

EU-HYBNET held its 4th Future Trends Workshop, #FTW2024

On the 23rd of April 2024, the EU-HYBNET consortium successfully held its 4th Future Trends Workshop in Valencia Spain. The workshop was attended by approximately 85 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations in person, with another 67 views on the streaming platform.

Building on the project findings from the last four years, the workshop addressed “Border Management to Counter Hybrid Threats” and served as a platform of interaction for all stakeholders to discuss recent hybrid threats or trends that have challenged EU border management and how effective border management can be used to counter future hybrid threats.



Border Management to Counter Hybrid Threats” and served as a platform of interaction for all stakeholders to discuss recent hybrid threats or trends that have challenged EU border management and how effective border management can be used to counter future hybrid threats.

In this fourth iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and current analytical models and dive deeper in the topic of hybrid threats, in what way it is related to border

management and border security, and how the EU and member states can adapt to be prepared for what comes next. The workshop’s aim was to highlight various ways border management could be used to counter hybrid threats and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

Changing the way we think about hybrid threats, foresight activities, and preparing for the unmanned futures – key points and conclusions from the Plenary session

The workshop included a plenary session with a keynote speech from the Belgian General Intelligence and Security Service outlining various conceptual models to analyse the hybrid threat landscape as well as a panel discussion on Border Management to counter future hybrid threats from the Finnish Ministry of Interior, Laurea University of Applied Sciences, Europol Innovation Lab and Satways.

Through this session, it became apparent that **the different conceptual models used to analyse conflicts, events, or threats all have built in biases or levels and therefore can skew understanding in a way that renders a common situational awareness difficult.** The question then arises how to move past these issues in a complex and multi-level environment such as border management where multiple actors are involved. Some suggestions offered to participants to think about were multi-faceted taxonomies or the standardisation of models to remove blind spots.

Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don’t pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to understand how



technology can be used in new ways to undermine border security or slow down border management processes.

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by refining conceptual models and participating in foresight activities when possible** (even based on the gaps and needs identified by consortium and network practitioners). We welcome the feedback of additional practitioners and look forward to welcoming them into our network, among other hybrid threats stakeholders.

What are the future trends of hybrid threats? – Key points and conclusions from the Break-out sessions

In the second part of the workshop, participants were split into four break-out sessions based on the project's core themes in an attempt to discuss and draw conclusions on the key trends for the future of border related hybrid threats in:

Future Trends in Cyber and Future Technologies: The session examined the future trends in cyber and future technologies. It allowed participants to think about the future threats arising from AI, Cyber-attacks, and Blockchain technologies. AI's exponential growth promises transformative advancements across industries, enabling automation, predictive analytics, and personalized experiences. However, with this innovation comes the looming threat of AI-driven cyber-attacks, leveraging sophisticated algorithms to orchestrate malicious activities such as deepfakes and automated phishing campaigns. Simultaneously, blockchain technology offers unprecedented transparency and security through decentralized ledgers, revolutionizing sectors like finance and supply chain management. As these technologies continue to shape the digital landscape, interdisciplinary collaboration and proactive strategies will be imperative to harness their potential while mitigating emerging cyber risks, ensuring a secure and resilient future for society.

Weaponisation of Migration: Analysing the weaponisation of migration as part of hybrid threats using the CORE Model shows that the majority of the 13 domains are concerned. For example, it affects diplomacy as it is a political issue and the response requires a calculated answer, infrastructure can be overwhelmed if an influx happens, etc. It also touches upon the Core Foundation of Democracy, as decision-making is mainly targeted through the weaponization of migration. 4 case studies were identified as examples and demonstrates that this will continue to be a tool used by hybrid threat actors to destabilise the EU. Additionally, Network Member ICDS gave an example of how Estonia increases its resilience to counter hybrid attacks from abroad.

Code of Practice on Disinformation and FIMI during the European Elections: A comprehensive framework aimed at **safeguarding the integrity of democratic processes** within the European Union. The session allowed participants learn all about a nuanced understanding of FIMI and its role as a tool in the upcoming European elections of June 2024. The session **emphasized transparency, accountability, and collaboration among all parties involved**, urging platforms to enhance their detection mechanisms for identifying and removing disinformation promptly.

Securing the EU's borders to 2040 – Thinking about the security landscape:

Using the futures triangle to **understand the push of the present, the pull of the future, and the weight of the past, participants were able to highlight possible future trends** of how borders may be affected by hybrid threats. Trends identified were **digitalisation**, and how the reliance on digital systems and the automation of borders could lead to new vulnerabilities in case of a coordinated cyber attack, **climate change**, which will cause more and open new routes of migration, which could be weaponised by hybrid



threat actors and **the weaponisation of migrants in general** continuing in the future as part of hybrid threat campaigns.

The next Future Trends Workshop will be held in February 2025.

If you would like to stay updated on the work and conclusions of the project and attend future events, you're welcome to [join the EU-HYBNET network](#); you can read the associated information and apply on the project's [website](#). For further information on EU-HYBNET, you can follow the project through [Mastodon](#), [Twitter](#) and [LinkedIn](#).

