EU-HYBNET

THIRD REPORT ON STANDARDISATION RECOMMENDATIONS

DELIVERABLE 4.10

Lead Author: PPHS

Contributors: KEMEA, L3CE, Laurea, RISE, ZITiS

Deliverable classification: Public (PU)

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

D4.9 SECOND REPORT ON STANDARDIZATION RECOMMENDATIONS

Deliverable number :	D4.10	
Version:	V1.0	
Delivery date:	07/10/2024	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status:	Ready	
Nature:	Report	
Main authors:	Małgorzata Wolbach, Magda Okuniewska, Rashel Talukder	PPHS
Contributors:	Alexios Koniaris Edmundas Piesarskas Päivi Mattila, Isto Mattila Michael Meisinger	KEMEA L3CE Laurea ZITiS

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	01.07.2024	Małgorzata Wolbach Magda Okuniewska Rashel Talukder / PPHS	First draft and update of the 3rd report template
0.2	16.08.2024	Małgorzata Wolbach / PPHS Alexios Koniaris / KEMEA Edmundas Piesarskas / L3CE Michael Meisinger / ZITiS	Integration of first contributions from partners
0.3	16.09.2024	Małgorzata Wolbach, Magda Okuniewska / PPHS	Final version for review
0.8	2.10.2024	Mihaela Teodor, Valentin Stoian, Ileana Surdu, Cristina Ivan / MVNIA	Review and evaluation form provided
0.9	3.10.2024	Małgorzata Wolbach, Magda Okuniewska, Rashel Talukder /PPHS	Corrections after review. Document ready for submission.
1.0	7.10.2024	Isto Mattila, Tiina Haapanen/ LAUREA	Final review and styling, submission of the document 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 CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The main goal of Task 4.3 (T4.3) within Work Package (WP) 4 "Recommendations for Innovation Uptake and Standardization" is to map the current status and identify needs and possibilities for standardisation in the context of innovations that are seen most promising to fulfil the practitioners' gaps and needs to counter hybrid threats – as it is described in "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) Grant Agreement.

The main objective of this deliverable is presenting how T4.3 partners have mapped the current status and developed recommendations in the area of standardisation, legal harmonisation and best practices[1], with reference to:

a) gaps and needs identified in Work Package 2 (Definition of Needs and Gaps of Practitioners' against Hybrid Threats) especially in "Deeper Analysis, delivery of short list of gaps and needs" (Deliverable 2.11);
b) the most promising innovations identified in the Work Package 3 (Surveys to Technology, Research and Innovations) especially in "Second Mid-Term Report on Improvement and Innovations (Deliverable 3.5);
c) selected feasible innovation areas and projects that counter hybrid threats and foster hybrid threat situational awareness described in Work Package 4 (Recommendations for Innovations Uptake and Standardization) especially in "Third Innovation Uptake, Industrialisation and Research Strategy" (Deliverable 4.6).

Based on the above outlines, Task 4.3 main partners: Polish Platform for Homeland Security (PPHS), Center for Security Studies (KEMEA), Lithuanian Cybercrime Center of Excellence for Training Research & Education (L3CE), Central Office for Information Technology in the Security Sector (ZITiS), started to work on the reports which are presented in this document.

The figure below shows where Work Package 4 is located on the EU-HYBNET structure of work packages and how it is related with other packages.

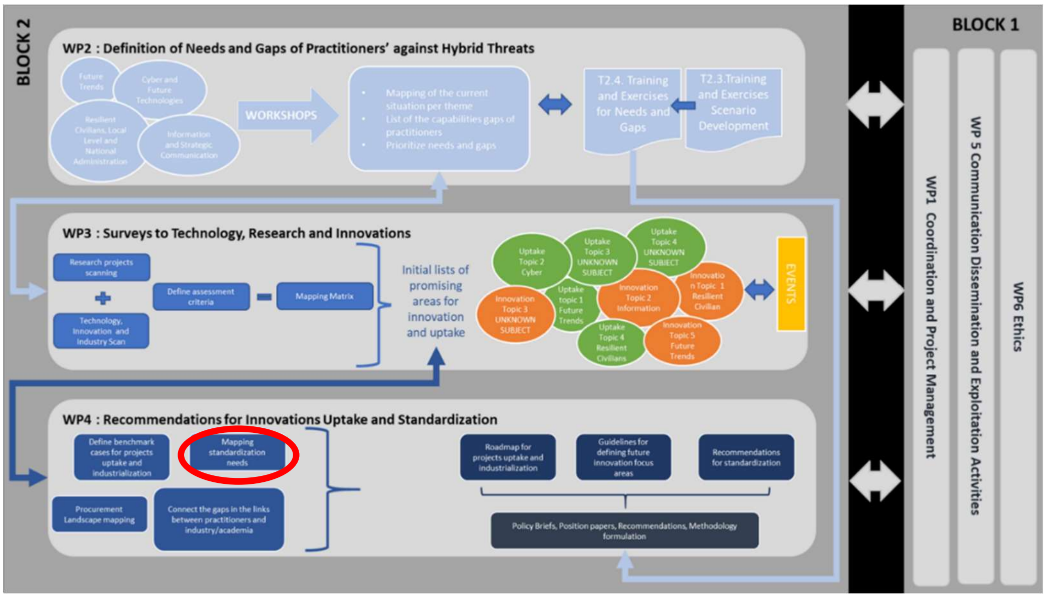

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

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

[1] It is important to underline that official ISO or CEN standards very often are being developed based on best practices.

1.2 METHODOLOGY AND MAIN OBJECTIVES OF TASK 4.3

The main objective of Task 4.3 is the description of the current state of play within the selected areas. The selection of areas to focus on was preceded by a thorough analysis done by Task 4.3 partners of the outcomes of Work Package 2, Work Package 3 and Work Package 4 with major emphasis on:

- Deliverable 4.6 (Third Innovation Uptake, Industrialisation and Research Strategy)
- Deliverable 3.5 (Second Mid-Term Report on Improvement and Innovations).

In Deliverable 4.6 four innovations relating to the EU-HYBNET core themes were selected. Based on D4.6 findings, four areas were selected for T4.3, and the work was distributed among partners:

1. Citizen – Responder Platform (CRP), core theme: Resilient Civilians, Local Level and National Administration) - **ZITiS**;
2. Citizens Reporting Tool (CiReTo), core theme: Future Trends of Hybrid Threats - **KEMEA**;
3. Local Media Hybrid Threats Tracker (LMHTT), core theme: Information and Strategic Communication - **PPHS;**
4. STARLIGHT, core theme: Cyber and Future Technologies - **L3CE**.

Within the aforementioned areas, each partner provided a report which consists of:

- the description of the current state,
- initiatives and documents supported by the relevant links,
- recommendations.

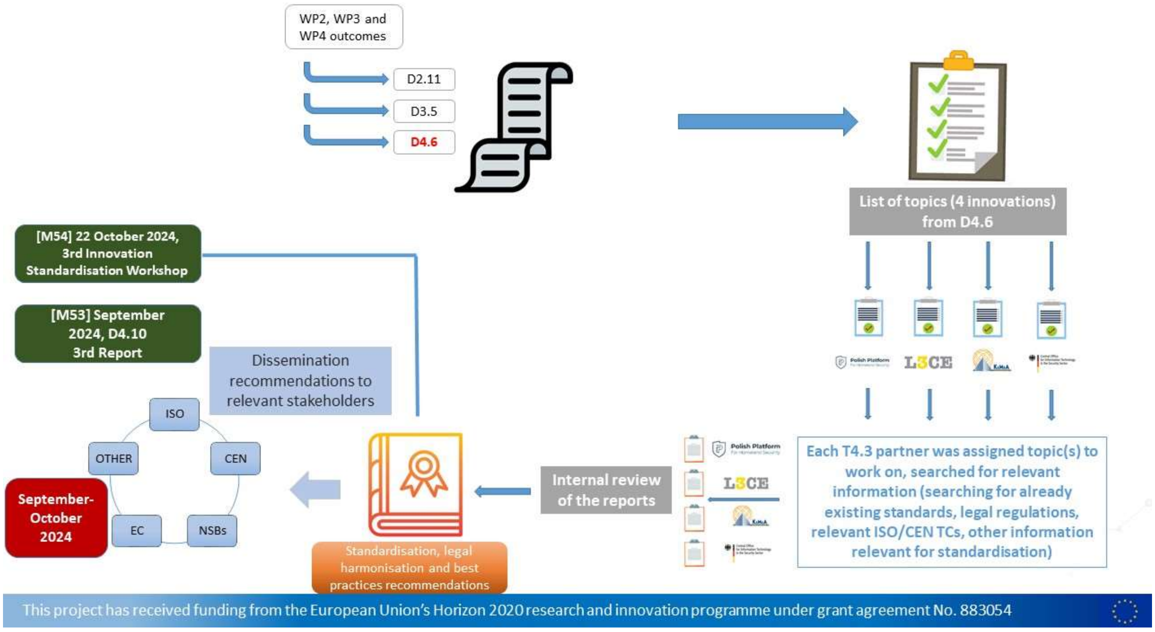
Recommendations provided in the reports from Section 2 of this deliverable are accompanied by a type of recommendation (legal, standard, best practice) and a relevant institution which was identified as the primary institution which should receive a given recommendation for their information and possible future actions regarding this area. Additionally, each recommendation is marked with information whether it is most feasible for implementation in the short, medium or long term.

Findings described in this document are a result of ongoing analysis including desktop research, discussion with experts, consultations with consortium partners and network partners within EU-HYBNET project but under no circumstances should be treated as a complete, finished and exhaustive work. The world of hybrid threats, gaps and needs accompanying them is the environment that is constantly changing. Certain features described in the reports were accurate and up-to-date at the time of reports creation.

In each of the reports described in this deliverable, more general or more specific recommendations (in the area of standardisation, legal harmonisation and best practices) were developed for actions to be taken at the level of the European Union and Member States. The purpose of developing the recommendations is to indicate particularly important aspects in each of the topics, which is proceeded by the description of the current state of play within a given area.

One of the points to be carried out within Task 4.3 is the dissemination of the recommendations to relevant entities and experts that a given recommendation refers to directly or with the idea that they might be interested with the solutions proposed in the report. Each recommendation was addressed to one or more of the institutions operating at the EU level – mostly referring to public institutions, private entities or civil society organisations. Additionally, the reports will be sent to all EU-HYBNET consortium and network members to see if they would like to contribute to any of the state-of-the-art points or recommendations.

The reports will be sent to the identified institutions by Laurea University of Applied Sciences, coordinator of the EU-HYBNET project, and by the Polish Platform for Homeland Security - the leader of Task 4.3 Recommendations for Standardization. Both institutions will monitor feedback from institutions that have received reports with recommendations. Feedback will be consulted among the partners of Task 4.3 and its content will be taken into account, as far as possible, in further project work.


WP2, WP3 and WP4 outcomes
D2.11
D3.5
D4.6
List of topics (4 innovations) from D4.6
[M54] 22 October 2024, 3rd Innovation Standardisation Workshop
[M53] September 2024, D4.10 3rd Report
Dissemination recommendations to relevant stakeholders
ISO
OTHER
CEN
EC
NSBs
September-October 2024
Standardisation, legal harmonisation and best practices recommendations
Internal review of the reports
Each T4.3 partner was assigned topic(s) to work on, searched for relevant information (searching for already existing standards, legal regulations, relevant ISO/CEN TCs, other information relevant for standardisation)
L3CE

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

Figure 2. EU-HYBNET workflow within Task 4.3 (Cycle 3)

1.3 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1: In this section an overview together with methodology is presented.
- Section 2: In this section all the reports from 4 main areas are presented (state of the art, most important documents and recommendations).

Section 2 contains following subsections:

- Description of the Innovation - taken from Deliverable 4.6; Complete and detailed descriptions of innovations can be found in D4.6 Third Innovation Uptake, Industrialisation and Research Strategy;
- State of play related to this specific innovation accompanied by relevant links with the description of state-of-the-art;
- Recommendations – the recommendations presented do not only refer to recommendations for standards per se, but also refer to recommendations for legal harmonisation and identified best practices that EU-HYBNET recommends to follow or be inspired by. It is relevant to underline, that very often best practices are the beginning of development of the official standards (ISO, CEN or national standard). Following this, 3 types of recommendations were introduced:
  - legal
  - standardisation

- best practice

For each recommendation, the probable term of its implementation (short/medium/long) is indicated. The timing of the implementation of the recommendations is due to the complexity of the recommendations, but the following timeframe has been adopted for consistency:

- Short term: up to 1 year
- Medium term: 1-3 years
- Long term: over 3 years

Each recommendation provides relevant institutions which should receive a given recommendation.

- Section 3: In this section it is explained how this deliverable contributes to three lines of actions.
- Section 4: In this section summary and future work are presented.

2. REPORTS

2.1 CITIZEN – RESPONDER PLATFORM (CRP)

Description of the Innovation

The AI Enhanced Disaster Emergency Communications solution, known as the Citizen – Responder Platform (CRP), has been developed to enhance the coordination and efficiency of emergency responses. This platform creates an Information Sharing Environment (ISE) that allows first- and second-line responders to access and utilize real-time, trusted information from citizens during crises. A significant feature of CRP is its ability to detect and mitigate false alarms, including those generated by adversaries aiming to destabilize society through hybrid threat campaigns.

The primary scope of CRP is to provide a secure technological solution for digital information sharing during emergencies. It aims to detect and counter hybrid threats effectively. The vision behind CRP is to ensure that trusted information about emergencies flows directly from citizens to responders while minimizing the impact of false alarms and adversary-driven hybrid threat campaigns.

The mission of CRP is to deliver a standardized, pan-European approach for analysing and verifying the authenticity of citizens' emergency reports. This involves creating methods to identify and address hybrid threats. The strategy for implementing CRP includes several key elements: studying existing solutions and defining a taxonomy for citizen reporting, integrating anonymization techniques to protect privacy, standardizing the reporting process, extending existing reporting protocols, and developing a language-adaptive interface to ensure usability across all EU member states. Additionally, AI-based analytical tools will be developed to authenticate data and differentiate between real and fake information, culminating in a proof-of-concept implementation.

CRP's success relies on the active participation of citizens and tool developers to establish and use information-sharing tools. Advanced AI is crucial for accurate data analysis, and robust security measures are necessary to prevent hacking. Ethical considerations also arise, as citizens might inadvertently violate privacy regulations while reporting incidents.

The rationale for CRP centres on the mantra "Sharing and analysis is the key" to detect hybrid threat-related events. The platform aims to provide accurate information that enables responders to act swiftly and effectively, even in large-scale crises. AI-powered analysis ensures that responders can focus on real emergencies by filtering out false alarms. Furthermore, CRP supports intelligence services by identifying adversaries' false information campaigns, thus aiding in the discovery of hybrid threats. By facilitating EU-level cooperation, CRP aims to enhance resilience and provide a comprehensive, pan-European response to emergencies and hybrid threats, ensuring stability in society.

State of play
The Citizen Responder Platform (CRP) is an innovative technological solution designed to facilitate the trusted exchange of information between citizens and first and second responders in emergencies and crises. This platform is unique in its use of AI-powered analysis and the ability to integrate new services, apps, and tools. While similar systems, such as CISE in the maritime sector, already exist, CRP stands out due to its broad applicability and inclusion of both citizens and authorities. The successful launch and development of CRP require an EU initiative that provides the necessary funding and facilitates integration into the existing systems of EU member states. Existing EU projects could support this effort and enhance the platform's acceptance, particularly through public procurement. However, the implementation of CRP faces several challenges. Technologically, standardized integration processes for apps and services need to be developed, and a robust AI analysis must be ensured to minimize false alarms. Interoperability issues may arise when integrating the platform into the existing systems of first and second responders. User acceptance is another critical factor. It will take time for new approaches to become popular and widely adopted. Intelligence agencies could develop additional interest in CRP if the platform effectively provides information on hybrid threat campaigns. Regulation and ethical acceptance are also important. The platform must comply with data protection regulations and be secure against hacking. Citizens could share videos and information that raise privacy concerns, which could impact societal acceptance. Economic barriers could arise if the costs of building and implementing the platform are too high. Operational barriers exist in implementing the necessary structures and cooperation between various stakeholders. Ultimately, it is crucial to involve and convince relevant practitioners, citizens, SMEs, and the industry in all EU member states of the benefits of CRP to ensure its broad acceptance and use.

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Standardization (Medium Term) • **Data standards** • **Interfaces (API, communication)** • **Security** • **Availability** **Best Practices (Short Term)**	To integrate apps, services, and tools with the CRP platform, a standardized approach is necessary. The platform's AI analysis must be robust to distinguish genuine emergencies from false alarms. Interoperability issues may arise with responders' existing systems. Additionally, intelligence services may need support to identify whether false alarms are part of hybrid threats or actions by uninformed citizens.	**The European Commission** **Ministry Level** **National and Local Authorities**

• **Reporting processes** • **Cyclic testing and practical exercises**		**EU Member States stakeholders (social care workers, police, emergency services, NGOs)**
Legal (Medium Term) • **Privacy Laws** • **Data Protection** • **Liability** • **Security Regulations** **Standardization (Medium Term)** • **Security** • **Availability** **Best Practices (Short Term)** • **Ethical Considerations**	CRP requires advanced AI to ensure accurate and reliable data analysis while complying with existing regulations and laws. The platform must be highly secure to prevent hacking and data leaks. Ethical concerns arise from the potential for citizens to share videos and information without adhering to privacy regulations, which could hinder societal acceptance and the positive impact of CRP.	**The European Commission** **Ministry Level** **National and Local Authorities** **Legislative authority** **Research institutes**
Standardization (Medium Term) • **Data standards** • **Interfaces (API, communication)** • **Security** • **Availability** **Best Practices (Medium Term)** • **Interfaces (API, communication)** • **Reporting processes** • **Cyclic testing and practical exercises** **Legal (Medium Term)** • **Privacy Laws**	CRP aims to facilitate information sharing between citizens and first- and second-line responders through various apps, tools, and solutions during large-scale crises and emergencies. This goal is likely to be well-received by end-users. Providers of these apps, tools, and services may view CRP as a valuable platform to offer their solutions. However, as with any new approach, it may take time for CRP to gain popularity and widespread adoption. If intelligence services recognize CRP's potential to identify signs of hybrid threat campaigns, it could further boost interest in the platform.	**National and Local Authorities** **Ministry Level** **The European Commission** **Legislative authority** **Providers of online services (social media, messenger applications, search engines)** **EU Member States stakeholders (social care**

- **Data Protection** - **Liability** **Security Regulations**		**workers, police, emergency services, NGOs)** **NGOs**
Best Practices (Medium Term) - **Planning of Invest** - **Sharing the costs** - **Cyclic testing and practical exercises** **Legal (Long Term)** - **budgetary law (EU member states, national)**	The development and implementation of the CRP across EU member states could face significant economic barriers due to high costs. These include expenses for advanced technologies, integration with existing systems, and training for responders. Financial constraints may lead to uneven adoption, and ongoing costs for updates and maintenance could create long-term economic challenges. Careful financial planning and potential cost-sharing will be necessary to overcome these barriers and ensure the platform's sustainability.	**National and Local Authorities** **The European Commission** **EU Member States stakeholders (social care workers, police, emergency services, NGOs)** **NGOs**
Best Practices (Medium Term) - **Interfaces (API and User)** - **Reporting processes** - **HowTo Guidelines** - **Ethical Considerations** - **Cyclic testing and practical exercises** **Legal (Medium Term)** - **Privacy Laws** - **Data Protection** - **Liability** - **Security Regulations**	Implementing the necessary operational structures and cooperation for the CRP is achievable, despite current gaps, due to the success of similar services like CISE and the 112 app. These platforms provide a strong foundation and positive user experiences that can be leveraged to ensure smooth integration and widespread adoption of the CRP across the EU. Utilizing existing frameworks reduces risks and fosters quicker acceptance, making it easier to achieve the desired level of information sharing and operational efficiency.	**The European Commission** **National and Local Authorities** **Legislative authority** **NGOs**

2.2 CITIZENS REPORTING TOOL (CIRETO)

Description of the Innovation
The aim of the innovation “Mobile application to pinpoint acts of harassment/violence on the street and online” (or Citizens Reporting Tool – CiReTo for short) is to use readily and widely available technology – i.e. smartphones – to record and geotag acts of harassment and violence (or calls for violence) in physical space as well as online. Such acts may occur in the form of physical action on the street, but also graffiti and/or leaflets in physical space and online. Smartphones integrate three important technologies to conduct such activities: • A clock to timestamp events; • A camera to record events and/or artifacts (action or written text) by video or audio; • A geotagging function to pinpoint where the event occurred. The possibility to report similar or related events online gives the users of the provided information, i.e. mainly law enforcement agencies, the opportunity to monitor evolving situations in real time and note the correlations in physical space and online. The application would be especially useful in crisis situations like riots if used by large number of users.
State of play
Attacks on societal structures and cohesion, both in the form of online harassment, as well as in the form of the spread of violence, present current but also future trends in hybrid threats that need to be challenged. To be challenged successfully, the first signs of such occurrences should be noted in order to provide situational awareness of the threat, if not to provide an early warning. In such a case, the responsible law enforcement agencies could react in a timely manner in both the virtual, but also in physical space and use their resources intelligently according to the situation. Should the situation continue to escalate, the response from rescue services may be needed as a precaution or to assist possible victims. Involving the public in detecting signs of harassment or hybrid threats serves multiple purposes. Firstly, it allows for saving on valuable resources, such as on expensive online monitoring systems or CCTV, or patrolling of the streets. Secondly, it significantly diminishes the required time for discovering and locating occurrences of the above-mentioned threats. Thirdly, it facilitates in society resilience building by providing everybody – especially the youth – with the opportunity and the option of participating in the creation of more security. Smartphones integrate three important technologies to conduct such activities: the clock to have a timestamp on the occurrence; the camera to record the action or written text as video or audio; the geolocation to pinpoint the occurrence on the virtual map. Adding an option to report occurrences online gives the users – law

enforcement agencies and other stakeholders – the opportunity to monitor evolving situations in real time and note the correlations in physical space and online. The application would be especially useful in crisis situations like riots if used by a large number of users.

Integration with other platforms, such as social media, public transportation systems and other platforms to enhance its functionality and reach, in addition to AI and machine learning can be used to predict high-risk areas and times, offering proactive safety suggestions to users.

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Legal Recommendations (Medium Term) • **Privacy Laws and Data Protection** • **Reporting and Liability** • **Security Regulations** • **Intellectual Property**	Privacy Laws and Data Protection recommendations refer to ensuring GDPR (General Data Protection Regulation) compliance for users in the European Union, CCPA (California Consumer Privacy Act) for users in California, USA, HIPAA (Health Insurance Portability and Accountability Act) if handling health-related data in the USA. These recommendations also refer to data minimization in terms of only collecting necessary data and ensuring anonymization where possible, as well as obtaining explicit consent from users before collecting, storing, or sharing their data. Reporting and liability recommendations refer to mandatory reporting laws for understanding and complying with laws related to mandatory reporting of violence or harassment in one's jurisdiction, as well as content moderation, in terms of developing clear guidelines for content moderation to avoid liability issues. Security Regulation recommendations refer to data encryption, both in transit and at rest, as well as to access controls, by implementing robust authentication and authorization mechanisms. Intellectual Property recommendations refer to copyright and trademarks, which are required to ensure non infringement on third-party intellectual property.	**European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online harassment/violence, as well as tech companies developing tools to combat such activities** **EU Member States stakeholders (social care workers, police, teachers, NGOs)** **Providers of online services (social media, private messaging applications, search engines)** **Legislative authority in EU Member States**

		Local and Regional Authorities in EU Member States **Research institutions** **NGOs**
Standardization Recommendations (Medium Term) • **Data Standards** • **Accessibility Standards** • **Security Standards**	Data Standards recommendations refer to interoperability, through the use of standard data formats (e.g. JSON, XML) for data exchange, as well as designing APIs following REST or GraphQL standards for consistency and one again interoperability. Accessibility Standards recommendations refer to following WCAG (Web Content Accessibility Guidelines) to ensure the app is accessible to users with disabilities. Security Standards recommendations refer to implementing an Information Security Management System (ISMS), to be compliant with ISO/IEC 27001, as well as following best practices to address top mobile security threats (i.e. OWASP Mobile Security Project[2]).	**European Commission** **Ministry Level** **National and Local Authorities** **Providers of online services (social media, private messaging applications, search engines)** **Legislative authority in EU Member States** **Research institutions** **NGOs** **Local and Regional Authorities in EU Member States** **EMSA:** The Common Information Sharing Environment (CISE) is an EU initiative which aims to make European and EU/EEA Member

[2] https://mas.owasp.org/

		States surveillance systems interoperable to give all concerned authorities from different sectors access to additional classified and unclassified information they need to conduct missions at sea.
<u>Best Practice Recommendations (Medium Term)</u> • **User Interface and Experience** • **Reporting Mechanisms** • **Community Guidelines** • **Collaboration with Authorities** • **Ethical Considerations** • **Regular Audits and Updates** • **User Education**	User Interface and Experience best practices refer to usability and localization, by designing a user-friendly interface with clear navigation and easy reporting mechanisms, in addition to offering multilingual support to cater to a global audience. Reporting Mechanisms best practices refer to allowing users to report incidents anonymously, as well as implementing a system to verify the authenticity of reports without compromising user privacy. Community Guidelines best practices refer to establishing and enforcing a code of conduct for users, in addition to employing both automated and human moderation to handle reports of harassment and violence. Collaboration with Authorities best practices refer to partnerships with law enforcement and local authorities for effective response and support and the development of clear protocols for escalating serious incidents to the relevant authorities. Ethical Considerations best practices refer to ensuring that algorithms and moderation practices are fair and free from bias and that transparency is guaranteed in how data is used, as well as in the criteria selection for content moderation.	**European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online harassment/violence, as well as tech companies developing tools to combat such activities** **EU Member States stakeholders (social care workers, police, teachers, NGOs)** **Europol** **The Radicalisation Awareness Network (RAN Practitioners)** **The VOX-Pol Network of Excellence (NoE)**

	Regular Audits and Updates refer to conducting regular security audits to identify and fix vulnerabilities and to the regular update of the app to include new features, security patches, and improvements. User Education refers to ensuring and promoting awareness, by providing resources and tips on recognizing and reporting harassment and violence and to offering links to support services and hotlines for victims.	**Providers of online services (social media, private** **messaging applications, search engines)** **Legislative authority in EU Member States** **Research institutions** **Local and Regional Authorities in EU Member States** **NGOs** **EMSA:** The Common Information Sharing Environment (CISE) is an EU initiative which aims to make European and EU/EEA Member States surveillance systems interoperable to give all concerned authorities from different sectors access to additional classified and unclassified information they need to conduct missions at sea.

2.3 LOCAL MEDIA HYBRID THREATS TRACKER (LMHTT)

Description of the Innovation

The Local Media Hybrid Threats Tracker (LMHTT) is a diagnostic tool for mapping potential risks to media pluralism and detecting foreign information manipulation and interference (FIMI) campaigns at regional and local media levels within EU and candidate countries. Designed for academic researchers, media literacy experts, and fact-checkers, the LMHTT enables comprehensive analysis and reporting, helping to alert national security agencies and governments to potential threats to the country and society. By gathering and analyzing data on media ownership, journalistic practices, and content diversity, it supports efforts to improve media pluralism and tackle FIMI campaigns, ultimately supporting to ensure national security and informing policy recommendations.

The rationale for implementing this solution is that it relates to the social domain. Manipulation of media messages and false narratives can cause cleavages in society, polarization and spread disinformation on a wider scale.

State of play

Media at the regional and local level are particularly important for democracy, and their relationship with local citizens tends to be closer if compared to national media. However, local and regional media are receiving less attention in the public discussion and the situation shows that they are increasingly struggling to survive.

The main issues and concerns relating to media pluralism, with a particular focus on the challenges facing local and regional media in the EU and candidate countries, are presented in the latest Media Pluralism Monitor 2024 Report (MPM)[3]. The report provided a comprehensive overview of the media pluralism situation in the European Union (EU) and candidate countries for 2023. The average risk level for media pluralism has generally increased across the EU and candidate countries, indicating a growing concern for media diversity and freedom. The report highlights a significant increase in risk concerning local and regional media. This is mainly due to the existence of the threat called "news deserts" - defined as "geographic or administrative area, or a social community, where it is difficult or impossible to access sufficient, reliable, diverse information from independent local, regional and community media” - in many countries, where local media outlets have diminished or disappeared altogether. Moreover, local and regional media are particularly vulnerable to economic pressures. The report notes a deepening crisis in the economic sustainability of local media, with traditional revenue models continuing to decline. Innovative practices and new models have not yet fully countered these challenges. This situation can also have a major impact on pluralism and media freedom.

As the report showed, many countries lack specific legal safeguards for local and regional media, which contributes to the overall increase in risk. The absence of dedicated support mechanisms and policies to sustain these media outlets makes them particularly vulnerable. Moreover, the indicator on media viability, which includes local and regional media, showed that economic situation has affected media revenue, with local media being the hardest hit. Employment within these outlets also remains

[3] https://cadmus.eui.eu/handle/1814/77028

precarious. When it comes to market plurality, the report showed that no country is at low risk. The Market Plurality area scores at high risk at 69%, the same level registered in the MPM2023. The main risks in this area have the source in the concentration of media ownership and the concentration in the digital markets, which are threatening the media pluralism.

The MPM2024 also found average risk of spreading disinformation high (71% for all countries studied). It has been found that there is a lack of comprehensive strategy that defines the role of different stakeholders involved and only six countries have taken significant steps to develop comprehensive strategies against disinformation.

Another point, which is not a new issue, is gender equality in media. It is an integral part of human rights that everyone shall care about and respect. It is a part of media social inclusiveness that is a key element of media pluralism. According to the report, there is an average medium or high risk when it comes to gender equality in media landscape.

The above findings highlight the crucial role of local and regional media in maintaining media pluralism and ensuring that diverse voices are heard in all regions. The decline of these media outlets poses a serious threat to the democratic process, and therefore encourages emerging FIMI campaigns and the spread of disinformation.

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Standardisation (implementation and maintenance) **(Medium Term)**	**For implementation of LMHTT:** Design a comprehensive LMHTT diagnostic tool by defining standardized procedures for data collection and reporting in a questionnaire. Develop comprehensive data analytics tools and an interactive dashboard for data visualisation. Delegate the maintenance of the LMHTT tools to a competent body, possibly ENISA. To integrate local/regional services, and tools with the LMHTT platform.	**The European Commission** **Ministry Level** **National and Local Authorities**
Legal (general recommendation) **(Long Term)**	**Establish clear, comprehensive gender equality policy as a social policy to all EU Member States and candidate countries** Social policies have the most prominent role in promoting gender equality. Since not all EU countries have gender equality policy, all EU states should implement some kinds of gender equality policy. Clear and comprehensive gender equality policy would strengthen the rights of women in media. Gender equality policies have a major impact on the equity in the labour market, access	**EU MS governments and governments of candidate countries**

	to employment, protection of groups and special vulnerability situations and thus significantly promote gender equality.	
Legal (market plurality) **(Long Term)**	**Establish common rules for the proper functioning of the internal market for media services with the strong focus on safeguarding independence and pluralism** (European Media Freedom Act). Establish harmonized law for media pluralism. The rules would promote independence of media and would protect journalists from external and internal influences. Legal framework to ensure independence of the media and safeguard media pluralism - Freedom of Expression (coe.int) European Media Freedom Act - European Commission (europa.eu)	**EU governments**
Best practice (market plurality) **(Short Term)**	**Create media ownership monitoring system that displays state-based ownership information database.** It contributes to transparency of media ownership. European Media Freedom Act - European Commission (europa.eu)	**Regulatory authorities**
Best practice (disinformation) **(Medium Term)**	**The need to define and establish a comprehensive strategy or action plan that focuses on the role of various stakeholders in protecting the EU against disinformation** (Ireland - a National Counter-Disinformation Strategy Group created in 2023, Estonia- having strategy combating disinformation focusing on 5 core elements, Lithuania- National Crisis Management Centre).	**Representatives of EDMO, EU governments, representatives of technological companies**
Best practice (disinformation, FIMI) / Legal **(Medium/Long Term)**	**Create/develop initiatives promoting digital literacy among the public**. This is to increase media literacy in the EU states, raise public awareness of disinformation in media and what impact it has on the civil society. Education of the public about the dangers of disinformation is crucial. There are multiple initiatives focused on promoting media literacy, for example EDMO, but there are also systemic solutions necessary on national and EU level.	**NGOs, Ministry of Education, EU governments, European Commission**
Standardisation **(Short Term)**	The ultimate goal of the "Journalism Trust Initiative" is to support the universal, individual freedom of opinion through access to information and independent, pluralistic media. The application of JTI means safeguarding professional standards, a more healthy digital media landscape should emerge, from which each citizen and media worker, but also societies at large, could benefit.	**Association of European Journalists**

	CEN/WS JTI - Journalism Trust Indicators	

2.4 STARLIGHT

Description of the Innovation
The initial concerns raised in the 3rd EU-HYBNET project cycle were around artificial amplification. This is one of the aspects to be considered on social platforms. There are many others, like spreading disinformation, hate speech, call for unrest, deepfakes, use of forbidden symbols, radicalisation and many others. Social platforms became a handy hybrid threat tool for different actors. The uptake recommendation, described in T4.2 D4.6, is focused on LEA specific tools and solutions, designed to fight disinformation and misinformation, that are developed specifically for them and are not available for other users. Specifically, this is the currently ongoing STARLIGHT project. There are two aspects of the Starlight considered useful for further exploitation. One is the primary aim of the project – development of AI supported tools for LEA. The other aspect is related to the methodology applied. D4.6 presents both aspects to be considered for up-take. First, we will introduce the technical developments of the Starlight project. The scope of the project covers development of a wide range of tools, supported by AI. They are grouped together according to their functionalities and intended use. One of them is disinformation and misinformation, directly related to the subject of hybrid threats. This group 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. Solutions under development include many different functionalities, including detection of DeepFakes, Forbidden symbols, bots, SPAM, also evaluation of content toxicity, clustering of reposting chains and others. Besides the technological solutions of the project, Agile co-development methodology, applied in the project implementation, is also pointed as a good practice. The project is organised in a way that there are co-development cycles in each of the target groups. Co-development means that each group has potential end-users of the solutions under development. Development is done based on aligned expectations, end-users provide use cases and are involved in the overall development process. Each co-development cycle ends up with the ToolFest, where all solutions are presented to end-users. Such an approach provides benefits for both developers and end-users. Developers are getting to understand the realistic needs of end-users during the development, so they can adjust functionalities, interface or other aspects during the early stage. At the same time, end-users can understand the solution better, get to know how they can use it and what results they can expect. Early involvement and co-development are essential for the uptake process. Such an approach can also be applied in other projects or uptake process in general.
State of play

At the time of writing this document Starlight project is still in progress and a limited number of final tangible results are produced. Technological solutions are still under development and will be made available at the end of the project. There are 3 different exploitation paths planned. Solutions expected to be made available through Europol, EACTDA on project own repository. Specificity of those solutions is that they are specifically tailored for LEA's and are not planned to be available for the wider audience, even though they are very relevant for different hybrid threats related practitioners. Thus, no particular recommendation can be formulated regarding standardisation. At this stage LEA's as EU-HYBNET project Network Members can be encouraged to follow developments in the Starlight project.

While the methodological approach can be explored and adopted by many other institutions beyond LEA. During the implementation of the project, the co-development methodology gained a lot of end-users' interest and involvement. Similar approaches with some modifications are also applied in other initiatives. EACTDA activities are end-user focused and they are involved in the evaluation and testing of innovative solutions at different stages. Concept of "test before invest" is also gaining popularity in many sectors. In the given circumstances this approach is rather novel for the security sector, especially LEA's, as they traditionally tend to be rather closed ecosystems. Uptake of innovative solutions and co-development is not a common practice in those institutions. There is no final evaluation of the efficiency and impact of the practice in scope, but current developments indicate good results.

Recommendation: Legal/Standardization/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations from the Starlight project at this stage can be considered as <u>best practice.</u> (short/medium/long term)	Long term (2-5 years) co-development, involving solution developers and end-users in security sector could influence the innovation up-take process in the domain heavily. Co-development can be described in more details, as joint efforts can be challenging to implement. The main reason is difference of relevant components – solution developers are focused on technological aspects (Solution internal components), while users are concerned with results (external components of the solution). Following the practice in Starlight project a few success factors can be highlighted: - Technical development preferable to be separated from the co-development process. There are separate meetings organised for technical development of tools. Data formats, pipelining, integration and other technical details are discussed. While other meetings, where end-users are involved are focused on inputs (e.g. data sources) and outputs (e.g. interface, accuracy, interface, etc.) aiming to understand the results and how they can be used (e.g. used as evidence, etc.). - Pace of work should be also rather intense. As co-development might take more than a year, sometimes few years, there should be some milestones	**All institutions in the security domain, ranging from policy makers to operational level.**

	for assessing the progress, relocation of resources, reprioritisation of functionalities and other changes. In Starlight project one co-development cycle is one year. Each cycle ends with ToolFest where solutions are presented and evaluated by wider group of end-users. Working meetings are organised on weekly – biweekly bases. One of the questions is how to include such practice into daily routine of security related organizations. This can be facilitated by dedicated financial instruments aiming to involve organisations in earlier stages of solution development. One of such instruments can be considered pre-commercial procurement or GovTech Lab in Lithuania. Such practice could also be facilitated by recommendations from policy makers or stakeholders to include innovation co-development related strategic measures and KPIs.	

3. THE THREE LINES OF ACTION

The EU-HYBNET needs to report to the EC on Three Lines of Action. Each deliverable should state and explain how it contributes and have provided input and results to the EC Three Lines of Action. Below you will find Task 4.3 contribution:

1) monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results
D4.10 contribution: During development of standardisation recommendations in the third
EU-HYBNET cycle, partners of T4.3 were analysing also what research and innovation projects are bringing to practitioners. Many of the recommendations or identified best practices are based on research and innovation projects and activities, conducted in Europe but also outside Europe. This analysis is a relevant input to the EU-HYBNET's Objective 4 goal 4.3. in order to develop a mapping matrix connecting gaps and needs of European actors to areas that highlight the most promising innovations in different domains.
D4.10 contributes also to the EU-HYBNET's Objective 4 goal 4.1. T4.3 recommendations refer also to the industrialisation and to public procurement. These recommendations are an important input concerning the appraisal of best innovations (both technical and non-technical).

2) common requirements as regards innovations that could fill in gaps and needs:
D4.10 contribution: Many of the described above recommendations are related to technological and non-technological innovations. It should be underlined that even best practices from one country can be innovative in many others. D4.10 contributes also to the EU-HYBNET's Objective 2, goal 2.4. enabling to define common requirements for new research and innovation possibilities that can fill knowledge gaps and enhance capabilities endeavours concerning hybrid threats. Above recommendations suggested key focus research, innovation areas and actions for the future in the field of countering hybrid threats.

3) priorities as regards of increasing knowledge and performance requiring standardisation.
D4.10 contribution: Many of the above described recommendations are related to increasing (disseminating) knowledge and performance related to standardization, also non-technological and technological innovations linked to the increase of knowledge and skills. It is not necessary to list all examples here, as it would be repeating what was written and described in this deliverable's standardisation recommendations reports.

4. CONCLUSION

4.1 SUMMARY

In "Third Report on Standardisation Recommendations" we have described the 4 areas selected to focus on in this deliverable and to construct the reports around them. In Section 2 we provide the most important aspects connected with selected areas happening currently together with offered recommendations linked to the innovations' recommendations for standardization. Section 3 presents three lines of actions.

Authors of this deliverable would like to highlight that within Task 4.3 of EU-HYBNET, we are working not only on recommendations for standards *per se*, but also on recommendations for legal harmonisations and identified best practices, which EU-HYBNET project recommends to use or be inspired by the best practices. It is relevant to underline, that very often best practices are the beginning of development of the official standard (ISO, CEN or national standard).

Due the fact that standardisation process is taking at least 2-3 years to develop the standard, we can observe that it is very difficult to keep standards in line with rapid changes in the area of hybrid threats. There are relevant standards related to safety, physical security and cybersecurity in general, but these standards mostly aren't tailor-made for hybrid threats described in this deliverable.

4.2 FUTURE WORK

T4.3 partners will share information collected in deliverable D4.10 with relevant stakeholders, in particular CEN, CENELEC and ISO technical committees, as well, through WP5 (communication and dissemination), with all other organisations, agencies, institutions and projects working in the area of countering hybrid threats.

Moreover, in M54 (October 2024), consortium partners, network members, experts, practitioners and invited guests will meet in Brussels (Belgium) for the 3rd Innovation Standardisation Workshop. The workshop will be the opportunity for in-depth discussions focused on selected recommendations described in this report.

In the final, fourth project cycle, the state of play will be revised and adapted based on the outcomes of EU-HYBNET reports created in the previous three cycles within other tasks relevant for recommendations for standardisation, especially T4.2 (Strategy for Innovation uptake and industrialisation).

ANNEX I. ACRONYMS

Term	Definition
AI	Artificial Intelligence
API	Application Programming Interface
CCPA	California Consumer Privacy Act
CEN	The European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CISE	The Common Information Sharing Environment
EACTDA	European Anti-Cybercrime Technology Development Association
EDMO	European Digital Media Observatory
EEA	European Economic Area
ENISA	The European Union Agency for Cybersecurity
EC	European Commission
EU	European Union
FIMI	Foreign Information Manipulation and Interference
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ISE	Information Sharing Environment
ISO	International Organization for Standardization
ISMS	Information Security Management System
JTI	Journalism Trust Initiative
KPI	Key performance indicators
LEA	Law Enforcement Agency
MS	Member state
NGO	Non-governmental organisation
SMEs	Small and medium-sized enterprises
WCAG	Web Content Accessibility Guidelines