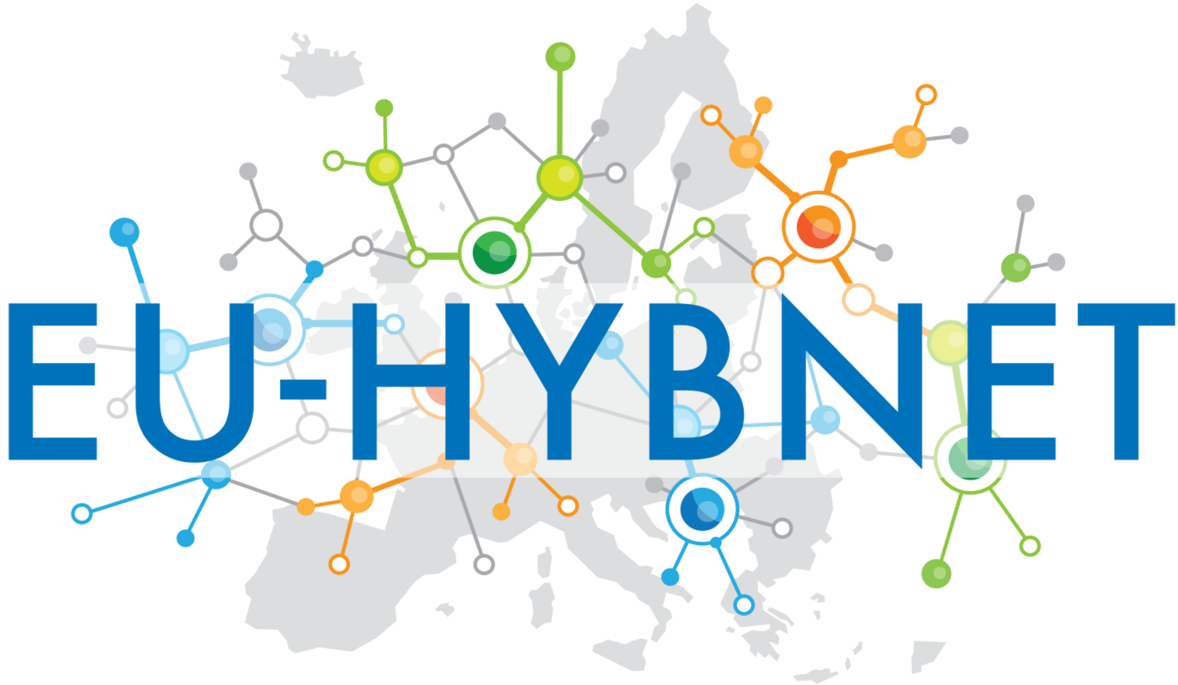


# 4th FUTURE TRENDS WORKSHOP REPORT

DELIVERABLE 3.17

Lead Author: PLV

Contributors: EOS, Laurea, EOS, DSB

Deliverable classification: Public (PU)

This project has received funding from the European Union’s Horizon 2020 – Research and Innovation Framework Programme, H2020-SU-SEC-2019, under grant agreement No. 883054

## D3.17 4TH FUTURE TRENDS WORKSHOP REPORT

| | | |
|---|---|---|
| **Deliverable number** | **3.17** | |
| **Version:** | **1.0** | |
| **Delivery date:** | **27/06/2024** | |
| **Dissemination level:** | **Public (PU)** | |
| **Classification level:** | **Public (PU)** | |
| **Status** | **Ready** | |
| **Nature:** | **Report** | |
| **Main authors:** | **Iván L. Martínez**<br>**Susana Sola** | **PLV** |
| **Contributors:** | **Vincent Perez, Kristian Reeson**<br>**Tiina Haapanen, Päivi Mattila**<br>**Orjan Karlson** | **EOS**<br>**Laurea**<br>**DSB** |

## DOCUMENT CONTROL

| Version | Date | Authors | Changes |
|---|---|---|---|
| 0.1 | 17/05/2024 | Iván L. Martínez , Susana Sola/PLV | First draft, text to all chapters |
| 0.2 | 20/05/2024 | Iván L. Martínez, Susana Sola/PLV | Second draft, content input and document structure |
| 0.3 | 15/05/2024 | Vincent Perez, Kristian Reeson/ EOS | Text contribution, material delivery |
| 0.4 | 25/06/2024 | Orjan Karlson/ DSB | Review and comments for the text |
| 0.41 | 27/06/2024 | Päivi Mattila/ Laurea | Review and comments for the text |
| 0.5 | 27/06/2024 | Iván L. Martínez, Susana Sola/PLV | Final editing |
| 1.0 | 27/06/2024 | Päivi Mattila/ Laurea | Final review and submission of the document to the EC |

## DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

## TABLE OF CONTENTS

## TABLES

## FIGURES

# 1. INTRODUCTION

The Annual Future Trends Workshop, part of the EU-HYBNET initiative (Pan-European Network to Counter Hybrid Threats), focuses on anticipating forthcoming hybrid threats and their potential evolution. This ensures that the project not only addresses current needs but also prepares for future challenges. This workshop falls under EU-HYBNET Task (T) 3.4 “Innovation and knowledge exchange events”.

The inaugural EU-HYBNET Future Trends Workshop was hosted by the Hybrid CoE, conducted virtually on March 31st, 2021. The second workshop, organized by the Catholic University of the Sacred Heart of Rome, Italy (UCSC), was a hybrid event held on April 5th, 2022, in Rome. The third workshop, held on April 19th, 2023, in Bucharest, Romania, was exclusively in-person and organized by the “Mihai Viteazul” National Intelligence Academy.

Most recently, the fourth workshop, arranged by the Valencia Local Police (PLV), was a hybrid event conducted on April 24th, 2024, in Valencia, Spain. This deliverable reports the methods and outcomes of this fourth workshop.

## 1.1 STRUCTURE OF THE DELIVERABLE

**This document includes the following chapters:**

Chapter 1: *Introduction.* Description of the different Annual Future Trends Workshops already organised.

Chapter 2: *Future trends in the EU-HYBNET project*. This section delineates the role of the annual Future Trends Workshop in advancing the project's goals and underscores the significance of forward-thinking in mitigating hybrid threats.

Chapter 2: *Methods*. Here, the methodology employed in the workshop, the nature of data gathered, and its intended utilization are elucidated.

Chapter 3: *Outcomes of the workshop: perceptions on future of hybrid threats.* This chapter outlines the key trends identified by participants as pivotal to understanding the future landscape of hybrid threats.

Chapter 4: *Workshop participants and feedback*. This section encapsulates the primary feedback received from participants and the key insights gleaned from the workshop.

Chapter 5: *Conclusions and way ahead*. This chapter expounds on how the insights garnered from the Future Trends Workshop will inform the EU-HYBNET Work Package (WP) 3 "Surveys to Technology, Research, and Innovations," particularly in mapping innovations to address gaps and needs in countering hybrid threats across Europe.

## 2. FUTURE TRENDS AND EU-HYBNET PROJECT

The Future Trends Workshop, integral to Task 3.4 of the EU-HYBNET project (“*Innovation and knowledge exchange event*s”), serves as a platform for fostering forward-looking perspectives among participants. Its primary aim is to cultivate innovative thinking and generate unconventional ideas that may unveil novel approaches to combating hybrid threats. Moreover, the workshop aids project partners in exploring both immediate and future-oriented solutions for addressing hybrid threats.

The fourth iteration of this workshop was organized and hosted by PLV in collaboration with the European Organisation for Security (EOS), the leader of EU-HYBNET's Task 3.4, and with support from Laurea University of Applied Sciences, the project coordinator. Core theme leaders (L3CE, UiT, URJC, Hybrid CoE and Satways) played a significant role in shaping the event and its breakout sessions.

As the security landscape grows increasingly intricate, the identification of emerging threats becomes more challenging. Hybrid threats, in particular, pose a formidable detection challenge. Operating below the threshold of overt conflict, these actors utilize multiple channels simultaneously and often lack clear delineation from one another. Furthermore, hybrid threats evolve over time, propelled by technological advancements and novel resilience-building strategies, making detection paramount for effective countermeasures. Without detection, countering these threats becomes an insurmountable task, leaving us lagging behind and at a disadvantage.

Managing such complexities begins with establishing a comprehensive, dynamic understanding of evolving security issues on a global scale. Foresight, particularly in trend detection and analysis, is indispensable in this endeavour. Adopting a multidisciplinary approach is crucial for comprehending trends related to hybrid threats and their evolutionary trajectories, necessitating input from various sectors including pan-European security practitioners, governmental entities, local administrations, NGOs, academia, and the private sector.

The 4th Future Trends Workshop, strategically positioned before the fourth EU-HYBNET Annual Workshop, aimed to maximize stakeholder participation. Within the project, foresight and trend assessment permeate every phase, with the Future Trends Workshop serving as a dedicated event to bolster this capability. Specifically, the workshop aligns with project Objective 7 (OB7), which seeks to forge effective synergies with existing European, national, and sub-national networks engaged in countering hybrid threats.

Under OB7, Goal 7.2 emphasizes empowering European practitioners, industry, SMEs, and academic stakeholders to discern critical innovations and trends. The Future Trends Workshop was designed with this objective in mind, focusing on identifying and analysing potential trends and innovations to address future needs in pan-European security. Through engagement with high-level speakers and panel discussions, participants gained insights into how megatrends could impact European security.

During the workshop, four breakout sessions were carried on to cover the maximum number of topics and to show the audience a complete overview of what is going on under the topic of hybrid threats and its future. Through collaborative exploration, they endeavoured to understand the contextual dynamics of hybrid threats within the broader framework of megatrends, thereby painting a comprehensive picture conducive to imagining potential innovations. Their task involved identifying the most pertinent trends shaping the future landscape of hybrid threats. Given its virtual and public nature, the event was accessible to all interested stakeholders, facilitating broad participation and knowledge exchange.

The table below highlights how the FTW in general will contribute to the project content and will support each EU-HYBNET Work Packages (WP) to proceed in their work.

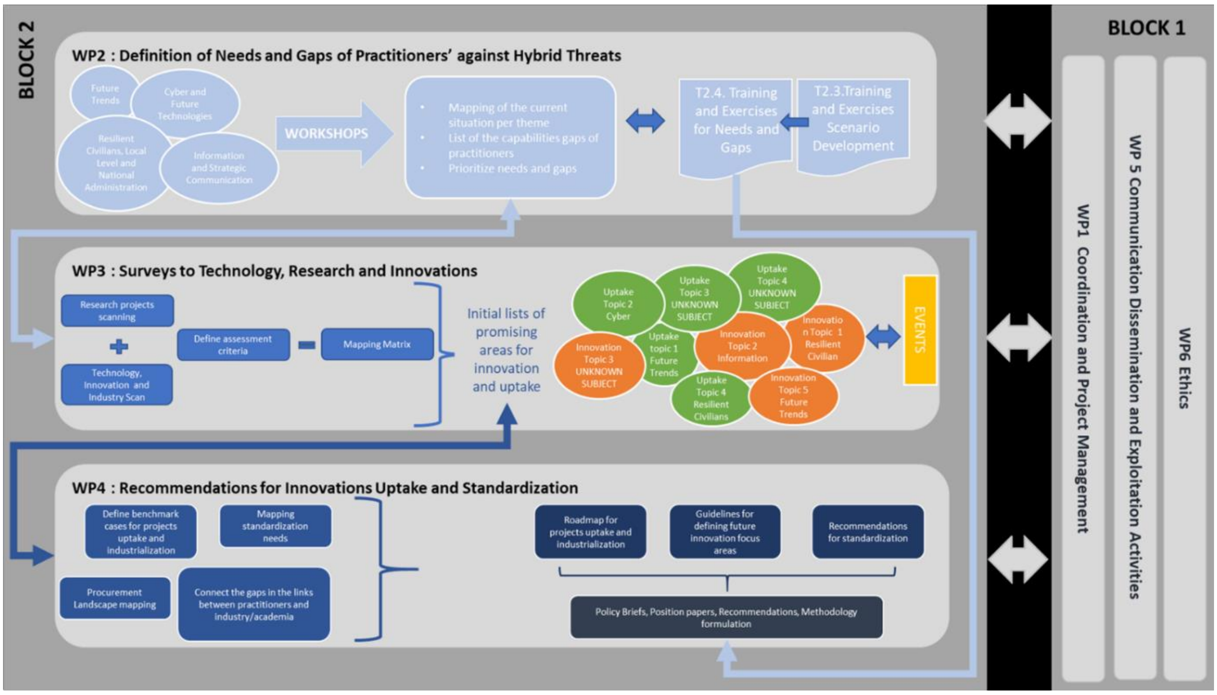

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities gaps of practitioners
Prioritize needs and gaps
T2.4. Training and Exercises for Needs and Gaps
T2.3.Training and Exercises Scenario Development
WP3 : Surveys to Technology, Research and Innovations
Research projects scanning
Technology, Innovation and Industry Scan
Define assessment criteria
Mapping Matrix
Initial lists of promising areas for innovation and uptake
Uptake Topic 2 Cyber
Uptake Topic 3 UNKNOWN SUBJECT
Uptake Topic 4 UNKNOWN SUBJECT
Innovation Topic 3 UNKNOWN SUBJECT
Uptake topic 1 Future Trends
Innovation Topic 2 Information
Innovatio n Topic 1 Resilient Civilian
Uptake Topic 4 Resilient Civilians
Innovation Topic 5 Future Trends
EVENTS
WP4 : Recommendations for Innovations Uptake and Standardization
Define benchmark cases for projects uptake and industrialization
Mapping standardization needs
Procurement Landscape mapping
Connect the gaps in the links between practitioners and industry/academia
Roadmap for projects uptake and industrialization
Guidelines for defining future innovation focus areas
Recommendations for standardization
Policy Briefs, Position papers, Recommendations, Methodology formulation
BLOCK 1
WP1 Coordination and Project Management
WP 5 Communication Dissemination and Exploitation Activities
WP6 Ethics

Figure 1: EU-HYBNET Structure of Work Packages and Main Activities

The organization of the FTWs directly aligns with **Project Objective (OB) 1:** *To enrich existing network for countering hybrid threats and ensure long term sustainability*. Furthermore, it supports **Project OB5:** *To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network*; **OB6:** *To foster capacity building and knowledge exchange on countering hybrid threats* and **OB7:** *To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats*. The Key Performance Indicators (KPIs) for network expansion include the minimum requirement of organizing at least three events annually. The detailed correlation between project objectives and event organization within EU-HYBNET KPIs is elaborated below.

Table 1: EU-HYBNET Objectives 1, 5, 6 and 7

| **OB1: To enrich the existing network countering hybrid threats and ensure long term sustainability** | | | |
|---|---|---|---|
| **Goal** | | **KPI description** | **KPI target value** |
| 1.3 | To arrange and host events where practitioners, industry, SME and | Events are organized to attract European actors | At least 3 events every year where |

| | | | |
|---|---|---|---|
| | academic actors can engage in information sharing | willing to participate in professional exchanges | over 100 actors, all professionals in specific areas, will engage in information sharing |
| **OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network** | | | |
| **Goal** | | **KPI description** | **KPI target value** |
| 5.2 | To set up community forums that will empower the European network to engage in productive exchanges on research and innovation, needs/gaps, uptake, policy issues, standardisation | Events for practitioners, industry/SMEs/academic actors are organised; forums established in relation to 4 core themes | -At least 3 events per year; at minimum100 participants<br>-Innovation arena (IA) and Web site are in use by at least 4 forums (see KPI for Goal 5.1) |
| **OB6: To foster capacity building and knowledge exchange on countering hybrid threats** | | | |
| **Goal** | | **KPI description** | **KPI target value** |
| 6.1 | To arrange dialogue sessions for EU practitioners, industry, SME and academic actors to strengthen capacity and hybrid threat knowledge exchange | Events are organised to communicate the new hybrid threat knowledge; and on latest best practices | -At least three yearly events are executed with a minimum of 100 participants each time |
| **OB7: To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats** | | | |
| **Goal** | | **KPI description** | **KPI target value** |
| 7.2 | To empower European practitioners, industry, SME and academic actors to recognise important innovations/trends | Events are organised on innovations and future trends | -At least 2 events yearly where information on innovations and future trends is shared |
| 7.5 | To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically | Events are structured to facilitate interactions among stakeholders to establish synergies | -At least 2 events yearly where over 100 actors will meet<br>- Newsletter, published every 6 months w. 60 new readers yearly |

In considering this workshop, it's essential to recognize that as the security landscape grows more intricate, so does the challenge of identifying emerging threats. Hybrid threats, by their very nature, present unique difficulties in detection. Operating beneath the threshold of overt conflict and utilizing multiple channels concurrently, these actors often lack clear distinctions from one another. Additionally, hybrid threats evolve over time, driven by technological advancements and novel strategies for resilience, deterrence, and countering. Without effective detection, countering such threats becomes an insurmountable task, leaving us consistently lagging behind and at a disadvantage.

Addressing these complexities requires the establishment of a comprehensive, dynamic understanding of evolving security issues on a global scale. Foresight, particularly in the detection and analysis of trends, emerges as a crucial capability in this endeavour. Understanding the trends of hybrid threats, or those influencing their evolution, demands a multidisciplinary approach where signals from every domain are pertinent. Consequently, it becomes imperative to convene diverse stakeholders - including government practitioners, local administrations, non-governmental organizations, academia, and the private sector - to facilitate mutual learning.

While foresight and trend assessment are integrated to some extent throughout the project's phases, the Future Trends Workshop stands as a singular event dedicated to enhancing this capability. Focused on perspectives relevant for the next two decades, these workshops significantly contribute to Project Objective 7 (OB.7), aimed at establishing effective synergies with existing European, national, and sub-national networks involved in countering hybrid threats.

The 4th Future Trends Workshop aimed to advance this goal by focusing on the identification and analysis of potential trends. Participants gained insights into how megatrends could impact European security through keynote speeches and panel discussions featuring high-level speakers. Building upon the project's findings three years into its duration, this workshop provided a platform for stakeholders to discuss hybrid threats in the EU's neighbourhood, their implications for EU security, and innovative approaches to counter them.

Given the continuously evolving landscape of hybrid threats, foresight and creative thinking were deemed central for understanding, detecting, and responding to emerging threats. Consequently, the workshop adopted a more anticipatory and prospective outlook, emphasizing the identification of weak signals and outliers indicative of disruptive changes to the European security environment.

Structured around the recognition that recent events in the EU neighbourhood have brought into focus a complex dynamic of adversarial tools and strategies, the workshop was designed to respond comprehensively to these evolving threats. It featured keynote speeches, panel presentations, and breakout sessions dedicated to key themes, including Cyber and Future Technologies, Resilient Civilians, Local Level and National Administration, and Information & Strategic Communication.

The breakout sessions provided participants with the opportunity to engage in discussions on existing and future trends, contextualizing hybrid threats within broader megatrends and envisioning potential innovations. Participants collaborated to define the most pertinent trends shaping the future landscape of hybrid threats. These discussions culminated in a final panel where the findings of each breakout session were presented, offering insights into future trends and innovations and drawing initial conclusions for their implications on the future of EU security.

The alignment of the workshop with other project objectives will be examined in the subsequent section.

# 3. METHOD

This chapter describes the objectives of the event, what kind of information was gathered and how.

## 3.1 OBJECTIVES

The primary aim of the 4th Future Trends Workshop (FTW) was to establish a platform facilitating interaction among EU-HYBNET partners, stakeholders, EAB members, network participants, and interested innovation providers, industry representatives, SMEs, and NGOs. Together, they delved into the topic of Hybrid Threats emerging in the EU neighbourhood and their implications for the future of EU security.

As elucidated earlier, the Future Trends Workshop endeavours to achieve project objective 1 (OB1), enriching the existing network countering hybrid threats and ensuring long-term sustainability. By hosting a publicly accessible event and engaging with its Spanish (through the Valencia Local Police partner links) and international network, the host organization broadened EU-HYBNET's outreach, enhancing its appeal to prospective members. Notable efforts were made to attract new organizations and presenters, fostering fresh perspectives on hybrid threat issues for both the consortium and the network. The local perspective and the involvement of Valencia's authorities (like the councillor and several Police Chief comissioners of the area) was more than evident.

Moreover, the event provided a platform for networking and information exchange, furthering project objective 5 (OB5) by fostering enhanced interaction within the network. As evidenced in this report, many network members not only attended but also actively participated in break-out sessions, facilitating connections and understanding of individual challenges. Furthermore, fostering forward-thinking directly supports the sustainability of all ideas and solutions generated by the project.

By identifying trends deemed most impactful in shaping the future of hybrid threats, the workshop also aligns with project objective 2 (OB2), defining common requirements to address knowledge gaps, performance needs, and enhance research, innovation, and training capabilities. This event specifically addressed Goal 2.3 under this objective by gathering and defining insights on trends.

The thematic focus of the Future Trends Workshop was developed collaboratively by organizing partners EOS, URJC and LAUREA, with input from WP 3 leader SATWAYS and core theme leaders, notably Hybrid CoE. Consideration was given to the current EU security landscape and the evolving nature of hybrid threats in its broader neighbourhood.

The framework was established through a series of two keynote lectures, showing several models for conflict analysis and how border management could counter future hybrid threats. These lectures provided valuable insights and set the stage for discussions during a complete round table and subsequent four break-out sessions dedicated to EU-HYBNET core pillars.

Panel speakers were selected to offer diverse perspectives, ranging from representatives of Belgian General Intelligence and Security Service and FRONTEX. Discussions during break-out sessions were open to all participants, fostering dialogue and exchange in a more intimate setting.

These reflections will inform future assessments of EU-HYBNET results, including identified gaps, needs, solutions, and innovations. The organization of participants into small working groups aimed to facilitate discussion and exchange on hybrid threats and trends in an environment conducive to fostering innovative ideas and discussing emerging trends and signals.

## 3.2 WORKSHOP STRUCTURE

The event organizers structured a comprehensive in-person and in remote workshop spanning a full day, divided into three parts:

a) The initial segment featured one keynote lecture about models of conflict analysis and a round table discussion led by Mr Isto Mattila, EU-HYBNET Innovation Manager experts focused on Hybrid Threats.

b) The subsequent interactive phase involved participants being grouped into four breakout sessions to delve into specific topics: Cyber & Future Technologies, Resilient Civilians, Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats and Securing the EU's borders to 2040 – Thinking about the security landscape.

c) The final part comprised a keynote lecture on FRONTEX's View on the Future of Hybrid Threats in Relation to Border Management, followed by a closing keynote speech delivered by Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police.

Keynote speeches were delivered by notable figures such as Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces; and Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX. Additionally, a round table discussion on Border Management to Counter Future Hybrid Threats included speakers like Dr. Souzanna Sofou, Satways, Dr. Jarmo Puustinen, Finnish MoI and Don Diederick, Europol Innovation Lab Representative.

The second phase featured four breakout sessions facilitated by core theme leaders L3CE, JRC, URJC and Hybrid CoE. These sessions explored Cyber & Future Technologies, Resilient Civilians, Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats and Securing the EU's borders to 2040 – Thinking about the security landscape.

Every breakout session was customized to address recognized deficiencies and requirements within its corresponding core theme. Participants actively engaged in conversations surrounding emerging trends, advancements, and hurdles associated with hybrid threats, with chances for hands-on demonstrations and dialogue focused on finding solutions.

These sessions served as a forum for thorough exploration and the exchange of ideas, enhancing comprehension of hybrid threats and guiding the development of future strategies and innovations for their effective mitigation.

# 4. OUTCOMES OF THE WORKSHOP: PERCEPTIONS ON FUTURE OF HYBRID THREATS

As previously noted, the plenary session of the workshop sought to establish the context and provide initial insights and perspectives to participants. This was intended to orient the discussions and facilitate the identification of both present and forthcoming trends in hybrid threats.

## 4.1 PERCEPTIONS PRESENTED BY KEYNOTE SPEAKERS

Two keynote speakers presented core ideas in the field of hybrid threats:

- Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces: “Models for Conflict Analysis & Some Critical Remarks on Dealing with Hybrid Threats”
- Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX: “FRONTEX’s View on the Future of Hybrid Threats in Relation to Border Management”

The aim of the plenary session was to change the way we think about hybrid threats, foresight activities, and to prepare ourselves for the unmanned.

The workshop included a plenary session with a keynote speech from the Belgian General Intelligence and Security Service outlining various conceptual models to analyse the hybrid threat landscape as well as a panel discussion on Border Management to counter future hybrid threats from the Finnish Ministry of Interior, Laurea University of Applied Sciences, Europol Innovation Lab and Satways.

Through this session, it became apparent that the different conceptual models used to analyse conflicts, events, or threats all have built in biases or levels and therefore can skew understanding in a way that renders a common situational awareness difficult. The question then arises how to move past these issues in a complex and multi-level environment such as border management where multiple actors are involved. Some suggestions offered to participants to think about were multi-faceted taxonomies or the standardisation of models to remove blind spots.

Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don’t pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to understand how technology can be used in new ways to undermine border security or slow down border management processes.

In this incredibly complex landscape, EU-HYBNET’s role is to find solutions by refining conceptual models and participating in foresight activities when possible (even based on the gaps and needs identified by consortium and network practitioners). We welcome the feedback of additional practitioners and look forward to welcoming them into our network, among other hybrid threats stakeholders.

## 4.2 PANEL DEBATES AND MAIN FINDINGS

The panel discussion on *Border management to counter future hybrid threats* involved: Dr. Souzanna Sofou, Satways, Dr. Jarmo Puustinen, Finnish MoI and Mr Don Diederick, Europol Innovation Lab Representative.

Moderated by Isto Mattila, EU-HYBNET Innovation Manager, Border management to counter future hybrid threats involves strategies and tactics aimed at protecting a nation's borders from a wide range of threats that may involve both conventional and unconventional elements. Hybrid threats typically combine conventional military force with non-military means such as cyberattacks, propaganda, and economic pressure to achieve their objectives.

Here are some key components and considerations for border management in countering hybrid threats:

1. Integrated Approach: Effective border management requires an integrated approach that combines military, law enforcement, intelligence, diplomatic, and other relevant agencies. Coordination and cooperation among these entities are essential to address the diverse nature of hybrid threats.

2. Intelligence Gathering and Analysis: Border security efforts rely heavily on intelligence gathering and analysis to identify potential threats before they materialize. This includes monitoring activities such as illicit trafficking, cyber intrusions, and hostile propaganda aimed at destabilizing the country.

3. Technology and Surveillance: Advanced technology, including drones, sensors, radar systems, and surveillance cameras, plays a crucial role in monitoring and securing borders. These technologies help in detecting and intercepting threats, including unauthorized border crossings and smuggling activities.

4. Cyber Defense: In the modern era, cyber threats are a significant component of hybrid warfare. Robust cybersecurity measures are essential to protect critical infrastructure, communication networks, and government systems from cyberattacks aimed at undermining national security.

5. Border Infrastructure: Investing in physical infrastructure such as border fences, checkpoints, and surveillance towers can enhance border security and deter unauthorized activities. Additionally, improving transportation infrastructure can facilitate the movement of security forces and enable rapid response to emerging threats.

6. International Cooperation: Hybrid threats often transcend national borders, requiring cooperation with other countries and international organizations. Information sharing, joint exercises, and collaborative initiatives can strengthen border security and counter hybrid threats more effectively.

7. Public Awareness and Resilience: Educating the public about potential threats and promoting resilience can enhance a nation's ability to withstand hybrid attacks. This includes raising awareness about cybersecurity best practices, emergency preparedness, and the role of citizens in reporting suspicious activities.

8. Adaptability and Flexibility: Border management strategies must be adaptable and flexible to respond to evolving threats. Continuous assessment of risks and vulnerabilities is essential to adjust tactics and allocate resources effectively.

## 4.3 TRENDS IDENTIFIED DURING BREAKOUT SESSIONS

In the second part of the FTW event, there were organised four breakout sessions, as follows:

Table 2: 3rd FTW Breakout sessions

| Breakout Sessions | |
|---|---|
| **Breakout Session #1:** Cyber & Future Technologies | Evaldas Bruze (L3CE) |
| **Breakout Session #2:** Resilient Civilians, Local Level and National Administration | Dr. Julien Theron, Researcher in Hybrid Threats at the JRC |
| **Breakout Session #3:** Information & Strategic Communication | Rubén Arcos Martín (URJC), Irena Chiru (MVNIA) and Jorge Gomes (VOST Europe) |
| **Breakout Session #4:** Future Trends of Hybrid Threats | Maxime Lebrun (HCoE) and Hanne Dumur-Laanila (HCoE) |

### BREAK-OUT SESSION #1

**Core theme:** Cyber and Future Technologies

**Title:** Future Trends in Cyber and Future Technologies

**Led by:** Evaldas Bružė (L3CE)

**Description:** During this breakout-session we will dive into recent technological developments and evolutions that impact cyber landscape of EU in relation to hybrid threats. As most debated topics we will start from next generation AI (Gen AI, LLMs, Deep learning algorithms) and will follow with blockchain, virtual and augmented reality, robotics, next development in computing and their impact on the security landscape of the EU. This session must explore technological developments globally, in the EU's and its member states' ecosystems, identify the key emerging tech trends that challenges current status quo and by looking into near future predict most prioritized technology uptake, identify least developed areas and try to understand what kind of response or resilience we need to establish to be able to safeguard our cyber & technological ecosystem as well what cyber components will are affecting of hybrid threats evolution.

### BREAK-OUT SESSION #2

**Core theme:** Resilient civilians, local level and national administration

**Title:** Hybrid threats in the Arctic

**Led by:** Julien Theron (JRC)

**Supported by:** Gunhild Hoogensen Gjørv (UiT), Marek Kohv (ICDS)

**Description:** This break-out session will address the question of the relations of the citizens with their local and national authorities with regard to the question of European borders in general and border security in particular. The various tools of weaponization of migration by state and non-state actors have indeed a certain echo on EU citizens and to their relations to governance. After a panorama backed by case studies on the diverse types of hybrid threats related to this issue, the session will address specific questions with the participants, enriching collective analysis with their various professional capacities. The session will continue with a presentation on the holistic society-state approach by the International Centre for Defence and Security, and will be concluded by debating the relation of the European citizens to their authorities with the Arctic University of Norway.

## BREAK-OUT SESSION #3

**Core theme:** Information & Strategic Communication

**Title:** Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats

**Led by:** Jorge Gomes (VOST Europe)

**Supported by:** MTES

**Description:** This session aims to equip participants with a nuanced understanding of FIMI and its role as a tool in hybrid warfare. We will explore the mechanisms through which disinformation spreads, the actors involved, their motives, and the impact on targeted populations and democratic institutions. Additionally, we will delve into the strategies for identifying, combating, and mitigating the effects of disinformation campaigns.

1. Nature and Mechanisms of FIMI: Understanding the ecosystem of false information, misinformation, foreign information manipulation and interference, and domestic information manipulation, and how they are used in hybrid threats.
2. Case Studies of Recent Disinformation Campaigns: Analysis of specific instances where disinformation has been weaponized, focusing on the techniques used, the actors behind them, and the intended outcomes.
3. Role of Social Media and Technology: Examination of how social media platforms and emerging technologies (like deepfakes and AI-generated content/Synthetic content) facilitate the spread of disinformation.
4. Counter-Strategies and Best Practices: Sharing of national and international efforts to combat disinformation, including legislative measures, fact-checking initiatives, and digital literacy programs.
5. EU-HYBNET partner’s Role and Future Actions: Discussing how EU-HYBNET and its partners, and network members, can cooperate to enhance resilience against this kind of hybrid threats, focusing on the development of a Rapid Response System, that can integrate different stakeholders, and the trusted flaggers role.

6. The Borderless Nature of Disinformation: Disinformation campaigns, by their very nature, exploit the interconnected fabric of our global society. They seamlessly traverse geographic and digital boundaries, leveraging cultural nuances and societal fissures within different countries to amplify their effects. This adaptability allows disinformation to resonate with diverse audiences, making it a potent tool in hybrid threats.
7. Adapting to Local Realities: The agility of disinformation campaigns to tailor their narratives to align with local sentiments, historical contexts, and socio-political dynamics is particularly alarming. This bespoke manipulation enhances their believability and potential to sow discord. For instance, the same overarching narrative can be spun differently to exploit specific local grievances or fears in various European countries, thus magnifying its disruptive impact.
    a. This inherent characteristic of disinformation to know no borders and to morph according to local contexts is a clarion call for more robust transboundary cooperation. No single nation can effectively combat this threat in isolation. It demands a collective effort involving:

- Sharing Intelligence and Best Practices: Countries need to collaborate closely in sharing intelligence about emerging disinformation campaigns and the tactics used. Pooling resources and expertise can lead to more effective identification and mitigation strategies.
- Unified Regulatory Frameworks: Establishing common regulatory standards and cooperative frameworks can help govern the digital landscape where much of this disinformation proliferates.
- Cross-Border Collaborative Initiatives: Initiatives like joint educational programs, public awareness campaigns, and cross-border fact-checking teams can significantly enhance the resilience of societies against disinformation.
- International Research and Dialogue: Encouraging research, dialogue, and exchange programs focused on understanding and addressing the global dynamics of disinformation can foster a unified approach.
- Participants are requested to prepare by selecting and researching at least one example of a disinformation campaign or propaganda effort that has impacted their country, European countries, or their allies in the past year. These examples will form the basis of our group discussions and analysis. Aim to understand the origins, development, dissemination mechanisms, and countermeasures taken in response to these campaigns.

Our goal is to foster a comprehensive understanding of disinformation as a hybrid threat and to catalyse collaborative efforts among EU-HYBNET members to strengthen our collective defense mechanisms. By sharing knowledge, experiences, and best practices, we can enhance our preparedness and response strategies against the evolving challenges posed by FIMI and propaganda in the hybrid warfare domain.

## BREAK-OUT SESSION #4

**Core theme:** Future Trends of Hybrid Threats

**Title:** Securing the EU’s borders to 2040 – Thinking the security landscape

**Led by:** Maxime Lebrun (HCoE) and Hanne Dumur-Laanila (HCoE)

**Description:** During this breakout-session we will delve into factors that impact the future of the EU's border management and its impact on the security landscape of the EU. This session must explore path dependencies in the EU's and its member states' policies, identify the factors that affect the current situation and from there, try to understand what kind of future plausible and what kind of consequences is the changes mean in terms of hybrid threats potential.

In the final speech, FRONTEX, the European Border and Coast Guard Agency (represented by Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX) plays a critical role in ensuring the security of the European Union's external borders. As threats to border security evolve, FRONTEX has been actively assessing and addressing the challenges posed by hybrid threats.

Hybrid threats encompass a wide range of tactics that blend conventional and unconventional methods to achieve strategic objectives. These threats can include cyberattacks, disinformation campaigns, irregular migration, smuggling, terrorism, and more. Hybrid threats are particularly complex because they often exploit vulnerabilities in multiple domains simultaneously, making them difficult to detect and counter.

In the context of border management, hybrid threats pose significant challenges for FRONTEX and other border security agencies. For example:

1. **Cyberattacks**: Hybrid threats may involve cyberattacks targeting critical border management systems, such as databases, surveillance networks, and communication infrastructure. These attacks can disrupt border operations, compromise sensitive information, and undermine the effectiveness of security measures.

2. **Disinformation**: Hybrid actors may spread disinformation to manipulate public opinion, create confusion, and undermine trust in border management authorities. False narratives about migration, border security, and EU policies can exacerbate tensions and complicate efforts to address security challenges.

3. **Irregular Migration and Smuggling**: Hybrid threats often exploit vulnerabilities in migration routes and border controls to facilitate irregular migration and smuggling activities. Criminal networks may use sophisticated tactics to evade detection, exploit legal loopholes, and circumvent border security measures.

4. **Terrorism and Extremism**: Hybrid threats may involve the infiltration of terrorist or extremist elements among migrant flows, posing a security risk to border management authorities and the wider community. Identifying and intercepting individuals with links to terrorist organizations or radical ideologies requires robust intelligence-gathering capabilities and effective cooperation with law enforcement agencies.

To address these challenges, FRONTEX adopts a multi-layered and integrated approach to border management, combining technological innovation, intelligence-led operations, cooperation with EU member states and third countries, and strategic partnerships with international organizations. By enhancing situational awareness, improving information sharing, and strengthening border controls, FRONTEX aims to mitigate the risks posed by hybrid threats and safeguard the integrity of the EU's external borders.

# 5. WORKSHOP PARTICIPANTS AND FEEDBACK

The event planning began in December 2023; the partners involved in the arrangements were LAUREA, EOS, SATWAYS and PLV. A save the date was created by EOS and shared with the EU-HYBNET consortium and network in this month. It was also published on the EU-HYBNET website and social media, while all partners were encouraged to share the date with their networks.

A draft agenda was created and circulated by EOS in January 2024.

After the event, EOS prepared a press release which was shared on the EU-HYBNET website and social media on May, 2024. The press release included an early overview of the key findings and trends identified during the event. It can be found in Annex IV.

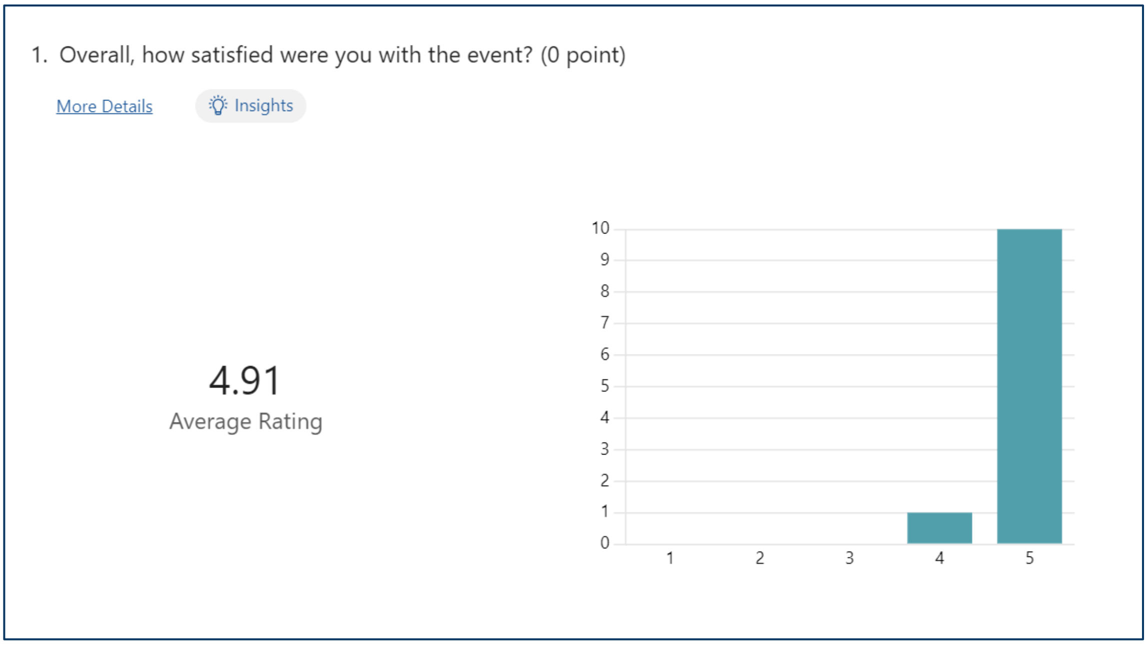
## 5.1 PARTICIPANTS

Participation was open to anyone, and there were no requirements for previous experience in future-oriented thinking. The event attracted around 85 participants in person with around 67 views online.

EU-HYBNET partners considered the participation level of the project's inaugural in-person event a success. Efforts will be made by the network manager to follow up on this event, ensuring that organizations new to EU-HYBNET become part of the network and maintain their involvement and interaction with the project.

## 5.2 PARTICIPANTS’ FEEDBACK AND LESSONS LEARNED

Feedback was collected immediately after the event via an anonymous online questionnaire on Microsoft Forms. QR codes linking to the questionnaires were shared with participants during the event, while a reminder was sent through email. Out of 85 participants, 18 provided feedback.

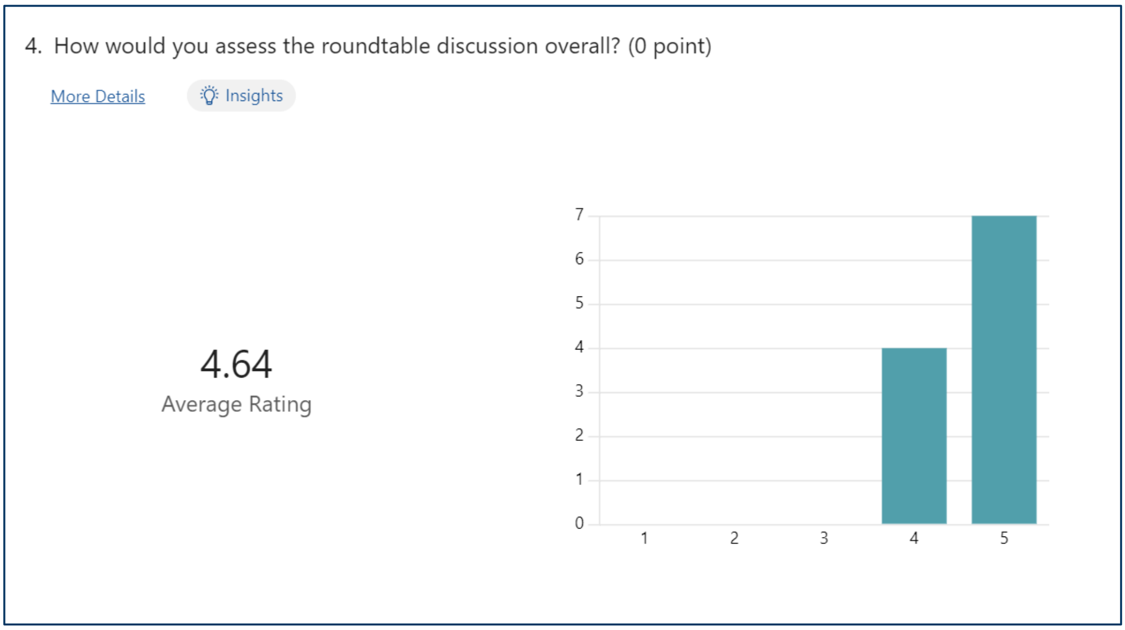


1. Overall, how satisfied were you with the event? (0 point)

4.91
Average Rating

**Figure 2: Participant satisfaction with the FTW event**

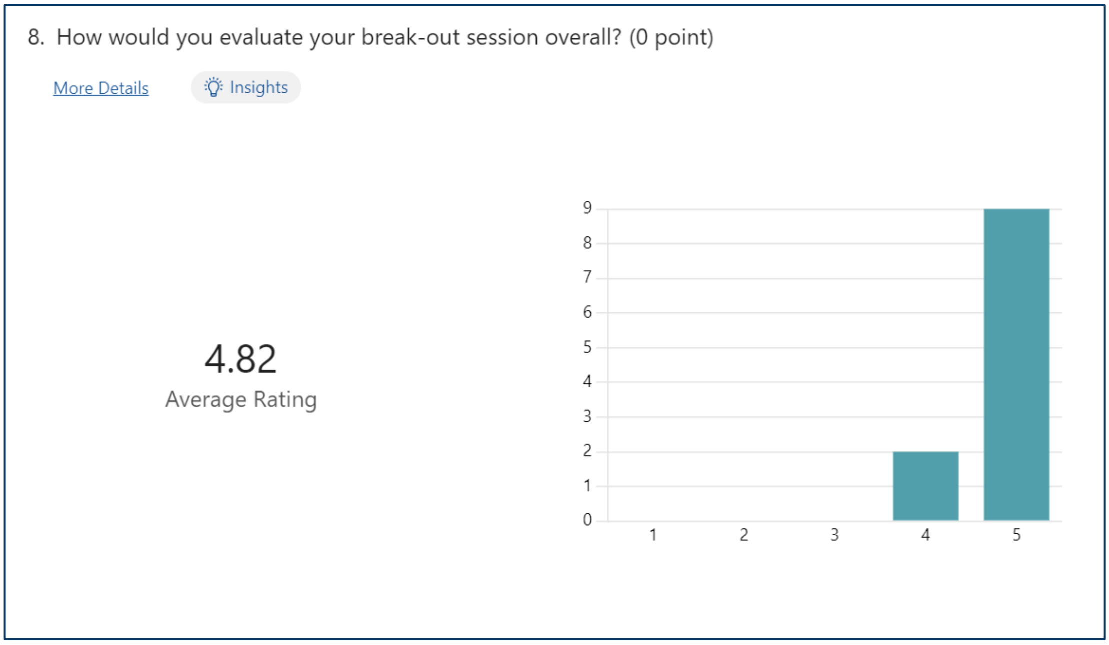
Participants were overall satisfied with the event (4.91 average rating) and its content (4.82 average rating), while the roundtable and the break-out sessions also received very high ratings (4.64 and 4.82, respectively).



4. How would you assess the roundtable discussion overall? (0 point)

4.64
Average Rating

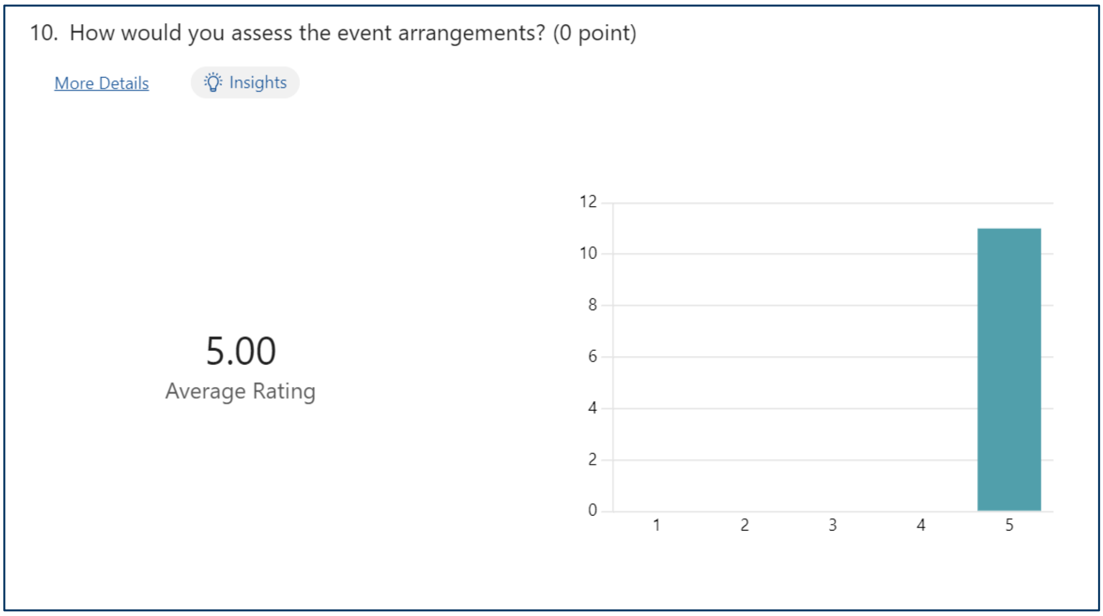
**Figure 3: Roundtable assessment**



8. How would you evaluate your break-out session overall? (0 point)

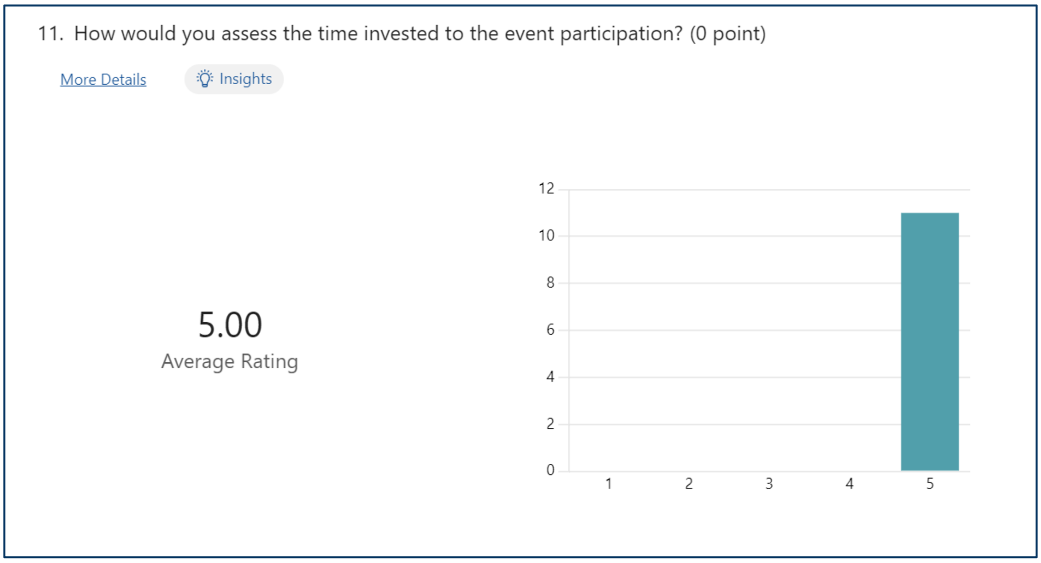
Figure 4: Break-out sessions assessment

Participants were also completely satisfied with the event arrangements (5 average rating), the organisation of the event (5 average rating) and the time dedicated to it (5 average rating); thus, the satisfaction of the audience with the organisation was perfect.



10. How would you assess the event arrangements? (0 point)

Figure 5: Event arrangements assessment


11. How would you assess the time invested to the event participation? (0 point)

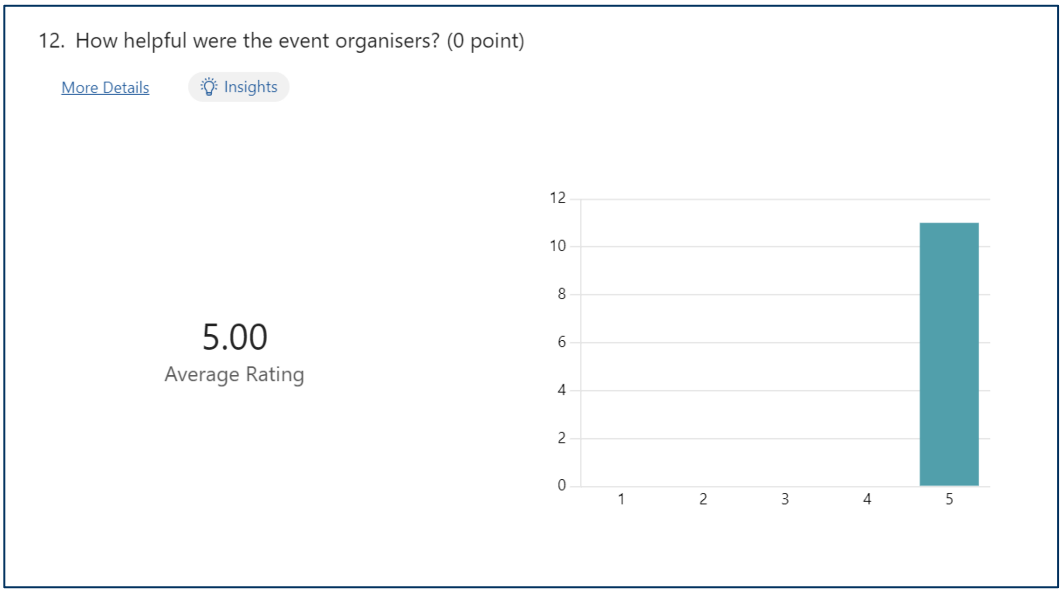
More Details

Insights

5.00

Average Rating

**Figure 6: Time invested to the event participation assessment**


12. How helpful were the event organisers? (0 point)

More Details

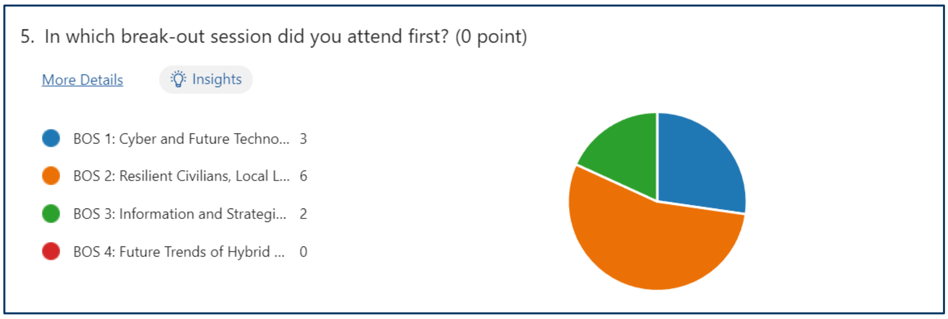
Insights

5.00

Average Rating

**Figure 7: Perception of the helpfulness from the organisers**

Regarding the attendance of the different break-out sessions, the majority of the participants attended physically the BS #2 (Resilient Civilians, Local Level and National Administration):


5. In which break-out session did you attend first? (0 point)

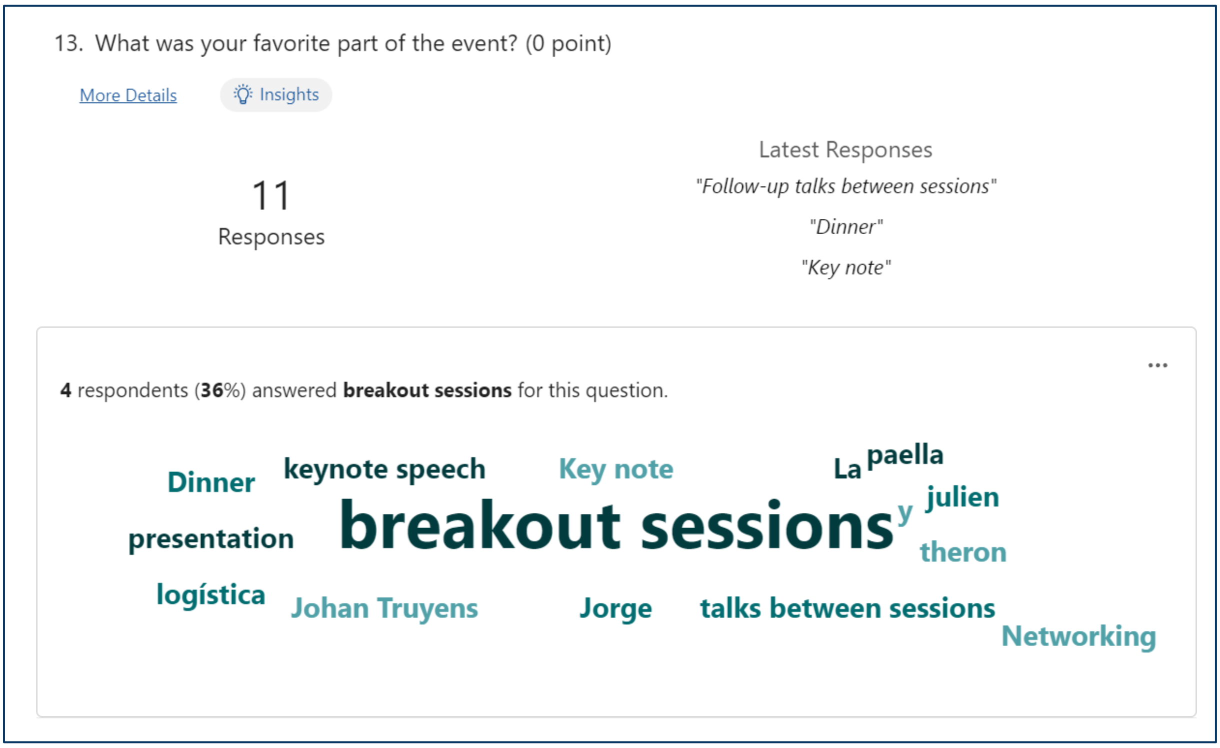
More Details

Insights

| | |
|---|---|
| ● BOS 1: Cyber and Future Techno... | 3 |
| ● BOS 2: Resilient Civilians, Local L... | 6 |
| ● BOS 3: Information and Strategi... | 2 |
| ● BOS 4: Future Trends of Hybrid ... | 0 |

**Figure 8: Break-out sessions participants' distribution**

The favourite part of the FTW were the break-out sessions:



13. What was your favorite part of the event? (0 point)

11
Responses

Latest Responses

*"Follow-up talks between sessions"*

*"Dinner"*

*"Key note"*

**4** respondents (**36**%) answered **breakout sessions** for this question.

Figure 9: Cloud of responses - Favourite part of the event

# 6. CONCLUSIONS AND FUTURE WORK

The 4th Future Trends Workshop proved to be a remarkable event. It facilitated valuable connections between European practitioners, industry, SMEs, and academics, all working together to identify crucial future trends and potential solutions for combating hybrid threats. The speeches and round table discussion served as a springboard, emphasizing the importance of foresight (anticipating future developments) in effectively tackling these threats.

The workshop wasn't just about information sharing; it fostered interaction and mutual learning through engaging small group sessions; the break-out sessions were well rated and the topics discussed there created a great impact in the audience, as shown in the forms received. Feedback overwhelmingly confirmed the event's value, with participants particularly appreciating the organisation of the event.

Identifying trends serves a critical purpose beyond simple observation. By understanding these trends, the project gains a powerful tool to assess the long-term relevance of its outcomes, recommendations, and innovations. These trends can be actively incorporated into future EU-HYBNET activities:

- **Task 2.1: Needs and Gaps Analysis:** They can be used as frameworks to identify additional categories of gaps.
- **Task 2.2: Research for Capacity and Knowledge Increase:** Research articles can explore the validity and implications of these trends.
- **Task 3.4: Future Workshops:** Upcoming workshops can delve deeper into these trends and potential future innovations.
- **Task 3.1: Target Areas for Improvement and Innovations:** Recommendations for innovations can consider the identified trends.

The real power lies in the fact that these trends and innovations are not isolated; they cut across all four core themes of the project. This holistic approach bridges the gap between practitioners' needs and future innovations, with a focus on understanding threats and vulnerabilities. The project welcomes both technical and non-technical (human science based) solutions to combat these evolving hybrid threats.

# ANNEX I. GLOSSARY AND ACRONYMS

Table 3: Glossary and Acronyms

| Term | Definition / Description[TH1] [U2] |
|---|---|
| ANIMV/MVNIA | “Mihai Viteazul” National Intelligence Academy |
| AW | Annual Workshop |
| EOS | European Organization for Security |
| EU-HYBNET | Pan-European Network to Counter Hybrid Threats |
| LAUREA | LAUREA University of Applied Sciences |
| EU-ISS | EU Institute for Security Studies |
| NIS1 | Directive (EU) 2016/1148 |
| NIS2 | Directive (EU) 2022/2555 |
| NGO | Non-governmental organization |
| FIMI | Foreign Information Manipulation Interference |
| EEAS | Euroepan Union External Action |
| CTI | Open Cyber Threat Intelligence Platform |
| EAB | External Advisory Board |
| SMEs | Small and medium-sized enterprises |
| SATWAYS | State of art Incident Management & Computer Aided Dispatch |
| KEMEA | Centre for Security Studies |
| TNO | Netherlands Organisation for Applied Scientific Research |

| | |
|---|---|
| **UiT** | The Arctic University of Norway |
| **L3CE** | Lithuanian Cybercrime Center of Excellence for Training, Research and Education |
| **URJC** | University King Juan Carlos University |
| **WP** | Work Package |
| **OB** | Objective |
| **KPI** | Key performance indicators |
| **UCSC** | Catholic University of the Sacred Heart of Rome |
| **CISE** | Common Information Sharing Environment |
| **EMSA** | European Maritime Safety Agency |
| **AI** | Artificial Intelligence |
| **GDPR** | General Data Protection Regulation |
| **FTW** | Future Trends Workshop |
| **EU** | European Union |
| **PFSA** | Polish Financial Supervision Authority |
| **ICDS** | International Centre for Defence and Security |
| **PLV** | Valencia Local Police |

## ANNEX II: LIST OF PARTICIPANTS,ORGANISATIONS AND COUNTRIES

Table 4: List of participants, organisations and countries

| Nr. | Organisation | Country | Type of Organisation |
|---|---|---|---|
| 1. | ANATASE | France | Industry - SME |
| 2. | ABW | Poland | Practitioner |
| 3. | Belgian General Intelligence and Security Service, Belgian Armed Forces (BEL DOD) | Belgium | Public Sector |
| 4. | CEA | France | Research/Academia |
| 5. | City of Vilnius | Lithuania | Public sector |
| 6. | City of Espoo | Finland | Public sector |
| 7. | Correcta Digital, SL | Spain | Industry - SME |
| 8. | CSIRT-CV, IT Security Center (Valencian Regional Government) | Spain | Public Sector |
| 9. | Cyberecocul Global Services | Cyprus | Industry/SME |
| 10. | DSB - Norwegian Directorate for Civil Protection | Norway | Public Sector |
| 11. | District Prosecution Office | Albania | Other (Law enforcement government institution) |
| 12. | Engineering Ingegneria Informatica S.p.A. | Italy | Industry/SME |
| 13. | European Commission, Joint Research Centre | EU | Research/Academia |
| 14. | European External Action Service (EEAS) | EU | Public Sector |
| 15. | European Organization for Security - EOS | Belgium | Industry - SME |
| 16. | European Parliament | EU | Public Sector |
| 17. | Europol Innovation Lab | EU | Public Sector |

| | | | |
|---|---|---|---|
| 18. | Finnish Ministry of Interior | Finland | Public Sector |
| 19. | GLOBSEC | Slovakia | Civil Society |
| 20. | Hellenic Foundation for European and Foreign Policy (ELIAMEP) | Greece | Research/Academia |
| 21. | Hybrid CoE | Finland | Other (An international, autonomous network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats) |
| 22. | International Security Agency | Poland | Public sector |
| 23. | International Centre for Defence and Security - ICDS | Estonia | Research/Academia |
| 24. | L3CE | Lithuania | Research/Academia |
| 25. | LAUREA University of Applied Sciences | Finland | Academic/RTO |
| 26. | MALDITA | Spain | Civil Society/ NGO |
| 27. | "Mihai Viteazul" National Intelligence Academy - MVNIA | Romania | Research/Academia |
| 28. | Ministry of Defense | Spain | Public Sector |
| 29. | Ministry of Ecological Transition in France | France | Public Sector |
| 30. | Ministry of the Interior | Spain | Public Sector |
| 31. | Ministry of the Interior | France | Public Sector |
| 32. | Polish Financial Supervision Authority | Poland | Public Sector |
| 33. | Prosegur Research | Spain | Industry (International) |
| 34. | Satways Ltd | Greece | Industry - SME |
| 35. | Spanish National Research Council (CSIC) | Spain | Public sector |
| 36. | TNO- Netherlands Organisation for Applied Scientific Research | Netherland | Academic/RTO |

| | | | |
|---|---|---|---|
| 37. | University of Georgia | Georgia | Research/Academia |
| 38. | Universidad CEU Cardenal Herrera | Spain | Research/Academia |
| 39. | Universidad Internacional de Valencia (VIU) | Spain | Research/Academia |
| 40. | Universidad Isabel 1 | Spain | Research/Academia |
| 41. | Università Cattolica del Sacro Cuore - UCSC | Italy | Research/Academia |
| 42. | University of the Bundeswehr Munich | Germany | Research/Academia |
| 43. | Valencia Local Police (Valencia City Council) | Spain | Public Sector (LEA) |
| 44. | VOST Europe | EU | Civil Society |
| 45. | FRONTEX | EU | Public Sector |

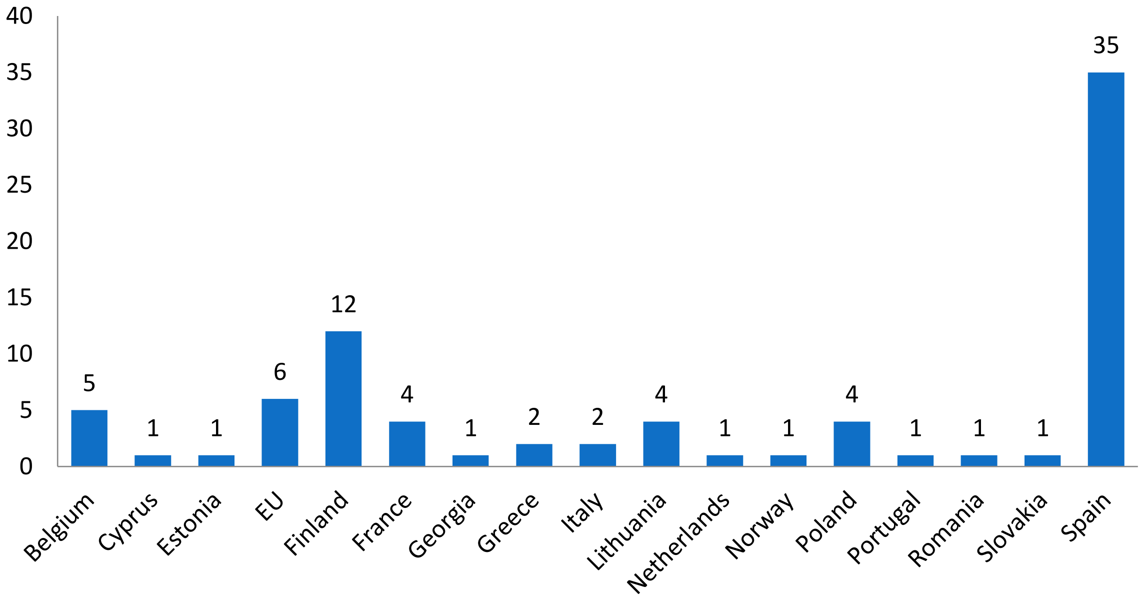


Figure 10: Distribution per countries

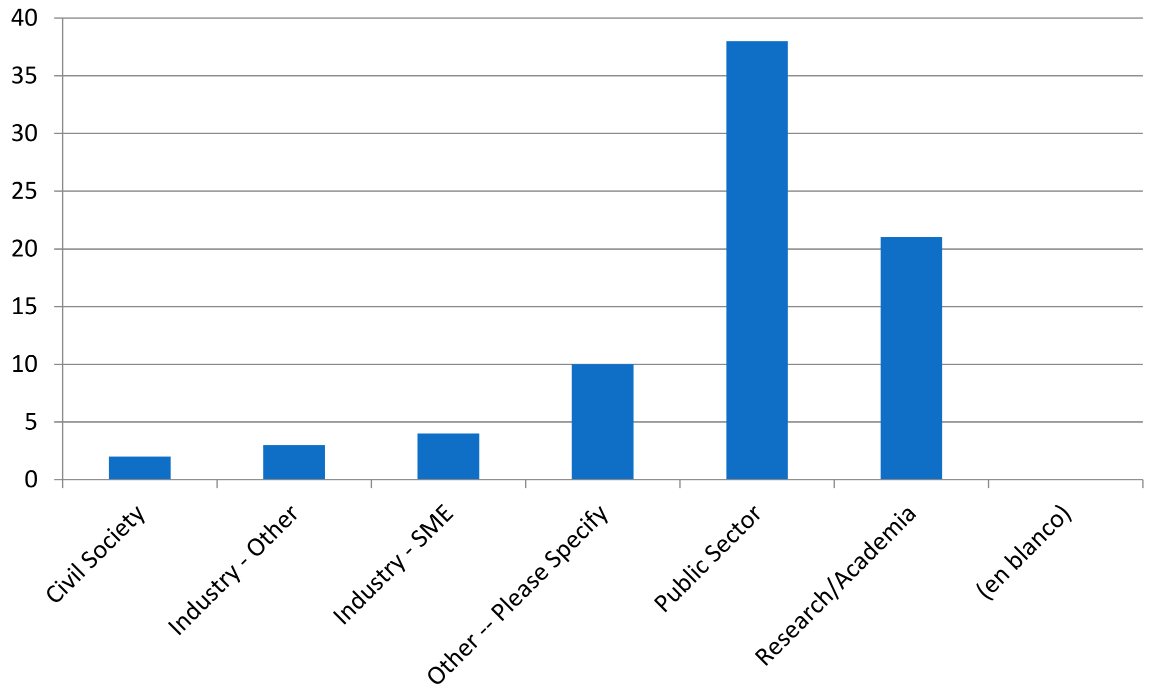


**Figure 11: Distribution of number of participant organizations per type of organization**

**Table 5: Distribution of number of participant organisations per type of organisation and country**

| Country | Civil Society/ NGO | Industry – SME and other | Public Sector | Resarch/Academia | Other | Grand Total |
|---|---|---|---|---|---|---|
| Belgium | | 4 | 1 | | | 5 |
| Cyprus | | 1 | | | | 1 |
| Estonia | | | | 1 | | 1 |
| Finland | | | 3 | 6 | 3 | 12 |
| France | | | 2 | 1 | | 3 |
| Georgia | | | | 1 | | 1 |
| Greece | | | | 1 | 1 | 2 |
| Italy | | 1 | | 1 | | 2 |
| Lithuania | | | | 1 | 3 | 4 |
| Netherlands | | | | 1 | | 1 |
| Norway | | | 1 | | | 1 |
| Poland | | | 4 | | | 4 |
| Portugal | | | | | 1 | 1 |
| Romania | | | 1 | | | 1 |
| Slovakia | 1 | | | | | 1 |
| Spain | 1 | 1 | 29 | 7 | 2 | 40 |
| EU | | | 4 | 1 | | 5 |
| **Total** | **2** | **7** | **38** | **21** | **10** | **85** |

## ANNEX III: WORKSHOP AGENDA

| Time EEST | Topic | Speaker |
|---|---|---|
| 09.00-09.30 | Registration | |
| | **Plenary session** | |
| 09.30-09.45 | Welcome & Practical Information | Mr Jesús Carbonell Aguilar, City Councillor, representative of the Valencia Local Police<br>Mr José Vicente Herrera Arrando, Chief Constable of the Valencia Local Police |
| 09.45-10.00 | "Models for Conflict Analysis & Some Critical Remarks on Dealing with Hybrid Threats" | Mr. Johan Truyens, Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces |
| 10:00-10:30 | Audience Q&A | ***Moderator:*** *Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police* |
| 10:30-10:45 | Coffee Break | |
| 10:45 – 12:15 | Border Management to Counter Future Hybrid Threats | ***Chair:*** *Isto Mattila, EU-HYBNET Innovation Manager*<br>*Panel speakers:*<br>• *Dr. Souzanna Sofou, Satways*<br>• *Dr. Jarmo Puustinen, Finnish MoI*<br>• *Europol Innovation Lab Representative* |
| 12:15 – 13:15 | Lunch Break | |
| | **Parallel Breakout Sessions** | |
| 13:15-14:15 | **Breakout Session #1:** Cyber & Future Technologies | Evaldas Bružė, Analyst and Consultant in Commercial Development at L3CE. |

| | | |
|---|---|---|
| | **Breakout Session #2:** Resilient Civilians, Local Level and National Administration | Dr. Julien Theron, Researcher in Hybrid Threats at the JRC |
| 14:15-14:30 | Coffee Break | |
| 14:30-15:30 | **Breakout Session #3: Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats**<br>Core Theme: Information & Strategic Communication | Rubén Arcos Martín (URJC) and Irena Chiru (MVNIA) |
| | **Breakout Session #4: Securing the EU's borders to 2040 – Thinking about the security landscape**<br>Core Theme: Future Trends of Hybrid Threats | Maxime Lebrun, Deputy Director R&A at The European Centre of Excellence for Countering Hybrid Threats<br>Hanne Dumur-Laanila, Analyst at the The European Centre of Excellence for Countering Hybrid Threats |
| 15:30-15:45 | Conclusions of the BOS & Audience Q&A | |
| 15:45 – 16:00 | **"FRONTEX's View on the Future of Hybrid Threats in Relation to Border Management"** | Mr. Dinesh Rempling, Head of Capability Programming Office at FRONTEX |
| 16:00 – 16:10 | Closing remarks & Practical Information for Annual Workshop | Mr. Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, Valencia Local Police |
| 16:10 – 17:10 | EU-HYBNET Societal Impacts Workshop | Tuomas Tammilehto, EU-HYBNET Ethics Manager |

# Speaker Bios

## Dinesh Rempling

Heading the Capability Programming Office, Mr Rempling has since joining Frontex in Warsaw, in 2017, has been integral to setting the strategic direction for European Integrated Border Management. He is responsible for the capability development planning process for the European Border and Coast Guard, and drives the development of the Standing Corps and the shared Technical Equipment Pool. He is also responsible for the annual force generation process. Mr. Rempling has a Master's of Science in Electrical Engineering, and began his career in 2001 at the Swedish Defence Materiel Administration in Stockholm, working on new-builds and upgrades of ships, submarines and amphibious craft, as well as leading research projects on novel energy supply approaches. Before Frontex Mr. Rempling worked for the European Defence Agency, the Swedish Ministry of Defence on EU defence policy matters and served as the Swedish Defence Research Programme Committee representative. He furthermore managed bilateral armaments and research cooperation with Germany, Poland and Singapore and led campaigns for submarine cooperation.

## Iván L. Martínez Villanueva

Mr Iván L. Martínez is a Project Manager at the Innovation & Project Management Division of PLV: Police officer in Valencia Local Police (Spain) since 2002, he studied Agricultural Engineering and Social Work; currently he is studying network systems administration and cybersecurity. In the professional field, he has worked in community policing, patrolling, police headquarters - police data analysis -, Security councillor consultancy and finally in the management of researching projects in the security field, being currently project manager in the R+D division of this LEA. He has managed PLV's participation in 7 H2020 projects over the last 7 years, currently managing 3 projects linked to Domestic Violence, AI, AR, Smart Cities and Hybrid Threats. As a teacher, he has given several training courses in various municipalities in the Valencian Community, especially in subjects related to school bullying, cyberbullying, cybersecurity, new technologies applied to LEAs, social media, etc. In addition, he is teacher at the Valencian police academy (IVASPE) in the Hate Crimes subject.

## Jesús Carbonell Aguilar

Jesús Carbonell Aguilar is the City Councillor for Citizen's Security, Mobility and Public Spaces since June of 2023, as well as a Law graduate and professional public servant at the Higher Technical Section of the General Administration of the Valencian Government.

He has previously worked in managerial-related positions within different departments of the Regional Government, such as the Education, Tax and Transport agencies from 2009 to 2023, in addition to the Undersecretariat for Education, Culture and Sport in 2014 and 2015.

## Johan Truyens

Johan Truyens is one of the Innovation Officers within the Belgian Departement of Defence.

He has 25 years of experience in intelligence and security.

Between 2007-2010, he was the project officer for information & intelligence capabilities development at the European Defence Agency. Between 2011-2016, he was the first chairman of the NATO OSINT Working Group, and between 2019-2021 he was head of third countries analysis, and divisional capability development coordinator for OSINT & an end-to-end intelligence software suite at EU Frontex.

He set up 2 brand new and unique courses at the University of Antwerp (Belgium): one on “Intelligence” (2012-2019), and another on “Insurgencies & Revolutions” (2017-2019).

## Jorge Gomes

Jorge Gomes is the European Operations Coordinator for VOST Europe, the federation of Virtual Operations Support Teams in Europe, with presence in Portugal, Spain, France, Germany, Slovakia and Greece.

Jorge is also the Chair of the Crisis Response Subgroup of the Permanent Task Force of the Code of Practice on Disinformation, an initiave of the European Commission to tackle disinformation at European level. VOST Europe is a member of the board of the EEAS's initiave FIMI ISAC

## José L. Diego

José L. Diego is Head of the Innovation and Project Management Division of Valencia Local Police and an expert-evaluator for the European Commission within different initiatives:

* Horizon Europe – Security

* EUROPOL Platform for experts

* DG JUSTICE Research Programmes

* DG HOME Research Programmes

* Radicalisation Awareness Network

He began his career as a consultant at Deloitte, and nowadays is a Police Inspector, Head of Innovation & Project Management in the Valencia Local Police, as well as International Lecturer, OSCE Hate crimes trainer & Liaison officer and also Professor for a Master on Human Resources, for two Masters in Criminology and for the Chiefs´ Police Academy as well. He has managed +30 EU projects (including 15 Horizon-Security projects) in matters like R&D, domestic violence, police mediation and training, community policing, forensics, youth offending, crime fighting, road traffic, police management, diversity, emergencies, environmental police, cybercrime, Police ICTs, hybrid threats, AI, AR, smart cities & security, etc. He holds Degrees in Law and in Criminology and a Master in Human Resources Management as well.

## Souzanna Sofou

Dr. Souzanna Sofou, Senior Research and Innovation Manager, is a Dipl. Mining and Metallurgical Engineer and a holder of an MBA in Engineering –Economic Systems. With respect to basic research, her Doctoral Thesis and most of her published research work fall in the fields of computational rheology, rheometry and polymer processing. She has worked in applied research FP7 & Horizon 2020 projects in various fields, including security, new product development, metallurgy, polymer processing, RET modelling, software development and value management. She also has background and experience in Intellectual Property, as she has received relevant training and has worked in this field as a Product Design Engineer for a multinational company. Dr. Sofou has served as the innovation, exploitation and dissemination manager in 3 H2020 projects (PROCETS, z-fact0r, OACTIVE) and as the Innovation Manager in InDeal H2020 project. For the last years, she has been working in security H2020 projects: as the dissemination & communication manager for the ANDROMEDA project, as the innovation manager for the INGENIOUS & the STRATEGY projects, leading the exploitation of the InfraStress project and the IP Management of the EFFECTOR project. She was also actively involved in the SATIE project and serves as the EU-HYBNET WP3 Leader: Surveys to Technology, Research and Innovations. Dr. Sofou is responsible for the Innovation Management of SATWAYS products.

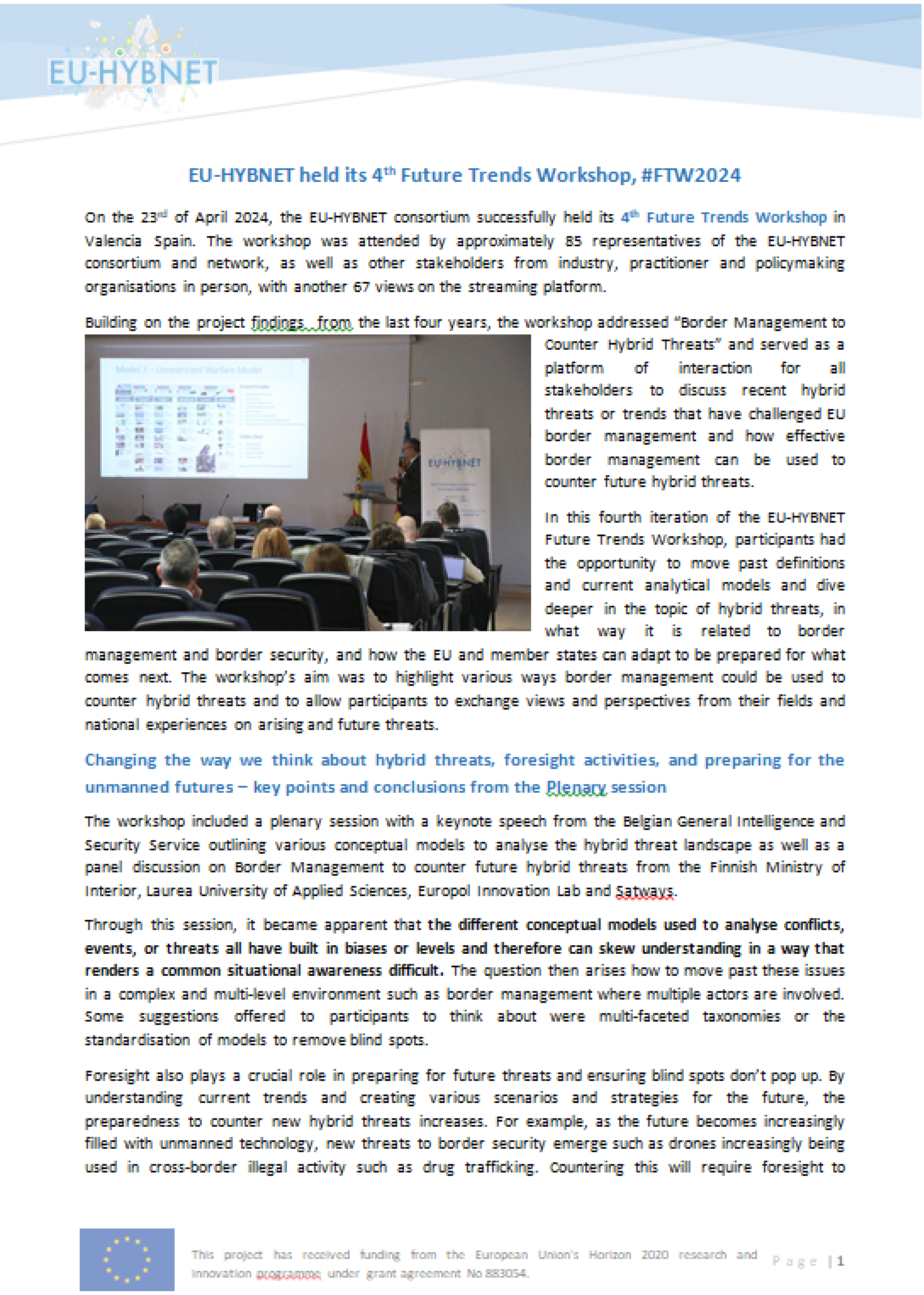
## José Vicente Herrera Arrando

Mr. José Vicente Herrera Arrando is Chief Constable of the Valencia Local Police, since March 2015.Previously he was head of Security in the Consorcio Valencia 2007 (from June 2004 until July 2012); in charge of the organisation of the 32nd and 33rd Edition of America´s Cup. Other relevant positions: Executive Counsellor to the Spanish General Direction of Police during the Spanish

Presidency of the European Union; Provincial Delegate of Spanish Government in Valencia and Director of the Cabinet of the General Director -National Police.

Mr. Herrera holds a Bachelor Degree in Law; a Post Degree in Management (IESE-University of Navarra), a specialization Post Degree in Government and Public Administration and a Master Degree in Public Administration (Complutense University).

# ANNEX IV: PRESS RELEASE



EU-HYBNET

## EU-HYBNET held its 4th Future Trends Workshop, #FTW2024

On the 23rd of April 2024, the EU-HYBNET consortium successfully held its 4th Future Trends Workshop in Valencia Spain. The workshop was attended by approximately 85 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations in person, with another 67 views on the streaming platform.

Building on the project findings from the last four years, the workshop addressed "Border Management to Counter Hybrid Threats" and served as a platform of interaction for all stakeholders to discuss recent hybrid threats or trends that have challenged EU border management and how effective border management can be used to counter future hybrid threats.

In this fourth iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and current analytical models and dive deeper in the topic of hybrid threats, in what way it is related to border management and border security, and how the EU and member states can adapt to be prepared for what comes next. The workshop's aim was to highlight various ways border management could be used to counter hybrid threats and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

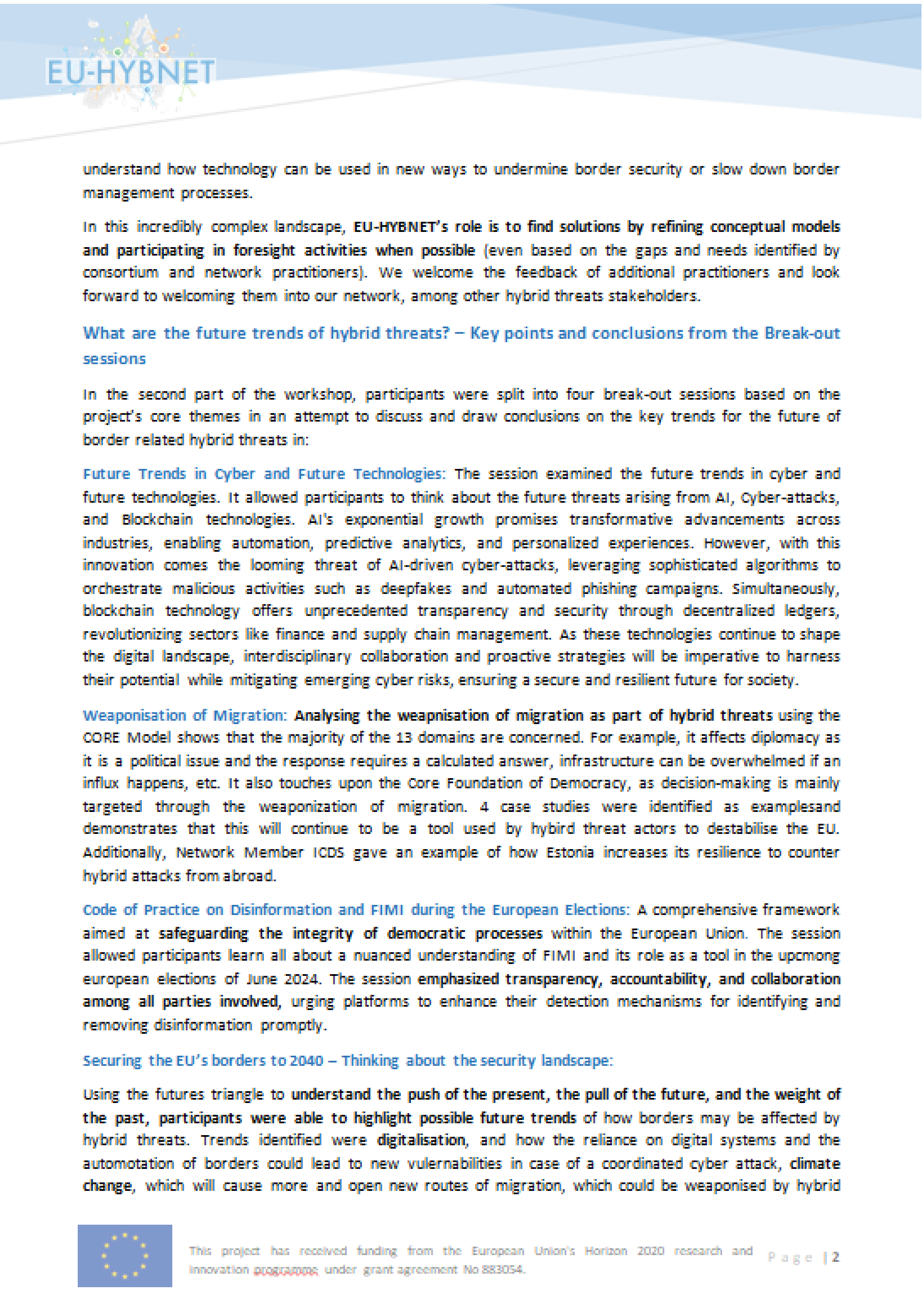
### Changing the way we think about hybrid threats, foresight activities, and preparing for the unmanned futures – key points and conclusions from the Plenary session

The workshop included a plenary session with a keynote speech from the Belgian General Intelligence and Security Service outlining various conceptual models to analyse the hybrid threat landscape as well as a panel discussion on Border Management to counter future hybrid threats from the Finnish Ministry of Interior, Laurea University of Applied Sciences, Europol Innovation Lab and Satways.

Through this session, it became apparent that **the different conceptual models used to analyse conflicts, events, or threats all have built in biases or levels and therefore can skew understanding in a way that renders a common situational awareness difficult.** The question then arises how to move past these issues in a complex and multi-level environment such as border management where multiple actors are involved. Some suggestions offered to participants to think about were multi-faceted taxonomies or the standardisation of models to remove blind spots.

Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don't pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to

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



EU-HYBNET

understand how technology can be used in new ways to undermine border security or slow down border management processes.

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by refining conceptual models and participating in foresight activities when possible** (even based on the gaps and needs identified by consortium and network practitioners). 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 into four 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 border related hybrid threats in:

Future Trends in Cyber and Future Technologies: The session examined the future trends in cyber and future technologies. It allowed participants to think about the future threats arising from AI, Cyber-attacks, and Blockchain technologies. AI's exponential growth promises transformative advancements across industries, enabling automation, predictive analytics, and personalized experiences. However, with this innovation comes the looming threat of AI-driven cyber-attacks, leveraging sophisticated algorithms to orchestrate malicious activities such as deepfakes and automated phishing campaigns. Simultaneously, blockchain technology offers unprecedented transparency and security through decentralized ledgers, revolutionizing sectors like finance and supply chain management. As these technologies continue to shape the digital landscape, interdisciplinary collaboration and proactive strategies will be imperative to harness their potential while mitigating emerging cyber risks, ensuring a secure and resilient future for society.

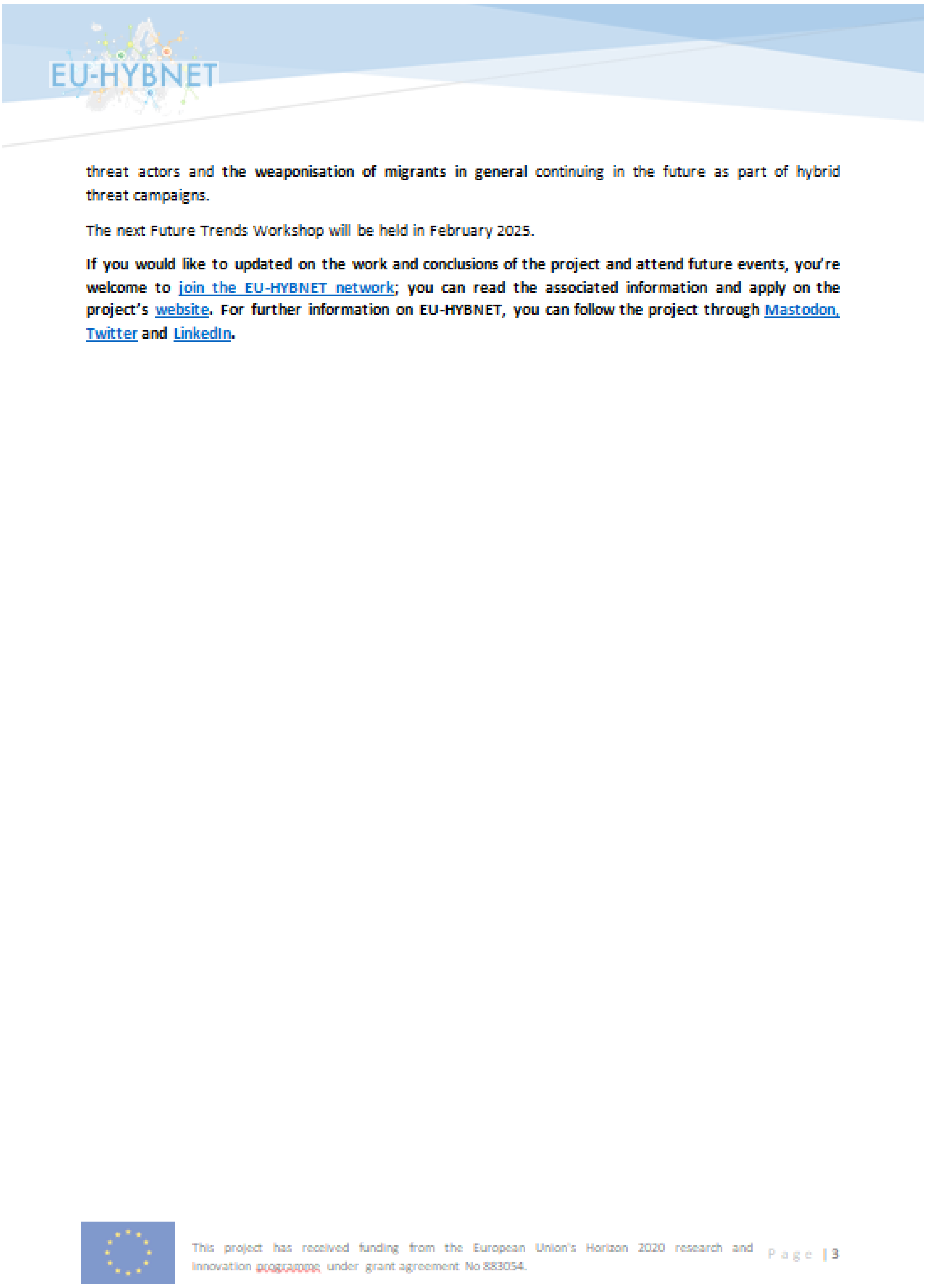
Weaponisation of Migration: **Analysing the weapnisation of migration as part of hybrid threats** using the CORE Model shows that the majority of the 13 domains are concerned. For example, it affects diplomacy as it is a political issue and the response requires a calculated answer, infrastructure can be overwhelmed if an influx happens, etc. It also touches upon the Core Foundation of Democracy, as decision-making is mainly targeted through the weaponization of migration. 4 case studies were identified as examplesand demonstrates that this will continue to be a tool used by hybird threat actors to destabilise the EU. Additionally, Network Member ICDS gave an example of how Estonia increases its resilience to counter hybrid attacks from abroad.

Code of Practice on Disinformation and FIMI during the European Elections: A comprehensive framework aimed at **safeguarding the integrity of democratic processes** within the European Union. The session allowed participants learn all about a nuanced understanding of FIMI and its role as a tool in the upcmong european elections of June 2024. The session **emphasized transparency, accountability, and collaboration among all parties involved,** urging platforms to enhance their detection mechanisms for identifying and removing disinformation promptly.

Securing the EU's borders to 2040 – Thinking about the security landscape:

Using the futures triangle to **understand the push of the present, the pull of the future, and the weight of the past, participants were able to highlight possible future trends** of how borders may be affected by hybrid threats. Trends identified were **digitalisation**, and how the reliance on digital systems and the automotation of borders could lead to new vulernabilities in case of a coordinated cyber attack, **climate change**, which will cause more and open new routes of migration, which could be weaponised by hybrid

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



threat actors and the weaponisation of migrants in general continuing in the future as part of hybrid threat campaigns.

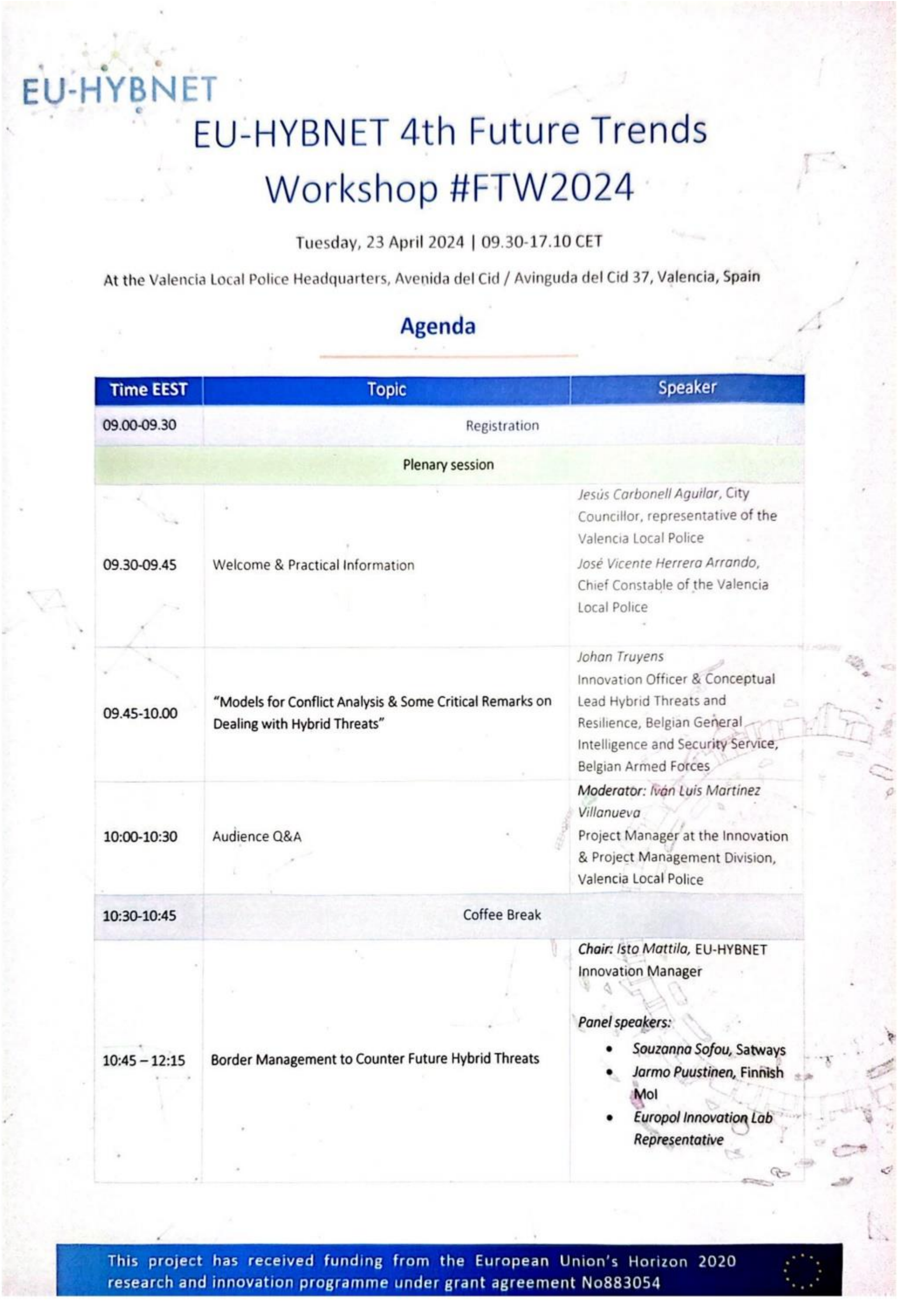
The next Future Trends Workshop will be held in February 2025.

**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 [Mastodon], [Twitter] and [LinkedIn].**

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

Page | 3

# ANNEX V: FUTURE TRENDS WORKSHOP PROMOTIONAL MATERIALS



EU-HYBNET

## EU-HYBNET 4th Future Trends Workshop #FTW2024

Tuesday, 23 April 2024 | 09.30-17.10 CET

At the Valencia Local Police Headquarters, Avenida del Cid / Avinguda del Cid 37, Valencia, Spain

### Agenda

| Time EEST | Topic | Speaker |
|---|---|---|
| 09.00-09.30 | Registration | |
| | Plenary session | |
| 09.30-09.45 | Welcome & Practical Information | *Jesús Carbonell Aguilar*, City Councillor, representative of the Valencia Local Police<br>*José Vicente Herrera Arrando*, Chief Constable of the Valencia Local Police |
| 09.45-10.00 | "Models for Conflict Analysis & Some Critical Remarks on Dealing with Hybrid Threats" | *Johan Truyens*<br>Innovation Officer & Conceptual Lead Hybrid Threats and Resilience, Belgian General Intelligence and Security Service, Belgian Armed Forces |
| 10:00-10:30 | Audience Q&A | *Moderator: Iván Luis Martinez Villanueva*<br>Project Manager at the Innovation & Project Management Division, Valencia Local Police |
| 10:30-10:45 | Coffee Break | |
| 10:45 – 12:15 | Border Management to Counter Future Hybrid Threats | *Chair: Isto Mattila*, EU-HYBNET Innovation Manager<br>*Panel speakers:*<br>• *Souzanna Sofou*, Satways<br>• *Jarmo Puustinen*, Finnish MoI<br>• *Europol Innovation Lab Representative* |

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

Figure 12 EU-HYBNET 4th FTW printed agenda

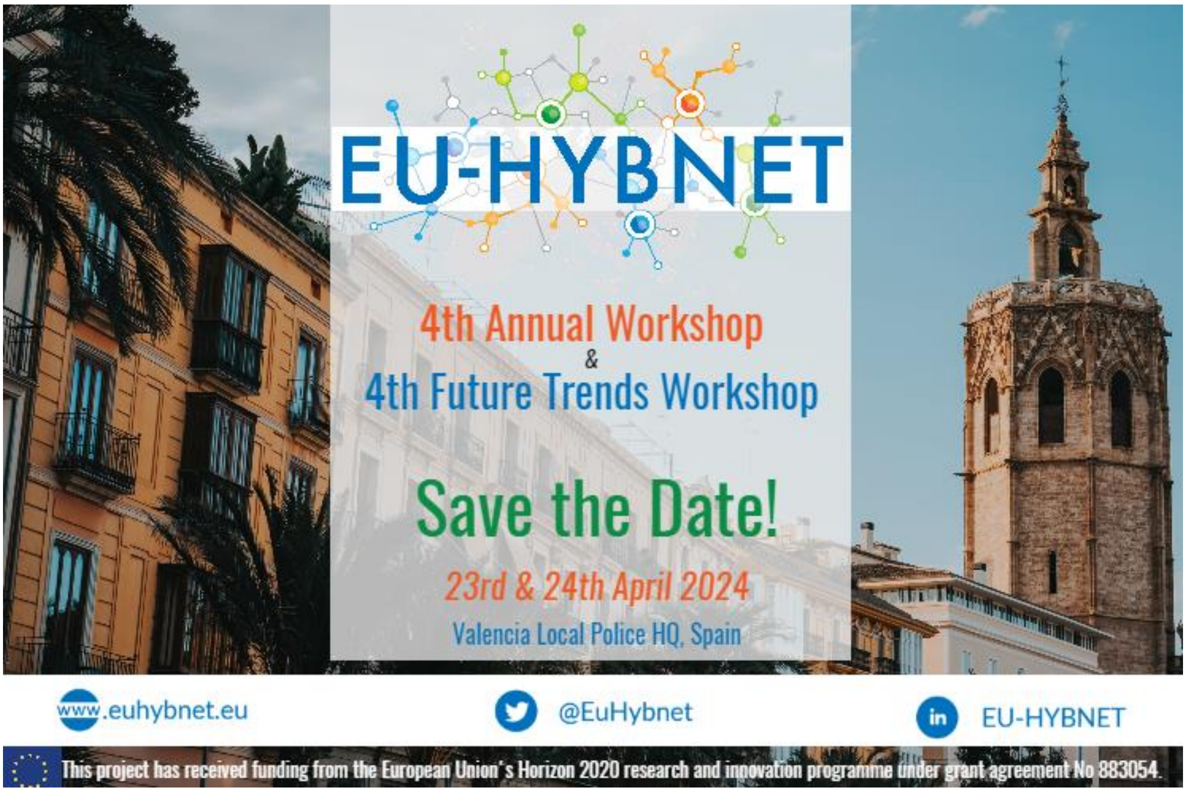
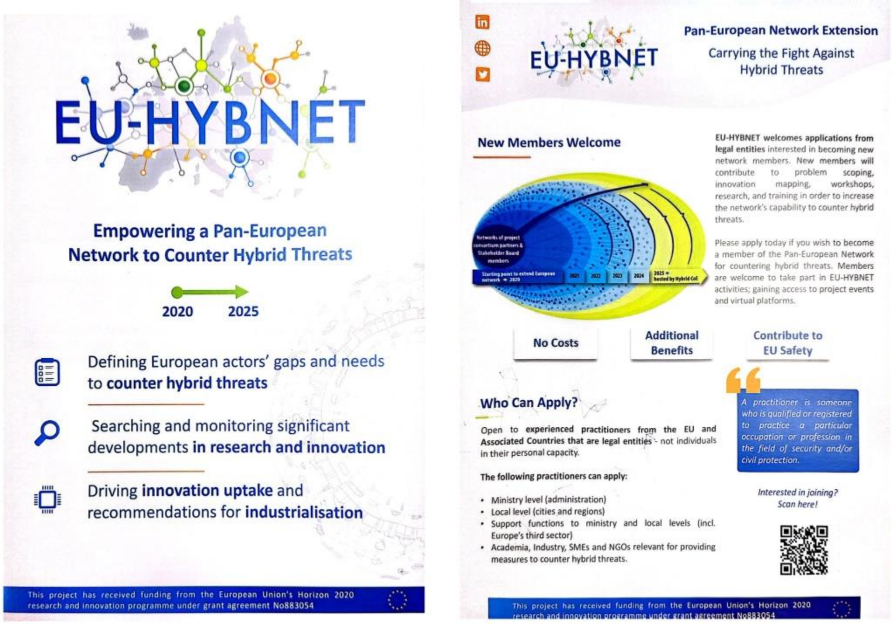

EU-HYBNET
4th Annual Workshop
&
4th Future Trends Workshop
Save the Date!
23rd & 24th April 2024
Valencia Local Police HQ, Spain
www.euhybnet.eu
@EuHybnet
EU-HYBNET
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054.

**Figure 13: 4th FTW Invitation**


Networks of project consortium partners & Stakeholder Board members
Starting point to extend European network → 2020
2021
2022
2023
2024
2025 → hosted by Hybrid CoE

EU-HYBNET

Empowering a Pan-European Network to Counter Hybrid Threats

2020 2025

Defining European actors' gaps and needs to **counter hybrid threats**

Searching and monitoring significant developments **in research and innovation**

Driving **innovation uptake** and recommendations for **industrialisation**

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

EU-HYBNET

Pan-European Network Extension

Carrying the Fight Against Hybrid Threats

New Members Welcome

**EU-HYBNET welcomes applications from legal entities** interested in becoming new network members. New members will contribute to problem scoping, innovation mapping, workshops, research, and training in order to increase the network's capability to counter hybrid threats.

Please apply today if you wish to become a member of the Pan-European Network for countering hybrid threats. Members are welcome to take part in EU-HYBNET activities; gaining access to project events and virtual platforms.

No Costs

Additional Benefits

Contribute to EU Safety

Who Can Apply?

Open to **experienced practitioners from the EU and Associated Countries that are legal entities** - not individuals in their personal capacity.

**The following practitioners can apply:**

- Ministry level (administration)
- Local level (cities and regions)
- Support functions to ministry and local levels (incl. Europe's third sector)
- Academia, Industry, SMEs and NGOs relevant for providing measures to counter hybrid threats.

*A practitioner is someone who is qualified or registered to practice a particular occupation or profession in the field of security and/or civil protection.*

*Interested in joining?*
*Scan here!*

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

**Figure 14: 4th FTW welcome pack - EU-HYBNET's leaflet**

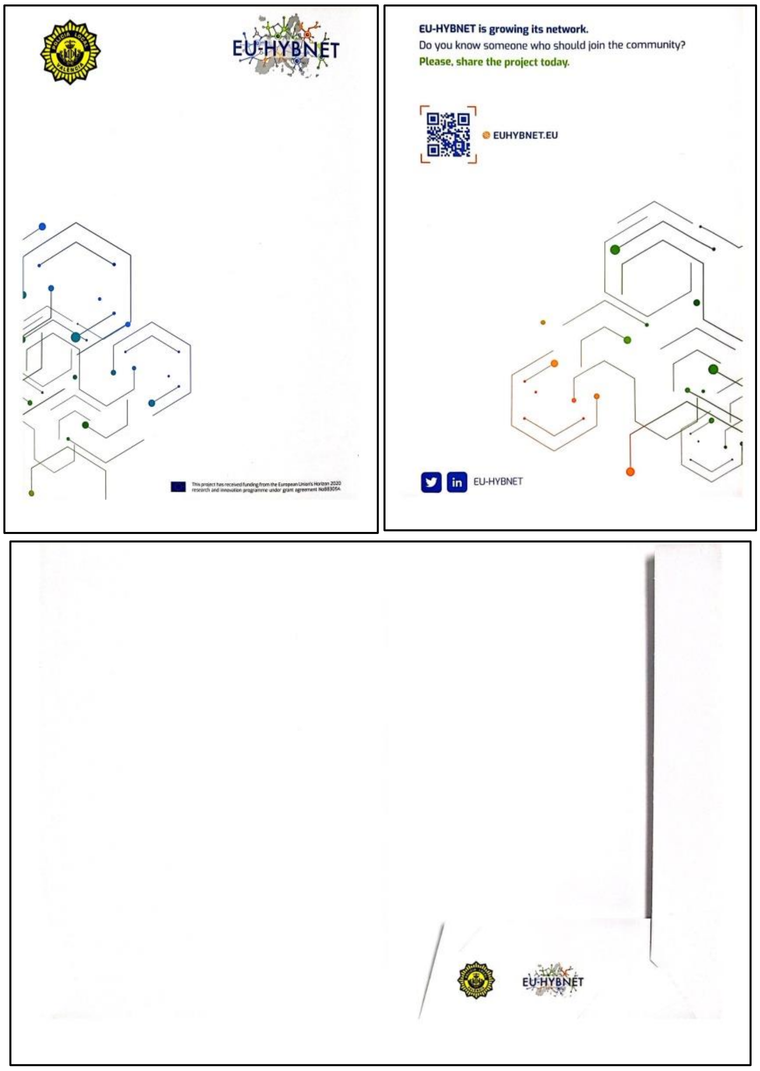

EU-HYBNET
EU-HYBNET is growing its network.
Do you know someone who should join the community?
Please, share the project today.
EUHYBNET.EU
EU-HYBNET

Figure 15: 4th FTW welcome pack - EU-HYBNET's folder

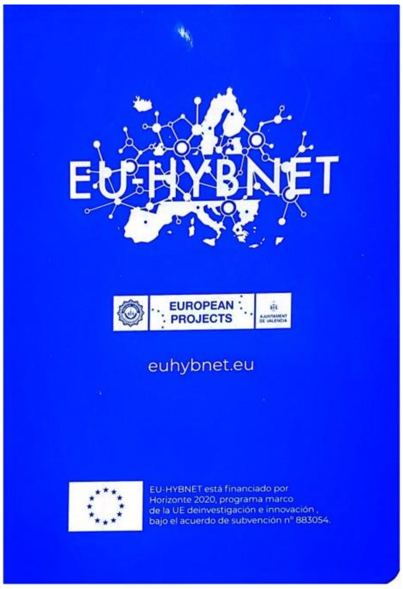

EU-HYBNET
EUROPEAN PROJECTS
euhybnet.eu
EU-HYBNET está financiado por Horizonte 2020, programa marco de la UE deinvestigación e innovación , bajo el acuerdo de subvención nº 883054.

Figure 16: 4th FTW welcome pack - EU-HYBNET's notebook

EU-HYBNET
EU-HYBNET está financiado por
Horizonte 2020, programa marco
de la UE deinvestigación e innovación ,
bajo el acuerdo de subvención nº 883054.
euhybnet.eu

Figure 17: 4th FTW welcome pack - EU-HYBNET's bag

Figure 18: 4th FTW welcome pack - EU-HYBNET's pen

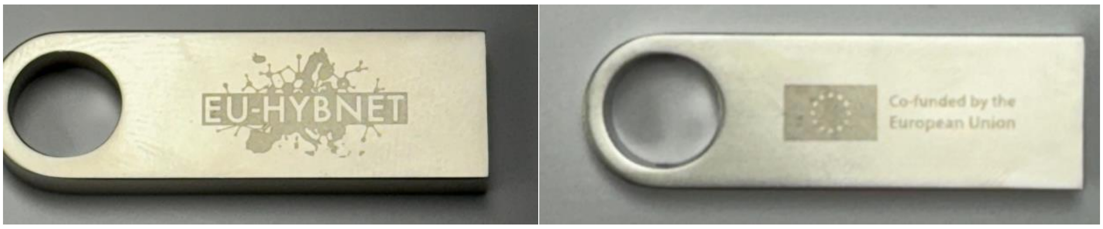


Figure 19: 4th FTW welcome pack - EU-HYBNET's 32Gb pendrive