrate vulnerability assessment as an integral part of its ongoing media pluralism monitoring process. This requires constant monitoring of emerging threats and periodic review of identified vulnerabilities to ensure monitoring remains relevant and updated over time.

- **Developing mitigation strategies:** The Media Pluralism Monitor should work with relevant stakeholders to develop and implement effective mitigation strategies for identified vulnerabilities. This could include adopting legislative and regulatory measures, establishing protection mechanisms for journalists and promoting transparency and accountability in the media sector.

Intellectual property rights (IPR) provisions.

Regarding the provisions on intellectual property rights in the context of a public procurement process, below are some recommendations:

- **Clarity on provisions relating to intellectual property rights:** The Media Pluralism Monitor should clarify in a transparent and detailed manner the provisions relating to intellectual property rights for all data, information and materials collected, processed or produced in the context of media pluralism monitoring average. This may include defining who owns the intellectual property rights to the data and reports produced, as well as the conditions for their use, sharing and distribution.

- **Respect for the intellectual property rights of third parties:** The Media Pluralism Monitor should ensure that it respects the intellectual property rights of third parties in the course of its media pluralism monitoring activities. This means obtaining the necessary permissions to use data, information and materials protected by copyright or other intellectual property rights and complying with any limitations or restrictions imposed by the rights holders.

- **Appropriate licenses and agreements:** The Media Pluralism Monitor should enter into appropriate licenses and agreements to regulate the use, sharing and distribution of data and materials collected in the course of monitoring media pluralism. This may include adopting open licenses or other ways of sharing data that allow broad and free access to the information collected.

- **Protection of sensitive data:** The Media Pluralism Monitor should take appropriate measures to protect sensitive data collected in the course of monitoring media pluralism from unauthorized access, misuse or unauthorized disclosure. This may include adopting cybersecurity measures, pseudonymizing data and limiting access to authorized personnel only.

- **Transparency and accessibility:** The Media Pluralism Monitor should promote the transparency and accessibility of information and materials produced in the course of monitoring media pluralism, ensuring that they are easily accessible to the public and relevant stakeholders. This can be achieved by publishing reports, data and other resources online and adopting open licensing or other ways of sharing data that allow for free and non-discriminatory use.

Open requirements.

Regarding open requirements in the context of a public procurement process, the Media Pluralism Monitor is recommended to adopt an open requirements policy that promotes transparency, accessibility and fair participation of all interested actors. Some specific recommendations:

- **Clear definition of requirements:** The Media Pluralism Monitor should clearly and with details define the requirements for participation in the public procurement process, including selection criteria, evaluation procedures and expectations relating to expected results. This will allow potential suppliers to fully understand expectations and prepare competitive and relevant proposals.

- **Promoting competition and innovation:** The Media Pluralism Monitor should design requirements to promote competition and innovation in the industry by enabling participation from a wide range of vendors and solutions. This can be achieved through the adoption of open requirements that do not favour a particular vendor or technology approach, but instead encourage diversity and creativity in meeting the needs of the public buyer.

- **Transparency and accessibility of requirements**: The Media Pluralism Monitor should ensure that requirements are published in a transparent and accessible way to all interested parties, providing clear and detailed information on selection criteria, evaluation procedures and how to submit proposals. This will allow all potential suppliers to participate in the process fairly and without discrimination.

- **Stakeholder involvement:** The Media Pluralism Monitor should actively involve relevant stakeholders in the requirements definition process, allowing them to provide feedback and contributions to improve the relevance and effectiveness of the requirements. This may include public consultation, the involvement of civil society organizations and industry experts, and the creation of opportunities for discussion and exchange of ideas.

- **Regularly updating and reviewing requirements:** The Media Pluralism Monitor should establish a formal mechanism for regularly updating and reviewing requirements, ensuring they remain relevant and aligned with the public buyer's evolving objectives and needs. This may include regularly evaluating stakeholder feedback, analyzing international best practices, and adapting to regulatory and technological changes.

Compatibility with legacy systems.

Regarding compatibility with legacy systems in the context of a public procurement process, the Media Pluralism Monitor is recommended to adopt an approach that allows the effective integration of new tools and data collected with the systems existing. Some specific recommendations:

- **Preliminary assessment of legacy systems:** Before proceeding with procurement, the Media Pluralism Monitor should conduct a thorough assessment of existing legacy systems used for the collection, analysis and management of media pluralism data. This will help identify any challenges or limitations that may affect the integration of new tools and data.

- **Defining Compatibility Requirements:** Based on the preliminary assessment, the Media Pluralism Monitor should clearly define the compatibility requirements that new tools and collected data must meet to integrate effectively with existing legacy systems. These requirements should include, for example, interoperability standards, compatible data formats and supported communication protocols.

- **Collaboration with vendors:** The Media Pluralism Monitor should actively collaborate with vendors of legacy systems and new tools to ensure design and implementation that takes integration needs into account. This may include the participation of suppliers in joint planning and development sessions, as well as the establishment of agreed technical specifications and data exchange protocols.

- **Testing and validation:** Before completing the implementation, the Media Pluralism Monitor should conduct extensive testing and validation to verify the effective compatibility and interoperability of the new tools and data with existing legacy systems. This may include integration testing, load testing, and compatibility testing to ensure smooth operation in the production environment.

- **Training and support:** The Media Pluralism Monitor should provide appropriate training and support to staff involved in using the new tools and integrating with existing legacy systems. This may include specific training sessions, detailed training materials, and dedicated technical support to address any issues or questions during the integration process.

Open procurement procedure is recommended.

To ensure an open procurement procedure in the context of the Media Pluralism Monitor. Some key recommendations:

- **Total transparency:** Ensure that the entire procurement process is completely transparent, with all phases and decisions publicly accessible. This includes the clear and timely dissemination of all procurement-related information, including selection criteria, evaluation methods and final decisions.

- **Open Participation:** Encourage open and inclusive participation of all potential qualified suppliers. This can be achieved by disseminating procurement opportunities on public platforms and explicitly inviting participation from national and international suppliers.

- **Fairness and non-discrimination:** Ensure that the procurement process is conducted in a fair and non-discriminatory manner, without favoring any supplier or group of suppliers. This requires an objective and impartial evaluation of the proposals submitted, based exclusively on the selection criteria established in advance.

- **Transparency in selection criteria:** Clearly set out the selection criteria used to evaluate and evaluate supplier proposals. This will allow suppliers to understand which aspects of their service or product will be evaluated and on what basis decisions will be made.

- **Monitoring and reporting:** Implement a monitoring and reporting system to follow the entire procurement process and ensure compliance with the principles of openness and transparency. This may include designating a responsible body to oversee the process and publishing regular reports on progress and decisions made.

- **Access to documents:** Provide easy and complete access to procurement-related documents, including technical specifications, terms of reference and proposals submitted by suppliers. This will allow greater transparency and a better understanding of the process by all interested parties.

Standards adoption.

To ensure the adoption of effective standards in the context of a public procurement process for the Media Pluralism Monitor, here are some recommendations:

- **Research and evaluation of best standards:** Before proceeding with procurement, the Media Pluralism Monitor should conduct research and evaluation of the best standards available in the field of media pluralism monitoring. This may include recognized international standards, guidelines issued by accredited organizations and best practices developed by industry experts.

- **Adoption of open and interoperable standards:** The Media Pluralism Monitor should prioritize the adoption of open and interoperable standards that enable interoperability and data exchange with other systems and platforms. This will allow the Media Pluralism Monitor to easily integrate its tools and data with other initiatives and initiatives in the field of media pluralism.

- **Customizing standards to specific needs:** If necessary, the Media Pluralism Monitor should customize or adapt existing standards to meet the specific needs of its operational context. This may include adding new indicators, changing evaluation criteria, or adapting data collection and analysis methodologies to respond to the unique characteristics of each country's media landscape.

- **Stakeholder involvement in the adoption of standards:** The Media Pluralism Monitor should actively involve relevant stakeholders, including representatives of the media, civil society organizations and

public authorities, in the process of adopting the standards. This can help ensure that adopted standards meet the needs and expectations of all stakeholders and enjoy broad support and acceptance.

- **Regularly updating and reviewing standards:** The Media Pluralism Monitor should establish a formal process for regularly updating and reviewing adopted standards, ensuring that they remain relevant and aligned with developments in the field of media pluralism monitoring. This may include regularly evaluating stakeholder feedback, analyzing international best practices, and adapting to regulatory and technological changes.

3.2.3.3.4 STARLIGHT DISINFORMATION-MISINFORMATION TOOLSET

Due to huge significant of the social platforms, external to the EU actors are known to invest in special instruments which leverage algorithms of platforms to promote specific content to attack democracies by manipulating online content. Such content is targeted to justification of war, sowing distrust in democratic governments and promoting all kinds of destructive theories under disguise of free speech. Artificial amplification is one of techniques applied and it has a potential to promote this usually marginal content and expose it to wide auditorium giving the impression that this is important and legitimate “other opinion”. Artificial amplification can be used many different circumstances (e.g.: by organised crime aiming to money laundering, etc.), but it is a clear vector of hybrid attacks, providing a necessary spread of information.

Social platforms (social networks and user generated content platforms like YouTube or mass messaging like Telegram) become key instruments for public debate and interaction. They in many aspects overcome traditional media companies by impact and become default communication media in various cases.

Russia’s war against Ukraine provides a new context of significance of these platforms – actual information wars are happening on the social platforms, bots spreading information and disinformation. Significant efforts and investments are observed by Russia trying to reach out to the western societies to impact their will to support Ukraine.

Artificial amplification can be carried out in many ways. Identification of artificial amplification is among the tasks of practitioners in hybrid threats and other fields. An example can be the elections phase where certain politicians use artificial amplification instruments to gain extensive electoral.

It is also needs to be noted that current legislation is not restricting artificial amplification in a straightforward way.

There are technological solutions for identification of bot reposts, clickbait, SPAM and other means of amplification. At the same time, social platforms seek after methodologies and tools to make them more resilient for this phenomenon.

The solution presented for this particular threat is about the complex evaluation of the content in social platforms providing access to deeper analysis of information on platforms and tools to identify artificial amplification. There are several solutions listed that can be viewed as standalone as well as integrated comprehensive solution.

The Starlight Disinformation-Misinformation solution aims to deliver an easy deployable toolset to address various needs of LEAs and other security practitioners with respect to a variety of threats linked to disinformation and misinformation. The innovation brings together a selection of different applications enabling deep access of information in social platforms and tools to detect different misleading aspects of the information.

Version 1 of the Starlight Disinformation-Misinformation toolset consists of the following modules:
Telegram Crawler, which analyses Telegram content (groups, posts, text, media);

DeepFake detection, which analyses changes in images and videos;
Forbiden Symbol Detection, which analyses forbidden symbolics;
Geolocalization, which analyses location;
Toxicity, which analyses toxic, offensive content, comments, hateful language;
Story Clustering, which analyses reposting chains;
Twitter Crawler, which analyses Twitter content (groups, posts, text, media);
Bot Detection, which analyses if posts were published by a bot;
Clickbait detection, which analyses if posts are clickbaits;
SPAM Detection, which analyses if posts are SPAM;
Sentiment Analysis, which provides semantic analysis of the post content based on basic emotions model;
Fake content Meta Detection Engine, which determines fake content on the basis of posts' URL analysis.

The innovation is integrated within one interface and its contents is planned to expand. The Starlight solution is generally multi-lingual, with only several modules in one (English or German) language.

At this point of time the Starlight project is developing solutions for LEAs, but it can be developed further for different target groups and serves as a good example of what is needed to handle artificial amplification complexity in information dissemination.

In reference to T4.1. and specifically D4.3, the focus of the deliverable will be on analyzing the application of the Specific Recommendations for EU-HYBNET uptake strategy (Section 4) of the Starlight Disinformation-Misinformation toolset and its uptake, with the focus on:

- Identifying the features the Innovation possesses which are relevant for the procurement process.
- Identifying whether public procurement instruments of the EU landscape actually allow procurement of the kind of appointed / selected innovation. In this context, one of the important conclusions will be that either the existing procurement and funding instruments are sufficient, otherwise recommendations can be provided.
- Practical recommendations regarding features of the appointed / selected innovation.

Analysis of the Starlight toolset (hereinafter: Starlight) against the Specific Recommendations for EU-HYBNET uptake strategy

Market Consultation. Prior to initiating ICT's public procurement process, it is recommended that public institutions consult the market to identify state-of-the-art and commercial solutions. Transparent market engagement is considered important in order to identify the feasibility of the tender by assessing their needs, identifying what standards and other technical specifications to use as well as to look for existing solutions that might be re-used, without having to "reinvent the wheel". On a European level there are several repositories that could be consulted in relation to identifying the aforementioned points such as Joinup, the European Federated Interoperability Repository (EFIR) and the European Interoperability Framework (EIF)[3].

- *Features of innovation relevant for procurement process.*
  Starlight is one of many solutions in the market for automated analysis of dis- and misinformation and with time, the number of similar products will possibly grow. This translates into a need for a market consultation in order to select a solution that would fit the needs of the ordering organisation. Depending on those needs, an appropriate tender procedure will have to be selected, although with Starlight being in TRL-8 level and expected time-to-market being 1-2 years, principal tender procedures will possibly apply. Also, Starlight's value is bound to be above the European threshold, confirming the need of such a procedure.

[3] https://ec.europa.eu/isa2/sites/default/files/isa_annex_ii_eif_en.pdf

- *Do EU procurement instruments allow for actual procurement of innovation?*
  Yes, Starlight may be procured under the current procurement instruments. The selection will be based on individual legal circumstances available in respective countries.

- *Recommendations regarding innovation.*
  Purchase and maintenance costs have to be determined, also with respect to future development of the innovation.

Available templates. Officials responsible for drafting public procurement specifications and documents would be very much facilitated in case they use as a starting point readily available template. Generally, regular procurement templates can be found in TED[4], whereas for innovation procurement public entities could consult the EAFIP toolkit[5]. At a national level, several initiatives have been set in place also. Indicatively, in Poland, Public Procurement Office is the responsible body for drafting public procurement policies and regulating and coordinating the national public procurement system. In addition, the PPO is in charge of the preparation of standardised tender documents, as well as guidance material. Similar initiative has been set in Luxemburg, the Business Process Management Office (BPMO) which provides several tools and templates to assist contracting authorities in the tender preparation.

- *Features of innovation relevant for procurement process.*
  The description of Starlight does not contain any information of guidance to assist contracting authorities in the tender preparation.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  To expedite the procurement process, a set of specifications and information necessary for contracting authorities to draft tender data could be advantageous.

Skilled personnel. It is highly recommended to involve in the procedure, experts from IT department. Their involvement is crucial in the needs' identification, the development of the technical specifications, the monitoring of the development of the solutions and their testing to ensure that expertise in cybersecurity aspects is considered. In this context cybersecurity threats should be considered when planning the procurement of a new system or service while threat identification should be continuous in the whole procurement lifecycle.

- *Features of innovation relevant for procurement process*.
  There is no data in the description on the skills of IT department, technical specifications etc. necessary to uptake the innovation.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  To expedite the procurement process, a set of specifications and information necessary for the IT side of the contracting authorities could be advantageous. This is key especially in the case of LEAs, who may have very specific requirements and/or limitations/expectations in this regard.

Adequate vulnerability assessment. Vulnerabilities should be considered before procuring new products or services and that vulnerabilities of existing products/services are monitored throughout their lifecycle.

[4] https://simap.ted.europa.eu/standard-forms-for-public-procurement
[5] https://eafip.eu/

Moreover, the procuring organisation should establish a minimum set of security tests to be performed on acquired products or system, depending on the product/system type. It is also important to note that a newly acquired or newly configured product must undergo a penetration test in its actual installed environment. In the same way, remediating action taken must be online with the operational parameters of the actual environment.

- *Features of innovation relevant for procurement process*
  The innovation operates in the internet, which results in it being prone to any external malicious activity. Vulnerability issues are one of key factors for LEAs when assessing the appropriateness and usability of a new solution in daily operations.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  Develop safeguards and thoroughly test the innovation, with respect to external and internal (user-originating) threats.

Intellectual property rights (IPR) provisions. The way in which ICT solutions are licensed may affect their possibility to be shared and re-used. To ensure that the procured solution can be re-used by other public authorities or redistributed in any other way it is important to include the right IPR provisions in the procurement documents. This is especially important while procuring ICT solutions that citizens and businesses have access to. An option is to include in the tender documents requirements that could ensure maximum public access for citizens and businesses. This can be covered by requesting access to the procured solution by several diverse systems, without being limited by the use of specific branded products or application. Accessibility needs for people with disabilities should also be taken into account.

- *Features of innovation relevant for procurement process.*
  There is no information on IPR in the innovation description.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  Develop IPR provisions, taking into account that data linked with search history, operational interests and results is not available to any party except the client.

Open requirements. The requirements should be presented in an open manner. When procuring ICT solutions, there might be the tendency to request very specific solutions in order to ensure that what is requested will do exactly what the procuring entity is expected to do. However, such an approach hides several risks and disadvantages. First, customised solutions are generally more expensive than standard 'off-the-shelf' options. In addition, they are more difficult to be reused. Finally, suppliers who develop and manage custom-made systems can retain all the information about the system and make it very difficult to migrate to another supplier or to maintain or upgrade the system in the future. Excessive customisations may lead to supplier dependence and thus should be avoided. This aspect has been covered earlier in the document, however, below are some specific instructions related to the procurement of ICT technologies:

a. Benchmarks should be used to indicate that products should meet or exceed overall performance ratings;
b. Use functional requirements or performance to ensure that the procurement specifies functional requirements in a vendor-neutral manner;
c. Refer to standards and technical specifications: to avoid mentioning a specific process or referring to a specific trademark;

d. Use specific references only exceptionally when there are no other possible descriptions that are both sufficiently precise and intelligible to potential tenderers.

- *Features of innovation relevant for procurement process.*
  At this stage, there is no concrete data on how customized the system can be, depending on the client.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  Keep the system as open as possible. Enable the internal client's IT department to customize the application.

Compatibility with legacy systems. A common mistake that contracting authorities generally make is not to request compatibility with previously purchased proprietary solutions or as they called legacy systems. It is recommended to request for their interoperability of the new solution with the existing ones. As discussed in the literature, public authorities can be inefficiently constrained in their purchase of ICT by the existence of legacy systems, or by being locked-in to existing ICT products and services. ICT lock-in is a widely known concept, which has negative implications for the procuring organisations. Its alleged causes are the lack of interoperability, the lack of compatibility as well as high switching costs. Some countermeasures have been implemented, first and foremost the adoption of open source and open standards and the creation of some guidelines. In this context in order to ensure also that the purchased solutions can be further used to deliver trans-EU services, it is recommended to support solutions that use standards and no proprietary elements. Public procurements should include only standards that are supported by the market and that are recognised by a formal standardisation organisation, or a technical specification that has been identified by the Commission or by a national organisation. Moreover, functionalities to make data transfer effective should be requested meaning the setting of gateways to keep legacy systems/machines connected. Another approach in order to avoid lock in is to include exit costs in the procurement.

- *Features of innovation relevant for procurement process.*
  No data in the description.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation*
  Enable interoperability with most popular LEA analysis tools and information exchange systems.

Open procurement procedure is recommended. Open procurement procedures are generally recommended when procuring ICT goods and services. Indeed, it can be seen that different procedures are chosen for different reasons: for instance, restricted procedures are preferred when procuring services requiring special features provided by one operator only (military purposes, personal data protection, public connectivity services, specific activities in strategic sites …), as well as when too many vendors could be involved. On the contrary, negotiated procedures can be better when there exist some time boundaries, or a supplier's services uniqueness; finally, there were some opposite comments on competitive dialogue in relation to the cost effectiveness it can bring.

- *Features of innovation relevant for procurement process.*
  No data in the description. However, there seems to no limitations to hold any type of procurement procedure with this solution.
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  Prepare for various types of procurement procedures.

Standards adoption. Cost considerations, quality control concerns, supplier's expertise and the need of direct control are driving factors behind "make-or-buy" decisions. Similarly, these factors should be used as "motivational drivers" to promote the adoption of ICT standards that indeed support the cost reduction and ensure a good level of quality.

- *Features of innovation relevant for procurement process.*
  Planned accreditation is an expected "motivational driver".
- *Do EU procurement instruments allow for actual procurement of innovation?*
  N/A
- *Recommendations regarding innovation.*
  Ensure the ability of the solution provider and his team to obtain any facility and personnel security clearances. Be able to provide expertise history with entities from LEA sector.

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

In EU-HYBNET WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.2 "*Research to Support Increase of Knowledge and Performance*"/ D2.15 "*Articles and publications on themes and measures*" (by UiT) describes the key content of EU-HYBNET's research articles that have been deliver from each of the project Four Core Themes during past year. The goal of the articles has been to provide more analysis and to suggest possible solutions to the identified latest gaps and needs described especially in T2.2/ D2.11 "*Deeper analysis, delivery of short list of gaps and needs*" (by JRC, in July 2023) during the 3rd project working cycle (M35/ March 2023 - M52/ August 2024). The articles **priorities as regards of increasing of knowledge and performance requiring standardization** are highlighted below according to the four Core Themes.

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

The EU-HYBNET has delivered following four articles from each of the project Four Core themes during the fourth project year. The articles and their take aways for **priorities as regards of increasing of knowledge and performance requiring standardization** are highlighted in subchapters below.

Core Theme: Future Trends of Hybrid Threats

Article "*Employment of uncrewed systems (US) in attacks on critical infrastructure: hybrid threat perspective. Challenges related to recent developments in US technology"* in Open Research Europe

Focus: The uncrewed systems, known colloquially as drones are nowadays widely used in various roles, including strictly civilian, law enforcement and military. The pace of technological development is high and includes use of modern technologies, like artificial intelligence. Due to the growing threat to critical infrastructure that includes physical attacks, a fundamental question arises: how the development of uncrewed systems shapes the threat to critical infrastructure. Therefore, the article is divided into several parts. The first one describes a legal definition of critical infrastructure. The second one describes the development of uncrewed systems. Finally, scenarios of possible attacks are described. The assessment of influence of modern technology (especially Artificial Intelligence on those scenarios) is provided.

Core Theme: Cyber and Future Technologies

Article "*Countering Hybrid Threats: Towards an Ontology for Securing 5G Networks*" in Conference Proceedings by SPRINGER Nature under Open Access programme. Conference 'Computer and Communication Engineering, Third International Conference,' CCCE 2024 in Oslo 24-26/5/2024.

Focus: The key findings, or research outcomes and results, can be summarized as follows:

- 5G Threat Taxonomy: Within the framework of the ENISA 5G taxonomy of threats, which classifies the major categories posing threats to 5G infrastructure, critical assets under threat, such as SDN, NFV, MANO, RAN, MEC, CLOUD, and others, are identified, reflecting key components of the 5G architecture.
- 5G Vulnerabilities: An extensive analysis of vulnerabilities within the 5G framework is provided. This covers the 5G Core Network, Network Slicing, RAN, NFV, SDN, MEC, and security and physical architecture considerations. Specific vulnerabilities in these areas are highlighted, offering insights into potential weaknesses and areas for improvement in 5G security.
- Development of a Basic 5G Ontology: The paper presents an initial ontology for 5G based on ENISA's recommendations from its 5G Threat Landscape Report. This ontology is grounded in the ISO 27005 standard and defines relationships between risks, owners, threats, vulnerabilities, assets, control measures, countermeasures, and attack vectors. This ontology is aligned with the overall design and architecture of the ENISA framework and forms the foundation for securing 5G infrastructure, particularly in support of the 5G Action Plan for Europe and the TEN-T transport corridors.
- Management of Hybrid Threats in 5G ROUTES Project: The paper discusses the management of hybrid threats, which often combine conventional and unconventional methods across different domains. The proposed ontological framework integrates specific risk management strategies to protect and defend against hybrid threats in the 5G ROUTES project. This includes identifying hybrid threat scenarios, assessing their impact on 5G infrastructure, and implementing tailored countermeasures such as enhanced network security protocols and revised operational guidelines.
- Applicability to TEN-T and 5G Action Plan for Europe: The ontological approach is deemed beneficial for the 5G ROUTES trials integral to the functioning of TEN-T corridors. The ontology enables comprehensive risk assessment and management, addressing the complex interactions between different 5G components. It offers a robust framework for managing hybrid threats and aligns with the objectives of the 5G Action Plan for Europe, ensuring the

protection and resilience of critical 5G infrastructure within the EU's transport corridors. These findings reflect a comprehensive and multidimensional approach to understanding and securing 5G networks against hybrid threats. They demonstrate the importance of a holistic and integrated framework that considers the complex interplay of various elements within the 5G ecosystem.

Core Theme: Resilient Civilians, Local Level and Administration

Article "*Weaponized humanitarian migration and potential EU-wide responses to it"* in Open Research Europe

Focus: The article addresses the European Union capabilities (tools) to support Member States (MS) facing disproportionate and engineered border pressures from humanitarian migration fluxes. This article only deals with weaponized international humanitarian migration in the form of asylum-seekers being forcibly displaced towards an EU border. It also addresses the strategies of buffer states and non-state actors in terms of extracting revenue from the EU for curbing migration fluxes while obtaining strategic advantages from the EU Member states by encouraging migration towards the EU. EU MS tend to have divergent national interests or priorities while the distribution of asylum-seekers, legal and policy gaps, additionally strain the European asylum system. Further, migration is highly politized issue, as witnessed recently in Finland, Latvia and Estonia. The article unpacks the kind of threat that weaponized migration actually poses to the EU. It should consider and list the feasible options for an EU member state to call for help in facing disproportionate pressure with full respect to human rights standards, especially the role of FRONTEX and the EUAA. The article sheds light on what are the key enablers and barriers and how EU could support more effectively its Member States.

Core Theme: Information and Strategic Communication

Article "*Rethinking education and training to counter AI-enhanced disinformation and information manipulations: a Delphi study"* in European Security.

Focus: The increasing power and capacity of techniques and technologies associated with the development of Artificial Intelligence have opened a new scenario for the spread of disinformation and propaganda, offering enhanced capabilities for future activities of foreign information manipulation and interference (FIMI). The potential instrumentalization of synthetic content through the presentation of AI-generated audiovisual objects as documentary evidence of events or statements by malicious actors for political aims or economic purposes has been assessed to represent a security threat. However, even if the recognition of the problem and the understanding of the threat are necessary, addressing the phenomenon ultimately requires capabilities and competences from both government authorities and practitioners, but also from a set of stakeholders within civil society. This research article framed under the EU-HYBNET project aims to examine the needs and existing competence gaps for dealing with advanced disinformation as part of hybrid threats and FIMI. Methodology: A Delphi study was conducted during 2023 as part of the research activities of the EU-HYBNET project and through different rounds of online questionaries with experts (n=12) from the EU-HYBNET consortium organizations, the EU-HYBNET network and other experts identified through the project. Existing European competence frameworks were also considered for the research design and

its core competences constitute some of the bases for interrogating the experts on present status and potential competence gaps and needs. After processing the data generated from experts and once a sufficient degree of consensus among experts was assessed to exist, we analyze the findings from study. Findings: The results from the Delphy study indicate that AI-based disinformation activities not only constitute already a key challenge for societies, but experts believe that advanced forms of disinformation/FIMI through the use of generative AI and other technologies will be widespread and dominant and will require a proficient level of competence by practitioners. Among other relevant results, the study indicates agreement of the experts (92% with a confidence level of 85%) in that the current Digital Competence Framework (DigComp) for citizens should be expanded with additional areas of competence aimed at practitioners, for providing contextual knowledge on disinformation/FIMI (e.g. threat actors, geopolitical conflicts, historical revisionism) and other additional skills (e.g. detection and analytic techniques, argument-checking). Discussion and conclusion: This suggest that addressing future forms of disinformation and FIMI from an anticipatory and strategic perspective, rather than reactively, would require adapting existing frameworks today and plan education and training approaches to provide competences at a fast pace. For the case of practitioners, this may involve building a formal system of micro-credentials with a practical focus (how-to approach, rather than a what-is approach) and technology-oriented in addition to utilize and augment the existing DigComp framework with additional competences relevant to countering disinformation and FIMI.

4. CONCLUSION

4.1 SUMMARY

In the chapter above it is described how the EU-HYBNET project activities from the past six project months (Nov 2023 – April 2024) contributed to the Three Lines of Action. In addition, chapters have described how the work in the project Tasks has been conducted now when the 3rd project cycle has started to deliver results. Furthermore, the goal of the document has partly also been to highlight what kind of results EU-HYBNET is expected to achieve in the Three Lines of Action during the next six months reporting period.

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

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

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

4.2 FUTURE WORK

The EU-HYBNET project results to the Three Lines of Actions from the mid of the 3rd project cycle (duration: M35-M52/ March 2023 – August 2024) have been now explained to the EC from the reporting period of this deliverables. The next Six Month Action Report (in October 2024) will continue to describe 3rd cycle results and findings to the Three Lines of Actions, and how the project has been able to implement the findings even more to the benefit of pan-European practitioners to counter hybrid threats. Definitely, best practices and lessons learned and key findings will be taken into further work in the fourth EU-HYBNET cycle that will kick-off in September 2024 until April 2025. The following eleven (11) deliverables will be delivered during next six-month period, and there is a milestones to take place during the reporting period.

Deliverables (D):

T5.3 Project Annual Workshops for Stakeholders

- D5.13 Annual Workshop report 4 (PLV), M49/ May 2024

T3.4 Innovation and Knowledge Exchange Events

- D3.17 4th Future Trends analysis Workshop Report (PLV), M49/ May 2024

T2.1 Needs and Gaps Analysis in Knowledge and Performance

- D2.4 4th Gaps and Needs Events (HybridCoE), M50/ June 2024

T3.1 Definition of Target Areas for Improvements and Innovations

- D3.19 Final Report with Overview mapped on gaps and needs (TNO), M50/ June 2024

T4.2 Strategy for Innovation uptake and industrialization

- D4.6 3rd Innovation Uptake, industrialization and research strategy (RISE), M51/ July 2024

T2.3 Training and Exercises Scenario Development

- D2.28 Training and exercises scenario& training material (KEMEA), M51/ July 2024

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

- D4.14 3rd Policy briefs, position papers, recommendations report (Hybrid CoE), M53/ Sept 2024

T4.3 Recommendations for Standardization

- D4.10 3rd Report for standardization recommendations (PPHS), M53/ Sept 2024

T1.1 Administrative and Financial Planning and Coordination

- D1.13 9th Six month action report (Laurea), M54/ Oct 2024

T5.1 Dissemination and Communication Strategy and Plan

- D5.7 Mid-term project dissemination impact assessment report 3. (URJC), M52/ Aug 2024
- D5.5 Updated dissemination, communication and exploitation plan 3. (EOS), M54/ Oct 2024

Milestones (MS):

- MS28 “3rd Policy briefs, position papers, or recommendations documents are published” in M53 (September 2024)

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

Furthermore, new project results to the Three Lines of Action will be reported especially because deliverables focusing on promising innovations to present pan-European security practitioners gaps and needs to counter hybrid threats (by T2.1, T2.2) will be available alike take aways from innovation analysis in EU-HYBNET events such as 3rd Innovation Standardization Event in 22/10/2024 in Brussels. Furthermore, analysis on EU-HYBNET Dissemination, Communication and Exploitation activities will support the project to consider new ways to tell about the project’s results for the pan-European stakeholders.

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

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threat –project, No. 883054
EC	European Commission
EU	European Union
GA	Grant Agreement
DoA	Description of Action Part A and B
H2020	Horizon2020, EC funding Program for EU projects' funding
FP7	The EC's 7th Framework Program to EU project funding
D	Deliverable
CO	Consortium only deliverable
WP	Work Package
T	Task
M	Month
MS	Milestone
OB	Objective
KPI	Key Performance Indicator
NoP	Network of Practitioners project
R&I	Research and innovations
EU MS	European Union Member State
G&N	gaps and needs
IKEW	Innovation and Knowledge Exchange Event
BOS	Break Out Session
ISW	Innovation Standardization Workshop
AW	Annual Workshop
IMI	Information Manipulation and Interference
FIMI	Foreign Information Manipulation and Interference
AI	Artificial Intelligence
VR	Virtual Reality
EEAS/ Strat.Comm.	European External Action Service/ Strategic Communication
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos

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

.

ANNEX II. REFERENCES

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

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

.

ANNEX III. IKEW AGENDA

.

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

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

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

.