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

14 JUNE

In the Hague and online

09.00-17.00 CEST

The purpose of 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.

The EU-HYBNET consortium will hold its 2nd Innovation Knowledge Exchange Workshop (#IKEW) in hybrid format on 14 June 2022 in the Hague and online!

The IKEW will maintain adherence to the project's four core themes, which are:

- Future trends of Hybrid Threats
- Cyber and future technologies
- Resilient civilians, local level, and administration
- Information and strategic communications

It will facilitate the continuous mapping of needs, monitoring of solutions, and providing a forum where practitioners can engage with innovation providers. It will ensure the exchange of knowledge and information about innovations to increase the likelihood of future uptake.

Who? The workshop is open to project partners and network members and external participants upon registration and aims at boosting cross-fertilization between the EU-HYBNET project activities, other EU projects and institutional and industrial operators.

When? 14th of June 2022 at 09.00-17.00 CEST

Where? The Babylon Hotel Den Haag, the Hague, Netherlands

More information: Event organizer at TNO: Ms Angela Kwaijtaal at angela.kwaijtaal@tno.nl and Ms Kimberley Kruijver at kimberley.kruijver@tno.nl.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Agenda

The 2nd IKEW will start with a plenary session held live in the Hague and live-streamed to participants attending digitally.

Two tracks of workshops will be organised in two rounds: live in the Hague or online for participants attending remotely. In each round, participants can express their preference between two live or online sessions.

The day will end in the plenary with pitches from the workshops and a closing key note (TBD).

<table>
<tr><th>Time CEST</th><th colspan="2">Topic</th><th colspan="2">Speakers</th></tr>
<tr><td colspan="5">Welcome and registration</td></tr>
<tr><td colspan="5">Plenary session (live in the Hague and online)</td></tr>
<tr><td>9:00-9:15</td><td colspan="2">Opening</td><td colspan="2">Moderator: Michel Rademaker (HCSS)</td></tr>
<tr><td>09:15-09:45</td><td colspan="2">Keynote on ‘Disinformation; The BadNews and resilience’</td><td colspan="2">Keynote speaker: Gwenda Nielen (TILT)</td></tr>
<tr><td>09:45-10:15</td><td colspan="2">NLD MoD – Counter Hybrid Unit: developments in Dutch context</td><td colspan="2">Hans van Leeuwe or Margriet Drent (Dutch Ministry of Defence)</td></tr>
<tr><td>10:15-10:45</td><td colspan="2">TNO – results EU-HYBNET project first cycle</td><td colspan="2">Rick Meessen, Okke Lucassen (TNO)</td></tr>
<tr><td>10:45-11:00</td><td colspan="4"><i>Coffee break</i></td></tr>
<tr><td colspan="5">Break-out sessions LIVE in The Hague
<i>In each round, in-person participants will be split in two parallel working groups.</i></td></tr>
<tr><td>11:00-12:30</td><td><i>Dilemma gaming</i>
Innovation: Hybrid online dilemma game</td><td>Anja van der Hulst (TNO) & Willem Verdaasdonk (TNO)</td><td><b><i>Cyber and future technologies – how to advance?</i></b>
Innovation: A Quantum-Resistant Trusted Platform Module
Establish Data Embassies or E-embassies</td><td>Evaldas Bruze (L3CE), Rimantas Zylius (L3CE)</td></tr>
<tr><td>12:30-13:30</td><td colspan="4"><i>Lunch break</i></td></tr>
<tr><td>13:30-15:00</td><td><i>Who do you trust?</i></td><td>Gunhild Hoogensen Gjørv (The Arctic University of Norway</td><td><b><i>Identifying and countering information manipulations:</i></b></td><td>Rubén Arcos (URJC) and Manuel Gértrudix (URJC)</td></tr>
</table>

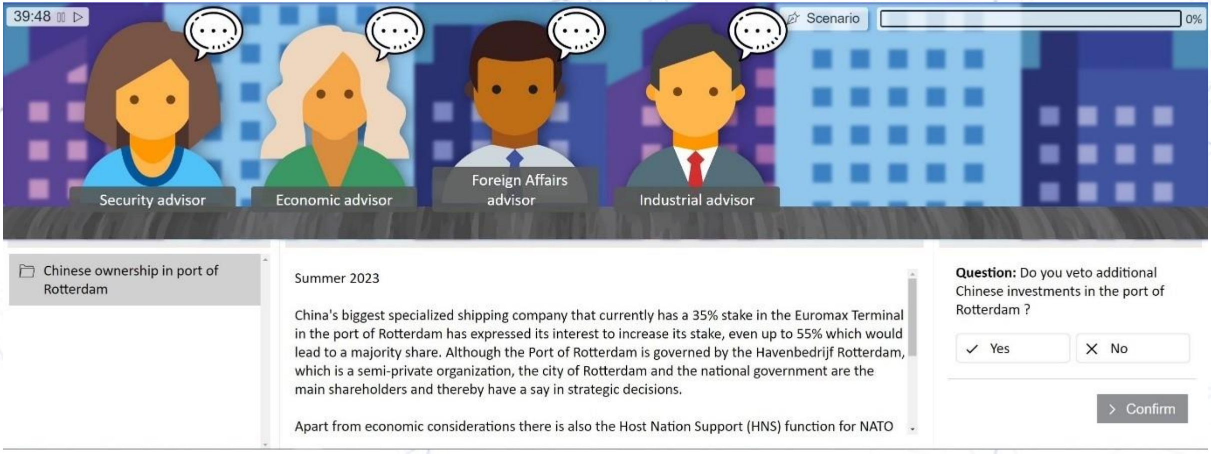
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No883054

	Innovation: Journalism trust initiative Government & social media cooperation framework to counter election interference		***professional tools and networks of fact-checkers and OSINT practitioners*** Innovation: Automated detection of hate speech in social media	In cooperation with Daniel Fritz (EEAS)
Break-out sessions ONLINE *In each round, online participants will be split in two parallel working groups.*				
11:00-12:30	***Hybrid threats impact on critical infrastructure disruption: existing measures and solutions needs*** Topic: Output from Gaps & needs 2nd cycle= Critical infrastructure	Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)	***Emerging technologies: from reactive to proactive use of innovations to counter hybrid threats*** Topic: Output from Gaps & needs 2nd cycle = disruptive technologies; what to pay attention to?	Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)
12:30-13:30	*Lunch break*			
13:30-15:00	***Crazy ideas gaming session*** Topic: Open brainstorm in the format of an online gaming session based on hybrid threats scenario's.	Rick Meessen (TNO) & Jesper van Putten (TNO)	***Political cleavages and hybrid threats: exploiting the new drivers*** Topic: Output from Gaps & needs 2nd cycle = Political cleavages – foreign interference	Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)
15:00-15:30	*Coffee break*			
Plenary session (live in the Hague and online)				
15:30-16:15	Pitch outcomes workshops		Organizers & Moderator	
16:15-16:45	Keynote speech on developments in hybrid threats		Keynote speaker: TBD	
16:45-17:00	Summary of the day & closing remarks		Moderator: Michel Rademaker (HCSS)	

Description of the break-out sessions

LIVE SESSIONS

BOS 1: Dilemma Gaming



Summer 2023

China's biggest specialized shipping company that currently has a 35% stake in the Euromax Terminal in the port of Rotterdam has expressed its interest to increase its stake, even up to 55% which would lead to a majority share. Although the Port of Rotterdam is governed by the Havenbedrijf Rotterdam, which is a semi-private organization, the city of Rotterdam and the national government are the main shareholders and thereby have a say in strategic decisions.

Apart from economic considerations there is also the Host Nation Support (HNS) function for NATO

Question: Do you veto additional Chinese investments in the port of Rotterdam ?

Name of organizer(s): Anja van der Hulst (TNO) & Willem Verdaasdonk (TNO)

Description: Strategic decision making in countering hybrid threats is highly situational, cognitively complex and performed under demanding circumstances. Substantial part of failure in countering hybrid threats results from inadequate (shared) situational awareness and decision-making. Building a shared situational awareness is complicated by the multidisciplinary nature of governmental departments of non-governmental actors involved. Also, the higher the level of decision making, the more political considerations play a role as strategic decision making in essence is about reconciling divergent interests. Hence, hybrid threats confront decision makers with complex dilemma's that require trade-of decisions such as choosing between economics and security or between external and internal frictions.

To make policy- and decision makers aware of such dilemma's and subsequently train them for decision making under such complex circumstances, we have developed a platform for dilemma gaming. It exposes decision makers to a rapidly unfolding scenario where they are confronted with dilemmas that need decisions. For this, they will have governmental and non-governmental advisers that help them build situational awareness.

In the session @ IKEW, we will allow participants to play the dilemma game that was built by the HCoE and TNO for HCoE's Hybrid Threat 101 course. We will have a short reflection on the content of the game and on the use of such a dilemma game-platform to make practitioners and policy makers aware of innovations in the field.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

BOS 2: CT2: Cyber and future technologies – how to advance?

Name of organizer(s): Evaldas Bruze (L3CE), Rimantas Zylius (L3CE)

Description: This session will focus on the future advancement of the cyber and other technologies impact and widespread use.

We have been experiencing exponential growth of the technology driven social processes overall last decade. Social networks and digital communications channels grew to a scale that shapes forms of influence, control, crime, and warfare. This year began with Russia's invasion to Ukraine that crystalized shifts in cyber, internet, social media domains:

- New levels of the information manipulation, misinformation, disinformation, fake information, propaganda (during first couple of days of the war more than 1.5M of artificially created pieces of content have been distributed over the internet channels).
- Information warfare is a new reality, and it showed its potential and success cases in this war. The bounty is huge, there are billions to gain and to lose in information warfare.
- Russia is showing the possibility to go for total control over the media, internet, and access to information.
- Cyber armies on social media platforms self-organize for attacks and defenses, making "crowdsourced" attacks.
- Hacking groups who have joined anti-Russian movements have become stars and heroes that trigger new phenomena like "cybercrime superstar" or "cybercrime celebrity".

These proven cyber-capabilities of the public can be manipulated and misused. In particular given not sufficient attention to the cybersecurity of the public, continuously increasing complexity of technologies and remaining low capability to validate sources of information.

We will discuss the trends in mass use of social networks and internet communication in the light of Russia's war in Ukraine. What risks must countries prepare for? What technological and social innovations will be needed to mitigate them?

BOS 3: Who do you trust?

Name of organizer(s): Gunhild Hoogensen Gjørv (The Arctic University of Norway)

Description: This session will focus on trust between civilians themselves, between civilians and technology, civilians and the private sector, and between civilians and their authorities/governments. After a brief introduction about the role of trust in security/stability of states and their societies, the group will brainstorm about how trust operates in society and amongst civilians – is it predictable? Is it logical or rational? What fosters distrust (emotions like fear, disgust?). In what ways does trust or distrust (general or particularized) manifest itself? On the basis of our brainstorming, we will gather indicators of trust/distrust and use these to further analyse two innovations: the journalism trust initiative and the government & social media cooperation framework. Can these innovations respond adequately to the trajectories of trust/distrust we have identified? What are the strengths of the innovations and what are their weaknesses?

Preparation: https://www.youtube.com/watch?v=a71VqHpza58

BOS 4: Identifying and countering information manipulations: professional tools and networks of fact-checkers and OSINT practitioners

Name of organizer(s): Rubén Arcos (URJC) and Manuel Gértrudix (URJC)

Description: In this interactive break-out session participants will discuss the role of professional solutions and innovations supporting the practice of open-source intelligence (OSINT) and fact-checking/debunking against information manipulations. After an introduction, participants will engage in a structured discussion around the following questions:

- What trends in information manipulations and disinformation can be observed in the current information environment?
- What are the challenges faced by communities of fact-checkers and OSINT practitioners when addressing identification, fact-checking, and debunking?
- What solutions/tools can support their task?
- What role is there for education and training programs on fact-checking and OSINT?

Also, a case study will be discussed on the identification of hostile narratives and historical revisionism using an existing solution in the market.

ONLINE SESSIONS

BOS 1: Hybrid threats impact on critical infrastructure disruption: existing measures and solution needs

Name of organizer(s): Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)

Description: Nowadays the changing risk landscape requires cross-sectoral approaches for boosting the resilience of critical interconnected networks and essential services against hybrid threats. This online break-out session invites European actors from the policy community, infrastructure operators, practitioners, industry, SMEs, academia and other relevant stakeholders to exchange on how to best strengthen critical infrastructure resilience against hybrid threats. This session aims to stimulate dialogue among stakeholders building upon a potential hybrid threats attack scenario. The session offers the opportunity to discuss solutions, innovations and other measures - either technological or non-technological - to counter the impact of hybrid threats on critical infrastructure disruption, including economic dependencies and cascading effects across sectors. It will also provide an opportunity to explore cross-cutting ideas on tools, methods and information needs to overcome security gaps in critical infrastructure capability against hybrid threats in the EU.

BOS 2: Emerging technologies: from reactive to proactive use of innovations to counter hybrid threats

Name of organizer(s): Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Description: Technological trends suggest that the landscape of hybrid threats will rapidly expand. With their disruptive potential, they open up new avenues and, at the same time, provide a means to counter hybrid threats. This online break-out session invites European actors from industry, SMEs, practitioners, research organizations and other relevant stakeholders to recognize knowledge needs on how new technological developments may offer options to better identify and defend against hybrid attacks. This session features focused discussions among stakeholders building upon a potential hybrid threats attack scenario, thus offering the opportunity to develop a comprehensive understanding of the implications of innovative technologies and their disruptive potential on business continuity and the need for viable strategies and foresight capacity to counter hybrid threat onslaughts.

BOS 3: Crazy ideas gaming session

Name of organizer(s): Rick Meessen (TNO) & Jesper van Putten (TNO)

Description: The crazy ideas gaming session is aimed at one of the IKEW objectives, which is to bring together out-of-the-box, nonconformist and creative thinkers in order find new threats or manifestations of hybrid threats as well as new innovative solutions for countering hybrid threats. Therefore we have designed an online game format in which red and blue teams play against each other. The red team is the hybrid aggressor employing hybrid threats and the blue team is the targeted state who tries to counter and mitigate the hybrid threats. In a series of very short rounds both teams will be asked to come up with unexpected, unknown, out-of-the-box and crazy moves, while playing a cat and mouse game. The context for the game will be 2-3 scenarios, in which hybrid threats and tactics will be commonplace. We will not put any restrictions on the means, actions and tactics both team might employ. One can think of emerging and disruptive technologies that lead to new manifestations of hybrid threats, new actors on the pitch or new vulnerabilities that will be targeted by using hybrid threats. Also weird tactics, probably beyond the current legal and ethical playground, are allowed, at least in this game. So in short, even the unthinkable, the undesirable or the impossible may be played!

BOS 4: Political cleavages and hybrid threats: exploiting the new drivers

Name of organizer(s): Maxime Lebrun (HCoE) & Monica Cardarilli (JRC)

Description: A very effective form of hybrid interference is designed to manipulate, and thereby exploit, existing political frictions and sow internal divisions in targeted EU countries or societies undermining trust in governments. This online break-out session invites European actors from public administrations, research organizations, practitioners, NGOs and other relevant stakeholders to investigate on how good governance, communication tools and technical strategies may be crucial to counter hybrid threats, building upon a potential hybrid threats attack scenario. This session aims to facilitate discussions among stakeholders on the need to exploit specific innovations and tailor adequate solutions as an important part of increasing threat awareness and resilience of EU target democracies against the exploitation and manipulation of political cleavages, social tensions and polarization by hybrid campaigns.

More info and updates on the 2nd #IKEW at:

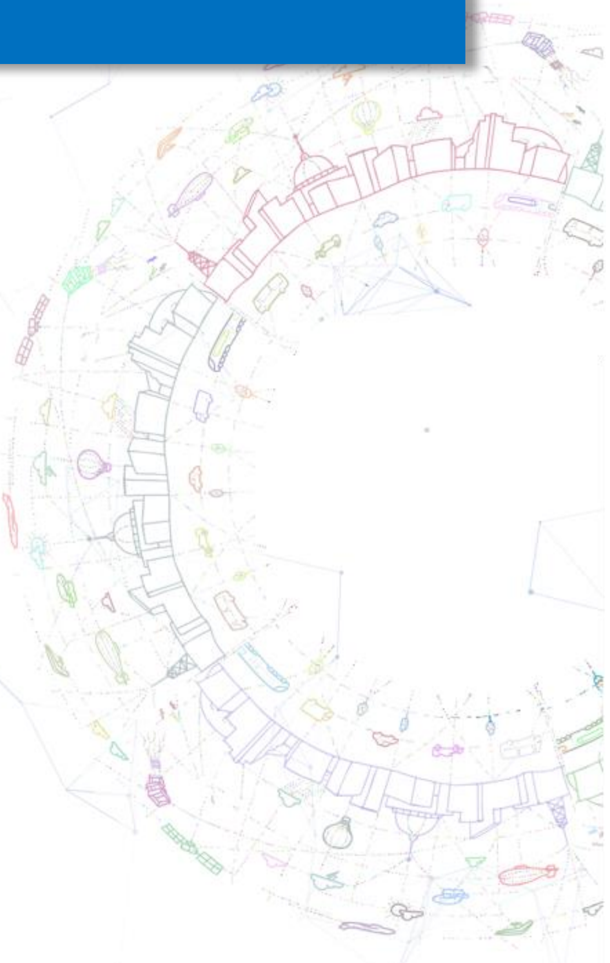
euhybnet.eu

EU-HYBNET LinkedIn Group

@EuHybnet

EU-HYBNET Project Coordinator Laurea University of Applied Sciences – Päivi Mattila paivi.mattila@laurea.fi

Don’t forget to use the Innovation Knowledge Exchange Workshop hashtag: #IKEW2022



This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No883054