SOCIETAL IMPACT FINAL REPORT

DELIVERABLE 1.18

Lead Author: Laurea

Deliverable classification: PU

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

D1.18 SOCIETAL IMPACT FINAL REPORT

Deliverable number	**D1.18**	
Version:	**V1.0**	
Delivery date:	**30.4.2025**	
Dissemination level:	**Public (PU)**	
Classification level:	**PU**	
Status	**Final**	
Nature:	**Report**	
Main author:	**Tuomas Tammilehto**	**Laurea**
Contributors:	**Tiina Haapanen**	**Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	1.9.2024	Tuomas Tammilehto/ Laurea	Initial version
0.2	5.2.2025	Tuomas Tammilehto / Laurea	More contend added, e.g., analysis on the final reports of various WPs.
0.3	15.4.2025	Tuomas Tammilehto / Laurea	Contributions of Tiina Haapanen / Laurea added
0.4	16.4.2025	Tuomas Tammilehto / Laurea	Document ready for review
0.5	16.4.2025	Iván L. Martínez / PLV; Jari Räsänen / Laurea	Review and text editing. Comments for improvements.
0.6	22.4.2025	Tuomas Tammilehto / Laurea	Reviewers' comments addressed
0.7	28.4.2025	Isto Mattila / Laurea	Final review
0.8	29.4.2025	Tuomas Tammilehto / Laurea	Text editing
1.0	30.4.2025	Tiina Haapanen / Laurea	Finalizing and submission 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

TABLES

FIGURES

1 INTRODUCTION

1.1 OVERVIEW

According to the Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project's description of Action (DoA) (WP) 1 "*Coordination and Project Management*"/ Task (T) 1.2 "*Project Management, Quality Control, Ethics and Risk Management*" (lead by Laurea) is to deliver "Societal Impact Final Report" deliverable D1.18 at the end of the project execution in April 2025, Month 60 of the project. In short, this report brings light to the EU-HYBNET's activities from the societal impacts point of view.

The D1.18 is connected to the WP1 being an integral part of the ethics work in EU-HYBNET project ensuring that the end-results and impacts to the society are ethically sustainable and societally acceptable, but also with all other WPs, since the impact to society is built through the tangible activities of our project, for example and especially

- activities related to the building and maintaining the EU-HYBNET network,
- activities in discovering and defining innovations based on requirements, monitoring both development of hybrid threats and the countermeasures, and pushing related standards to help the industry,
- all tasks and doings towards enabling the different encounterings between academia, practitioners and industry, i.e., the different events, venues, and happenings whether online or face-to-face onsite, and not forgetting
- dissemination of all above and more, which are intertwined with all the EU-HYBNET activities.

The picture below describes the role of WP1 to support and to guide the whole project to gain tangible results, also from the societal impact perspective.

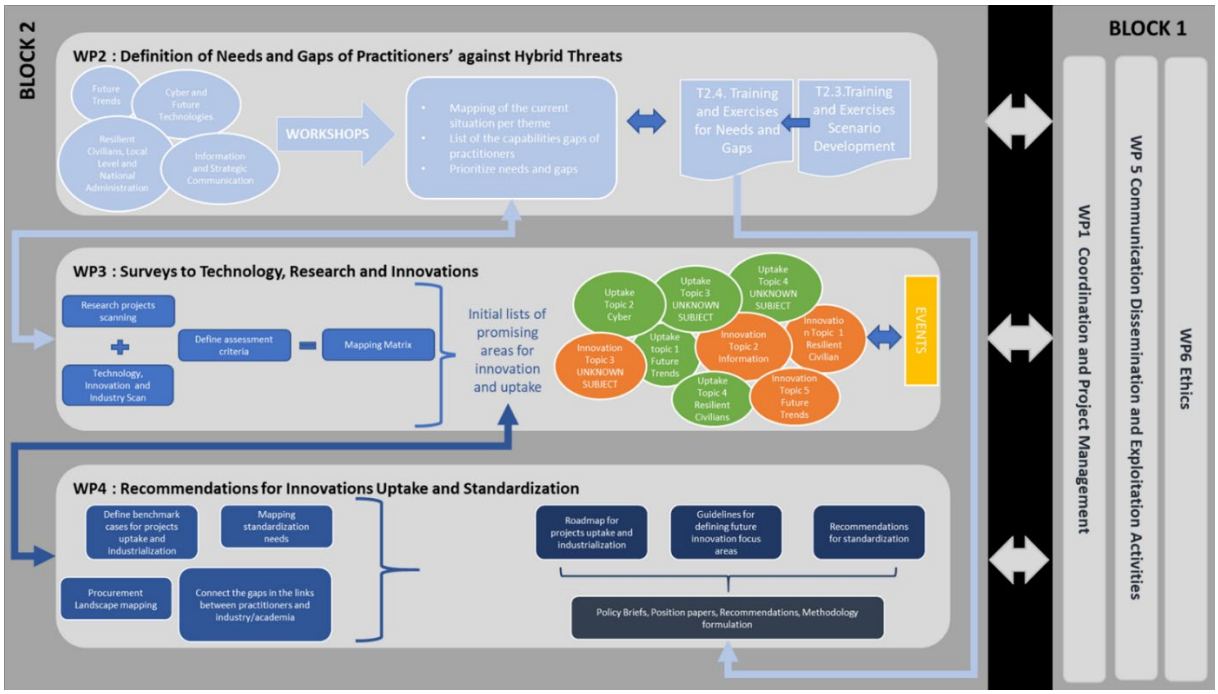

Figure 1: EU-HYBNET Structure of Work Packages and Main Activities

1.2 STRUCTURE OF THE DELIVERABLE

In order to describe the societal impacts of EU-HYBNET, in this document, after the Introduction (Section 1) are first presented the objectives of EU-HYBNET and then described their impact on society (Section 2). This is followed by presenting the most obvious impact on society – the network itself and the events it held (Section 3) – following detailed information on the tangible activities divided in subsections of Innovations, Standardisation and Dissemination (Section 4). Then after are presented the analysis of the joint exercise on Societal Impact Assessment, that was conducted in our Valencia event in April 2024 (Section 4). And at the end, there is a summative analysis of the societal impacts (Section 5).

2 THE PROJECT OBJECTIVES AND ASSESSING THE SOCIETAL IMPACTS

Whilst this societal impact report is not the official mean to describe how our project met the objectives set for us, few can argue that meeting the objectives are not relevant to the impacts on societies. Isn't this what any project attempts to achieve? I.e., that objectives are met, and they have an impact. Therefore, in this section are first presented the EU-HYBNET objectives, and then followed by an analysis of possible impacts to the society, if and when the objective is met. At times, a number of objectives are collated because of their close proximity vis-à-vis each other's and the related impacts.

EU-HYBNET objective:

- *OB1. To enrich the existing network countering hybrid threats and ensure long term sustainability*

The impacts:

The network itself is impacting European societies. The network focusing on hybrid threats is arguably vitally important, as it enables academics, policymakers, practitioners, and institutions from diverse backgrounds to collaborate closely in identifying, understanding, and countering complex security challenges. For example, a robust research network in this field significantly enhances the collective ability to detect, analyse, and respond to these multidimensional threats swiftly and effectively.

By fostering active communication and information exchange, a dedicated network such as EU-HYBNET, promotes a deeper and more comprehensive understanding of evolving security risks. It allows for rapid sharing of research findings, intelligence analyses, and best practices among participating researchers and institutions. This collaborative approach significantly strengthens national and international capacities to predict, prevent, and mitigate the potential impacts of hybrid tactics, thus improving overall resilience.

Moreover, such a research network positively impacts society by increasing awareness among the general public and decision-makers regarding the subtle and often covert nature of hybrid threats. Greater awareness leads to enhanced societal resilience, as individuals and communities become better equipped to recognise and critically assess potential misinformation, cyber threats, and manipulative tactics. Furthermore, policy frameworks can be more precisely formulated and adjusted based on the evidence-based recommendations emerging from collaborative research, thereby strengthening democratic institutions, protecting civil liberties, and safeguarding social cohesion.

However, the interconnected nature of these research networks also underscores the necessity of robust ethical standards, rigorous data protection, and comprehensive cybersecurity measures. Effective governance of these networks helps ensure their integrity, protecting sensitive information from malicious exploitation while promoting transparent and accountable collaboration.

A dedicated network on hybrid threats is pivotal for addressing contemporary security challenges and significantly contributes to societal stability by fostering resilience, informed policy decisions, and European and international responses.

EU-HYBNET objectives:

- *OB2. To define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats;*
- *OB3. To monitor developments in research and innovation activities as applied to hybrid threats;*

and

- *OB4. To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats*

The impacts:

Defining common requirements that specifically address knowledge gaps and performance needs significantly enhances the capabilities of research, innovation, and training initiatives aimed at countering hybrid threats, resulting arguably in considerable societal benefits. When clear, unified criteria are established, researchers and practitioners across multiple sectors can collaborate more effectively, facilitating a cohesive approach towards identifying and mitigating emerging hybrid threats. This enables that resources are allocated efficiently, duplication of efforts is minimised, and critical vulnerabilities within societies are more swiftly recognised and addressed.

Moreover, by bridging these knowledge and capability gaps, societies benefit from improved resilience to complex security challenges. Enhanced training programmes, underpinned by clearly articulated common requirements, equip professionals, decision-makers, and even the wider public with the necessary skills to better recognise, understand, and respond to hybrid threats such as cyber-attacks, disinformation campaigns, and economic coercion. This heightened preparedness helps preserve social cohesion, maintain democratic integrity, and safeguard public confidence in institutions.

Furthermore, consistent innovation fostered through defined common requirements accelerates the development of cutting-edge technological and methodological solutions. These advancements not only boost defensive capacities against hybrid threats but also contribute to wider economic growth and technological progress, creating spill-over effects beneficial to various sectors of society. Ultimately, through targeted research, informed policymaking, and coordinated European collaboration driven by shared objectives and clear requirements, European societies are better positioned to navigate the complexities of modern security threats, ensuring long-term stability and prosperity.

Furthermore, monitoring developments in research and innovation activities related to hybrid threats brings substantial benefits to society by ensuring continuous awareness and perhaps also early detection of emerging risks and vulnerabilities. By systematically tracking advancements and ongoing studies in this rapidly evolving field, societies can swiftly adapt their security strategies and responses

to align with the latest insights and methodologies. This approach may enable institutions, governments, and communities to remain resilient and agile, effectively mitigating the impacts of hybrid threats such as cyber-attacks, mis- and disinformation, economic disruption, and attempts to undermine democratic processes and institutions.

Moreover, carefully monitoring hybrid threats enhances transparency and accountability, contributing significantly to public trust in governmental and institutional capabilities. An informed and engaged public, aware that developments are consistently monitored and addressed, is more resilient to manipulation and less susceptible to divisive tactics. Consequently, societal cohesion, trust in democratic institutions, and overall stability are strengthened, safeguarding the principles of democracy, rule of law, and respect for fundamental rights and freedoms: all core European values.

Again, determining priorities for standardisation for industry to effectively counter hybrid threats has also clear societal advantages. By establishing standardised practices and protocols, industries and businesses become better equipped to recognise vulnerabilities and efficiently implement measures to protect critical infrastructure and digital networks from hybrid threats. It is a known fact that standardisation enhances interoperability between sectors, facilitating coherent responses and collaborative defence mechanisms, thereby reducing risks of widespread disruption or damage to essential services and supply chains that society relies upon daily.

Furthermore, clearly defined industry standards accelerate innovation, as businesses have precise benchmarks and guidelines to strive toward. This leads to the faster development of advanced technological solutions and services that directly improve security and resilience against hybrid threats. As industry becomes more adept at addressing these complex challenges, societies benefit through improved economic stability, strengthened national security, and enhanced public safety. Overall, effective monitoring and prioritised standardisation collectively equip society to confidently manage and overcome the multifaceted challenges posed by hybrid threats, thereby promoting long-term societal prosperity and well-being.

EU-HYBNET objectives:

- *OB5. To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network*
- *OB6. To foster capacity building and knowledge exchange on countering hybrid threats*
- *OB7. To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats*

The impacts

When researchers, practitioners, and industry representatives focusing on countering hybrid threats (or any other fields) regularly come together to meet and engage in meaningful dialogue during various events, society as a whole experiences numerous positive impacts. Such interactions can facilitate an open exchange of knowledge, experiences, and innovative ideas, significantly enhancing the collective understanding and expertise in addressing complex security challenges. This interdisciplinary and cross-sectoral collaboration ensures that the solutions developed are not only theoretically sound but practically effective and aligned with real-world needs.

Additionally, these interactions foster the establishment and strengthening of professional networks, encouraging trust and cooperation among different stakeholders. As relationships develop, joint initiatives, partnerships, and cooperative projects become more feasible, leading to a coordinated and comprehensive response to hybrid threats. Through sustained dialogue, stakeholders from research institutions, government agencies, security services, and industry are better able to align their efforts, share resources, and leverage complementary strengths, ultimately improving resilience against emerging threats.

Moreover, events that promote meaningful dialogue among various experts and sectors contribute to societal awareness by highlighting and clarifying critical issues to a broader audience. Enhanced public understanding of hybrid threats and the ways to counter them strengthens societal resilience, enabling individuals and communities to become more vigilant and less vulnerable to misinformation or manipulation. This increased awareness also builds confidence in the capabilities of institutions and organisations tasked with safeguarding society, reinforcing trust and stability.

Furthermore, such dialogue-driven interactions often inspire innovation and accelerate technological advancements, providing society with improved tools, strategies, and methodologies to effectively counter hybrid threats. In the longer term, the resulting innovations and advancements frequently benefit other sectors beyond security, promoting broader societal development, economic growth, and well-being.

In conclusion, meaningful dialogue and regular engagement among researchers, practitioners, and industry representatives create powerful synergies that substantially improve societal resilience, foster innovative solutions, and strengthen public trust, ultimately promoting a secure, informed, and cohesive society.

Regular meetings and events involving researchers, practitioners, and industry representatives play a vital role in fostering capacity building and knowledge exchange in the field of countering hybrid threats, which in turn has a profoundly positive impact on society. These gatherings serve as dynamic platforms where expertise is shared, skills are developed, and emerging challenges are addressed collaboratively. By engaging in continuous dialogue, participants gain deeper insights into the evolving nature of hybrid threats, acquire new methods and tools for responding effectively, and refine existing strategies based on practical experience and scientific research.

Capacity building through these events ensures that individuals and institutions across different sectors are better equipped to identify, assess, and mitigate hybrid threats in a timely and coordinated manner. This includes enhancing analytical capabilities, improving decision-making processes, and strengthening the ability to communicate risk effectively to the public. The development of such competencies is crucial for building robust national and international defence mechanisms that can adapt to the increasingly complex threat landscape.

At the same time, the exchange of knowledge among diverse stakeholders encourages the dissemination of best practices, lessons learned, and innovative approaches that can be scaled or adapted to different contexts. This process of shared learning contributes to the harmonisation of practices across borders and sectors, which is particularly important when dealing with transnational threats that require unified responses. It also helps prevent fragmentation and duplication of efforts, making the collective response more efficient and impactful.

For society, the benefits are significant. As institutions become more capable and informed, the public is better protected from the destabilising effects of hybrid threats such as dis- and misinformation, cyberattacks, or economic coercion. Moreover, the open and cooperative spirit of these events helps cultivate a culture of preparedness and resilience, encouraging not only experts but also communities to play an active role in safeguarding democratic values and societal integrity.

In essence, regular meetings and events are not merely networking opportunities—they are strategic mechanisms for building enduring capacities and fostering knowledge ecosystems that empower society to face hybrid threats with greater confidence, unity, and effectiveness.

These events, which bring together experts from research, practice, and industry, create a crucial foundation for establishing effective synergies with existing European, national, and sub-national networks that are actively involved in countering hybrid threats. By providing a shared space for dialogue, collaboration, and mutual learning, such gatherings enable participants to identify common goals, align their approaches, and coordinate actions more effectively. This alignment is essential in a field as complex and multifaceted as hybrid threats, where no single actor or level of governance can respond comprehensively on its own.

Moreover, through in-person and virtual engagement, participants can map out complementary strengths and capacities across different networks, leading to a more integrated and coherent landscape of action. These synergies enhance the ability to share resources, methodologies, and intelligence, avoiding duplication and reinforcing each other's efforts. When experts connect at these events, they often initiate longer-term collaborations that continue beyond the event itself, embedding their knowledge and strategies into ongoing regional and cross-border initiatives. This sustained cooperation strengthens Europe's collective capacity to detect, prevent, and respond to hybrid threats in a unified and timely manner.

Furthermore, these events foster trust and mutual understanding among diverse stakeholders, which are essential preconditions for effective cooperation across institutional and national boundaries. They also help surface and disseminate best practices developed in local or sector-specific contexts, which can then be adapted and scaled across broader European frameworks. This creates a continuous feedback loop between local innovation and European-level strategy, ensuring that policies and actions remain grounded in practical experience and real-world relevance.

For European societies, these synergies possibly translate into stronger protection of democratic systems, enhanced resilience of critical infrastructures, and improved public awareness and preparedness. Citizens benefit from more efficient use of public resources, quicker responses to hybrid incidents, and greater confidence in their institutions' ability to safeguard national and collective security. In essence, these events do more than facilitate knowledge exchange—they serve as catalysts for deeper integration and strategic coherence across Europe's hybrid threat response ecosystem, ultimately contributing to a more secure, stable, and resilient European society.

3 THE NETWORK

3.1 NETWORK IN SHORT

As the EU-HYBNET is a network project, a so-called Communication and Support Action (CSA), one can argue that the project's primary outcome is the network itself. And, as stated earlier, the raison d'être of the network is to foster knowledge exchange and strengthened cooperation among industry, practitioners, academics, NGOs, and other key stakeholders. The overarching aim has been to align resources, innovations, and solutions with the most pressing gaps and needs faced by European practitioners in the field of countering hybrid threats. Once the project officially ends, the network is the tangible outcome that remains.

The functions and the details of the network can be found in numerous EU-HYBNET's deliverables, so there is little point of recapping all of them.[1] Maybe more futile is to simply state that the central strength and defining value of EU-HYBNET has been its network extension process. This process served as a vital mechanism for strengthening the EU-HYBNET network and supporting the work of project partners and stakeholder group members. By continuously identifying and engaging potential new key actors, the extension process enhanced the network's reach, relevance, and capacity to address evolving challenges related to hybrid threats.

Here below are two illustrations. One to clarify the idea of the network, and the other picturing the growth of the network from the beginning of the project to March 2025:

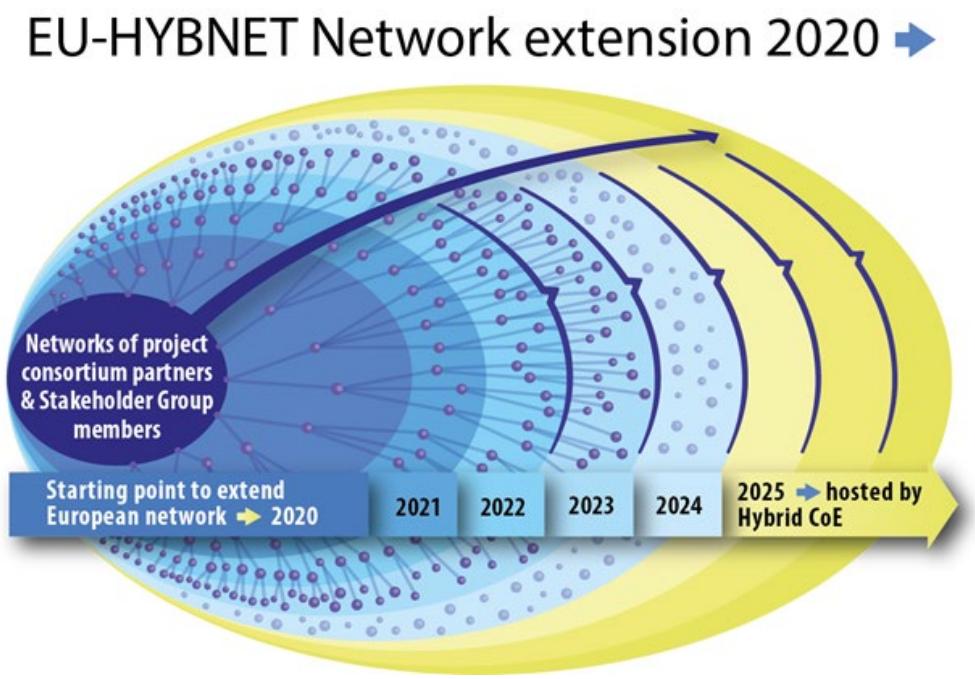

Figure 2: EU-HYBNET Network extension 2020 (the plan)

[1] See for example, the deliverables "D1.23 List of actors to the extended EU-HYBNET Network" and "D1.25 EU-HYBNET Network Sustainability Final Report".

The growth of EU-HYBNET Network (incl. Network Members, Stakeholders and Consortium Partners)

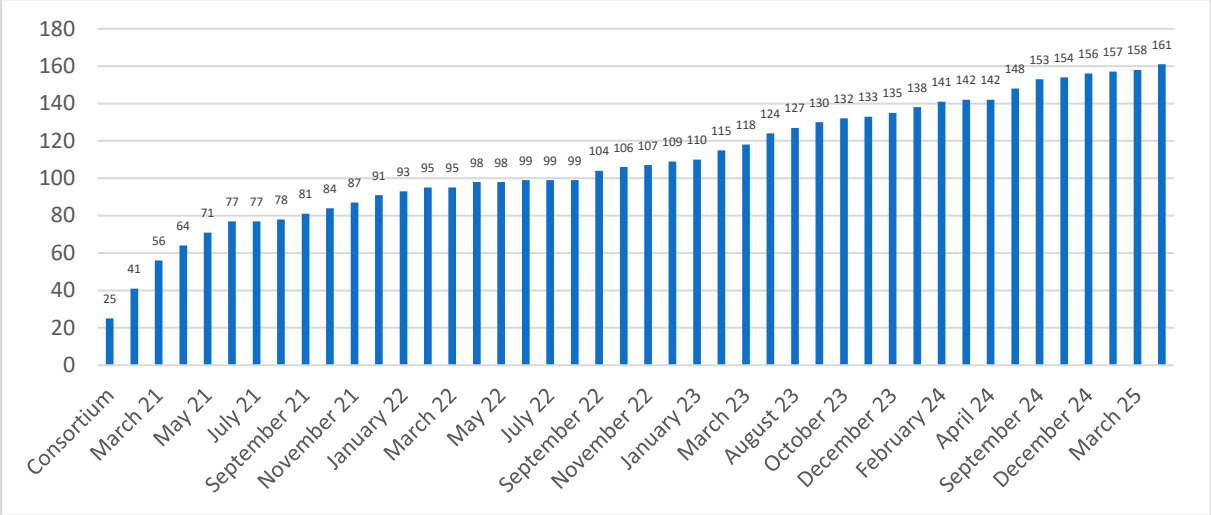

Figure 3: The growth of EU-HYBNET Network

3.2 THE COMPOSITION OF THE NETWORK

The members are representing so-called practitioners, meaning "someone who is qualified or registered to practice a particular occupation or profession in the field of security or civil protection"[2], for example, those operating at the ministry or administrative level, those at the local level, including cities and regions, and those support functions that serve both ministry and local levels, including organisations from Europe's third sector. In addition to practitioners, the network was strengthened by the active participation of representatives from European industry, SMEs, academia, and NGOs.

These actors together played a key role in delivering innovative solutions tailored to the needs of practitioners and contributed significantly through research and development efforts, supporting the broader community of stakeholders working to counter hybrid threats.

Here can be found the network members in more details: https://euhybnet.eu/network_members/

[2] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156

3.3 NETWORK ACTIVITIES

The network activities are presented more in details in the respective deliverables[3] and on EU-HYBNET's webpage[4] and it would be futile to copy the vast information here. However, since and as stated already earlier, the impacts of EU-HYBNET materialised very much in the different venues and events it is meaningful to present the overall picture.

EU-HYBNET organised several key events aimed at enhancing collaboration and knowledge exchange among stakeholders involved in countering hybrid threats. These key events can be divided into four types. The first were the *Future Trends Workshops (FTWs*). These workshops explore anticipated developments in hybrid threats and assess the applicability of current innovations and solutions in future contexts. They provide a platform for stakeholders to discuss strategic planning and the long-term implications of policy decisions. The *Annual Stakeholder Group Meetings* brought together members of the EU-HYBNET network to discuss progress, share insights, and coordinate efforts in addressing hybrid threats. The *Training and Exercise Events* of the EU-HYBNET conducted training sessions and exercises to build capabilities and test responses to hybrid threat scenarios. And the *Dissemination Workshops* aimed to share findings, best practices, and innovative solutions developed within the EU-HYBNET project with a broader audience.

Here below are the various events presented in a table format, and as stated earlier, the full spectrum of the events can be found at our webpage.

[3] See for example, "D2.4 4th Gaps and Needs Events".
[4] https://euhybnet.eu/events/

Event Name	Date	Place
EU-HYBNET 5th & Final Future Trends Workshop	13.2.2025	Brussels, Belgium
EU-HYBNET 5th & Final Annual Workshop	12.2.2025	Brussels, Belgium
EU-HYBNET 3rd Innovation Standardisation Workshop	22.10.2024	Brussels, Belgium
EU-HYBNET Final Gaps and Needs Event	12.6.2024	Madrid, Spain
EU-HYBNET 4th Annual Workshop	24.4.2024	Valencia, Spain
EU-HYBNET 4th Future Trends Workshop	23.4.2024	Valencia, Spain
EU-HYBNET 3rd Training & Exercise Event	18.1.2024	Vilnius, Lithuania
EU-HYBNET 2nd Innovation Standardisation Workshop	8.11.2023	Valencia, Spain
EU-HYBNET 3rd Innovation and Knowledge Exchange Workshop	7.11.2023	Valencia, Spain
EU-HYBNET Webinar – Role of LEAs in combating hybrid threats	26.11.2023	Online
EU-HYBNET 3rd Annual Workshop	20.4.2023	Bucharest, Romania
EU-HYBNET 3rd Future Trends Workshop	19.4.2023	Bucharest, Romania
EU-HYBNET 3rd Gaps and Needs Event	28.3.2023	Rome, Italy
EU-HYBNET 2nd Training & Exercise Event	29.9.2022	Vilnius, Lithuania
EU-HYBNET Workshop at CRITIS2022	15.9.2022	Neubiberg, Germany
EU-HYBNET Innovation Standardisation Workshop	15.6.2022	The Hague, Netherlands
EU-HYBNET 2nd Innovation and Knowledge Exchange Workshop	14.6.2022	The Hague, Netherlands
EU-HYBNET 2nd Annual Workshop	6.4.2022	Rome, Italy
EU-HYBNET 2nd Future Trends Workshop	5.4.2022	Rome, Italy
Responding to Hybrid Threats Workshop	14.6.2021	Online
EU-HYBNET 'Defined Innovations to Hybrid Threats' Event	4.10.2021	Online
EU-HYBNET 2nd Gaps and Needs Event	7.9.2021	Online
CERIS Scenario-based Innovation Workshop	29.9.2021	Online
INCLUDING 2nd Annual Workshop on Nuclear Security	24.6.2021	Online
EU-HYBNET 1st Training Event (Part 2)	29.4.2021	Online
EU-HYBNET 1st Training Event (Part 1)	22.4.2021	Online
EU-HYBNET 1st Annual Workshop and Stakeholders Group Meeting	13.4.2021	Online
1st Future Trends Workshop	31.3.2021	Online
1st Innovation and Knowledge Exchange Workshop	19.1.2021	Online
SPARTA EUHYBNET Cross-Network Collaboration Event	19.10.2020	Online

Table 1: EU-HYBNET events

As we can see from the table above, quite many events have been organised, first because of the global pandemic caused by COVID-19 held mostly online, and then from April 2022 onward mainly on site face-to-face.

All in all, the project engaged in the events successfully over 160 organisations, representing a wide range of backgrounds and areas of expertise. This diversity has been one of the project's key strengths, with network members coming together through events and meetings, collaborating on the

development of policy briefs and other key documents, and directly contributing knowledge and insights from their respective fields. These activities have formed the essential building blocks for ensuring the network's future sustainability.

The EU-HYBNET network's diversity is central to its ability to generate detailed and nuanced observations of the hybrid threat landscape in Europe. One of the core objectives of the network's activities has been to maintain cohesion amidst this diversity of expertise. Addressing hybrid threats effectively requires the ability to connect disparate elements and build a comprehensive picture—enhancing situational awareness, which is the foundational step in mounting an adequate and efficient response.

A crucial aspect of maintaining this cohesion has been the use of a shared conceptual model of hybrid threats [5], which has enabled network partners to speak a common language. This common understanding is not only vital for current collaboration but also serves as a cornerstone for the long-term sustainability of the network, helping to ensure that situational awareness continues to improve across Europe.

The conceptual model of hybrid threats is a framework used to understand and categorise the complex, multi-dimensional nature of hybrid threats. Hybrid threats typically combine conventional and unconventional methods—military and non-military, overt and covert—used in a coordinated manner to exploit vulnerabilities in target societies, institutions, or systems. The conceptual model helps stakeholders systematically assess these threats by identifying their characteristics, mechanisms, and potential impact areas. In EU-HYBNET's context, the conceptual model provided a common language and analytical framework that allowed stakeholders from diverse fields — such as academia, law enforcement, civil society, and private industry — to coordinate their understanding of hybrid threats. It also enabled joint identification of capability gaps and supports the development of effective countermeasures, enhancing collective preparedness and response across Europe.

The conceptual model is further developed to CORE model.[6] The CORE model, a strategic tool, developed by the JRC and Hybrid CoE, applies a holistic 'whole-of-society' approach, covering various societal "spaces" (governance, civic engagement, essential services) and operating at international, national, and local levels. It illustrates how incremental hybrid threats gradually erode democracies by impacting these interconnected areas. This this new framework was used during the latter part of our project, for example, when analysing the gaps and needs.

The gaps and needs analysis were another important EU-HYBNET's outcome from societal impact point-of-view, as were the innovations and the dissemination of the results. Since the gaps and needs analysis are restricted, only the two latter will be disclosed here in the following section.

[5] The conceptual model is presented in all of its details in Giannopoulos, G., Smith, H. & Theocharidou, M (2021). *The landscape of Hybrid Threats: A conceptual model*. Available online at: https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

[6] More details of the CORE model can be found in: Jungwirth, R. et al. (2023) Hybrid Threats: A Comprehensive Resilience Ecosystem,Publications Office of the European Union, Luxembourg. Available online at: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC129019/JRC129019_01.pdf

4 INNOVATIONS AND DISSEMINATION

4.1 INNOVATIONS

The path toward innovations in the EU-HYBNET methodology begun from gaps and needs analysis. However, because this information is restricted and this deliverable being a public one, in the societal impact considerations we jump directly to the innovations. The innovation uptakes are presented in detail in the related deliverables of WP4.[7]

In general, innovations benefit greatly society in profound and far-reaching ways by introducing new ideas, technologies, processes, and solutions that address existing problems, improve quality of life, and drive progress across all sectors. Humanity is nothing but innovations, might one say.

In the context of EU-HYBNET, innovations lead into more resilient and secure society by enhancing national security, and safeguarding democratic institutions in the face of increasingly complex and evolving challenges. Hybrid threats demand a multifaceted and adaptive responses, and innovations are key to staying ahead of the threats. Ultimately, innovations in the hybrid threat domain equip societies with the tools and knowledge needed to defend against threats that are often ambiguous, adaptive, and hard to attribute. By continuously evolving and integrating new technologies and strategies, societies can not only react to hybrid threats more effectively, but also proactively strengthen their systems, norms, and values against future challenges.

The key inputs that EU-HYBNET delivered were the 13 most promising and potential solutions that the project wanted to promote, for example, toward standardisation. They covered generic components for information sharing, situational awareness and handling of IMI as well as important enablers like development work models and validation of AI-models. These innovations are presented in the table here below:

[7] See for example, D4.4 1st Innovation uptake, industrialisation and research strategy, D4.5 2nd Innovation uptake, industrialisation and research strategy, D4.6 3rd Innovation uptake, industrialisation and research strategy, and especially D4.7 Final report for innovation uptake industrialisation and research strategy.

Solution	Main area of application			End users				
	Info sharing	Situational Awareness	IMI	Citizens	Public admin	CE & CI	LE	Developers
CISAE: A Common Information Sharing and Analysis Environment	x	x				x		
SARD: Situational Awareness Regarding Disinformation		x	x		x		x	
ML4S: Media Literacy for Students			x	x				
CiToDeFaMe: Citizens Tools to Detect “Fake" Media			x	x				
WINS: What Information Needs to be Shared	x	x				x		
EESCM: Enhanced and Extended Supply Chain Management		x				x		
MIMI: A Market place for IMI Information	x	x	x		x		x	
GECHO: Gatekeeping ECHO Chambers		x			x			
CRP: Citizen - Responder Platform	x	x			x			
CiReTo: Citizens Reporting Tool	x	x		x	x		x	
LMHTT: Local Media Hybrid Threat Tracker			x		x			
STARLIGHT: Starlight Disinformation-Misinformation Toolset			(x)		x		x	x
AIMVVP: AI-Model Verification and Validation platform	x	x	x	x	x	x	x	x

Figure 4: EU-HYBNET assessed promising innovations

4.2 STANDARDISATION

In EU-HYBNET, the work goes beyond proposing recommendations for formal standards; we also provided guidance on legal harmonisation and highlight best practices that the project encourages stakeholders to adopt or draw inspiration from. It is important to emphasise that best practices often serve as the foundation for the future development of official standards, whether at the ISO, CEN, or national level. Another thing to notice is that given that the standardisation process typically takes at least two to three years, it is challenging for existing standards to keep pace with the rapidly evolving nature of hybrid threats. While there are relevant standards concerning safety, physical security, and cybersecurity more broadly, these are generally not specifically designed to address the complex and multifaceted characteristics of hybrid threats as outlined in this deliverable.

The standardisation recommendations are presented in the related deliverables.[8] Here is more touched the relevance to societal impact. The recommendations are made in order to provide clearer, more agreed-upon framework that ensure consistency, safety, quality, and efficiency when tackling hybrid threats. They underpin trust, enable interoperability, and support innovation while protecting the interests of individuals, organisations, and governments.

[8] See for example, D4.8 1st report for standardisation recommendations, D4.9 2nd report for standardisation recommendations, D4.10 3rd Report for standardisation recommendations, and especially D4.11 Final report for standardisation recommendations.

The key societal benefits of standards encompass, for example, enhancing public safety and security. Whether related to infrastructure, technology, health, or cyber domains, standards help ensure that products, systems, and services meet established safety requirements. This reduces risks to individuals and communities, particularly in critical areas such as transportation, energy, other elements of critical infrastructure and information security – all relevant domains when tackling in hybrid threats.

Standards also promote quality and reliability. When people know that a product complies with recognised standards, they can expect a certain level of performance and durability.

Thirdly, standards support economic efficiency and innovation. They streamline processes, reduce duplication, and facilitate compatibility between systems and technologies. At the same time, by establishing common foundations, standards can accelerate innovation by allowing developers to build upon shared frameworks rather than starting from scratch.

Standards also contribute to legal clarity and regulatory alignment, providing benchmarks that can support or inform legislation and public policy. In areas such as hybrid threats, where rapid technological change can outpace legal frameworks, standards help fill gaps and create a basis for common understanding and action.

Standards enhance also interoperability and cooperation, both within and across borders. They enable diverse systems, technologies, and institutions to work together effectively, thus fostering trust and cohesion in increasingly interconnected societies.

The main message to the society from EU-HYBNET on standardisation is that CISAE standardisation and situational awareness solutions are among the key recommendations. Effective information sharing remains crucial, as do tools that enable near real-time situational awareness. Also, AI will play a vital role in addressing hybrid threats. However, current solutions lack proper verification and validation processes, which must be prioritised. Thirdly, media literacy, the management of information manipulation and interference (IMI) campaigns, and tools for detecting disinformation and so-called "fake news" still face significant challenges. These areas require further attention and development. Moreover, public-private cooperation needs a more structured framework. Issues related to trust and legal uncertainty continue to hinder private sector participation. And lastly, procurement and funding pose additional obstacles. Existing financial and regulatory barriers highlight the need to reassess current frameworks to better support innovation and implementation.

Here below is presented further examples of the technologies/innovations on which EU-HYBNET made standardisation recommendations.

Innovation	Recommendation
MIMI – A Marketplace for IMI Information	Standard regarding the exchange of Data between the stakeholders: STIX, a language and serialization format for exchange of Cyber Threat Information (CTI) and TAXII, a CTI data exchange protocol.
EESCM, Enhanced and Extended Supply Chain Management (EESCM)	Best Practices: A Strategic Compass for Security and Defence (2022)
Detection of Disinformation Delivery Proxy Actors; Alerting on and Reacting to Disinformation in Real Time (Upgrade of Rapid Alert System on Disinformation)	Best Practices and legal solutions for better situational awareness more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels: The 2022 Code of Practice of Disinformation, upscale of RAS: FIMI Toolbox, multisectoral cooperation between fact-checkers, NGOs, research institutes, government units at different level
Identify and Safeguarding Vulnerable Individuals – GECHO (Gatekeeping ECHO Chambers)	Best Practices and legal solutions for increasing resilience and reducing vulnerability to disinformation on local and regional level: The 2022 Code of Practice of Disinformation (Transparency Centre signatories), improving educational systems, legislation allowing to verify kids' age in SM, multidisciplinary research teams
What Information Needs to Be Shared Between CI Entities to Detect Hybrid Threats and Attacks	Standards: ISO/TC 292, ISO 22343:2023 and other relevant Best practices: ENISA, The Common Information Sharing Environment (CISE) - EU initiative

Table 2: EU-HYBNET's standardisation recommendations (examples)

4.3 DISSEMINATION

Having an impact on society is often related heavily with dissemination and communication, i.e., how well the project has communicated its results to wider society.

Dissemination is presented more in details in the respective deliverables.[9] In short, dissemination encompasses all activities and tools used to communicate the outcomes of a project to relevant

[9] See for example, D5.5 Updated Dissemination, Communication and Exploitation Plan

audiences. The ultimate aim is not only to share information, but to ensure it is understood, appreciated, and ideally put to use. Dissemination, in this sense, is strategic outreach rather than mere publications.

The dissemination process involves a variety of communication activities: written outputs such as academic publications and policy briefs, of course the public deliverables, press releases, presentations at various events, blog posts, our webpage, social media, videos etc. The material is typically adapted to suit different stakeholders.

The key for dissemination to have an impact is to make it visible, useful and that the message is transformative in the real world, i.e., that the end result is not just adding to existing knowledge or practices, but that the message changes something fundamental about how people think, act, or make decisions: real-world change with lasting effects.

Thus, here in the report on societal impacts, the chapter that concerns dissemination is not interested with the amount of papers or clicks on website, but rather to evaluate the possible impact in the real world, inasmuch as one can say what is the real world.

As known for many who are involved with research projects, dissemination plays a crucial role in making an impact on society by ensuring that valuable knowledge, research findings, innovations, and best practices reach the right audiences in a clear, accessible, and actionable way. Without effective dissemination, even the most ground-breaking ideas risk remaining confined within academic or institutional boundaries, limiting their potential to benefit society at large.

Dissemination bridges the gap between knowledge and action. By translating complex research into practical messages and tools tailored for policymakers, practitioners, industry, and the public, dissemination enables evidence-based decision-making and real-world application of innovations. This is particularly important in areas like our theme – hybrid threads – where timely and accurate information can influence resilience and response strategies.

Dissemination also raises awareness and fosters public understanding. When people are informed about new challenges, technologies, or policy developments—such as those related to hybrid threats, dis- and misinformation, or cybersecurity — they are better prepared to engage, adapt, and contribute to solutions. This empowers individuals and communities, strengthening democratic participation and societal cohesion.

Moreover, dissemination enhances transparency and accountability, especially in publicly funded projects. Sharing results and progress with stakeholders builds trust and demonstrates the value and relevance of the work being carried out, contributing to public confidence in institutions and investments.

It also supports collaboration and knowledge exchange across disciplines, sectors, and borders. By creating opportunities for dialogue, feedback, and mutual learning, dissemination helps build networks that accelerate innovation and strengthen collective capacity to address complex societal challenges.

Finally, dissemination contributes to the sustainability and scalability of initiatives. By engaging end-users and decision-makers early and throughout the process, it increases the likelihood that findings

or innovations will be adopted, adapted, and maintained beyond the lifetime of a specific project or programme.

In short, the dissemination followed the following structure. First was the launch phase of EU-HYBNET focused on creating awareness among targeted stakeholders and establishing the project's visibility across Europe. Running from Month 1 (May 2020) to Month 7 (October 2020), this foundational phase aimed to inform stakeholders about the project's objectives and initial activities. It included the creation and launch of several key communication channels and platforms, such as the EU-HYBNET Twitter and LinkedIn accounts, the different platforms, and the project's official website and promotional materials. The activities collectively ensured that all relevant stakeholders were reached and became aware of EU-HYBNET's mission from the outset.

Then was the so-called implementation phase that formed the core of EU-HYBNET's lifecycle, extending from Month 8 through to Month 56. This period was dedicated to deepening stakeholder engagement, fostering dialogue, and collecting feedback to shape project outcomes. Stakeholders identified through the project's prioritisation system were actively consulted and involved. Key dissemination, communication, and engagement (DCE) activities during this phase included the organisation of various EU-HYBNET events, regular updates and contributions to the Innovation Arena platform, and sustained communication through social media moderation, website content development, and the publication of reports, briefs, and articles. The aim was not only to inform stakeholders but to build meaningful engagement, encouraging their active participation in shaping the solutions developed through the project.

The final phase, i.e., the sustainable phase, running from Month 57 to Month 60, focused on consolidating results, evaluating the impact, and ensuring the sustainability of EU-HYBNET's contributions. This phase requires the highest level of stakeholder involvement, as it brings together all actors to reflect on achievements and carry the results forward. The most significant event in this phase will be the final Annual and Future Trends workshops. These events will serve as key platforms to disseminate final results, showcase innovations, and explore future directions for collaboration and knowledge sharing beyond the project's conclusion.

The core dissemination activities in EU-HYBNET can be divided by their nature into two. The first are the dissemination activities supporting delivering the EU-HYBNET messages, for example, dissemination materials such as leaflets and videos etc. however, not forgetting strategic planning for the delivery of the key EU-HYBNET messages.

The second category are more targeted messages, perhaps more oriented toward having an impact, such as the policy briefs. The policy briefs are concise, focused documents that present research findings, analysis, and recommendations on specific policy issues to inform and influence mainly decision-makers. Their primary goal is to translate complex evidence or insights into clear, actionable guidance for policymakers, practitioners, and other stakeholders who may not be experts in the topic.

The EU-HYBNET policy briefs are accessible via our webpage.[10] Here below is an extract from our webpage:

[10] https://euhybnet.eu/policy-briefs-and-reports/

Figure 5: EU-HYBNET's Policy Briefs (examples)

EU-HYBNET also published various other publications. Here is an extract from the webpage.[11]

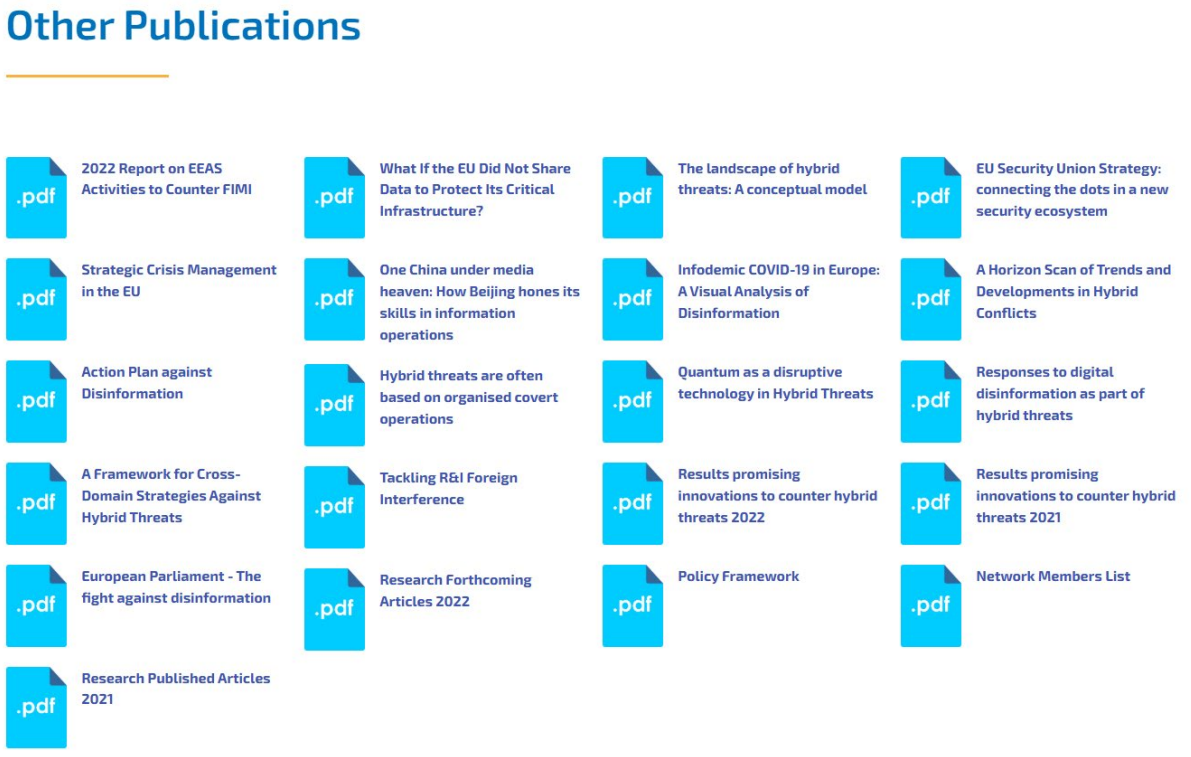

Figure 6: EU-HYBNET's Other Publications (examples)

[11] https://euhybnet.eu/other-publications/

5 SOCIETAL IMPACT ASSESSMENT (SIA)

In the D1.7 Societal Impact Mid-Term Review is presented the background and methodology for conducting a Societal Impact Assessment. In short, three main questions are addressed.

1) What may be the negative impacts/ethically questionable issues on individuals or societies that one could foresee arising with the EU-HYBNET project?
2) How these challenges could be resolved and/or how the problems could be mitigated?
3) What could be the possible positive outcomes or impacts to individuals or societies of EU-HYBNET?

Here below is presented the analysis of the collaborative work that the consortium did in April 2024 in Valencia.

5.1 THE FIRST QUESTION: CHALLENGES AND NEGATIVE IMPACTS

First are presented the analysis of the answers to the first question.[12]

During the SIA workshop, participants were invited to critically reflect on the potential challenges and negative impacts the project might pose. The diverse and thoughtful responses from the 22 participants shed light on a range of issues—some conceptual, others practical—that deserve serious attention as EU-HYBNET continues its work in the complex domain of hybrid threats.

A recurring concern centred around the potential for over-securitisation. Some participants warned that drawing too many societal issues into the internal security sphere could lead to overreach, where even uninformed or poorly judged actions are interpreted as foreign interference. This dynamic, they noted, risks criminalising more people than necessary and could result in diminished public trust, particularly among those who feel unjustly scrutinised. Related to this was a cautionary note about the unintended consequences of raising awareness: while increasing knowledge is essential for resilience, it could also evoke anxiety or unease among the general population, particularly if the scope and scale of hybrid threats are overwhelming.

Several participants highlighted structural and strategic limitations, including the EU's lack of a unified federal security apparatus. They expressed concern that while EU-HYBNET may successfully map out the hybrid threat landscape, the absence of a cohesive, pan-European response strategy could hinder the project's practical impact. This was further compounded by differing national perceptions of hybrid threats and the varying strategic cultures across member states, which can make unified action difficult.

Communication and engagement were also noted as key areas of concern. Participants emphasised the importance of reaching audiences beyond the project's immediate network and cautioned against the risk of knowledge being confined to a small, specialised group. There was a sense that more effort is needed to connect the rich body of knowledge generated by the project to end-users in a meaningful and lasting way. Others raised concerns about the depth and practicality of some discussions,

[12] Altogether 26 answers were from 23 different participants.

suggesting a need for more specific, actionable solutions and clearer guidance tailored to practitioners' needs.

Ethical and political implications were another common thread. Some participants feared that authorities might use the broad and ambiguous nature of hybrid threats as justification to curtail civil liberties in the name of national security. Others warned that EU-HYBNET's outputs could potentially be exploited by adversaries seeking to understand Europe's vulnerabilities and areas of focus. Concerns were also raised about the risks of increased suspicion towards external communities or individuals from outside the EU, potentially reinforcing negative stereotypes or exclusionary attitudes.

Technology was a focal point of several reflections, particularly the dual-use nature of AI and other emerging tools. While participants recognised the potential of these innovations in detecting and mitigating hybrid threats, they also pointed out the danger of such technologies being misused or manipulated by malicious actors, especially in environments where public trust in institutions is fragile.

Finally, participants acknowledged the challenge of translating the knowledge, expertise, and momentum built within EU-HYBNET into sustained and impactful action. Delivering concrete results to the right audiences and ensuring that those outcomes are embedded in long-term practice was described as a critical but complex task.

In conclusion, the feedback from this session demonstrates a healthy, constructive scepticism and a shared commitment to responsible, inclusive, and effective responses to hybrid threats. These reflections not only highlight important risks and blind spots but also serve as a reminder of the delicate balance between security and liberty, awareness and fear, coordination and fragmentation. Acknowledging and addressing these concerns is essential to maximising the societal benefit of the EU-HYBNET project and ensuring its legacy is one of resilience, trust, and collaboration.

5.2 THE SECOND QUESTION: MITIGATING CHALLENGES

The second question answers are analysed here below:

In response to the second workshop question — how the identified challenges and problems of the EU-HYBNET project could be resolved or mitigated — participants offered a wide array of constructive suggestions. These insights reflect both the complexity of the hybrid threat landscape and the importance of sustained, inclusive, and ethical approaches to counter it effectively.

One key theme that emerged was the need for sustained investment and long-term thinking. Participants noted that while securing research and development funding at the outset is often feasible, ensuring adequate operational expenditure (OPEX) for the maintenance, evolution, and continuity of the project is more difficult. Therefore, building a financial framework that supports ongoing activity beyond the project's formal conclusion is essential for long-term impact and resilience.

Transparency and openness were frequently mentioned as foundational principles. Maintaining openness, both within the network and in relation to the broader public, was seen as vital in establishing trust, credibility, and accountability. Participants stressed that EU-HYBNET should treat the public as equal stakeholders and embrace transparent communication as a tool for deflecting

misinformation or potential criticism. At the same time, they advised caution when dealing with sensitive topics, particularly when individuals are involved, urging project leaders to remain conscious of how their work might be perceived or misrepresented in public discourse.

Participants also highlighted the importance of inclusive, multi-stakeholder collaboration, not only across institutional boundaries but across generations. Bringing younger researchers into the project and cultivating the next wave of experts was seen as a vital step in ensuring continuity and fostering innovative thinking. In parallel, strengthening cooperation with other projects and networks was suggested as a way to combat knowledge fragmentation and create a broader reference point for countering hybrid threats.

Another critical point raised was the need for balance between openness and security. While knowledge sharing was broadly encouraged, participants urged caution regarding the publication of sensitive data that adversaries might exploit. Suggestions such as the use of Chatham House Rule meetings, careful vetting of those with access to network resources, and even formal use contracts were proposed to ensure that openness does not come at the expense of security or integrity.

Communication and engagement strategies were also seen as central to overcoming challenges. Participants called for more consistent and accessible messaging to decision-makers, ensuring that the work of EU-HYBNET is clearly understood and supported at the political level. Likewise, public awareness campaigns were encouraged, with an emphasis on positive messaging and minimising polarising or fear-based narratives. In particular, it was suggested that innovative solutions should be developed with genuine input from practitioners, ensuring that the end-users' perspectives remain at the heart of any response.

Participants also recognised the importance of practicality and real-world relevance. There were calls for more use cases, concrete KPIs, and measurable outputs, ensuring that the project maintains a strong link to operational realities. The theoretical work, while valuable, should be complemented by direct feedback and insights from those working on the ground.

Finally, some responses underscored the importance of open-mindedness and adaptability. Horizon scanning, proactive problem-solving, and a willingness to view issues from multiple perspectives were all identified as essential mindsets for navigating the uncertainty and complexity that define hybrid threats.

Taken together, these reflections highlight a shared commitment among stakeholders to improving the EU-HYBNET project and ensuring it serves as a resilient, inclusive, and responsive platform for addressing one of Europe's most pressing security challenges. They offer not only a roadmap for mitigation but a vision of collaboration grounded in transparency, practicality, and trust.

5.3 THE THIRD QUESTION: POSITIVE OUTCOME

When asked about the possible positive outcomes and impacts of EU-HYBNET on individuals and societies, participants offered a rich and optimistic range of responses, highlighting the transformative potential of the project in both tangible and intangible ways. At the heart of their reflections was the recognition that EU-HYBNET is not merely a research initiative, but a catalyst for building trust, strengthening cooperation, and enhancing societal resilience across Europe.

A key achievement identified was the creation of a pan-European network that brings together security practitioners, industry, SMEs, academia, and civil society. Participants noted that few other platforms offer such a comprehensive and inclusive space for the exchange of knowledge, solutions, and experiences. The strength of this network lies in its ability to foster collaboration across sectors, regions, and disciplines, creating opportunities for individuals from different countries and professional backgrounds to learn from one another and to develop a common understanding of hybrid threats.

Many responses emphasised the value of knowledge sharing and increased awareness. By deepening the understanding of hybrid threats, EU-HYBNET equips stakeholders with the tools needed for more effective and timely interventions. Participants underlined that the more we understand the nature of hybrid threats, the better our chances are of developing appropriate and strategic responses. This growing awareness also leads to greater public engagement and a more informed debate on how European values should be upheld in the face of emerging security challenges.

Another significant benefit identified was the enhancement of coordination and connectivity. Through EU-HYBNET, organisations have come to know who to contact, and how to act collectively. This has not only strengthened operational capabilities but also fostered a sense of community and shared responsibility. The project has shown how connecting the dots—both conceptually and interpersonally—can result in a stronger, more coherent response to complex threats.

Several participants spoke about the positive message EU-HYBNET sends, both within the EU and to international partners. By actively addressing hybrid threats and investing in resilience and capacity-building, the project demonstrates that Europe is preparing for the future with seriousness and solidarity. Even if some results are not immediately quantifiable, the symbolic strength of this collective effort should not be underestimated.

From a more practical perspective, participants pointed to problem-solving mechanisms, new ideas, and the development of solutions grounded in real user needs. By engaging with end users, EU-HYBNET has contributed to more targeted innovations and a better alignment between policy, research, and practice.

Some reflections touched on the cultural and human aspects of the project. Respondents noted the value of exchanging perspectives, discovering best practices from across Europe, and creating an environment rooted in mutual respect and openness. The mention of “peace and love” may have been light-hearted, but it captures a deeper truth: that trust, empathy, and cooperation are vital in countering division and fear, which are often exploited by hybrid threats.

Importantly, many participants recognised EU-HYBNET’s ability to mobilise and sustain a vibrant, functional network, something many similar projects struggle to achieve. This ongoing engagement

ensures that the knowledge generated is not static, but continuously evolving and responsive to changing conditions.

In conclusion, the positive impacts of EU-HYBNET span from improved knowledge and institutional coordination to stronger societal awareness and unity. By creating a space for dialogue, exchange, and action, EU-HYBNET not only counters hybrid threats but also contributes to building a more connected, resilient, and confident Europe.

5.4 SUMMARY OF REFLECTIONS ON EU-HYBNET'S CHALLENGES, SOLUTIONS, AND IMPACT

Stakeholder reflections from EU-HYBNET workshops reveal a balanced perspective on the project's challenges, solutions, and positive societal contributions. Concerns were raised about the risk of over-securitisation, fragmentation in EU-wide strategies, and the potential misuse of shared knowledge or emerging technologies. Participants also noted the difficulty in sustaining momentum and translating awareness into action without clear, long-term structures and support.

To address these challenges, solutions focused on greater transparency, inclusive communication, and stronger engagement with both practitioners and the public. Emphasis was placed on practical improvements — such as sustainable funding, user-driven outputs, and secure but open knowledge sharing — as well as fostering cooperation across sectors, generations, and national borders.

Despite the complexities, the project was widely recognised for its achievements. EU-HYBNET has built a unique, pan-European network that enables knowledge exchange, strengthens resilience, and brings diverse actors together around a shared goal. It has raised awareness, fostered trust, and delivered a clear message that Europe is taking hybrid threats seriously. By maintaining its inclusive, action-oriented approach, EU-HYBNET is well-positioned to contribute to a more resilient and united Europe.

6 CONCLUSION

The EU-HYBNET project set out with an ambitious yet crucial objective: to build and empower a Pan-European network capable of responding effectively to hybrid threats. As this final report demonstrates, the project has achieved much more than the sum of its parts: laying a strong foundation for societal resilience, innovation, and cooperation in the face of complex and evolving security challenges.

At the heart of EU-HYBNET's societal impact is the network itself: a diverse and dynamic community of practitioners, researchers, policymakers, civil society actors, and industry representatives, united by a shared commitment to understanding and countering hybrid threats. This network has enabled valuable exchanges of knowledge and expertise, promoted joint problem-solving, and forged relationships that will endure beyond the project's formal conclusion. By fostering trust and mutual understanding, EU-HYBNET has helped to align efforts across sectors and countries, enhancing both local and European capacities to identify, assess, and respond to threats that transcend traditional boundaries.

Equally impactful has been EU-HYBNET's role in defining common requirements, supporting innovation, and guiding standardisation. By identifying capability gaps and supporting the development of new tools, methods, and frameworks, the project has directly contributed to strengthening Europe's security and societal preparedness. These efforts have helped ensure that the tools used to counter hybrid threats are not only technically advanced, but ethically sound, practically useful, and societally acceptable.

The importance of dissemination and communication in achieving real-world impact has also been made clear. EU-HYBNET's structured approach to stakeholder engagement: through various events, publications, policy briefs, and digital platforms has ensured that knowledge is not only produced but shared, applied, and embedded into practice. The project has raised public awareness of hybrid threats, encouraged debate on European values, and demonstrated the power of transparency and open dialogue.

The reflections gathered through the Societal Impact Assessment offer a balanced and thoughtful view of both the challenges and opportunities on societal impacts that EU-HYBNET presents. Concerns about over-securitisation, the ethical use of technology, and maintaining momentum are valid and must continue to guide future work. At the same time, participants overwhelmingly acknowledged the project's positive impacts on individuals, institutions, and societies alike.

In conclusion, EU-HYBNET has succeeded in creating a collaborative ecosystem that empowers Europe to face hybrid threats with resilience, innovation, and unity. It has shown that enhancing security vis-à-vis hybrid threats is not only about protecting borders or infrastructures, but about fostering trust, strengthening democratic values, and building a more informed and connected society. As the project ends, its legacy continues in the form of a living, evolving network, that HybridCoE will take over. It will be one that remains ready to respond, adapt, and lead in the ever-changing security landscape of the ever-evolving future.

7 ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
CI	Critical Infrastructure
CISE	Common Information Sharing Environment
DoA	Description of Action
DCE	Dissemination, Communication, and Engagement
EESCM	Enhanced and Extended Supply Chain Management
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU MS	European Union Member State
EC	European Commission
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats
FIMI	Foreign Information Manipulation and Interference
GDPR	General Data Protection Regulation
HybridCoE	Hybrid Threads Centre of Excellence
IMI	Internal Market Information System
NGO	Non-profit organisation
OB	Objective
OPEX	Operational expenditure
RAS	Rapid Alert System
SIA	Societal Impact Assessment
SME	Small or Midsize Enterprise
WP	Work Package
MS	Milestone
WP	Work Package
T	Task