EU-HYBNET held its 3rd Innovation and Knowledge Exchange Workshop, #IKEW2023

On the 7th of November 2023, the EU-HYBNET consortium successfully held its **3rd Innovation and Knowledge Exchange Workshop** in Valencia, Spain.

The workshop was attended by approximately 60 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations. 90 people also followed the workshop online through Youtube.

This third and final edition of the Innovation and Knowledge Exchange Workshop presented four innovations for practitioners countering hybrid threats. These innovations were selected based on the gaps and needs of pan-European practitioners identified and assessed by EU-HYBNET partners over the past year across the four core themes of the project: Cyber and Future Technologies, Information and Strategic Communication, Resilient Civilians, Local Level and National Administration, Future Trends of Hybrid Threats.

Key innovations presented:

- AI Toolbox for countering (online) terrorism, STRALIGHT EU Project (GA No. 101021797):

STARLIGHT aims to create a community that brings together LEAs, researchers, industry and practitioners in the security ecosystem under a coordinated and strategic effort to bring AI into operational practices across a number of high priority threats, such as counter-terrorism, child sexual exploitation, cybersecurity and more. The presentation focused on the tools developed to counter online terrorism, with the set of tools being able to do individual instance assessment, multi-instance assessment and monitor rapidly developing phenomena through online detection analysis. One tool highlighted was the telegram crawler, able to analyse various topics and subtopics and create inter-topic distance mapping. With these AI-enabled tools, LEAs are able to focus on extreme and harmful disinformation, detect symbolism of banned movements, conduct a toxicity analysis to determine those moving towards radicalisation and conduct a more thorough sentiment analysis to understand the effects of online terrorism and disinformation campaigns.

The discussion with participants focused on if there was a framework for hate speech, which is not standardised across Europe, and if legal narratives that could be activated for extremism were taken into consideration by STARLIGHT. In response, it was noted that the tools would be used to give more situational awareness to LEAs and giving them focus areas, and any frameworks in hate speech was in the instances. Other key challenges identified were the need to ensure that the tools are used carefully in order to not clamp down on legal speech and staying ahead of the rapid rise in the use of malicious technology.

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

- Disinformation toolbox, VIGILANT EU Project (GA No. 101073921):

VIGILANT is bringing together over 30 tools to support European practitioners in analysing disinformation campaigns. The tools are offered in a flexible and modular system that allows practitioners to choose the tools needed to address each case. The key aim is to build a sustainable, ethical but also easy to use system where the final decision on what is disinformation lies with the human in command of the system. The presentation of the platform was followed by a lively discussion with the audience. Key challenges included the criteria used for identifying disinformation, the variety of practitioners dealing with disinformation in each Member State, as well as the continuous progress in the development of AI and deepfake images.

- Next Generation EIBM platform, CONNECTOR EU Project (GA No. 101073921):

The CONNECTOR project's main goal is to take the current Common Information Sharing Environment (CISE) and develop and add the customs element. The end result, Customs Extended CISE (CE-CISE) would allow for customs authorities to safely and securely exchange data to improve the customs environment and operations across the EU. After the presentation of the project and its objectives, the discussion turned to the benefits of adding customs to CISE and how this could affect the deterring of hybrid threats. One main challenge identified was that data-sharing cannot happen by force; therefore, there needs to be a trigger to motivate authorities to share data. Another challenge is the assumption of similar values. Not every country, even in the EU, shares every value, and therefore this could be another barrier to participation, as the issues faced are not the same and the values are not always the same. A potential solution included the EU Customs Authority and the role it could play in fostering collaboration and motivating authorities to work together. To paraphrase a participant, illegal activities do not stop at the border, so many of Spain's customs issues also affect Norway, for example. Therefore, it is in everyone's best interest to collaborate.

- Developments and threats related to AI technologies

The session provided a stark assessment of the transformative impact of Artificial Intelligence on our society. The launch of ChatGPT in September 2021 marked a major turning point, ushering in a world where AI becomes a simplified and widely accessible model with potential generative AI threats, including a 'renaissance' of disinformation, advanced microtargeting and privacy erosion, and a new era of AI-based psychological manipulation. The session concluded by underlining the need for enhanced resilience that can only come from a unified global effort to navigate the complexities of an AI-enhanced threats era.

Innovation uptake and practitioners' needs:

Participants also had the opportunity to consider the crucial issue of innovation uptake and best practices for linking innovation providers and practitioners.

- Research results must translate into practical value for end-users to make a real impact. The EU-HYBNET method of identifying gaps and needs, mapping innovations and finally making recommendations for capability development was presented as a good example of fostering innovation uptake.

- Projects are as strong as their communities; it is crucial that end-users include the innovations produced or identified during a project in their procurement plans. The main challenge lies in convincing national authorities to invest in innovation and not only in procurement.

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

- Law enforcement agencies (LEAs) operate with a clear mission defined in national law. This can often create silos and challenges with emerging hybrid threats. The Europol Innovation Lab and tool repository can act as a platform that links that needs of LEAs with the results produced by industry innovators and research projects. Integration and standardisation are crucial here as tools must work together to serve the needs of practitioners.

- Models similar to the one followed by the European Anti-Cybercrime Technology Development Association (EACTDA) can also be crucial in tailoring research results and solutions to the needs of LEAs and bridging the gap between security prototypes and practical implementation. EACTDA maps existing innovations and prepares a catalogue of tools from which end-users select the ones that address their needs; these then receive funding for further development.

The EU-HYBNET project will continue to assess and test innovations to ensure they meet the needs of pan-European practitioners countering hybrid threats. **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 X/Twitter and LinkedIn.**

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