

EU-HYBNET held its 2nd Innovation and Standardisation Workshop, #ISW2023

On the 8th of November 2023, the EU-HYBNET consortium successfully held its **2nd Innovation and Standardisation Workshop** in Valencia, Spain. The workshop was attended by approximately 54 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations.



Building on the themes defined during the first iteration of this workshop, this edition allowed participants to discuss standardisation recommendations and case studies for countering hybrid threats in two thematic areas, **Foreign Information Manipulation and Interference (FIMI) & Protection of Critical Infrastructure**.

Following a plenary session featuring insightful keynote speeches on both topics, participants engaged in parallel breakout sessions, fostering interactive discussions, audience interventions, and the exchange of innovative ideas.

Key Takeaways for Foreign Information Manipulation and Interference (FIMI):

- ❖ Daniel Fritz of the European External Action Service (EEAS) explored the key role of standards in successfully defending Europe against Foreign Information Manipulation and Interference. He highlighted the importance of information sharing between different institutions and organisations, and emphasised the **need for effective coordination, consistent communication and a collaborative approach**.
- ❖ Daniel Milo, from the Centre for Countering Hybrid Threats, shared insights into Slovakia's whole-of-government approach to countering Russian disinformation. Among the lessons learned, he highlighted the need for coordinating policy development with project implementation, **clear task division between Ministries, effective sharing of knowledge, and consistency in communication**.
- ❖ The European Commission's Joint Research Centre representative, Julien Theron, presented 14 trends in disinformation, shedding light on the evolving landscape of deceptive practices.
- ❖ Paula Rejkiewicz, from the Ministry of Foreign Affairs Republic of Poland, presented a case study on challenges and responses to disinformation affecting Poles and Ukrainians.
- ❖ Esther Jacobs, from TILT Insights, presented a case study on coordinated inauthentic campaigns on Twitter, showcasing innovative solutions for detection.

- ❖ David Arroyo, from the Spanish National Research Council (CSIC), addressed the challenges of early detection in advanced manipulation campaigns, contributing to the ongoing conversation on countering hybrid threats.

Key takeaways for Critical Infrastructure Protection:

- ❖ Kimini Delfos, from the Dutch Ministry of Infrastructure and Water Management, presented the **Dutch approach to security** and critical infrastructure resilience. The Dutch methodology employs the polder model, emphasising a **whole-of-governance approach to counter hybrid threats and work towards resilience**.
- ❖ Georgios Kolliarakis, from the German Council on Foreign Relations, noted that there is currently a multitude of regulatory instruments across jurisdictions focusing on critical infrastructure protection, but there appears to be a common understanding and a level of convergence. He emphasised that a **mix of instruments is necessary** as today's interconnected society is vulnerable to new types of threats.
- ❖ Karolina Wojtasik, from the Government Centre for Security (RCB) in Poland, explained the Polish approach for identifying critical infrastructures, pointing out that the criteria and results of this process are restricted – citizens are not aware of which infrastructures are considered critical. She also analysed a case study into Russian hybrid activities targeting Polish Critical Infrastructure.
- ❖ Paola Tessari, from the Istituto Affari Internazionali, discussed hybrid threats against critical infrastructures with a focus on Italy's maritime interests, highlighting the importance of safeguarding critical assets and the dynamic nature of hybrid threats.

The Innovation and Standardisation Workshop, a pivotal platform for collaboration, best practice sharing, and strategy shaping, will be followed by a detailed event report in the coming months. The EU-HYBNET consortium remains committed to addressing standardisation gaps and needs identified during the workshop. **To join the network and participate in discussions on countering hybrid threats, including standardisation recommendations, 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 [X/Twitter](#) and [LinkedIn](#).**

