EU-HYBNET held its 3rd Future Trends Workshop, #FTW2023

On the 19th of April 2023, the EU-HYBNET consortium successfully held its **3rd Future Trends Workshop** in Bucharest, Romania. The workshop was attended by approximately 90 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations.

Building on the project findings from the last three years, the workshop addressed “Hybrid Threats in the EU Neighbourhood – Implications for the future of EU security” and served as a platform of interaction for all stakeholders to discuss hybrid threats in the EU’s neighbourhood, implications for the future of EU security and innovations to counter them.

In this third iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and dive deeper in the topic of hybrid threats, their manifestations and the actions taken by the EU and its Member States to counter them. The workshop’s aim was to highlight the many manifestations of hybrid threats across domains and Member States and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

Providing context on the current hybrid threats landscape and its future manifestations – key points and conclusions from the Plenary session

The workshop included a plenary session with keynote speeches from local and EU stakeholders (Euro-Atlantic Resilience Centre, Romanian Directorate for Cyber Security, European Commission DG MARE, EMSA), as well as a panel discussion with perspectives on hybrid threats from the Romanian Ministry of Foreign Affairs, the Ukrainian Parliament, the European Centre for Disease Control (ECDC) and Satways.

Through this session, it became apparent that **the weaponisation of information, new technologies, the cyber domain, critical infrastructures, science and CBRN materials has intensified and will continue in the future** as they are cost-effective. The war in Ukraine is an example of hybrid threats translating into military measures, but we see that hybrid threats go beyond the traditional notions of military conflict and defence, and daily target and affect civilians, taking advantage also of cultural and national characteristics in each Member State. In such a context of “overlapping crises”, **enhancing societal resilience** should become a priority.

All domains should be prepared to counter such threats – for example DG MARE’s 2023 EU Maritime Security Strategy (EUMSS) foresees concrete actions, such as trainings and exercises to support Member States in countering hybrid threats. Information exchange is also crucial in this regard; EMSA’s CISE is an example of a system that could also be looked at for the benefit of hybrid threats practitioners.

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

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by each time looking into one dimension of a multidimensional problem** – based on the gaps and needs identified by consortium and network practitioners in the EU-HYBNET Gaps and Needs events. 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 in three 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 hybrid threats in each field:

Future Trends in Cyber and Future Technologies: The ongoing transformation of the global order together with the development of new technologies are changing the landscape of hybrid threats today and for the future. The technologies identified include distributed ledger technologies, AI, decentralised infrastrcutures, digital currencies, the increasing speed of innovation, the race for developing quantum computation capabilities, the actors in control of supply chains needed for innovative technologies.

Hybrid Threats in the Arctic: In this session, participants recognised the strategic importance of the Arctic region for EU and NATO resilience. This region although often ignored by the mainstream EU security and policy discourse, is already being targeted by hybrid threats.

Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats: To effectively counter disinformation, an anticipatory approach including legislative and technological solutions, as well as intelligence and information sharing between private and public orgnanisations is needed. EU and national projects, including public actors and developing innovative technologies to anticipate and address disinformation (through AI, for example), the EU Code of Practice on Disinfromation and the Digital Services Act can be key in that regard.

The EU-HYBNET project will keep monitoring how the trends identified develop and will be proposing and reviewing innovative solutions and technologies that can respond to practitioners' gaps and needs when it comes to countering these hybrid threats.

Thanks to our partners 'Mihai Viteazul' National intelligence Academy, European Organization for Security & Laurea University of Applied Sciences for organising the event, and to all of our EU-HYBNET partners, network members and stakeholders who joined and helped fuel the discussions.

The next Future Trends Workshop will be held in Valencia in Spring 2024.

If you would like to 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 Twitter and LinkedIn.

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