EU-HYBNET held its 2nd Innovation and Knowledge Exchange Workshop, #IKEW

On the 14th of June 2022, the EU-HYBNET consortium held its 2nd Innovation and Knowledge Exchange Workshop #IKEW in a hybrid format (in person, in The Hague and online). Hybrid threats are characterised by an everchanging threat landscape and tools, and therefore there is a constant need for innovations to counter hybrid threats. The point of the IKEW is to provide practitioners, industry, SMEs, and academia an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to answer them. During the 2nd IKEW, consortium partners and external participants (practitioners, industry, academia and NGOs) discussed the project's latest Innovation Assessment results and exchanged new ideas regarding how the innovations could be further improved to counter hybrid threats.

The 2nd IKEW, organised by TNO, included morningplenary sessions, two tracks of break-out sessions – one track offered live in The Hague and one catered for online participants – and afternoon plenary sessions.

During the morning plenary session, the first keynote speaker Hester Somsen, the Dutch National Coordinator for Security and Counterterrorism (NCTV), discussed *"Hybrid Threats in a Dutch context"*, focusing on the NCTV's work in countering hybrid threats and some of the best practices developed in the Netherlands, while Geert Kuiper from the Dutch Ministry of Defence gave the second keynote speech *"Connecting the Dots to Counter Hybrid Threats – the Role of Dutch Defence"* , allowing participants to understand the Dutch Ministry of Defence's view on hybrid threats. Finally, Okke Lucassen, Junior Scientist at TNO, presented the project's Innovation Assessment results from its first cycle and highlighted the innovations identified as 'promising', which were later discussed during the live break-out sessions. There were 9 innovations in total identified by EU-HYBNET as promising solutions to help combat hybrid threats; however, a main conclusion regarding these innovations was that there was some finetuning needed in order to improve them. The IKEW provided the opportunity to discuss these challenges and possible improvements.

Subsequently, four different break-out sessions were held live in the Hague, while four other online break-out sessions took place online simultaneously. This way people could either participate in a break-out session with others completely in person or completely digitally.

- In *"Dilemma gaming"*, Anja van der Hulst (TNO) and Willem Verdaasdonk (TNO) guided participants through a platform developed by TNO/Hybrid CoE, exposing them to a rapidly unfolding crisis scenario and discussed ideas to further scale up the game. In response to this discussion, the organiser raised the question is scaling up the game would actually be of any benefit, and could in fact harm it. In the end the conclusion was scaling up was perhaps not the best option; however, he game still allowed participants to experience the decision making process during a crisis and understand the nuance behind such decisions, including who is involved in the process, how to communicate with the public and different groups, and what are the different economic, political, societal and security concerns that must be taken into consideration.
- In "*Hybrid threats impact on critical infrastructure disruption: existing measures and solution needs*", Monica Cardarilli (JRC) had an open discussion with participants on how to best strengthen critical infrastructure resilience against hybrid threats. Such measures includedtooling (both technical and

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

non-technical) for awareness/ detection on disruption, a good registration of critical infrastructures in Europe that need to be defended, and finally a EU legislation for developing critical infrastructure.

- In "*Cyber and future technologies – how to advance?*", Evaldas Bruze (L3CE) presented current trends in mass use of social networks and internet communication and discussed with participants the technological and social innovations needed to mitigate them, including quantum computing and data embassies. These innovations were approached with a lot of caution, as participants focused on the threats related to data embassies and quantum computing just as much as the added benefits. The need for a European test-bed for quantum computing was also highlighted.
- In "*Emerging technologies: from reactive to proactive use of innovations to counter hybrid threats",* Maxime Lebrun (Hybrid CoE) identified knowledge needs on how new technological developments may offer options to better identify and defend against hybrid attacks. One example was how individual data aggregation and computing can give unique insights into societal fault lines.In *"Who to trust?",* Gunhild Hogensen Gjørv (UiT) analysed the journalism trust initiative and the government and social media cooperation framework innovations and noted that they could benefit from a more person-centric approach. There were many different definitions of trust and parts of the discussion focused on the goals of the government and social media cooperation, and whether it was even possible to trust these initiatives.
- In the *"Crazy ideas gaming session",* Rick Meessen (TNO) and Jesper van Putten (TNO) organised an open brainstorming session in the format of an online game to identify completely new ideas to counter hybrid threats. Several scenarios were presented, in which the participants were asked to think of innovative hybrid threats to employ against each other – whitout the usual legal and ethical restrictions you would have in real life. A total of 41 ideas wwas gathered within the hour. Participants really enjoyed the format of the exercise, and the amount of unique ideas gathered showed its insightfulness.
- In *"Identifying and countering information manipulations: professional tools and networks of fact-checkers and OSINT practitioners",* Rubén Arcos (URJC) and Manuel Gértrudix (URJC) with the support of Daniel Fritz (EEAS) and Pablo Hernandez (Maldita.es) discussed current trends in information manipulations and the available innovations and solutions supporting the practice of open-source intelligence (OSINT) and fact-checking/debunking. The conversation with participants also focused on developing cooperation between multiple fact-checker organizations in order to bolster their efforts, increase efficiency in debunking myths and creating "fact-checker communities".
- In *"Political cleavages and hybrid threats: exploiting the new drivers"*, Monica Cardarilli (JRC) discussed how good governance, communication tools and technical strategies are crucial steps in countering hybrid threats. The discussion revolved around what the EU, among others, can do in order to improve in this area, such as the development of a deepfake detection system, among others.

The workshop concluded with a final plenary session: a keynote speech on "Disinformation; The BadNews and resilience" by Gwenda Nielen (TITL) who gave participants the opportunity to discover the impact of a disinformation campaign first hand by participating in an online game. The game allowed participants to gain a better understanding of disinformation by letting them play the 'bad guy' and thereby exposing them to tactics commonly used in disinformation.

The 2nd EU-HYBNET Innovation and Knowledge Exchange Workshop was a successful event and provided fruitful exchange between the audience, the consortium and the keynote speakers. The results of the IKEW

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

and further analysis of the event will be included in Deliverable 3.12: *2nd Innovation and Knowledge Exchange Events Report*, which will be available publicly towards the end of 2022.

If you are interested in joining EU-HYBNET's 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.