



# EU-HYBNET

Final Results Booklet



Funded by  
the European Union

2020 - 2025



# FOREWORD

---



**Isto Mattila**  
Project Coordinator

Welcome to the EU-HYBNET Final Results Booklet, where we present the outcomes of our five-year journey to understand and counter hybrid threats. While our project concludes here, the challenges posed by hybrid threats are ongoing and evolving.

It is encouraging to see growing recognition of these threats at institutional levels. Europol, for example, recently released its Serious and Organised Crime Threat Assessment (SOCTA), which highlights a notable trend: non-state actors (NSAs) increasingly operate on behalf of foreign state actors to advance hybrid threat agendas. This convergence of criminal and geopolitical motives received considerable

attention during the publication event and is expected to shape the priorities of the upcoming policy cycle. These developments reinforce a key finding of our project—that criminal networks are becoming deeply intertwined with hybrid threat activities, often serving as proxies. While financial gain remains their primary driver, their actions also further the strategic interests of state sponsors.

The Hybrid CoE's February 2025 report, "Countering State-Sponsored Proxies: Designing a Robust Policy," echoes this view. It underscores that delegating hybrid operations to proxies is a strategic choice by state actors: it is cost-effective, deniable, and minimizes risks. Proxies benefit from increased access to resources and strategic opportunities, while state sponsors exploit their local expertise and plausible deniability.

Building on this understanding, LAUREA University of Applied Sciences has launched a new initiative under Horizon Europe funding—Project Vigimare. This project addresses hybrid campaigns targeting maritime infrastructure, a sector critical to EU and NATO operations. Vigimare aims to detect anomalies near submarine and land-based infrastructure, and visualize them in a Virtual Control Room accessible to a broad network of stakeholders. This proactive approach enhances our ability to anticipate and mitigate attacks, increasing the risk of exposure for NSAs.

Encouragingly, early implementation of this approach has coincided with a period free of new cable or pipeline attacks, suggesting its potential as a model for protecting other sectors of critical infrastructure. This framework aligns with the resilience goals of the CER Directive, and we strongly recommend its consideration in the next Cluster 3 R&D program.

Coordinating the EU-HYBNET project has been an immensely rewarding experience. Our success is rooted in the dedication of our partner network—committed experts who have contributed solutions, explored opportunities for standardization, and fostered innovation throughout the project. As we transition to the next phase, we are proud to pass the baton to Hybrid CoE, which will host and build upon the EU-HYBNET network. On behalf of LAUREA's coordination team, we extend our deepest gratitude to all partners and supporters. We look forward to continued collaboration in the shared mission to counter hybrid threats and safeguard our societies.

With best regards,  
**EU-HYBNET Coordinator, Isto Mattila**



# ABOUT EU-HYBNET

---

The EU-HYBNET project, formally titled "Empowering a Pan-European Network to Counter Hybrid Threats," is a five-year initiative (2020–2025) funded by the European Union's Horizon 2020 programme.

The main goal is to enhance Europe's ability to detect, prevent, and respond to hybrid threats by fostering cooperation among security practitioners, industry stakeholders, academia, and policymakers. The project focused on expanding and maintaining a strong network dedicated to countering hybrid threats, identifying common needs to address gaps in knowledge, performance, research, and training, and keeping track of relevant research and innovation to guide priorities for further development and standardization. It also aimed to create opportunities for meaningful interaction between stakeholders, promote knowledge sharing and capacity building, and lay the foundation for synergies with existing national and European networks. EU-HYBNET operated using a cyclical and adaptive methodology structured around four core themes:

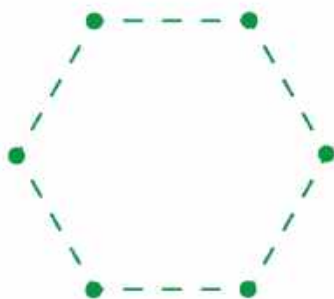
- Future trends of hybrid threats
- Cyber and future technologies,
- Resilient Civilians, Local Level and National Administration
- Information and strategic communication.

The EU-HYBNET has been producing valuable results throughout its lifetime, such as research papers, policy briefs, trainings and various events for the hybrid threat community; however, one of its main results remains the EU-HYBNET Network that has been created and sustained, with 158 member organisations.

This present booklet is a culmination of EU-HYBNET results. It aims to bring together the main outcomes of the 5-year project and all of the work carried out by our motivated consortium. In order to allow an easier read and for new stakeholders to quickly jump in, the results are synthesized, but more in-depth reading of our results can be found in our project documents, such as deliverables, policy briefs, reports and more. All of these can be found on the EU-HYBNET website, which will be online until 2028. As mentioned in the foreword, EU-HYBNET does not end with the project in April 2025. The Hybrid Center of Excellence will be taking over the network, and if you would like to know more about the future of EU-HYBNET, please contact [eu-hybnet@hybridcoe.fi](mailto:eu-hybnet@hybridcoe.fi).







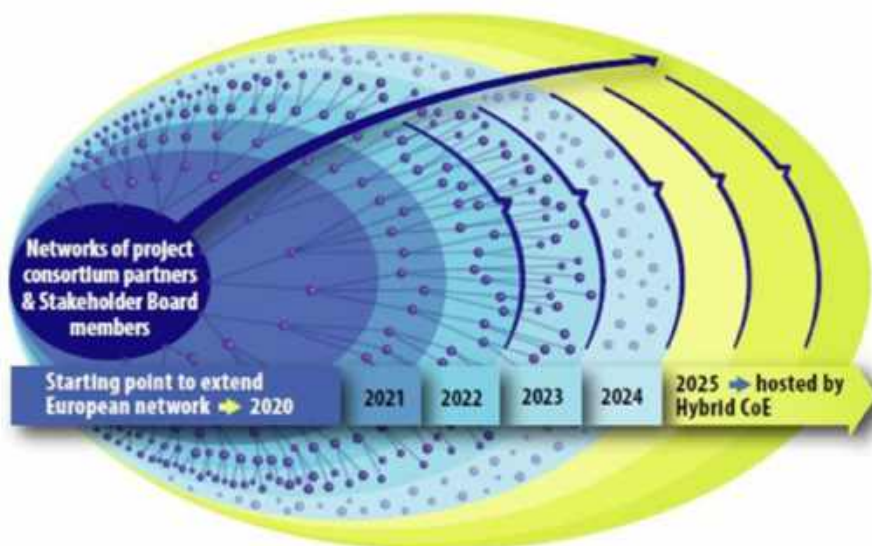
# THE NETWORK

As a Network of Practitioners (NoP) project, EU-HYBNET's goal was to empower a pan-European network of security practitioners, stakeholders, academics, and industry (including SMEs) to collaborate to better counter hybrid threats.

The network was built into EU-HYBNET activities, such as the gaps and needs related research activities in each of the four core themes, which was conducted jointly with the project consortium partners and new or potential members of the extended EU-HYBNET Network. Additionally, yearly events such as the Annual Workshops or Innovation and Knowledge Exchange Workshops were planned around attracting new members to the network, and interacting with the existing ones, in order to share expertise in the field. The network also represents a measure of the impact of the project, as it has gained the ability to gather members from all over Europe from various domains, as well as create lasting collaborations between the network members. As of April 2025, the project finish date, the EU-HYBNET network has over 160 entities from 26 countries. Thank you to all of our network members who have joined our events, collaborated endlessly, and shown that the community to counter hybrid threats is thriving and excited to keep working together. We hope to be able to continue collaborating in the future!

As previously mentioned, the EU-HYBNET network does not end with the project. The Hybrid Centre of Excellence will take over the network, as planned since the start of the project. Activities will look different than they did while the project was ongoing, but make sure to stay up to date to not miss what's next!

## EU-HYBNET Network extension 2020 ➔



# The EU-HYBNET Network in Numbers

## Practitioners



**30 Institutions**  
**17 Countries**

## Academia & RTO



**48 Institutions**  
**19 Countries**

## Industry/SME



**32 Institutions**  
**13 Countries**

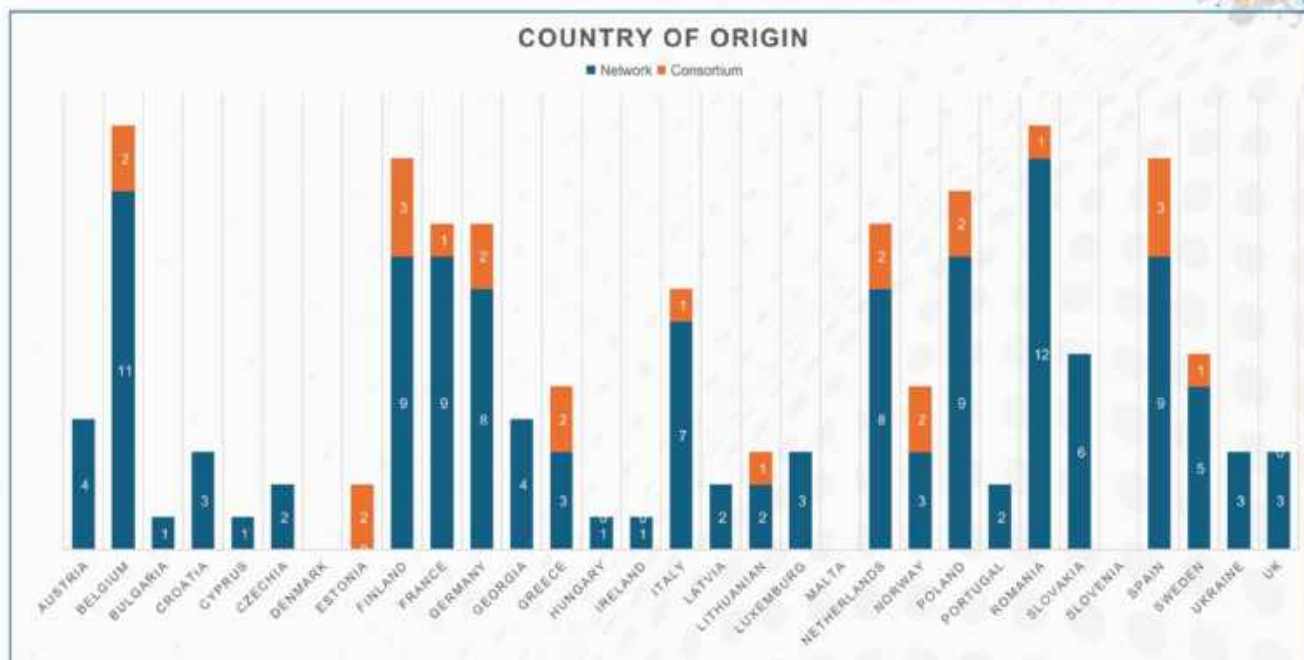
## NGOs



**22 Institutions**  
**15 Countries**

## EU-HYBNET Network by country

EU-HYBNET



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



# EU-HYBNET Network Members

## by Core Theme



*Future Trends of Hybrid Threats*



56



*Cyber & Future Technologies*



36



*Resilient Civilians, Local Level, and Administration*



28



*Information & Strategic Communications*

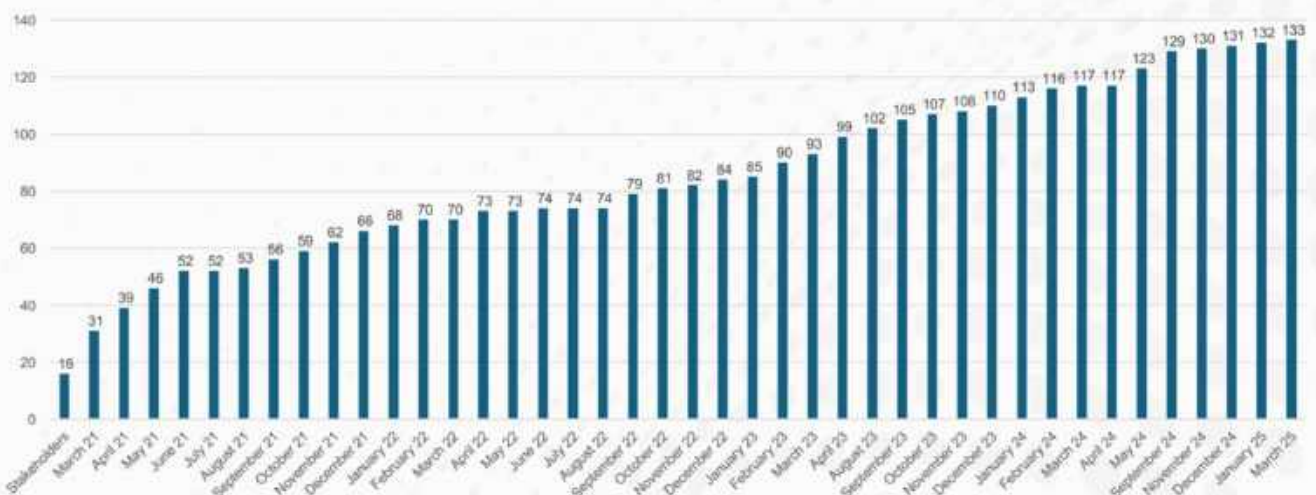


33

### The growth of EU-HYBNET Network March 2025



Including network members and Stakeholders



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



## Identifying the Gaps & Needs of the Hybrid Threat Ecosystem

EUHYBNET has systematically mapped, analyzed and addressed the critical gaps and needs of European practitioners, industry and academia in countering hybrid threats—and in doing so laid the foundation for a resilient, innovation-driven network across the continent.

In its first phase: the Gaps & Needs (G&N) events, EU-HYBNET convened stakeholders from government, private sector, research and civil society to share concrete observations on operational challenges. Recognizing that no single organization would disclose all of its vulnerabilities, the project adopted a cross-domain, qualitative methodology. Through four iterative G&N cycles and a final stocktaking workshop, participants collectively identified and prioritized recurring shortfalls in knowledge, performance and innovation. The final evaluation report (Deliverable D2.8) catalogued these needs, linked them to candidate solutions, and sketched emerging capability trends, thereby directly supporting EUHYBNET objectives to build a sustainable practitioner network, bridge knowledge and performance gaps, and foster capacity-building and knowledge exchange.

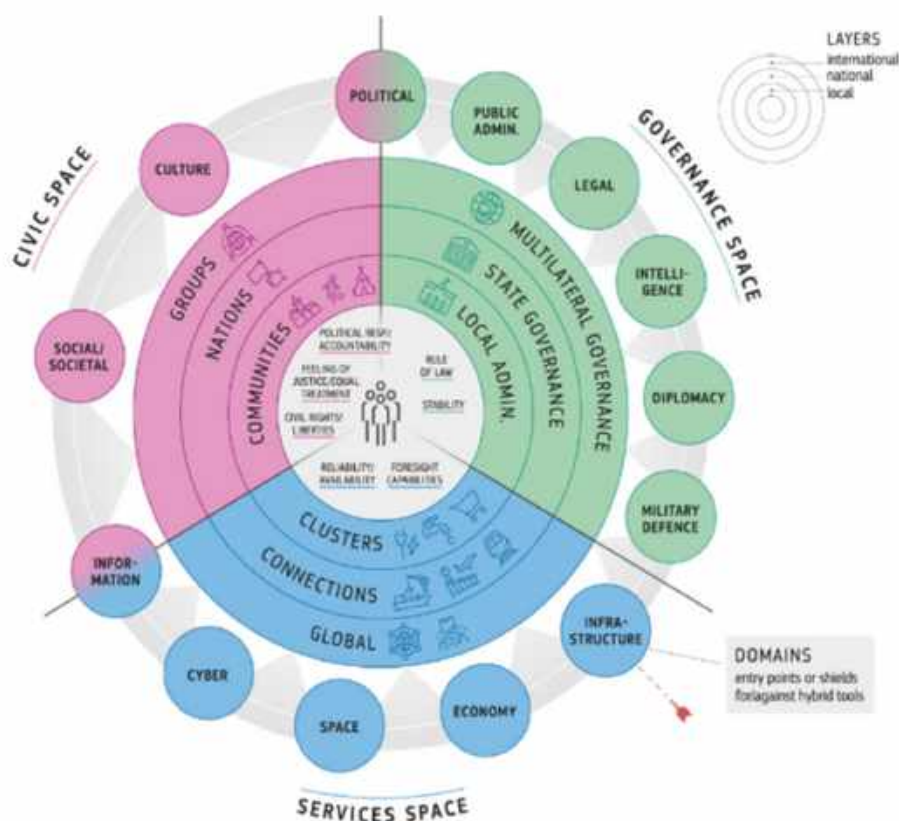
Building on those insights, EU-HYBNET translated the long list of needs into four thematic research strands: Future Trends of Hybrid Threats, Cyber and Future Technologies, Resilient Civilians, Local and National Administration, and Information and Strategic Communication. In Year 3, consortium members and network experts coauthored at least one research article per theme—examining topics from droneborne attacks on critical infrastructure and 5G security ontologies to weaponized migration and AI-enhanced disinformation. Each article offers early-stage recommendations and practical guidelines for stakeholders, while



feeding directly into EU-HYBNET's innovation surveys and uptake recommendations. Grounded in the Horizon 2020 GM01 call, D2.15 not only met the requirement to monitor cutting-edge research and technology developments, but also set a clear, cycle-based methodology for successive research, training and innovation testing.

Finally, the report on “Training & Exercise Lessons Learned” distilled the outcomes of the project's three scenario-based exercises, culminating in January 2024's final training in Vilnius. Using the Disruptive Technology Assessment Game (DTAG), participants experimented with “Ideas of Systems” (IoSs)—from conceptual frameworks to concrete tools—to tackle hybrid threat vignettes. Incorporating feedback from earlier cycles, the last exercise featured simplified scenarios, inperson engagement, redteaming and direct involvement of innovation providers. Attended by practitioners, industry and academic actors from 10 countries, the Vilnius event confirmed the value of tightly focused exercises (limiting innovation trials to one or two IoSs), clear preparatory materials and skilled moderation. Its lessons now guide future EU-level training design and underpin the validation and standardization of promising solutions.

Across mapping, research and exercises, EU-HYBNET has not only achieved its objectives of gap identification, knowledge enhancement, network extension and innovation testing—but has also forged a sustainable, pan-European community equipped with evidence-based insights and practical tools to anticipate, counter and outpace hybrid threats.



**Comprehensive Resilience Ecosystem CORE Model**  
developed by HCoE & JRC





# Innovation Mapping & Surveys to Technology and Research

The work carried out by the project has been instrumental in monitoring and analyzing research projects, identifying gaps, and proposing recommendations to strengthen Europe's resilience against hybrid threats. Hybrid threats exploit the interconnectedness of modern societies, targeting vulnerabilities across economic, political, and social systems. EU-HYBNET recognizes this complexity and structured its work around the four core themes previously mentioned. By focusing on these themes, the project ensured a holistic approach to understanding and countering hybrid threats, acknowledging their multifaceted nature and the need for cross-disciplinary collaboration.

The methodology adopted by EU-HYBNET partners combined rigorous research with practical insights from stakeholders. The process involved identifying gaps and needs (see previous section) through engagement with practitioners, scanning the research landscape to map existing projects, and analyzing and reporting findings to highlight the state of research, identify gaps, and propose actionable recommendations. This iterative process ensured that project's innovation mapping work remained relevant, practical, and forward-looking, providing valuable insights for both researchers and policymakers.

To effectively counter hybrid threats, it is essential to integrate hybrid threats into various research domains, ensuring a comprehensive understanding and response. Societal resilience, built on social trust and effective institutions, is key to preventing governance breakdown and violent conflict. Enhancing pan-European collaboration through strengthened cooperation and coordination among EU members will improve situational awareness and response capabilities. Sustained research efforts, especially in the turbulent global political landscape, are crucial to address evolving hybrid threats.

Continued investment in research and innovation, along with the integration of hybrid threats into educational curricula and professional training programs, will ensure that future generations are equipped to recognize and counter these threats. Policymakers should engage with the hybrid threats community to shape regulations and standards that reflect the complexities of these threats. Additionally, fostering a culture of open dialogue and collaboration between governments and citizens will build trust and strengthen societal resilience. These actions will be instrumental in guiding future research, policy initiatives, and practical efforts to counter hybrid threats, ensuring Europe's resilience in an increasingly complex and interconnected world.



# Key Innovation Mapping Findings per Core Theme



## *Resilient Civilians, Local Level, and Administration*

Research from this core theme emphasized empowering communities and strengthening local governance to resist hybrid threats. Innovations from the third and fourth cycles addressed challenges like normalized violence, civil society intimidation, and manipulation through conspiracy theories. Legislative proposals expanded directives on violence in public discourse. Solutions like Breach Guard and the Anti-SLAPP Support Network aimed to shield civic actors from legal harassment. The HIPSTER initiative and FIMI-related frameworks provided tools to counter manipulative narratives and disinformation. These innovations strengthen civilian resilience, reinforce democratic trust, and enhance administrations' capacity to respond to hybrid threats.



## *Cyber & Future Technologies*

Research under this theme addressed the complexity of digital threats and the potential of emerging technologies. Innovations included strategies for mitigating supply chain disruptions using Digital Twins to simulate and stress-test responses and the CYBERSECURITY SKILLS ALLIANCE (REWIRE) project which aimed to develop a European cybersecurity skills framework. To combat the weaponization of mass data, projects proposed platforms like NordLayer for data protection, addressing privacy and security in increasingly interconnected environments. Additionally, tools aimed at regulating digital actors and securing personal data. These efforts reflect a proactive approach to preparing cybersecurity systems for future challenges, from algorithmic risks to systemic digital vulnerabilities.



## *Information & Strategic Communications*

Information & Strategic Communication research highlights the economic challenges faced by traditional media contributing to the spread of disinformation. Initiatives like JOLT and MeDeMAP are exploring sustainable business models for quality journalism, while projects such as COMPROP and RUSINFORM are developing tools for fact-checking and content moderation to combat misinformation on social media. The Journalism Trust Initiative (JTI) aims to promote trustworthy journalism through standardized evaluation processes. Additionally, blockchain-based verification is emerging as a crucial technology for ensuring the authenticity of digital content, enhancing credibility and trust in the media landscape.



## *Future Trends of Hybrid Threats*

The Future Trends research has revealed vulnerabilities in critical infrastructures and supply chains, with initiatives like EUCISE2020 and ANDROMEDA improving situational awareness and information sharing. The rise of populism and the weaponization of migration are significant hybrid threats, highlighting the urgent need for better data sharing and security measures. Tools like We-VERIFY and the Media Pluralism Monitor help combat misinformation and protect media pluralism, while proposals for enhanced EU intelligence cooperation and platforms to detect foreign interference aim to bolster resilience against these evolving threats.



# Innovation Uptake & Standardisation

For its Innovation Uptake and Standardisation activities, EU-HYBNET translated the accumulated gap analyses, innovation surveys and exercise learnings into a coherent set of policy-level outputs and standardization roadmaps designed to accelerate the uptake and industrialization of hybrid threat countermeasures across Europe. The project produced a series of policy briefs, position papers and recommendation reports for policymakers, training developers and technology providers, with a target of at least seven briefs over five years. One notable contribution is the EU-HYBNET Innovation which proposes the creation of MIMI, a marketplace for sharing Information Manipulation and Interference (IMI) information to enhance societal resilience and improve responses to hybrid threats.

EU-HYBNET applied the MCUIR (Methodology for Creation of Uptake, Industrialization, and Research strategies) to chart how innovations within the hybrid threat domain can progress toward market adoption, uptake, industrialization, and exploitation across the EU. Innovations were assessed and developed through a structured process involving stakeholder feedback, strategic roadmapping, and the use of an Innovation Uptake Canvas. Two EU projects are currently collaborating with EU-HYBNET partners to further refine and advance this approach.

Following the analysis of the mapped innovations, it became evident that the proposed solutions address critical areas within the hybrid threat landscape and deliver clear benefits to a wide array of end-users. Many of these solutions act as enablers—most notably, the final solution AIMVVP (AI-Model Verification and Validation Platform) and CISAE (Common Information Sharing and Analysis Environment). The project's outcomes include both research-driven insights and structured, implementation-oriented strategies. Key thematic areas include: the standardization of CISAE to improve secure information sharing; the deployment of AI-driven tools for disinformation detection and complex data flow analysis; and the development of media literacy training and tools for identifying fake media. Additionally, increased private sector participation and targeted procurement mechanisms are crucial for





# Policy Briefs


Over the past five years, the EU-HYBNET project has produced a series of 6 policy briefs that provide deep insights into the state of play in various research areas, identify gaps, and propose actionable recommendations. The following section encapsulates the key results and contributions of EU-HYBNET's work in this area. The full briefs are on the EU-HYBNET website.

EU-HYBNET's policy briefs and recommendations aimed to facilitate policy dialogues, indicate priorities for innovation uptake and industrialization, and determine priorities for standardization. The methodology involved:

- **Identifying Key Areas:** Focusing on critical themes such as information domain vulnerabilities, countering hybrid threats, and building societal resilience.
- **Engaging Stakeholders:** Collaborating with practitioners, researchers, and policymakers to ensure the relevance and practicality of the findings.
- **Analyzing and Reporting:** Structuring the findings into deliverables that highlight the state of research, identify gaps, and propose actionable recommendations.

This iterative process ensured that EU-HYBNET's work remained relevant, practical, and forward-looking, providing valuable insights for both researchers and policymakers.

To effectively address hybrid threats, it is essential to integrate them across diverse research domains. This calls for interdisciplinary collaboration, ensuring that these complex threats are not studied in isolation but rather in conjunction with broader societal, technological, and political contexts. A critical component of this approach is enhancing societal resilience—fostering social trust and reinforcing the strength of democratic institutions. Building cohesive communities that can resist and recover from hybrid threats is vital for maintaining stability and preventing governance breakdowns or violent conflict. Moreover, pan-European collaboration must be strengthened to boost situational awareness and response capabilities. Improved mechanisms for sharing information, best practices, and lessons learned among EU member states will enhance a coordinated and unified response to emerging challenges. Continued research is also crucial, particularly in the face of an increasingly volatile global political environment. Keeping pace with technological advancements and geopolitical shifts will ensure preparedness for the evolving nature of hybrid threats. Finally, ethical considerations must remain at the forefront. It is imperative that strategies to counter these threats uphold democratic values and human rights, guided by robust ethical frameworks for research, policy development, and technology use.





securing funding and overcoming regulatory barriers. The analysis also underscores that hybrid threats evolve faster than regulatory frameworks, highlighting the pressing need for EU-wide standardization. AI and Big Data technologies are central to enabling real-time threat analysis, media verification, and crisis response, while early involvement of end-users ensures that resulting tools are practical, effective, and fit for purpose. Expanding media literacy across education systems is essential for long-term resilience against misinformation. Cross-sector collaboration between government, academia, and industry is vital. EU-HYBNET recommends fostering public-private partnerships and enhancing citizen engagement to address trust issues and legal challenges. Collectively, the proposed solutions represent a multi-layered strategy that reinforces societal resilience across governance, civic, and service domains. By integrating technological innovation with structured governance and community engagement, these initiatives contribute to a robust ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats. Finally, while most solutions are independent, CISAE emerges as a foundational enabler. Other solutions—such as Situational Awareness Regarding Disinformation (SARD) and additional sharing platforms—can be built upon it. Consequently, the roadmap for implementation should prioritize CISAE in the early stages, with other innovations progressing in parallel.

Together, EU-HYBNET’s policy briefs and standardization recommendations fulfill Objective 4—“to indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation” By weaving policy guidance, practical training lessons and concrete technical roadmaps into a unified narrative, the innovation and standardisation work ensures that EUHYBNET’s end-to-end pipeline—from gap identification to exercise validation to policy and standardization—is positioned to bolster European resilience against hybrid threats well beyond the project’s lifespan.

### Solutions mapped on three main areas of applications and five end-user categories

Project cycle	Solution	Main area of application			End users				
		Info sharing	Situational Awareness	IMI	Citizens	Public admin	CE & CI	LE	Developers
1	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				
2	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			
3	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
4	AIMVVP: AI-Model Verification and Validation platform	x	x	x	x	x	x	x	x



## Policy Brief #1: “Framing the Information Domain Vulnerabilities”

The policy brief "Framing the Information Domain Vulnerabilities" highlighted the erosion of traditional journalism's business model due to digital disruption and the rise of disinformation. It emphasized the need for sustainable business models for quality journalism and the challenges posed by the digital landscape. The brief also discussed the societal demand for disinformation and misinformation, driven by confirmation bias and echo chambers. It highlighted the role of social media in amplifying misinformation and the need for media literacy to counter this phenomenon. The recommendations put forward the need for regulatory frameworks to govern the use of personal data in targeting individuals.


---



## Policy Brief #2: “Countering Hybrid Threats: Areas for Improvement and Developing Innovations”

The policy brief "Framing the Information Domain Vulnerabilities" highlighted the erosion of traditional journalism's business model due to digital disruption and the rise of disinformation. It emphasized the need for sustainable business models for quality journalism and the challenges posed by the digital landscape. The brief also discussed the societal demand for disinformation and misinformation, driven by confirmation bias and echo chambers. It highlighted the role of social media in amplifying misinformation and the need for media literacy to counter this phenomenon. The recommendations put forward the need for regulatory frameworks to govern the use of personal data in targeting individuals.

---



## Policy Brief #3: “Information Manipulation and Interference”

The policy brief "Framing the Information Domain Vulnerabilities" highlighted the erosion of traditional journalism's business model due to digital disruption and the rise of disinformation. It emphasized the need for sustainable business models for quality journalism and the challenges posed by the digital landscape. The brief also discussed the societal demand for disinformation and misinformation, driven by confirmation bias and echo chambers. It highlighted the role of social media in amplifying misinformation and the need for media literacy to counter this phenomenon. The recommendations put forward the need for regulatory frameworks to govern the use of personal data in targeting individuals.



## Policy Brief #4: “Fame on social media, a new currency of cybercrime?”

This policy brief explores the emerging trend of cybercriminal groups leveraging social media for publicity, recruitment, and operational expansion, highlighting how these groups have evolved from operating in the shadows to actively seeking fame and attention on platforms like Telegram and Twitter. This shift has led to the normalization of cybercrime, attracting younger individuals and creating new challenges for law enforcement and the research community. The brief discusses the rise of ransomware as a service (RaaS) and the role of state-sponsored cyberwarfare, as seen during the Russian invasion of Ukraine. It emphasizes the need for enhanced technical expertise, timely communication, and robust security measures within organizations to counter this evolving threat, and leveraging existing exchange platforms to intensify information sharing and collaboration at the European level.



## Policy Brief #5: “On Information Sharing between Critical Entities for early and efficient detection and mitigation of Hybrid Threats”

The brief explores the need for enhanced information sharing to counter hybrid threats, which exploit societal vulnerabilities and combine tactics to undermine democratic societies. It highlights that current asset-focused protection strategies overlook interdependencies and cascading risks, proposing the WINS methodology to identify and share essential Indicators of Hybrid Threats (IoHT) using privacy-preserving technologies. This approach enables early detection and mitigation of hybrid threats, fostering resilience across sectors. The brief recommends extending the Critical Entities Resilience (CER) Directive to include near-real-time cross-domain sharing of IoHT data and urges the European research community to develop tools and architectures for analyzing shared IoHT, along with privacy-enhancing technologies. It concludes by advocating a live test and demonstration solution to validate these proposals.



## Policy Brief #6: “Reflections on the use of the DTAG Methodology for EU-HYBNET trainings (2020-2025)”

The EU-HYBNET policy brief highlights the effectiveness of the Disruptive Technology Assessment Game (DTAG) methodology—developed by TNO and adapted for EU-HYBNET—in evaluating innovative solutions to counter hybrid threats. It emphasizes the importance of consistent methodology, expert moderation, and manageable participant numbers (capped at 50) to ensure productive training sessions. Recommendations include tailoring scenarios to training goals, dividing participants into smaller groups, and allowing time for open discussion. While focused on security-related training, the DTAG approach is adaptable to other fields with proper preparation.



# OUR PARTNERS

The EU-HYBNET consortium has 25 partners from 14 different EU Member States and associated countries. The consortium comprises of 12 practitioner partners, and the remaining partners represent industry, SMEs, academia and other organisations.







# THANK YOU FOR READING!

---

[www.euhybnet.eu](http://www.euhybnet.eu)

@EUHYBNET

[eu-hybnet@hybridcoe.fi](mailto:eu-hybnet@hybridcoe.fi)



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