EU-HYBNET

EU-HYBNET

Final Newsletter – March 2025

Welcome to the ninth and Final EU-HYBNET Newsletter focusing on the project activities in the last project mini-cycle!

The past months have been active when finalizing our successful project in 4th and final cycle. The EU-HYBNET community has had the opportunity to gather in several project events. 3rd Innovation standardisation workshop was held in Brussels in October and the final events, 5th Annual workshop and 5th Future Trends workshop in Brussels in February. These events once again proved the success of EU-HYBNET in building an active network of experts in different expertise areas in the hybrid threats field.

Hybrid threats are phenomena that don't end after our project ends. It's good to recognise that also Europol is starting to see a shift to more attention for hybrid threats. Europol released its Serious and Organised Crime Threat Assessment recently. This document mentions that criminals (NSA = Non-State Actor) are also increasingly acting on behalf of foreign state actors to facilitate hybrid threats, and this was given some serious attention in the event around the report publication. That report is an important factor in setting the priorities for the next policy cycle. Criminal networks are increasingly intertwined with external hybrid threats, encompassing a wide range of criminal activities and tactics, often executed through criminal proxies. While the financial gains remain the primary motivation for these networks, their actions also serve – directly or indirectly – the geopolitical interests of those orchestrating hybrid threats.

Similarly, in the HybridCoE report from February 2025 "Countering state-sponsored proxies: Designing a robust policy" it is stated that the reasons why states delegate

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

hybrid threat activities to NSAs are well-established, as they follow the familiar logic of conflict delegation. It is cost-effective, deniable, and risk averse. It allows the sponsor to benefit from the proxy's local or specialist knowledge, while minimizing the risk of retribution. For the proxy, it provides an avenue for resource maximization and increases their chances of attaining strategic goals.

The LAUREA University of Applied Sciences has recognised this area of threat campaigns and was funded (HorizonEuropa) with a new project called Vigimare. The reasoning of the new project lies in this new way of harming our society using NSA's. Maritime infrastructure supports a range of essential services. The critical contribution made by maritime assets across the EU and NATO has heightened concerns over their vulnerability to sabotage and other deliberate attacks, including those forming part of a hybrid campaign. The main idea of the project is to detect anomalies close to submarine infrastructure and also in the land area, and visualize findings in the Virtual Control Room for a wide stakeholder group. This way we can predict attacks and raise NSA's risk of getting caught.

Above mentioned research has already shown its strength, and no new attacks to the cables or pipelines have occurred. This model of preventing and safeguarding our society can also be seen as a successful model to other areas of critical infrastructure and it can also be used in other sectors for resilience building in the 11 sectors of critical infrastructure mentioned in the CER directive. In the next Cluster 3 R&D program, this topic is highly recommended to take new actions.

The role of the coordinator in the EU-HYBNET project has been a very satisfactory task. This is because our partner network has the dedication and willingness to solve, to a certain extent, the hybrid phenomena proposing solutions to stakeholders, looking for possible standardization activities, and discussing new innovations throughout the project. This teamwork has resulted in a wonderful network, which will now, after the project, be hosted by the HybridCoE. On behalf of the LAUREA's coordination team, we sincerely thank all partners and all individuals supporting us in this important project. We look forward to collaborating with you in the future and to counter hybrid threats together!

With best regards,

EU-HYBNET Coordinator, Isto Mattila

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Hybrid threats domains and focus areas in EU-HYBNET

EU-HYBNET General Project Coordination, Management and Network Extension Activities

The final months of the EU-HYBNET are upon as and project has been busy finalizing the project work. The EU-HYBNET project has just turned to its final year, running until April 2025. This also means that plenty of efforts will be placed to the hand-over of the network compiled during the project into the hands and lead of EU-HYBNET core partner the European Center of Excellence for Countering Hybrid threats (Hybrid CoE). More about the form and activities of the network in the lead of Hybrid CoE will be shared in coming months in EU-HYBNET events and other channels.

The past months of the project also included 3rd EC project review that was very giving and inspiring for the project. Of course review recommendations will be followed and more emphasis will be laid to strategic messaging from the project and underlining its key take ways and input to stakeholders also for the future.

EU-HYBNET also wishes to continue contributing to pan-European measures to counter hybrid threats in the form of new projects and hence new proposal are under work supporting critical infrastructure protection and LEAs work.

Network Extension

The EU-HYBNET network continues to grow steadily and has welcomed new members to the network on a monthly basis. The network now has a total of **133 organisations from 26 countries**. This includes 30 practitioners, 48 research and/or education institutions, 22 NGOs, and 33 SMEs.

We thank our network members and partners for their contribution and efforts for the project outcomes and increasing visibility of the project across Europe!

EU-HYBNET welcomes the following new members to the network:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

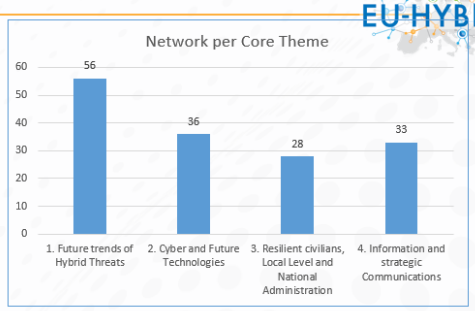
Name	Country	Type of organisation
Universidad Cardenal Herrera CEU	Spain	Academia
Fraunhofer FOKUS	Germany	Academia
Seeders	Greece	SME
Center for East European Policy Studies (CEEPS)	Latvia	NGO
GraphAware	UK	SME
Foreign Affairs Institute (FAINST)	Greece	NGO
University of Turku	Finland	Academia
Vilnius City Municipality Administration	Lithuania	Practitioner
Home Office	UK	Practitioner
IRI Europe ASBL (International Republican Institute)	Belgium	NGO
Logically	UK	SME
Ghent University BIGFATPOL	Belgium	Academia
The Elcano Royal Institute for International and Strategic Studies	Spain	Academia
Center of Excellence for Police and Security Research (CEPOLIS) at the Bavarian Police Academy	Germany	Academia
Turku Ammattikorkeakoulu	Finland	Academia

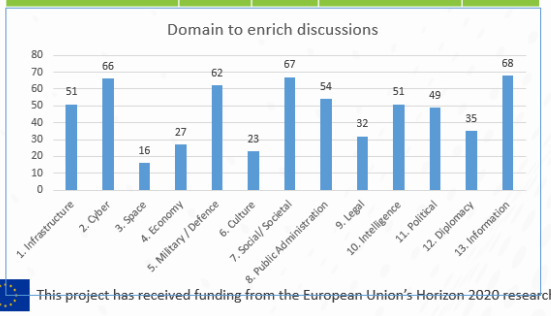
Our network manager regularly analyses the network, reflecting on the information provided in the applications. The analysis supports our aim to raise awareness of the project to the right target groups by inviting them to our events and presenting EU-HYBNET in other EU projects and EU organisation initiatives. The figures below present the status of our network at the end of March 2025:

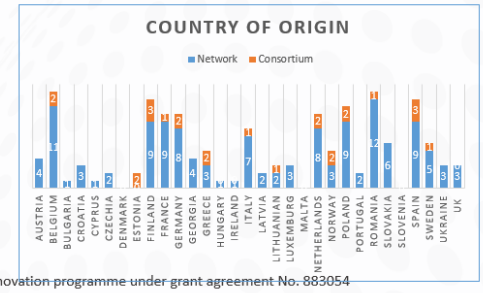
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

EU-HYBNET Network Members in March 2025

Category	Nr	MS	Consortium	All
Practitioner	30	17	10	40
NGO	22	15	2	24
Academic/RTO	48	19	11	59
Industry/ SME	33	13	2	35
In total	133	26	25	158







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

The EU-HYBNET project officially ends in April 2025, and there are no further upcoming activities or events for it. The possibility to apply for membership closed at the end of February, and the acceptance process is ongoing for some applicants. The Hybrid CoE will inherit the network after the project's conclusion, and more details on this will be communicated to network partners in due course.

Gaps and needs of European actors against Hybrid Threats

The Gaps and Needs Event in Madrid allowed the Hybrid CoE to conduct the final gaps and needs analysis of the EU-HYBNET project. This final analysis covered all four core themes of the project, while taking stock of the gaps and needs results of the previous project cycles. This stocktaking practically resulted in the definition of a series of priority areas where progress potential was observed for European actors against hybrid threats. Gaps and needs were then associated to those priority areas.

The results have been disseminated to the Consortium Partners and are compiled in the relevant deliverable. The results were presented in a webinar for the EU-HYBNET network in November 2024 through the Comprehensive Resilience Ecosystem Model (CORE Model) innovative visualization provided by Hahmota Oy. The webinar allowed for fruitful exchanges of viewpoints and considerations which enriched the overall analysis and diffusion of knowledge both on the gaps and needs results and the general concept of hybrid threats too.

Surveys to Technologies, Research and Innovations

In the last project cycle, emphasis was given to highlighting the most important findings of the past cycles, including the most important innovations that were selected and mapped to gaps and needs and primary contexts per cycle, but also the most interesting research projects that have been studied, expected to deliver solutions that could be utilised to tackle hybrid threats .

This process involved sharing the main findings with the participants of the last EU-Hybnet events, namely the 5th Annual Workshop that took place in Brussels, where the WP3 Leader (Dr. Souzanna Sofou, SATWAYS) presented the main innovations identified during the past cycles. Additionally, a session for academia was held by the WP3 Leader, where the scientific papers the consortium has published were briefly presented and discussed. This material was discussed with the participants, and interesting insights were provided. Additionally, a series of teleconferences took place for the separate Tasks, in order to discuss the opinions raised in the event, but also to verify that the selected innovations remain relevant to the current gaps and needs. It was found that even though hybrid threats are evolving, some of the innovations selected in previous cycles can be utilised to respond not only to the current, but also to the future dimensions of hybrid threats. Among others, i)training the public in recognising certain dimensions of hybrid attacks (especially with respect to disinformation and attacks against public participation) ii) arming the European Critical Infrastructures with dedicated tools for combined cyber/physical and hybrid attacks, and iii) supporting ethical and professional journalism can help safeguard the trust in democracy and its values.

Recommendations for Innovations Uptake and Standardisation

During the past months EU-HYBNET has identified four most promising innovative solutions to the project's latest identified challenges to counter hybrid threats. The innovative solutions are:

1. *Mobile application to pinpoint acts of harassment/violence on the street and online.* To support citizens to announce possible early signals of hybrid threats campaigns to security authorities.
2. *AI enhanced Disaster Emergency Communications.* To support crises communication between citizens and authorities in crises with more secured and multifunctional communication system.
3. *Media Pluralism Monitor.* To support countries to analyze their vulnerability to foreign `information manipulation and interference (FIMI).
4. *Starlight Disinformation-Misinformation toolset.* To support Starlight project's innovative FIMI solutions uptake for law enforcement needs.

The innovations were under procurement process analysis and creation of innovation uptake strategy incl. possible industrialization. The results of this work had been shared to wider audience during the EU-HYBNET event, the 3rd 'Innovation Standardization Workshop' in Brussels 22nd OCT 2024. This event brought together EU-HYBNET network members, policy makers, representatives from industry, SMEs, academia and NGOs to map the current status of standardization efforts and needs, also to learn on best practices in the dedicated focus areas in order to enhancing the solutions uptake. You may familiarize more on the key take aways from the event report that is available in EU-HYBNET website – enjoy! https://euhybnet.eu/policy-briefs-and-reports/

Communication, Dissemination and Exploitation Activities

As the project continues to conduct the work in the final cycle, the partners engaged in several continuous Dissemination, Communication and Exploitation activities to promote the results and vision of the EU-HYBNET project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Have you decided to switch off of Twitter/X but want to stay up to date with everything EU-HYBNET? No need to worry, we have opened a Mastodon account where you can follow us to see what we post. It can be found right here!

Dissemination through EU-HYBNET Events

After the organisation of the project workshops focusing on highlighting innovations that answer the aforementioned gaps and needs, the project, nearing its completion, has shifted focus on presenting the results of the project and looking to the future. As mentioned above, the EU-HYBNET project held its final innovation standardisation workshop (ISW) on October 22nd, wrapping up EU-HYBNET's work on standardisation.

Additionally, EU-HYBNET held its 5th and final Future Trends Workshop as described in the WP3 section and its final Annual Workshop on the 12th and 13th of February in Brussels, Belgium. The 5th Annual Workshop presented the final project results to stakeholders and through discussions with Q&As looked to the future of Hybrid threats. This was also the final opportunity to gather EU-HYBNET stakeholders together to discuss hybrid threats before the end of the project. A lot of stakeholders expressed their appreciation for the Network and inquired about continuations. This work was continued on the following day with the final future trends workshop.

Dissemination through project synergies and external events

EU-HYBNET will be presented at the European Police Congress, on the 20th and 21st of May in Berlin by EOS. EOS will present project results as part of a panel discussing solutions to critical infrastructure protection, allowing for some project results to be presented to a wide audience of practitioners. If you would like to join the event, more information can be found here!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054