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.

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 keynote speech.

Time CEST	Topic		Speakers	
	Welcome and registration			
	Plenary session (live in the Hague and online) *Room: Lange Voorhout*			
9:00-9:15	Opening		Moderator: Michel Rademaker (HCSS)	
09:15-09:45	Keynote on Dutch developments in hybrid threats		Keynote speaker: Hester Somsen (Dutch National Coordinator for Security and Counterterrorism)	
09:45-10:15	Keynote speech on 'Connecting the Dots to Counter Hybrid Threats – the Role of Dutch Defence'		EU-HYBNET Speaker: Geert Kuiper (Dutch Ministry of Defence)	
10:15-10:45	Results of Innovation Assessment 1st EU-HYBNET Cycle		EU-HYBNET speaker: Okke Lucassen (TNO)	
10:45-11:00	*Coffee break*			
	Break-out sessions LIVE in The Hague *In each round, in-person participants will be split in two parallel working groups.*			
	Room: Vijverberg		*Room: Noord-einde*	
11:00-12:30	*BOS 1: Dilemma gaming* Innovation: Hybrid online dilemma game	Anja van der Hulst (TNO) & Willem Verdaasdonk (TNO)	*BOS 2: Cyber and future technologies – how to advance?* Innovation: A Quantum-Resistant Trusted Platform Module Establish Data Embassies or E-embassies	Evaldas Bruze (L3CE), Rimantas Zylius (L3CE)
12:30-13:30	*Lunch break*			

	Room: *Vijverberg*		Room: *Noord-einde*	
13:30-15:00	*BOS 3: Who do you trust?* Innovation: Journalism trust initiative Government & social media cooperation framework to counter election interference	Gunhild Hoogensen Gjørv (The Arctic University of Norway	*BOS 4: Identifying and countering information manipulations: professional tools and networks of fact-checkers and OSINT practitioners* Innovation: Automated detection of hate speech in social media	Rubén Arcos (URJC) and Manuel Gértrudix (URJC) 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	*BOS1: Hybrid threats impact on critical infrastructure disruption: existing measures and solutions needs* Topic: Output from Gaps & needs 2nd cycle= Critical infrastructure	Monica Cardarilli (JRC)	*BOS 2: 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)
12:30-13:30	*Lunch break*			
13:30-15:00	*BOS 3: 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)	*BOS 4: 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) Room: *Lange Voorhout*				
15:30-16:15	Keynote speech on 'Disinformation; The BadNews and resilience'		Key note speaker: Gwenda Nielen (TILT)	
16:15-16:45	Pitch outcomes workshops		Organisers & Moderator	
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

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.

BOS 2: 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)

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.

Speaker bios

Michel Rademaker (Moderator)

Michel Rademaker is one of the co-founders of HCSS and the deputy Director. He has fifteen years of hands-on experience as an officer in The Royal Netherlands Army, where he held various military operational and staff posts and also served a term in former Yugoslavia. At HCSS he is responsible for product and project development. He is particularly interested in setting up (inter)national multi-stakeholder projects, both with a combined qualitative as well as quantitative focus, on new and upcoming strategic security and geo-economic themes like cyber and raw materials etc. His fields of expertise include security strategy, policy, concepts and doctrines, technology assessments, geopolitical and economic security implications of climate change, raw materials and energy supply and serious gaming techniques.

Geert Kuiper (Keynote speaker)

Geert Kuiper, Director Strategy and Technology at the Netherlands Ministry of Defence, began his career at the Ministry of Defence in 1987. He has supported the Ministry's development when the armed forces transformed into expeditionary forces and was charged with tasks in former Yugoslavia, Iraq and Afghanistan. He has been involved in various inquiries such as into NLD DISS's performance (Dessens Committee I, 2006, the fall of Srebenica (2002), and an independent inquiry into the Dutch government's political support for the war in Iraq (Davids Committee, 2009). In 2012 Geert Kuiper joined NLD DISS to serve as head of the intelligence department. He has served as Deputy Director of NLD DISS since August 2014. In 2019 he joined the policy division of the Ministry of Defence as director of strategy and R&T.

Gwenda Nielen (Keynote speaker)

Gwenda Nielen is a director of Tilt, sociologist, behavioural researcher and former lieutenant-colonel of the Dutch army. Over the years she has built her expertise on disinformation, online & offline manipulation and hybrid conflict by combining knowledge with operational experience. By bringing theoretical concepts in operational context in Afghanistan, Syria, Georgia and the Sahel Region she grew an understanding of the multifaceted and complex system dynamics behind several societal and security challenges. From her current role she works with the Tilt team to limit the impact of online originated manipulation of perception and behaviour. By generating insight with online disinformation monitoring and building resilience against online harm with serious games they enable people and organisations to protect themselves against disinformation.

Hester Somsen (Keynote speaker)

Hester Somsen started working at the Dutch Ministry of Foreign Affairs in 1997. She has worked on issues relating to the former Yugoslavia between 1997-2000, on parliamentary relations upon return, at the Department of European Integration, in the Dutch embassy in Tanzania, as Head of the Crisis management and Peacekeeping Operations Division in the Security Policy Department, and as Ambassador to Lebanon. In September 2016 she was appointed Director Security Policy at the Dutch Ministry of Foreign Affairs. In that capacity she is responsible for the articulation and implementation of Dutch policy in the fields of Counter-Terrorism, Cyber, Hybrid, NATO, EU and OSCE policy, Peacekeeping and Crisis management Operations and Non-proliferation, Arms Control and

Disarmament and Arms Export Control related to Weapons of Mass Destruction and Conventional Arms.

Rubén Arcos

Dr. Rubén Arcos is a professor of communication sciences at URJC and a member Ciberimaginario. He is co-founder and co-director of IntelHub, an international network for the study of intelligence. He is a freelance contributor to Jane's Intelligence Review and Deputy Editor of The International Journal of Intelligence, Security, and Public Affairs. He is a member of the Hybrid CoE's information expert pool. His main research interest are intelligence, strategic communication and hybrid threats.

Monica Cardarilli

Dr. Monica Cardarilli is Project Officer at the European Commission's Joint Research Centre. She provides scientific support to European Commission Services and Member States by conducting research on threat mitigation and security aspects for critical infrastructure protection and resilience. Within the EU-HYBNET project, she facilitates common understanding and raises the awareness of the relevant authorities around the issue of hybrid threats, supporting research and innovation activities to counter them.

Gunhild Hoogensen Gjørv

Gunhild Hoogensen Gjørv is professor of security studies at UiT The Arctic University of Norway. She leads "The Grey Zone" research group, which includes a number of research projects investigating civilian responses to hybrid threats and warfare, and the role of trust in European societies.

Maxime Lebrun

Maxime Lebrun, Senior Analyst, Research and Analysis. Prior to taking up his post at the European Centre of Excellence for Countering Hybrid Threats, Maxime worked at the Baltic Defence College in Tartu as a Lecturer in War and Conflict Studies and as Acting Department Director. During that time, he was also a Non-Resident Research Fellow at the International Centre for Defence and Security. Maxime holds a master's degree in International Relations from Sciences Po Lyon with a specialization in strategic, military and security studies from Sciences Po Aix-en-Provence.

Rick Meessen

Rick Meessen is currently Principal Advisor for Defence and Security at TNO. He completed his study in Mathematics and Operational Research in 1988. After that he served for 2 years in the Dutch Army. In 1990 he started at TNO, holding several positions: project and program manager for operational analysis and procurement support, department manager for Command & Control and for Training Innovations, business unit manager for Operational Analysis and Simulation and program director for Military Operations. Between 2014 and 2016 he was director defence research at TNO and member of the NATO Science and Technology Board. His current research activities relate to hybrid warfare, technology scanning and assessment, horizon scanning and future defence and security policymaking. For hybrid warfare he wrote several publications and reports, such as "Hybrid: the new Normal" and "Trends and Developments in Hybrid Conflicts Set to Shape 2020 and Beyond". He also has an advisory role to the Dutch Ministry of Defence on Strategic Knowledge and Innovation.

Anja van der Hulst

Anja van der Hulst holds a MSc in Educational Technology and received her PhD in Artificial Intelligence and Education from the University of Amsterdam. From 1995, she specialized in military simulations and conducted a series of training needs analysis studies for military simulations within the RNLD navy, army and mil. police. She is lead designer and facilitator of a series of war/conflict games from tactical up to strategic level. The latter includes games for top level government, among which Nato's North Atlantic Council, NLD cross-departmental and NLD chief of defence and commanders of the armed forces services.

Jesper van Putten

Jesper van Putten is currently program- and projectleader and researcher at TNO. He completed his Master of International Relations in 2010. In 2012 he started working for the Dutch National Police as a specialist of policing. The first five years he served in a number of operational functions, both on the street and as investigator, mainly in the field of subversive crimes. As a specialist of policing he tried to solve wicked problems. After this he worked one year as a political advisor for the police chief in the city Centre of Rotterdam. The final three years Jesper worked for the Director of Strategy and Innovation, to help building the Police of the Day after Tomorrow, with a focus on cultural change, new methods of working and innovation. In his final six months in 2021 Jesper was detached to the European Commission to work as a National Expert in the cabinet of Commissioner Johansson of Migration and Home Affairs. Jesper started working for TNO in October 2021. He now works as a project leader mainly in the field of safety and security, and recently joint the Hybrid Team to work on studies in this field.

Willem Verdaasdonk

Willem is a researcher at TNO within the unit Defense, Safety and Security. He has an educational background in International Studies (BA) and Crisis and Security Management (MSc). He has previously worked as a crisis management consultant, as a well as a senior tutor for the B.Sc. Security Studies at the Institute of Security and Global Affairs at Leiden University. In his present capacity at TNO, Willem's main focus and area of expertise is the development of (war)games for governmental agencies in the Netherlands and Europe as well as the development of risk/threat methodology for Dutch National Security.
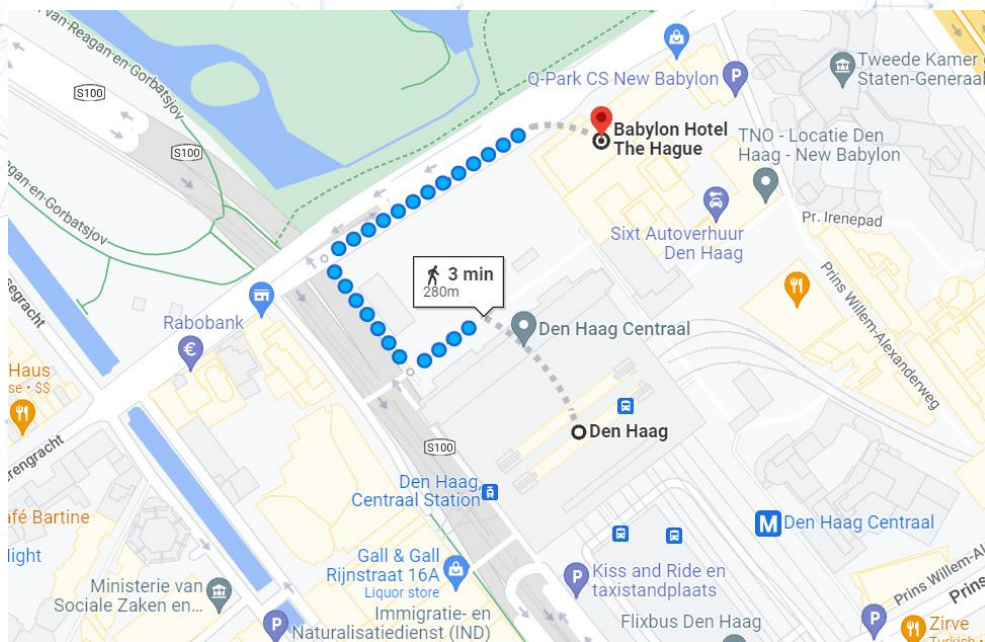
Practical information

VENUE

The IKEW will be held at the **Babylon Hotel Den Haag**, at Bezuidenhoutseweg 53, 2594 AC Den Haag, Netherlands (location).

Please follow the signs for the EU-HYBNET IKEW 2022 meetings.

The Babylon Hotel is only a couple of minutes away from the Hague Central Station. You can find the exact directions to access the venue from the station below and here:

All participants are welcome to contact the Babylon Hotel about accommodation options.

LEISURE & NETWORKING

Following the IKEW, a networking event, including foods and drinks, will take place at **MingleMush Foodhall Den Haag** at Anna van Buerenplein 712, 2595 BH Den Haag, Netherlands – a walking distance from the Babylon Hotel (location).

A space has been reserved for the EU-HYBNET IKEW & ISW events. All participants are welcome to join **at own cost**. Registration is **not** needed.

Additional information about the city of the Hague can be found here.

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

🌐 euhybnet.eu

in 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