FINAL REPORT ON STANDARDISATION RECOMMENDATIONS

DELIVERABLE 4.11

Lead Author: PPHS

Contributors: KEMEA, L3CE, Laurea, 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 STANDARDISATION RECOMMENDATIONS

Deliverable number :	D4.11	
Version:	1.0	
Delivery date:	01.04.2025	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status:	Final	
Nature:	Report	
Main authors:	Małgorzata Wolbach, Magda Okuniewska, Kacper Murawa, Rashel Talukder	PPHS
Contributors:	Edmundas Piesarskas	L3CE

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	09.01.2025	Małgorzata Wolbach Magda Okuniewska Rashel Talukder / PPHS	First draft, creation of a table of contents and methodology
0.2	13.02.2025	Małgorzata Wolbach Magda Okuniewska Kacper Murawa / PPHS	Second draft, Integration of contributions for the Reports section
0.3	26.02.2025	Małgorzata Wolbach Magda Okuniewska Kacper Murawa Rasel Talukder / PPHS	Third draft
0.4	14.03.2025	Małgorzata Wolbach Kacper Murawa / PPHS Edmundas Piesarskas / LC3E	Integration of contribution from partner
0.5	17.03.2025	Małgorzata Wolbach Kacper Murawa / PPHS	Final version for review
0.6	25.03.2025	Petteri Partanen / LAUREA Michael Meisinger / ZITiS	Review and evaluation form provided
0.7	31.03.2025	Magda Okuniewska, Kacper Murawa Małgorzata Wolbach / PPHS	Corrections after review. Document ready for submission.
1.0	01.04.2025	Tiina Haapanen / LAUREA	Document finalization, submission to EC

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The main goal of Task 4.3 (T4.3) within Work Package 4 (WP4) "Recommendations for Innovation Uptake and Standardisation" 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 areas of standardisation, legal harmonisation and best practices[1] during the final EU-HYBNET cycle, with reference to:

a) gaps and needs identified in Work Package 2 (Definition of Needs and Gaps of Practitioners' against Hybrid Threats) especially in "Final Gaps and Need Evaluation" (Deliverable 2.8);
b) the most promising innovations identified in the Work Package 3 (Surveys to Technology, Research and Innovations);
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 Standardisation).

Based on the above outlines, the main partners of T4.3 - Polish Platform for Homeland Security (PPHS), Centre for Security Studies (KEMEA), Lithuanian Cybercrime Centre 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.

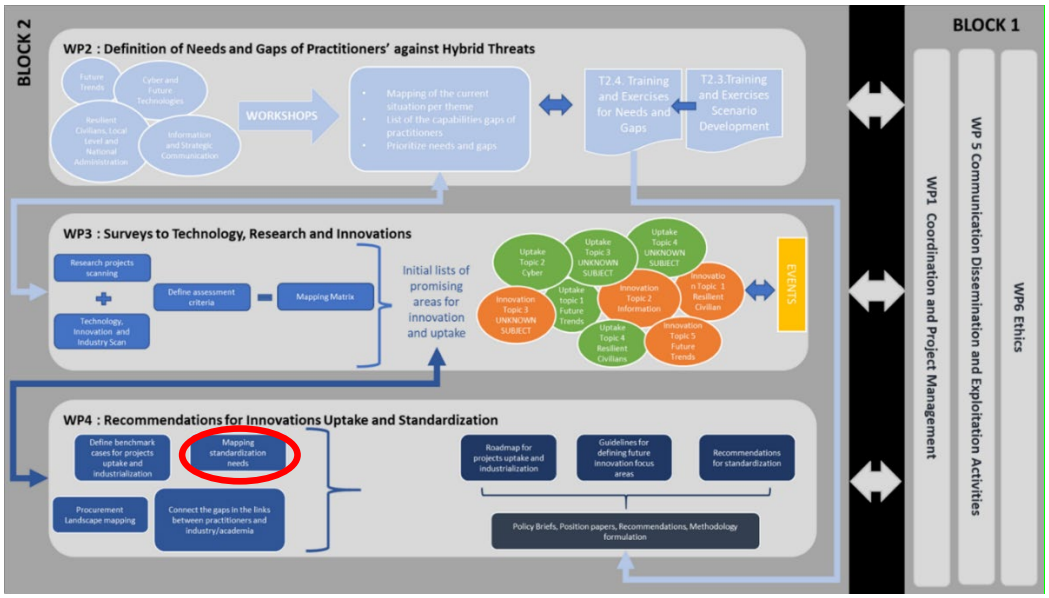

Figure 1. EU-HYBNET Structure of Work Packages and Main Activities

[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 purpose of this deliverable is to present a final analysis based on the findings of all *Reports on Standardisation Recommendations* prepared throughout the entire five-year project cycle, including:

- D4.8 First *Report on Standardisation Recommendations*
- D4.9 Second *Report on Standardisation Recommendations*
- D4.10 Third *Report on Standardisation Recommendations*

The state of play was reviewed and adapted based on the outcomes of EU-HYBNET reports created in the previous cycles. The authors have re-examined all identified recommendations from the project's duration, as documented in the above-mentioned reports, and compiled the *Final Report on Standardisation Recommendations*.

This report is structured around the Four Core Themes of the EU-HYBNET project:

- Future Trends of Hybrid Threats
- Cyber and Future Technologies
- Resilient Civilians, Local Level and National Administration
- Information and Strategic Communication

For each Core Theme, a separate report has been developed, including the following elements:

- The original description of the EU-HYBNET Core Theme
- A bullet-point summary of the current situation, highlighting the main issues and main needs
- Recommendations for the respective area

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 (up to 1 year), medium (1-3 years) or long term (over 3 years). 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.

Findings described in this document are a result of analysis of the previous reports within T4.3, ongoing analysis - including desktop research, discussion with experts, consultations with consortium partners and network partners within EU-HYBNET project. However, under no circumstances should they be considered a complete, final or exhaustive work. The landscape of hybrid threats, along with the gaps and needs associated with them, is constantly evolving. Certain aspects described in the reports were accurate and up-to-date at the time of their report.

One of the key actions within T4.3 is the dissemination of recommendations to relevant entities and experts—either those directly addressed by a given recommendation or those who may have an interest in the proposed solutions. Each recommendation has been directed to one or more institutions operating at the EU level, primarily public institutions, civil society organisations, or private entities. Additionally, the reports will be shared with all EU-HYBNET consortium and network members to determine whether they wish to contribute to any state-of-the-art points or recommendations. The identified institutions will receive the reports from Laurea University of Applied Sciences (the coordinator of the EU-HYBNET project) and the Polish Platform for Homeland Security (the leader of

Task 4.3: Recommendations for Standardisation). Both institutions will monitor and track feedback from the recipients of the reports.

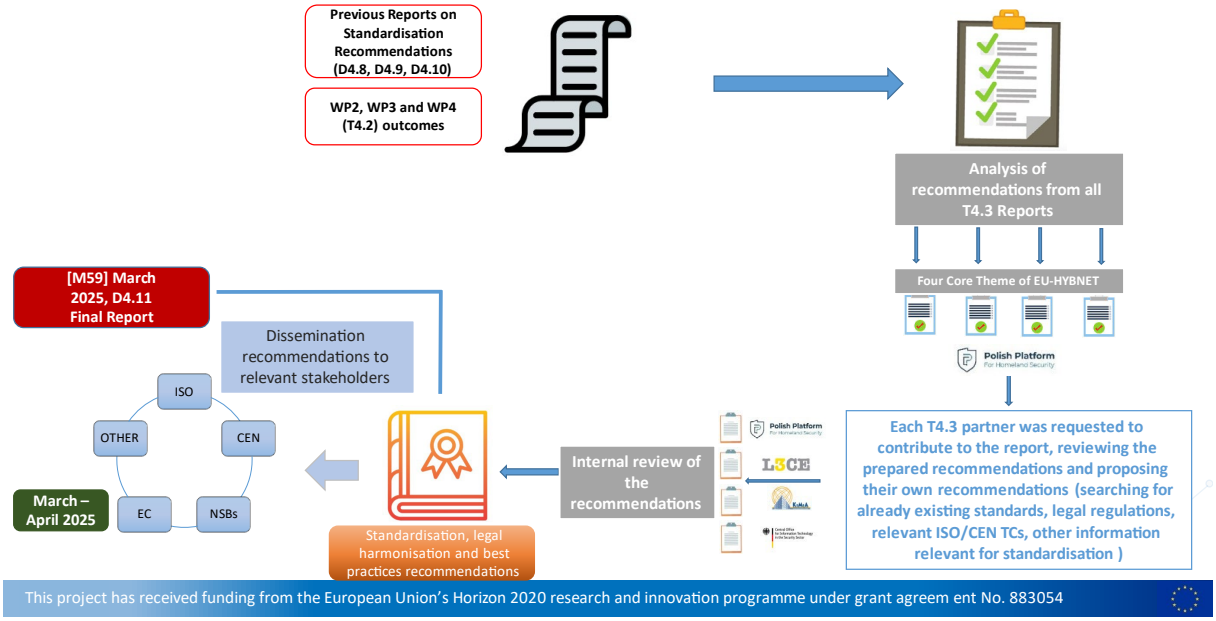

Figure 2. EU-HYBNET workflow within Task 4.3 (Final Cycle)

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 under the four Core Theme of the EU-HYBNET (core theme description, state of play, recommendations).
- Section 3: This section explains how this deliverable contributes to the Three Lines of Action.
- Section 4: This section presents a summary.

Section 2 contains following subsections:

- Original description of the EU-HYBNET Core Theme
- State of play for this specific Core Theme following the analysis of the three previous reports.
- Recommendations - the presented recommendations go beyond standardisation alone; they also include recommendations for legal harmonisation and identified best practices that EU-HYBNET suggests following or drawing inspiration from. It is important to emphasise that best practices often serve as the foundation for the development of official standards (ISO, CEN, or national standards). Based on this, three types of recommendations have been introduced:
  - legal
  - standardisation
  - best practice.

For each recommendation, the estimated implementation timeframe (short, medium, or long term) is indicated. The duration of implementation depends on the complexity of the recommendation. To ensure consistency, the following timeframes have been adopted:

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

- Long term: over 3 years

Each recommendation specifies the relevant institutions that should receive it.

2. REPORTS

2.1 CORE THEME: FUTURE TRENDS OF HYBRID THREATS

EU-HYBNET CORE THEME: FUTURE TRENDS OF HYBRID THREATS

To analyse trends has become even more vital than before due to the changed security environment. Hybrid Threats are by character difficult to detect. However, without detection, countering becomes difficult and responses might always be two steps behind. Hybrid threats also have an ever-changing nature. Approach seldom repeats itself and combination of tools is tailor made for the target. For this reason, analysis relating to different security related trends will be essential to be able to have foresight and build early warning systems.

Hybrid threat trend analysis needs to be multidisciplinary and multidimensional using also scenario-based thinking. The future trends of hybrid threats cover also the three other EU-HYBNET themes connecting them to wider security context. This will strengthen situational awareness and identify new and emerging capability needs for countering hybrid threats.

State of play

Main issues:

1. Detection and awareness gaps: current early detection mechanisms are inadequate, relying on fragmented intelligence-sharing practices. A lack of cross-border cooperation and standardisation hinders real-time threat identification and response coordination, leaving the EU vulnerable to rapidly evolving hybrid threats.
2. Vulnerability in critical sectors: limited screening protocols for Foreign Direct Investments (FDI) increase the risk of foreign interference in critical sectors. Additionally, the underdevelopment of Public-Private Partnerships (PPPs) leaves critical infrastructure and essential services exposed to hybrid threats. A foresight approach involving scenario modeling could help identify potential vulnerabilities in advance.
3. Data governance challenges: inconsistent regulations and uncertainties in data ownership and sharing frameworks weaken digital security. Vulnerabilities arise from poorly defined data-sharing practices, which can be exploited in hybrid threat scenarios.
4. Supply chain fragility: existing supply chain monitoring tools fail to address services and overlook geopolitical risks. The limited use of digital twins without integrated geopolitical modeling prevents effective disruption simulations and contingency planning. Foresight-based digital twin simulations, incorporating foresight methodologies, such as horizon scanning, can help identify emerging data exploitation threats.
5. Public engagement deficit: low public awareness of hybrid threats and insufficient promotion of citizen reporting tools (e.g., mobile apps) result in underutilized community participation in threat detection and situational awareness.

Main needs:

1. Enhanced situational awareness: establish a network of national situation centres supported by cross-border intelligence-sharing protocols to enable real-time detection and coordinated responses to hybrid threats.
2. Strengthened state capacities: Develop strict regulatory frameworks to address vulnerabilities in FDI screening, data-sharing protocols, and social media platform regulations to protect democratic institutions and critical sectors, incorporating foresight tools like risk forecasting and impact assessments to address emerging vulnerabilities.
3. Resource sharing and best practices: Promote EU-wide adoption of PPP frameworks with standardised protocols for crisis response, ensuring joint public-private efforts to mitigate hybrid threats.
4. Multidimensional threat analysis: integrate advanced hybrid threat modeling into digital twins with foresight-based scenario planning, including simulations of geopolitical crises and cascading effects to enhance supply chain resilience.
5. Public Awareness and Engagement: Launch targeted public awareness campaigns emphasizing the importance of citizen participation in threat detection. Provide accessible reporting tools with strong privacy safeguards to foster public trust and participation in security initiatives.

Recommendation ***Legal/Standardisation/Best Practices*** ***Short term: up to 1 year, Medium term: 1-3 years*** ***Long term: over 3 years***	**Explanation on recommendation**	**Relevant Institution**
Legal (Short term)	**Establish a Network of National Situation Centres** Develop a centralized EU-wide intelligence-sharing platform with secure channels, real-time data exchange, automated threat detection tools, and collaborative analytical exercises. Incorporate a foresight approach by utilizing trend analysis, predictive analytics, and scenario planning to identify emerging hybrid threat patterns. Establish protocols for sharing foresight insights with EU Member States to support predicting measures.	European Commission, EU Member States
Standardisation (Medium term)	**Develop EU-wide FDI screening standards** Introduce a unified framework for foreign direct investment screening, including risk indicators, cross-border information-sharing protocols, and a standardised review mechanism for high-risk acquisitions to secure critical assets.	European Commission, European Council

Best Practices (Short term)	**Strengthen Public-Private Partnerships (PPPs) for strategic assets** Introduce a unified framework for foreign direct investment screening, including risk indicators, cross-border information-sharing protocols, and a standardised review mechanism for high-risk acquisitions to secure critical assets.	European Commission, European Council
Legal (Medium term)	**Enforce data-sharing standards with privacy protection** Implement legislative measures requiring secure data-sharing protocols with strong privacy safeguards, such as encryption and anonymization. Develop an oversight mechanism for regulatory compliance and regular audits.	European Parliament, European Data Protection Board
Standardisation (Long term)	**Incorporate hybrid threat modeling into Digital Twins for supply chains** Develop EU-wide standards for digital twin technologies to simulate and analyse hybrid threat scenarios such as cyberattacks and geopolitical disruptions. Implement a foresight approach by integrating future-oriented simulations, stress-testing supply chains under various hypothetical scenarios, and using predictive models to assess cascading effects and disruptions. Ensure that digital twins provide actionable insights for adaptive contingency planning.	CEN, CENELEC, European Commission
Best Practices (Short term)	**Promote use of reporting tools such as *Citizen Reporting Tools (CIRETO)*** Initiate multilingual outreach campaigns to raise awareness of citizen reporting tools such as CIRETO. Offer interactive tutorials, incentivize participation through gamification, and encourage public involvement via partnerships with local communities.	Law enforcement agencies, EU Member States
Legal (Medium term)	**Enforce stricter social media regulations** Introduce new legislative measures to combat disinformation on social media platforms. Ensure transparency in political advertising, impose clear content moderation rules, and mandate rapid response mechanisms for harmful content removal.	European Parliament, European Commission
Standardisation (Medium term)	**Develop cybersecurity protocols for digital services** Establish EU-wide cybersecurity protocols covering encryption standards, incident response frameworks, multi-factor authentication, and regular security testing. Adopt a foresight approach by developing predictive models to anticipate emerging cyber threats and vulnerabilities, leveraging trend analysis and threat	ENISA, European Commission

	intelligence sharing to address evolving risks. Include future-proofing measures to adapt protocols as technologies and threat landscapes change.	
Best Practices (Long term)	**Conduct scenario-based training for hybrid threat response** Organise multi-stakeholder annual simulation exercises on hybrid threat scenarios. Publish after-action reports to share insights and highlight improvements, ensuring cross-agency coordination and preparedness.	European Commission, European Defence Agency

2.2 CYBER AND FUTURE TECHNOLOGIES

Cyber and Future Technologies
At present, cyber is treated as a domain of activity or knowledge where there are no rules. With regards to hybrid threats specifically, cyber and future technologies are key components through which new developments produce not only new kinds of hybrid threats, but also act as powerful countering measures in the fight against such threats. Todays' technological upheavals and those of the future suggest that the portfolio of tools used in the realm of hybrid threats will continue to expand rapidly. Computers are ubiquitous, and getting smaller, while processing power is increasing at enormous rates. Other fundamental breakthroughs include robotics, nano- and biotechnologies, artificial intelligence, sensor and 5G technologies. Taken together, these technologies connect symbiotically with people; and they structure society in all spheres – from the interpersonal to the social, and to the military. To be sure, communication technologies are driving these developments, there is still a great deal to learn about how an adversary can make use of these new tools and technologies, how cyber is connecting areas previously not connected to realm of security, like hospitals, and how we can in fact use these same tools to detect and counter hybrid threats.
State of play
Main issues: 1. The EU technologies of the future, related services and initiatives are among others: 5G, AI, Big Data, Tackling online disinformation, Internet of Things and Quantum Computing. 2. As technology develops strikingly fast, new challenges have arisen, namely Deepfakes. These are videos, images and video clips that are created using Artificial Intelligence for instance to manipulate or replace a person's likeness or voice. They use machine learning techniques as deep neural networks to create highly realistic content that can be a source of disinformation, and harmful for the broader society. In the past, creation of realistic synthetic output required a lot of expertise, time and money; however now, due to AI automated processes, it happens in fraction of the time, giving striking results. 3. With the emergence and continuous development of AI technologies, new opportunities for cyber criminals to launch and spread harmful cyberattacks have emerged. 4. Big Data is linked to large and complex data sets that traditional data processing tools cannot effectively manage or analyse, hence it demands cost-effective and innovative forms of information processing for enhanced insight and decision making. There is a concern that these information assets can facilitate various ethical issues; political influencing, breach of personal data protection and privacy if not adequately regulated.

Main needs:

1. Having regard to these technological advancements, cybersecurity measures as securing network and information systems in the EU are essential to promote cyber-resilience. As a result, citizens and businesses have access to trustworthy services and digital tools.
2. The need of IT- Security certification with regards to international cybersecurity standard ISO 27001 for Big Data and all businesses dealing with data of individuals has been brought into attention so to guarantee compliance with the basic rules for information safety.
3. A relatively novel approach; co-development methodology is gaining popularity and should be explored and adopted by many other institutions beyond LEAs to make it a common and cost-efficient practice.

Recommendation ***Legal/Standardisation/Best Practices*** ***Short term: up to 1 year, Medium term: 1-3 years*** ***Long term: over 3 years***	**Explanation on recommendation**	**Relevant Institution**
Standardisation HiPEAC Vision 2025 (long term)	**Enhancing Automated Cybersecurity using Artificial Intelligence** There is a strong need to encourage research and develop tools on: - advanced threat detection AI models, based on deep learning, graph-based analysis, natural language processing and large language models to improve detection and monitoring capabilities - autonomous threat mitigation systems that can perform automatic actions such as isolating compromised components of NCP (Next Computing Platform), applying patches to vulnerabilities, restoring services. The use of EU-based open AI models should be favoured so to boost EU cybersecurity. It is the power of AI-driven algorithms that can scrutinize extensive datasets to find deviations from standard behaviour and identify anomalies very quickly. As a result, threat detection time is minimal. Development of AI technologies that bring about automated threat detection and incident response enhances adjustment to emerging threats, thus promoting advanced security and functional defence strategies.	European Commission Directorate-General for Communications Networks, Content and Technology, European Commission Directorate-General for Migration and Home Affairs, ENISA

Legal (long term)	**The harmful use of synthetic media such as Deepfakes should be regulated** Deepfakes fall under the wider category of AI- generated 'synthetic media'; they appear in the form of videos, images or audio clips. The specific harms and capabilities of synthetic media should be addressed and specific law, such as UK's legislation that made creation and distribution of sexually explicit deepfakes a criminal offence, should be enforced. In addition, social media platforms could be exploited in dealing with synthetic media since they exert major control over a wide range of content compared to State-level actors.	The Ministry of Justice (all EU Member States), EU AI Board, EU legislators/ governments
Legal (long term)	**Regulated use of Big Data methods in political campaigns** Unregulated use of large personal data for political purposes not only violates the privacy rights of voters, but also has the potential to jeopardize the future of the democratic process. Key regulatory and ethical issues resulting from mining, using and storing vast amounts of voter data should be addressed and resolved. It would mitigate political micro-targeting and its potential to influence opinions, mobilize supporters and ultimately get votes.	European Commission DG EAC-Education, Youth, Sport and Culture-EAC.B Youth, Education and Erasmus+, European Parliament-Committee on Culture and Education, European Economic and Social Committee: Section for Employment, Social Affairs and Citizenship
Best Practices/ standardisation (medium term)	**IT Security certification (ISO 27001) should become mandatory for all businesses dealing with data of individuals and Big Data as well** ISO 27001 is the world's best-known standard for information security management systems that promotes security of data. IT- security certification (ISO 27001) must become mandatory for all businesses dealing with data of individuals as well as in the field of Big Data.	European Commission Directorate-General for Communications Networks, Content and Technology, European Commission Directorate-General for Migration and Home Affairs
Standardisation (medium term)	**Creating Big Data ethical framework** There should be a dynamic multi-stakeholder process designed to capture the latest science on privacy, analytical methods, available safeguards, community and social norms, and research ethics best practices that would lead to development of a new ethical framework with regards to Big Data processes. It	European Commission, European Data Protection Board, National Data Protection Institutions,

	would help to establish responsible data handling and facilitate management of reliable complex data assessment. It would be best practice to include experts in ethics into research, legislation and standardisation so to enhance the process. Because of the fact that handling of Big Data uses AI in critical applications, it requires a great amount of trust. The proposed solution that would possibly promote trustworthiness and ethical behaviour is the AI Model Validation and Verification Platform (AIMVVP). Its aim is to evaluate AI systems across parameters as fairness, bias detection, robustness against adversarial attacks, explainability, and compliance with ethical and legal standards. It serves as a centralized environment where AI developers, regulators, security practitioners and crisis management teams can collaboratively assess, verify, and validate AI-models, making them ready for deployment in critical areas like healthcare, cybersecurity and public safety.	European Group on Ethics-Research and Innovation, European Data Protection Supervisor, National Governments Entities responsible for Public Security Issue Coordination
Best practice (short/ medium/long term)	**Co-development methodology for security organisations and institutions** Co-development methodology is linked to the EU Starlight project and highlights active involvement of end-users in the development of solutions. Consequently, developers understand the realistic needs of end-users during the development of innovative solutions, and can adjust functionalities during early stage. End-users, however, can have better insight into the solution, they can get to know how they can use it and what results are to be expected. Long term (1-5 years) co-development, involving solution developers and end-users in security sector could influence the innovation up-take process in the domain heavily. There should be thus an end-user focus that would emphasise involvement of this party in evaluation and testing of innovative solutions at different stages of solution development process.	All institutions in the security domain, ranging from policy makers to operational level (Europol, Eurojust), EU Commission (DG Home, DG Connect)

2.3 RESILIENT CIVILIANS, LOCAL LEVEL AND NATIONAL ADMINISTRATION

Resilient Civilians, Local Level and National Administration
Civilians are central not only as targets but also as active participants in seeking human and societal security. Hybrid threats have often been examined primarily through the lens of state or governmental responses, resulting in an exploration of their impacts on civil society. More research is needed to understand how these threats manifest within the broader security environment. Gaining deeper insights into societal vulnerabilities can empower communities and their diverse populations to develop strategies that foster trust, solidarity, and resilience, thereby reducing their susceptibility to manipulation. Such understanding is vital for enhancing resilience across all EU member states. Civilians are not passive recipients of information or government directives. Trust dynamics between the governed and the governing bodies require critical reassessment. In democratic societies, political decision-making and public opinion are shaped through various means of influence, which, in many cases, constitute legitimate and deliberative political activities. For instance, social or communicative influence, such as public discourse and governmental diplomacy, is a natural aspect of political engagement. However, external interference or coercive influence can pose a significant threat. Identifying such threats involves normative classification: a threat is something perceived as harmful, wrongful, or malicious. A significant share of the political decisions affecting citizens' daily lives occurs at the municipal level, where local councils and boards manage essential services such as social welfare, healthcare, and education. Local law enforcement agencies are often on the front lines in detecting and addressing hybrid threats. Recent cases have demonstrated that local governments play a pivotal role not only in countering hybrid threats but, in some instances, in enabling them. Strengthening local-level resilience and awareness is, therefore, crucial to national and EU-wide security efforts.
State of play
Main issues: 1. The growing acceptance and mainstreaming of violence weaken democratic politics: The increasing normalisation and acceptance of violence undermine democratic politics. Employing violence as a tool for destabilisation—such as through protests, accusations of police brutality, or the rise of far-right movements—serves as a destructive tactic in hybrid threat operations. Actors exploiting hybrid threats may leverage these movements to incite repression or amplify societal instability. 2. The spread and demand of conspiracy theories weaken democratic politics: The proliferation and growing influence of conspiracy theories undermine democratic politics. Combating their spread requires raising public awareness and promoting media literacy across society. However, regulating harmful speech presents both legal and political challenges. 3. Emotions and narratives of victimhood in social relations serve as tools for hybrid threat activities. The exploitation of grievances and resentment fuels division, deepens societal polarisation, and drives groups into conflict with one another.

4. Civil society and political engagement at risk of intimidation: Civil society and political participation face growing threats of intimidation. Increasingly, hostile and toxic political discourse is making it more challenging for individuals to engage in political activities. Alarming tactics such as doxing, Strategic Lawsuits Against Public Participation (SLAPPs), and swatting are contributing to this climate of fear and suppression.
5. Authorities under institutional stress: In times of crisis, authorities often have limited time, information, and situational awareness to respond effectively. Rapid, short-term decision-making can impair their ability to fully understand situations and act prudently. This vulnerability can be exploited as a lever for hybrid threat activities, increasing the risk of counterproductive decisions that may amplify the impact of such threats.

Main needs:

1. Media Literacy: Enhancing media literacy is crucial for empowering citizens to critically assess information and resist disinformation.
2. Societal Resilience: Building societal resilience involves fostering critical thinking and awareness among citizens.
3. Local Level and National Administration: Empowering local authorities enhances responsiveness and adaptability in crisis situations.
4. Community Engagement: Engaging local communities in resilience-building activities fosters trust and cooperation between citizens and authorities.
5. Inclusive Strategies: Addressing the needs of marginalised groups is essential for comprehensive resilience. Tailored communication strategies and support mechanisms ensure that all societal segments are equipped to withstand hybrid threats.
6. Adopting a Whole-Society Approach: Hybrid threats require multi-sector collaboration, integrating government agencies, private companies, civil society organisations, media, and academia.

Recommendation ***Legal/Standardisation/Best Practices*** ***Short term: up to 1 year, Medium term: 1-3 years*** ***Long term: over 3 years***	**Explanation on recommendation**	**Relevant Institution**
Legal/Standardisation/Best Practices (medium term)	**Work on capacities to monitor social media convincingly to anticipate violence and understand the main actors of it:** - Develop a unified body responsible for social media surveillance, trend analysis, and real-time threat identification. - Partner with Social Media Platforms: Secure data-sharing agreements for rapid detection and mitigation of threats. Ensure transparency and ethical cooperation with platforms to remove content promoting violence. - Utilize Advanced Technology: Deploy AI-driven sentiment analysis, keyword tracking, and anomaly detection to identify hate speech, violent rhetoric, and extremist propaganda. - Implement ethical oversight and ensure GDPR compliance: Establish clear guidelines to ensure privacy protection and data security in all social media monitoring activities, task a regulatory authority with auditing monitoring	The European Commission, EU MS governments and governments of candidate countries, National and Local Authorities, Actors specialised in monitoring of online harassment/violence, as well as tech companies developing tools to combat such activities, EU Member States stakeholders (social care

	activities, ensuring ethical practices, and handling public complaints, provide regular public updates on monitoring efforts, methodologies, and key findings.	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
Standardisation/Best Practices (medium term)	**Promote public engagement and counter-narrative campaigns:** - Develop accessible platforms for citizens to report harmful online content. - Deploy Counter-Propaganda Initiatives: multi-sectoral cooperation to debunk extremist narratives and promote positive discourse. - Introduce Digital Literacy Programmes: Promote education on recognizing fake news, propaganda, and violent rhetoric.	
Legal/Standardisation/Best Practices (medium term)	**Develop Crisis Response Protocols for Social Media Threats:** - Create a team equipped to respond to online crises, including the spread of violent content or disinformation. - Implement EU-wide, national and local tools for notifying relevant authorities of imminent threats based on social media activity. - Organise EU-wide drills (cascaded to national and local level) to test readiness and refine response protocols for digital crises.	
Legal/Standardisation/Best Practices (short term)	**Establish a Clear Definition of Political Intimidation** The EU should establish a comprehensive, legally recognized definition of political intimidation. This definition should encompass a broad spectrum of intimidating practices, ensuring that all forms of coercion and suppression of political expression are covered. Key elements of this definition should include cyberbullying and online attacks: Digital harassment, doxing, and other forms of online intimidation that prevent individuals from engaging freely in political discussions.	
Standardisation/Best Practices (medium term)	**Wide Promotion of Media Literacy Initiatives** Media-literacy teaching should be stretched across all age groups including kindergarten groups and seniors. It can take different forms – lectures, discussion panels, workshops, awareness campaigns etc. with age and education-appropriate tools. European governments should make critical media literacy a permanent part of the school and university curriculum and of all teacher trainings.	

	A broad training system should be set up especially for representatives of public trust professions: journalists, officials, teachers or opinion leaders. Entrepreneurs should also be reached through chambers of commerce or clusters. Awareness campaigns connected with disinformation and citizens' resilience building should be organised across all the EU but adapted to local conditions.	
Best Practices (short term)	**There is a need to work out ways to reach marginalised groups of society** Access to these groups is not easy, so the strategy must be deeply thought out and pragmatic. It is important to work with organisations that support marginalised groups on a daily basis and are reliable for the end-user. Tools for working with marginalised groups must be tailored to their needs, understandable and practical.	

2.4 INFORMATION AND STRATEGIC COMMUNICATION

Information and Strategic Communication

Information, strategic communication and propaganda are among the areas that, together with cyber, have been linked to hybrid threats most often. The range of hostile and covert influence activities employed in the past include falsely attributed or non-attributed press materials, leaks, the development and control of media assets, overt propaganda, unattributed and black propaganda, forgeries, disinformation, the spread of false rumors, and clandestinely supported organisations, among others. These activities are recognized to be part of the hybrid playbook.

Internet and social media channels have changed the game board for covert influence actions, providing a fertile context for the massive dissemination of overt and covert propaganda by hostile States and non-governmental groups: anyone can produce and disseminate content; connections, funders and identities are blurred; information flows are huge; the speed of information dissemination is breathtaking. AI-generated audiovisual forgeries and the likely future improvements in deep fakes technology appear on the horizon as an insidious threat for democracies that will require developing analytic capabilities to detect and counter them. All these require a sound understanding of communication processes and information flows, developing analytic capabilities and skills for assessing open sources and content, raising strong disinformation awareness, critical thinking, and media literacy, and building positive narratives instead of being on the defensive.

While social media networks provide an unprecedented dimension for adversely impacting the potential exposure of target audiences, gathering empirical evidence on disinformation content is required for a full understanding of the effects of influencing campaigns, and thus developing effective strategies and tactics to counter influence.

State of play		
Main issues: 1.Due to the technological advancements, it is relatively easy to fall prey to disinformation, especially for vulnerable individuals. The content online can be extremist in nature and used to recruit and incorporate new followers, what poses a major threat to media pluralism and broader society. 2.There is the rising emergence of fact-checking platforms, programmes and tools that assess and analyse information posted online if it is trustworthy, however not every social media platform or website is equipped with them, let alone regional or local media. 3. Journalism Trust Initiative international standard that protects reliability and trustworthiness of information has been brought into attention so to promote media pluralism, transparency and integrity. **Main needs:** 1. Since EU actively promotes media freedom and pluralism through initiatives as European Democracy Action Plan or the 2022 Code of Practice on Disinformation, it needs to put emphasis not only on national but also on regional and local media that are important part of the fabric of local communities and seem to diminish due to crisis in the economic sustainability. 2. The existing gap of cooperation between national governments and local authorities has to be addressed in order to bring about successful anti-disinformation system. 3. EU communities need to be resilient and know the factors and dynamics of disinformation, how it is created and what can be done in order to mitigate its harmful effects. The focus on education, diverse media literacy and competences programmes seem to be effective in tackling fake news.		
Recommendation: Legal/Standardisation/Best Practices	**Explanation on recommendation**	**Relevant Institution**
Best Practices (medium term)	**The 2022 (strengthened) Code of Practice on Disinformation should have more signatories and should be also applied to platforms functioning only locally in relevant countries** More online social platforms should sign the Code of Practice that sets obligations, self-regulatory standards and accountability to tackle disinformation. The principles of the Code should be propagated in all EU Member States and implemented not only to pan-European but also local platforms that facilitate media pluralism to a great extent. As a result, new signatories would be a part of an EU-wide forum bringing together relevant partners who seek to share best practices, care about cooperation and	European Commission: DG Connect: Directorate I Media Policy, European Commission - DG Communication-Directorate C Representation & Communication in Member States, European Digital Media Observatory,

	strengthening actions in order to mitigate the risks stemming from disinformation in the EU.	European Parliament – Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, Association of European Journalists, Council of Europe: Congress of Local and Regional Authority Secretary General, European Committee of the Regions – thematic commission, CIVEX
Best Practices (long term)	**Rapid Alert System should work uniformly in all EU countries, not only at governmental level but also local level** Rapid Alert System is set to provide alerts on disinformation campaigns in real-time through dedicated technological infrastructure. It is a relevant tool to make citizens aware of disinformation campaigns since it promotes common situational awareness. Public officials of all EU Member States should address and explain these campaigns to the public. Furthermore, the system should work beyond governmental level so crucial disinformation alerts could reach local authorities.	European Commission- DG HOME- Unit HOME.F Audit& Situational Awareness, National Governments-Entities responsible for Public Security Issue Coordination (Government Centre for Security in Poland - RCB), CIVEX, Council of EU: Congress of Local and Regional Authority Secretary General, European Parliament Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation,

		European Committee of Regions-thematic commission
Standardisation (long term)	**Communication and cooperation between national governments and local authorities has to be improved** Particular standards of communication between national governments and local authorities should be set out and developed with assistance of representatives of local authorities and organisations. The standards should take into consideration specific needs and competences of local authorities and their development should draw the attention of local authorities to the problem of disinformation to highlight its local context (not just international or national one). By the same token, a platform for debate between government and local authorities is to be created.	European Parliament Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, CIVEX, European Committee of Regions-thematic commission, International Fact Checking Network, Members of the High Level Group on Fake News and Online Disinformation, Association of European Journalists, European Digital Media Observatory, ALDA- European Association for Local Democracy, CEMR- Council of European Municipalities and Regions, Council of Europe: Congress of Local and Regional Authority Secretary General,

		European Commission: DG Connect: Directorate H Digital Society, Trust & Cybersecurity
Best practices (medium term)	**Safeguarding vulnerable people against violent extremism and terrorism online** GECHO solution (Gatekeeping ECHO chambers) monitors the online environment, identifies where interventions are needed, what builds the resilience in vulnerable young people against possible entrapment in violent extremism and terrorism. A sharing and analysis platform for GECHO should be developed. It would promote information sharing, analysis and joint actions between organisations in the Member States to provide detailed and local situational awareness about activities in online environments linked to violent extremism and terrorism. It would be relevant for efficient protection of vulnerable young people from recruitment and such influences. In addition, AI tools could be helpful in quick and accurate discovery and recognition of new sites, visitors and changes in activity levels at known sites. Moreover, a research network with focus on GECHO needs and factors influencing the online radicalisation process should be established what would facilitate development of easy to follow and validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremism and terrorism.	The European Commission, Ministry Level, National and Local Authorities Actors specialised in monitoring of online activities by violent extremism and terrorism groups as well as tech companies developing tool, EU Member States stakeholders (social care workers, police, teachers, NGOs), EUROPOL, EU Knowledge Hub on Prevention of Radicalisation, The VOX-Pol Network of Excellence (NoE), European Digital Media Observatory (EDMO)
Best Practice (medium/long term)	**Enhancing Media Literacy through Education at national, regional and local level** EU governments should endorse curriculum that teaches children/students critical thinking skills in order to develop an ability to spot and recognize fabricated information on social media. Basing on the example of Finnish educational system, teachers should promote the aforementioned skills for instance in math classes explaining how statistics can be manipulated.	Ministries of Education in EU countries, The European Education Area Local and Regional Authorities in EU Member States,

	Developing media literacy skills as well as building awareness of social media users about online radicalisation, disinformation, how they are created, what are their characteristics and how to deal with these issues should be constantly in progress. There are many engaging and interactive ways to promote and teach media literacy skills as “Aces of Internet” initiative in Poland. It is a free educational programme for teachers and educators working with children and young people at all educational levels and every EU Member State should invest in this kind of programmes to fight disinformation and improve societal resilience to it. In addition, local non-governmental institutions’ role in education in the field of media competences could be put into practice since they have knowledge of specific needs and opportunities for education in a particular area.	NGOs (The Centre for Citizenship Education in Poland, The Finnish Society for Media Education, The Flemish Knowledge Centre for Media Literacy, Klicksafe in Germany)

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
D4.11 contribution: in the final cycle of the EU-HYBNET project, the development of standardisation recommendations included an in-depth analysis of the contributions of research and innovation projects to practitioners. The recommendations and best practices identified in this process stem from both European and international research and innovation activities. This approach ensures that the EU-HYBNET project remains aligned with emerging trends and technological advancements in countering hybrid threats. The analysis conducted within D4.11 serves as a crucial input to EU-HYBNET's Objective 4, goal 4.3, by contributing to the development of a mapping matrix that links identified gaps and needs of European actors to the most promising innovations across various domains. Additionally, D4.11 supports EU-HYBNET's Objective 4, goal 4.1, by addressing industrialisation and public procurement aspects. These recommendations play a vital role in appraising best innovations—both technical and non-technical—thereby facilitating their potential industrial uptake.

2) common requirements as regards innovations that could fill in gaps and needs:
D4.11 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. D4.11 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 recommendations presented in D4.11 contribute directly to the dissemination of knowledge and the enhancement of performance in standardisation efforts. These recommendations not only focus on technological advancements but also encompass non-technological innovations that contribute to capacity-building and skill development in addressing hybrid threats. Given that D4.11 builds upon previous deliverables (D4.8, D4.9, D4.10), it integrates prior findings while updating and refining insights to ensure continued relevance. The focus remains on advancing the standardisation landscape by identifying and advocating for best practices, fostering harmonisation, and supporting the evolution of counter-hybrid threat capabilities.

By aligning with the Three Lines of Action, D4.11 ensures that EU-HYBNET's contributions to research, innovation uptake, and standardisation are effectively documented and communicated to the European Commission, reinforcing the project's impact and legacy.

4. CONCLUSION

In the final, fourth project cycle, the state of play was revised and adapted based on the outcomes of EU-HYBNET reports from the previous three cycles. These revisions were conducted within various tasks relevant to the recommendations for standardisation.
The "Final Report on Standardisation Recommendations" presents recommendations across the four EU-HYBNET Core Themes, building upon the work completed in all project cycles. Section 2 outlines

the most significant aspects related to the selected areas—the four aforementioned Core Themes—highlighting current state of play, main issues, and needs. This section also links the identified issues to innovation recommendations for standardisation. Section 3 elaborates on the Three Lines of Action.

The authors emphasise that T4.3 of EE-HYBNET not only focused on recommendations for standards *per se*, but also addressed legal harmonisation and the identification of best practices. The project encourages the adoption of these best practices, as they often serve as the foundation for the development of official standards (e.g., ISO, CEN, or national standards). Given that the standardisation process typically takes at least 2-3 years, it is challenging to ensure that standards remain aligned with the rapidly evolving landscape of hybrid threats. While relevant standards exist in areas such as safety, physical security, and cybersecurity, they are generally not specifically tailored to hybrid threats as described in this deliverable.

As this is the final report under Task 4.3 within EU-HYBNET, the recommendations presented serve as a foundation for future discussions and developments in the field of hybrid threat mitigation. These recommendations aim to provide strategic guidance on standardisation efforts, legal harmonisation, and best practices that can enhance the resilience of European and international actors against hybrid threats. Given the dynamic and evolving nature of hybrid threats, continuous adaptation and proactive engagement from stakeholders will be necessary to ensure that standardisation efforts remain relevant and effective. To advance these efforts, collaboration among multiple stakeholders is essential. This includes engagement between public authorities, private sector actors, industry representatives, research institutions, and policymakers at both the national and EU levels. The European Commission plays a pivotal role in facilitating this coordination by aligning research and innovation funding, regulatory frameworks, and policy guidelines to support the implementation of the proposed recommendations. Strengthening synergies between different standardisation bodies, such as CEN, CENELEC, and ISO technical committees, will be crucial to developing comprehensive and widely accepted standards that address the unique challenges posed by hybrid threats.

Moreover, fostering cross-sectoral cooperation between security agencies, technology providers, and academia will help bridge gaps in knowledge, accelerate the uptake of innovative solutions, and promote a harmonised approach to standardisation across Europe. Future efforts should also include continuous monitoring and evaluation of existing standards to ensure their applicability in addressing emerging hybrid threats. Ultimately, the success of these standardisation recommendations depends on sustained commitment, resource allocation, and policy support from all relevant actors.

The Task 4.3 team will share insights from Deliverable D4.10 with relevant stakeholders, including CEN, CENELEC, and ISO technical committees. Additionally, through Work Package 5 (Communication and Dissemination), this information will be shared with other organisations, agencies, institutions, and projects working in the field of countering hybrid threats.

ANNEX I. ACRONYMS

Term	Definition
5G	Fifth Generation Wireless Technology
AI	Artificial Intelligence
ALDA	European Association for Local Democracy
CEMR	Council of European Municipalities and Regions
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
CIRETO	Citizen Reporting Tools
CIVEX	Commission for Citizenship, Governance, Institutional and External Affairs (European Committee of the Regions)
DG Connect	Directorate-General for Communications Networks, Content and Technology
DG EAC	Directorate-General for Education, Youth, Sport and Culture
DG HOME	Directorate-General for Migration and Home Affairs
EAC.B	Education and Erasmus+ Section of DG EAC
EC	European Commission
EDMO	European Digital Media Observatory
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
FDI	Foreign Direct Investment
GDPR	General Data Protection Regulation
GECHO	Gatekeeping ECHO Chambers (an initiative for monitoring extremism online)
HiPEAC	High Performance Embedded Architecture and Compilation
HW/SW	Hardware/Software
ISO	International Organisation for Standardisation
ISO 27001	Information Security Management certification
IT	Information Technology