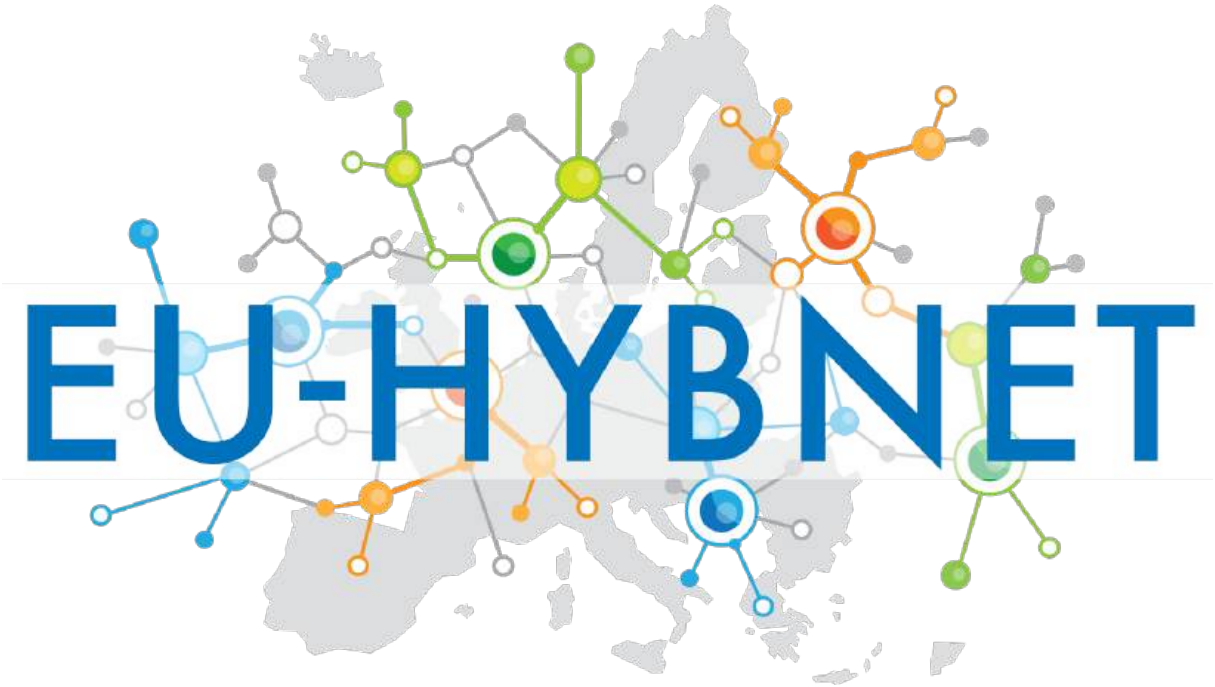



# 5th FUTURE TRENDS WORKSHOP REPORT

DELIVERABLE 3.18

Lead Author: JRC

Contributors: EOS, Laurea, 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

# D3.18 5TH FUTURE TRENDS WORKSHOP REPORT

| | | |
|---|---|---|
| **Deliverable number** | **3.18** | |
| **Version:** | **1.0** | |
| **Delivery date:** | **30/04/2025** | |
| **Dissemination level:** | **Public (PU)** | |
| **Classification level:** | **Public (PU)** | |
| **Status** | **Ready** | |
| **Nature:** | **Report** | |
| **Main authors:** | Julien Theron | JRC |
| **Contributors:** | Vincent Perez, Kristian Reeson | EOS |
| | Tiina Haapanen, Isto Mattila, Petteri Partanen | LAUREA |
| | Ørjan N. Karlsson | DSB |

## DOCUMENT CONTROL

| Version | Date | Authors | Changes |
|---|---|---|---|
| 0.1 | 3/03/2025 | Kristian Reeson (EOS) | First draft, distribution of sections |
| 0.2 | 07/03/2025 | Tiina Haapanen (LAU) | Second draft, text to sections 1 and 5 |
| 0.3 | 15/03/2025 | Julien Theron (JRC) | Text contribution, material delivery |
| 0.4 | 02/04/2025 | Julien Theron (JRC) | Text contribution, material delivery |
| 0.5 | 10/04/2025 | Tiina Haapanen (LAU) | Text editing, material delivery |
| 0.6 | 16/04/2025 | Tiina Haapanen (LAU) | Text editing, material delivery |
| 0.7 | 17/04/2025 | Petteri Partanen (LAU) | Review |
| 0.8 | 23/04/2025 | Ørjan N. Karlsson (DSB) | Review |
| 0.9 | 28/04/2025 | Tiina Haapanen (LAU) | Content editing based on review, finalization of the deliverable |
| 1.0 | 30/04/2025 | Isto Mattila, Tiina Haapanen | Final review and submission of the document to the EC |

## DISCLAIMER

## 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. The fourth workshop was a hybrid event held on April 24th, 2024, in Valencia, Spain.

Most recently, the fifth and final Future Trends Workshop (FTW), arranged by the European Commission Joint Research Centre (EC RC), was a hybrid event conducted on February 13th, 2025, in Brussels, Belgium. This deliverable reports the methods and outcomes of this fifth workshop.

The context in which this fifth FTW intervened was a support for great exchanges, but appeared also particularly complex. Indeed, hybrid threats against Europe progressively grew all along the project to reach an all-time high at its conclusion. The radicalisation and open antagonism from Russia, the less clear but real antagonism from China, the intervention of regional actors such as Iran or North Korea, as well as diverse non-state actors drew a more challenging threat environment. Certain domains appeared to be the objects of more and more attacks, such as information, cyber and infrastructure, while strong attempts in other domains also rose concern, such as intelligence, military/defence, economy, public administration, political or social/societal. If Europe is more way more aware of these evolutions than at the beginning of EU-HYBNET, some recent developments also made hybrid threats a sharper challenge to address, and in particular the continuation and evolution of the large-scale war of aggression against Ukraine and its multi-domain links on the continent or the recent change of leadership in the United States. The evolution of imbricated conflicts in the Middle East, competition in Eastern and Southeastern Asia, or the persistence of global jihadi groups are also objects of concern. While the European Union (EU) and its Member States (EU MS) are now fully aware of the threats and the level they reached, the Future Trends Workshop was the perfect occasion to analyse the current evolution and envision future developments in terms of threat analysis and countering solutions.

As this FTW was the final occurrence of the project, the organisers had several ambitions:

- Keep gathering scholars, industry, practitioners and policymakers

This multiplicity of positions is not only a fundamental part of the project, it also corresponds to the JRC'S view of comprehensive, whole-of-society approach. To better analyse hybrid threats and to better prepare the European societies to hybrid attacks, the different angles of analysis should be considered to fairly distribute presentations.

- Offer a space and slots for transdisciplinary and cross-professional exchanges

It is not enough to bring different professions and different domains together, it is also imperative to provoke their fertile confrontation in dedicated spaces and time, through interactions, Q/A, timely breaks, lunches and dinner, with available material on site (information, posters) to invite the participants to exchange. This is through a fruitful exploitation of these exchanges that can be built a better societal resilience over the civic, services and governance spaces, as described in the CORE model.

- Deliver high quality analysis of future trends

If European security in general and hybrid threats in particular relate to extremely challenging necessity, thinking the future trends of hybrid threats is even harsher. Anticipation, foresight, prospective, prediction, etc.: A lot of methods exist, but the most important is to select the right people and right topics that might foster forward-looking perspectives and sketch, in a non-exhaustive way, the perimeter of plausible futures.

- Offer an in-depth workshop on anticipation

From a European Commission Joint Research Centre point of view, it would have been a fault not to use the anticipation methodology developed by the JRC itself, and in use beyond the Commission. Indeed, the European Strategy and Policy Analysis System (ESPAS) is an inter-institutional EU process promoting foresight and anticipatory governance, established in the early 2010s, to support policy-makers.

- Invite high-level representatives

For this last event, it was necessary to represent EU institutions in all their diversity at high level, and particularly the Commission and the Council. It is also a good platform to represent the original arrival of the concept of Hybrid Threats at the Commission, and to share views from officials over the incoming threats.

Overall, the event also had to be open, balanced, content-based while not too difficult after the Annual Workshop, technical while didactic as it is interdisciplinary. Finally, it had to reflect the whole project, with a certain sense of grand finale.

## 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 events*"), serves as a platform for fostering forward-looking perspectives among participants. Hybrid threats are indeed based on innovation, rather innovation concerns the invention of new tools (technology, social engineering), the combination of domains, the locations, the narratives or the timing. This induces, for countering hybrid threats, to focus not only on the threats that already occurred – although exemplification from case studies can always be instructive – but to work also on the possible future attacks to come. Hybrid threats is therefore particularly oriented toward future trends, the lack of their identification leading necessarily to the impossibility to provide adequate deterrence and resilience against incoming attacks.

This state of facts has numerous consequences. For instance, it means that case studies could and should always be considered as patterns that can be reproduced under other conditions, such as a different country, but also in the same country under particular political stress, or just to follow the general scheme of an attack, but with different or complementary tools. It can also mean that a permanent survey of adversary practices is necessary to understand the ongoing practices and try to identify main trends in future operations. Additionally, investigating on technological edge should also permit to understand the possible use of advanced technology to invent new tools. Sharing good practices is also, eventually, a necessity to provide insights to allies on attacks they were victims of and which might be used in the future.

It also carries many teachings in term of countering strategies. Indeed, deterrence as well as resilience induce to be able to understand the state of the threats, and the multiple development that the security environment is encountering. Multiple perspectives are needed in this purpose, such as scientists (political science, economics, law, media studies, high technologies, etc.) engineers, security and defence practitioners, policymakers, or political decision-makers. Altogether, they can cross their various expert knowledge and analytical approaches, and better understand through cross-fertilisation what adversaries can prepare.

To respond to this need, during the workshop, numerous approaches and topics have displayed to the audience a dense overview of future trends related to hybrid threats, from information to economics through cyber and social/societal domains. In this respect, like the previous edition, the workshop still complied 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 underlines the need to empower European practitioners, industry, SMEs, and academic stakeholders to discern critical innovations and trends. The Final Future Trends Workshop was conceived according to this approach, to identify and respond to future needs of European security at a time of growing challenges.

The fifth iteration of this workshop was organized and hosted by the JRC, 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. This tripartite group worked in close concertation and collaboration during several months in order to provide the optimal event for this

final iteration of the FTW. The most remarkable traits of this cooperation has certainly been the flexibility between the participants, as well as the good will to provide support to the others. Core theme leaders L3CE, UiT, URJC and Hybrid CoE and WP3 leader Satways played a significant role in shaping the event and its Core theme sessions, offering regular valuable insights in the preparation of the event

The 5th Future Trends Workshop took place, for once, after the 5th EU-HYBNET Annual Workshop. The idea was indeed to finish the project with a deep and strong insight into future trends, particularly at a time where hybrid threats rise in intensity and in volume.

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.

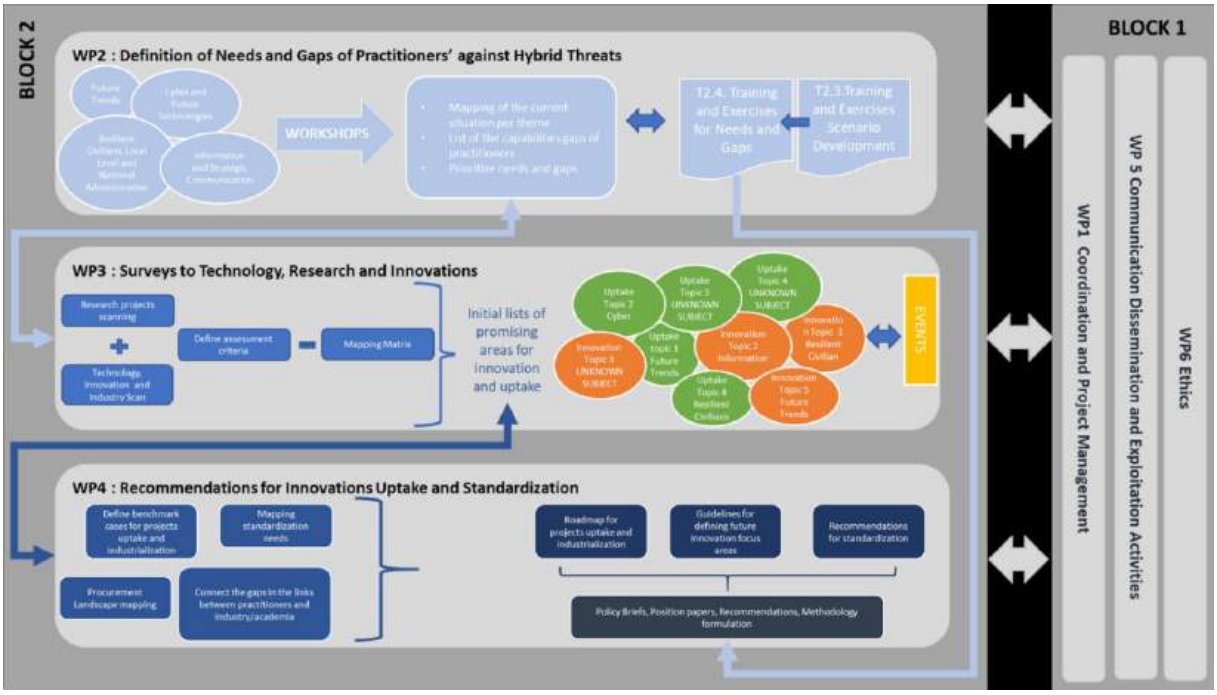



**Figure 1: EU-HYBNET Structure of Work Packages and Main Activities**

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 academic actors can engage in information sharing | Events are organized to attract European actors willing to participate in professional exchanges | At least 3 events every year where 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 |

Several underlying topics related to future trends have been approached during this 5th and final workshop. The question of detection, particularly related to future threats, were at the centre of presentations and debates. Indeed, the multiplicity of domains challenges the different signals that are to be detected. Inversely, such a workshop was the perfect occasion to exchange about the diverse

ways that practitioners from institutions and private sectors analyse the future needs and priorities to put on the agenda for further research and development (participating to OB1, 5, 6 & 7).

In the same vein, the question of determination of multidomain attacks have been explored by several speakers. Indeed, the combination of sometimes very different domains, such as legal, economic, intelligence, social/societal or cyber, is giving a hard time to security practitioners, not only regarding the detection of single-domain attacks, but the determination of the reality and perimeter of hybrid campaigns (participating to OB5 & 6).

Furthermore, an important question rose on how to actively respond to these hybrid campaigns. Several participants invited to do more and more proactively to deter not only by denial, but also by punishment, hybrid campaigns. This induced incidental debates on the need for efficient countering policies to attribute more, collectively and in a clearer way, on the tools needed in a democratic framework to respond, as well as on the need for political engagement and resolve to better secure European democratic societies (participating to OB6).

Another key topic approached during the workshop was anticipation and foresight. Anticipation has been underlined to be a real necessity to better understand future trends. Several exchanges focused, for instance, on how the JRC-Hybrid CoE CORE model could be used in this way: case studies, trainings, tabletop exercises, etc. A lot of discussion also addressed the impact of the rapidly changing global security environment and its consequence on European threat landscape. These discussions underlined an even greater need to anticipate future threats (participating to OB5, 6 & 7).

Having pre-analysed this need, the organisation committee of this final workshop had previously decided to organise a dedicate a specific timeslot to foresight, through a presentation on European Commission's preparedness and resilience: European Strategy and Policy Analysis System's (ESPAS) horizon scanning process, Risks on the Horizon foresight report and Polycrisis exploration workshop toolkit (participating to OB1, 5, 6 & 7).

Finally, to mark the specificity of this final workshop with openness and trans-domain spirit, the organisation committee decided not to organise break-out sessions, but to assemble, on the contrary, the different CORE theme leaders' presentations into the main conference room, to improve mutual understanding, identify convergences and favour future cooperation (participating to OB1, 5, 6 & 7).

# 3. METHOD

This chapter describes the objectives and methodology and structure of the event

## 3.1 OBJECTIVES

The capstone objective of the 5th and Final Future Trends Workshop (FTW) was to offer a framework to EU-HYBNET partners, stakeholders, EAB members, network participants, and interested innovation providers, industry representatives, SMEs, and NGOs, in order to exchange and improve the awareness and skills in countering hybrid threats. At a time of increasing challenged European security environment, this capstone objective appeared more essential than ever to secure and protect European democracies.

Beyond this specific capstone objective, the Final FTW had the ambition to respond to EU-HYBNET's seven project objectives.

OB1: To enrich the existing network countering hybrid threats and ensure long term sustainability

- 1.2 "To strengthen European capabilities in detection, reaction and response in confronting hybrid threats by leveraging collaborative network efforts": The discussions on detection, reaction and response have been central during the event, as displayed above.
- 1.3 "To arrange and host events where practitioners, industry, SME and academic actors can engage in information sharing": the event was not only fulfilling this goal, but its organisation itself was also associating policy, SME and academic actors.
- 1.4 "To achieve sustainability, Hybrid CoE will lead the post-project activities for EUHYBNET with established EU, national /sub-national networks of practitioners": The event has been a framework for participants to engage cooperation in the future, some of them having been initiated during the workshop informal talks.

OB2: To define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats

- 2.1 "To identify needs and gaps in areas of knowledge/performance (research, innovations, training) of practitioners (priority), industry, SMEs and academic actors": Investigating future trends are deeply driven by the identification of needs and gaps, and to the necessary adaptation to cope with them.
- 2.2 "To define innovations that can overcome the identified gaps and needs in certain focus areas in order to enhance practitioners (priority), industry, SME and academic actors capabilities": Certain innovative methods and processes to study various types of hybrid threats have been displayed during the event.
- 2.3 "To gather and define insights from European practitioners, industry, SME and academic actors on future trends": This objective corresponds to the very object of the Future Trends Workshop.

OB3: To monitor developments in research and innovation activities as applied to hybrid threats

- 3.1 “To monitor significant developments in research areas and activities in order to define and recommend solutions for European actors”: The event has proposed, through exposing advanced research developments, such as in CORE themes.
- 3.2 “To monitor significant developments in technology that will lead to recommending solutions for European actors’ gaps and needs”: Although technology was not necessarily at the heart of the even, several presentations and observations gathered interesting outputs related to it, such as the use of AI in detection, or the possibility to counter cyberattacks.

OB4: To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats

- 4.3 “To develop a mapping matrix connecting gaps and needs of European actors to areas that highlight the most promising innovations”: Not dedicated to matrix mapping, the event certainly participated to enhance awareness and information in this regard.
- 4.4 “To facilitate policy dialogues on future European research and innovation focus areas supporting innovation uptake”: Policy dialogues have been at the heart of the event, and particularly during the introductory and concluding remarks by key EU policymakers from the Commission and the Council.

OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network

- 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”: Open forum, the 5th FTW has empowered the community to exchange on these issues.

OB6: To foster capacity building and knowledge exchange on countering hybrid threats

- 6.1 “To arrange dialogue sessions for EU practitioners, industry, SME and academic actors to strengthen capacity and hybrid threat knowledge exchange”: The event was not structured around open breakout discussions, but the organisation committee took care of proposing Q&A sessions and comfortable breaks to favour the exchanges among the participants.
- 6.2 “To increase cooperation between European research actors working on crucial topics related to hybrid threats”: Research has taken a strong place during the event; not only from an academic perspective, but also through institutional research, private research and development, and various synergies between them.
- 6.3 “To enhance knowledge exchange, increase knowledge/capacity of actor-actor interactions, esp. with industry”: Exchanging knowledge – rather related to the geopolitical evolutions, security-related policies, technologies or the landscape of counter-HT actors – has been at the centre of the event.
- 6.4 “To empower European practitioners, industry, SME and academic actors’ capacity to counter hybrid threats by offering relevant trainings and materials”: Trainings have occupied a specific place for this final workshop, mainly through ESPAS session, but also during various exchanges related to good practices sharing, tabletop exercises and other types of simulations.

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

- 7.1 “To share information on EU-HYBNET activities and training possibilities among European stakeholders”: Specific material has been shared by ESPAS representatives and by the JRC related to training possibilities, but also, on the project, by EU-HYBNET project managing team, ensuring connections in this area.
- 7.2 “To empower European practitioners, industry, SME and academic actors to recognise important innovations/trends”: The organisation committee aimed at putting these actors at the centre of the event.
- 7.3 “To establish links with other European Networks and missions in related fields of interest (e.g. Community of Users)”: The networks of participants to the event were openly described and opportunities of inter-network cooperation have been observed during several exchanges.
- 7.4 “To inform EU MS national policymaking bodies and other European actors with EU-HYBNET results”: Several EU MS were represented by staff working on different HT-related domains at the workshop.
- 7.5 “To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically”: Many participants had in mind the necessity to continue to engage with the network even after the end of the project, and several cooperations tracks between them rose from the event.

## 3.2 WORKSHOP STRUCTURE

The event was organised into four parts:

1) Introductory part

Although this Final Future Trends Workshop intervened exceptionally after the Annual Workshop, inducing the presence of a certain number of participants since the day before, some came specifically for this event. It was therefore necessary to welcome properly the ensemble of participants. Furthermore, this final event was also the occasion to propose a very specific opening, officialising this last but important collaborative moment.

This is why Georgios Giannopoulos, at the origin of the introduction of the concept of hybrid threats at the European Commission Joint Research Centre, working alongside with the emerging European Centre of Excellence for Countering Hybrid Threats, and at the beginning of EU-HYBNET, was chosen. He gave indeed a vivid presentation on the history of the concept until this final event of the project. Additionally, the European External Action Service was also associated, as a spearhead of the European Union in the fight against hybrid threats, rather they involve diplomacy, intelligence, or Foreign Information Manipulation and Interference (FIMI).

2) Foresight part

As stated above, the organisation committee wished to propose to the participants a specific part dedicated to foresight to better analyse future trends. The JRC team dedicated to this methodology

accepted to explain how foresight can increase preparedness and disaster resilience by presenting ESPAS Horizon Scanning and Risks on the Horizon.

Members of the EU Policy Lab, they explained that their role is "providing strategic and future-oriented input, developing an anticipatory culture inside the European Commission, continuously experimenting and developing different methods and tools to make foresight practically useful for decision-making processes", which was perfectly in line with the need identified by the organisation committee with regards to hybrid threats.

3) CORE theme part

A both traditional and innovative part was dedicated to CORE themes. It was traditional regarding former FTWs to include CORE theme leaders' presentations of their topics, with underlining the future trends they identified, but also their individual and collective works related to these trends. But it was also innovative, thanks to the four CORE theme leaders, for three reasons:

- The CORE themes "Cyber and Future Technologies" & "Resilient Civilians, Local Level and National Administration" decided, as a prime and led by a synergetic dynamics, to conduct a common presentation to understand how future trends in cyber and future technologies are impacting the society, and how the society is a full—fledged actor of resilience against hybrid threats.
- The leader of CORE theme "Information & Strategic Communication", an experienced scholar, decided to host a policymaking guest, Beatriz Marin Garcia, Data analyst at the European External Action Service, who presented her investigations into countering Foreign Information Manipulation and Interference.
- The CORE theme "Future Trends of Hybrid Threats" proposed to integrate the three other CORE themes advances in order to better and comprehensively understand the future threat landscape.

4) Concluding part

The concluding part presented a challenge, as it was not only the final Future Trends Workshop, but also the last event of the project. The organisation committee decided to choose two speakers which represented two key EU institutions, the Commission and the Council. The crossed vision related to these institutions, animated at high level, offered a unique insight into future trends and concluded perfectly both Final Future Trends Workshop and EU-HYBNET final event.

To mark the importance of this final FTW, important Keynote speeches were delivered by remarkable actors:

- Georgios Giannopoulos, Deputy Director, Directorate E – Societal Resilience and Security Unit, European Commission Joint Research Centre (EC DG JRC)
- Jacob Tamm, Deputy Head of Division, Information Integrity & Countering Foreign Information Manipulation and Interference, European External Action Service (EEAS)
- Nicolas Bessot, Head of Unit, Unit F.2 – Innovation & Security Research, Directorate-General for Migration and Home Affairs (EC DG HOME)
- Tomasz Tokarski, Representative of the Polish presidency of the Council of the European Union

Altogether, they offered to the participants a sharp and top-level insight of the future trends of hybrid threats.

# 4. WORKSHOP AGENDA

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 KEYNOTE SPEACH

- Mr Georgios Giannopoulos, *Deputy Director, EC DG Joint Research Centre*
- Mr Jacob Tamm, *Deputy Head of Division from the European External Action Service*

At the Future Trends Workshop, keynote speeches were delivered by Mr. Georgios Giannopoulos, *Deputy Director of the European Commission's DG Joint Research Centre (JRC)*, and Mr. Jacob Tamm, *Deputy Head of Division at the European External Action Service (EEAS)*. Their insights provided a strategic perspective on the evolving landscape of hybrid threats, the role of emerging technologies, and the necessary policy responses at the EU level.

Mr. Georgios Giannopoulos (EC DG JRC) focused on the importance of foresight and research in addressing hybrid threats. He emphasized that hybrid threats are continuously evolving, with cyber vulnerabilities, AI-driven disinformation, and quantum computing risks posing significant challenges for security frameworks. He underscored the need for robust, science-based risk assessments, technological innovation, and cross-sector collaboration to anticipate and mitigate future hybrid security risks. The role of the JRC in supporting evidence-based policymaking and developing tools for resilience was highlighted as a key asset in the EU's security strategy.

Mr. Jacob Tamm (EEAS) provided a geopolitical and policy-oriented perspective, discussing how hybrid threats are increasingly used as tools of foreign interference. He highlighted state and non-state actors leveraging disinformation, cyberattacks, and economic coercion to destabilize democratic institutions. Stressing the role of strategic communication, intelligence-sharing, and diplomatic coordination, he underscored the EEAS's efforts in countering foreign information manipulation and interference (FIMI). He also addressed the growing complexity of hybrid threats in a multipolar world, advocating for stronger EU-wide and international cooperation to enhance resilience, particularly in cyber defense and strategic infrastructure protection.

Both speakers reinforced the urgent need for foresight-driven policymaking, technological resilience, and a coordinated European response to hybrid threats, setting the tone for discussions throughout the Future Trends Workshop.

## 4.2 PANELS

*How foresight can increase preparedness and disaster resilience – Presentation of the European Strategy and Policy Analysis System's (ESPAS) horizon scanning process and the Risks on the Horizon foresight report with the Polycrisis exploration workshop toolkit.*

The presentation "*ESPAS Horizon Scanning and Risks on the Horizon*", delivered by Tommi Asikainen & Maija Knutti (*European Commission, EU Policy Lab*), highlights the role of foresight and horizon scanning in enhancing preparedness and resilience against emerging risks and crises. The ESPAS Horizon Scanning process systematically monitors weak signals, emerging issues, and megatrends to help policymakers anticipate future disruptions. The Risks on the Horizon project has identified 135 risk indications across 40 risks and 10 risk clusters, covering areas such as geopolitical instability,

climate change, supply chain disruptions, and technological vulnerabilities. A key focus is polycrises, where interconnected crises amplify each other, requiring integrated risk management strategies. The Polycrisis Exploration Workshop introduces a participatory risk assessment tool to help decision-makers navigate complex risks, assess cascading effects, and develop policy interventions. The presentation concludes that embracing uncertainty through proactive foresight, strategic risk monitoring, and cross-sector collaboration is crucial for building Europe's resilience against future hybrid threats.

## 4.3 CORE THEME SESSIONS

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

**Table 2: 5th FTW Core Theme sessions**

| Core Theme Sessions | |
|---|---|
| **Core Theme Session #1:** Future Trends of Hybrid Threats | Maxime Lebrun, *Hybrid CoE* |
| **Core Theme Session #2:** Cyber & Future Technologies & Resilient Civilians, Local Level and National Administration | Evaldas Bruze (*L3CE*) and Gunhild Hoogensen Gjørv (*UiT*) |
| **Core Theme Session #3:** Information & Strategic Communication | Rubén Arcos Martín (*Rey Juan Carlos University*) and Beatriz Marin Garcia (*European External Action Service)* |

### CORE THEME SESSION #1

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

**Title:** Intro session - Future Trends of Hybrid Threats

**Chair:** Maxime Lebrun, *Hybrid CoE*

**Description:** This introductory session will explore the evolving landscape of hybrid threats, focusing on how emerging cyber and future technologies are shaping new vulnerabilities and risks. Maxime Lebrun *(Hybrid CoE*) will lead the discussion, providing an overview of key trends, including the weaponization of artificial intelligence, quantum computing risks, deepfake-driven disinformation, and cyber-enabled influence operations. The session will also highlight strategic foresight methodologies to anticipate future hybrid threat scenarios, emphasizing the need for cross-sector collaboration, technological resilience, and adaptive policy responses. This session will set the stage for deeper discussions throughout the Future Trends Workshop, equipping participants with insights into the next generation of hybrid security challenges and potential mitigation strategies.

### CORE THEME SESSION #2

**Core theme:** Cyber & Future Technologies & Resilient Civilians, Local Level and National Administration

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

**Co-Chairs :** Evaldas Bruze (*L3CE*) and Gunhild Hoogensen Gjørv (*UiT*)

**Description:** This theme will focus on how the interplay between technological advancements and security dynamics increasingly defines the vulnerabilities of democracies, critical infrastructures, and societal resilience, and how recent (as well predicted for near future) application of next generation technologies changes risks through their potential misuse for disinformation, sabotage, and targeted disruption of essential services. Dynamically evolving domains like Generative AI, Cognitive AI, LLMs, quantum computing, edge AI, autonomous systems and neurotechnology are particularly topical, as they represent the cutting edge of innovation and areas where hybrid threats are likely to manifest through weaponization of tech economy, exploitation of digital arena and development of digital cognitive warfare. The workshop will address broader societal impacts, such as the influence of synthetic media on public trust, the fragility of global supply chains, and the rising threats to shared cultural and natural resources. By anticipating the convergence of technological, social, and geopolitical drivers, this FTW session seeks to discuss strategies that can mitigate risks and foster innovation in countering hybrid threats, including threats to democratic processes, economies, cultural and historical heritage, rise of offensive AI and AI defence models, cybersecurity in autonomous systems, weaponization of open-source intelligence, LLMs and GenAI based systems and global digital environments.

Key points:

- Next generation AI
- Global shifts in technological supremacy
- Speed of next generation technologies adoption
- Societal and Policy resilience to new types and scales of hybrid threats
- New era of dual use technologies and solutions
- Increased societal tiredness and apathy

## CORE THEME SESSION #3

**Core theme:** Information & Strategic Communication

**Title:** Trends and emerging issues in disinformation/FIMI: anticipatory analysis and identity-based disinformation/FIMI

**Co-Chairs:** Rubén Arcos Martín (*Rey Juan Carlos University*) and Beatriz Marin Garcia (*European External Action Service)*

**Description:** At the EU-HYBNET Future Trends Workshop (13 February 2025), Beatriz Marin Garcia (EEAS Stratcom Data Team) and Rubén Arcos (University Rey Juan Carlos) presented on identity-based disinformation (IBD) and Foreign Information Manipulation and Interference (FIMI), emphasizing their role as hybrid threats designed to exploit societal vulnerabilities, destabilize democracies, and serve geopolitical agendas. Garcia's presentation focused on IBD/FIMI as a tool to silence marginalized communities, targeting identity-based characteristics such as gender, sexuality, race, ethnicity, and religion. She detailed key manipulation tactics, including inauthentic documents, impersonation of legitimate entities, cyber-enabled disinformation, and coordinated calls to offline action, often leveraging low-frequency but high-impact strategies like gamification and cyberattacks. A case study

on Moldova illustrated how identity-based disinformation is weaponized to polarize societies. The EEAS proposes a standardized methodology for data collection and analysis, an open-source investigation guide, and policy recommendations to counter these threats through expert discussions, communication campaigns, and awareness initiatives.

Mr Rubén Arcos Martín expanded on FIMI as an evolving challenge, stressing the need for a proactive, anticipatory approach rather than relying solely on reactive fact-checking. He introduced a systematic methodology for early disinformation detection, using capability, intention, and vulnerability indicators to identify threats before they escalate. Capability indicators include fake social media accounts, state-funded foreign media, and fringe platforms, while intention indicators highlight public statements, increased diplomatic activities, and cyberattacks. Vulnerability indicators focus on low public awareness, declining trust in democratic institutions, and weak independent media ecosystems. A sample scenario demonstrated how foreign actors could manipulate European legislative debates through coordinated campaigns. Both presentations concluded that anticipatory threat detection, strategic foresight, and early-warning mechanisms are critical to mitigating FIMI threats and strengthening resilience against hybrid disinformation campaigns, underscoring the urgent need for coordinated international efforts to detect, analyze, and counteract these evolving threats.

# 5. WORKSHOP PARTICIPANTS AND FEEDBACK

The event planning began in October 2024; the partners involved in the arrangements were LAUREA, EOS, SATWAYS, HYBRID CoE and JRC. 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 December 2025 and finalised in January 2025.

## 5.1 PARTICIPANTS

Participation was open to anyone, and there were no requirements for previous experience in future-oriented thinking. The amount of people registering to join the Future Trends Workshop in person was 82, while the online registration had 27 people. The event attracted around 53 participants in person with around 21 participants online.

The organising team would also like to note that the week of the events, it was announced that a strike would occur on the day of the Future Trends Workshop, disrupting travel plans[1] as many participants were planning to travel back to their country of origin the night of February the 13th. This caused a number of participants to drop down, compared to other events, as well as a few speakers change their in-person attendance to online. Despite this setback, the organising team continued to move forward with the event, and assisted the participants with their travel plans as best as possible.

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 53 participants, 7 provided feedback.

[1] https://www.reuters.com/world/europe/anti-government-protest-halts-air-traffic-belgium-2025-02-13/

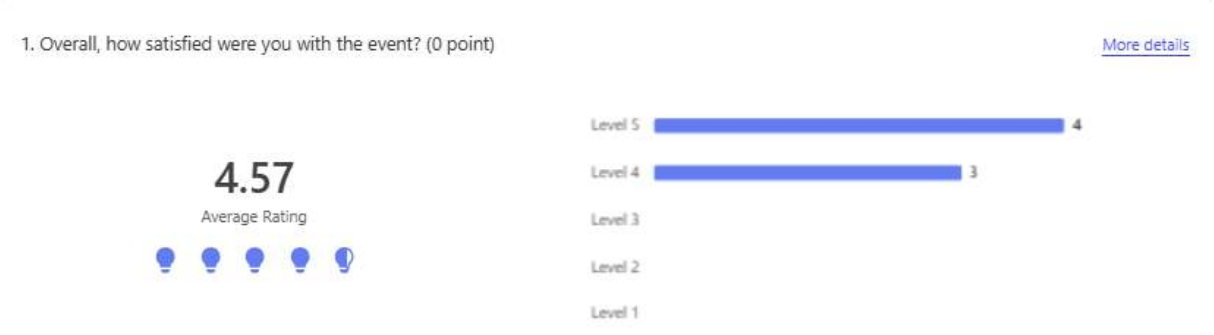



**Figure 2: Participant satisfaction with the FTW event**

Participants were overall satisfied with the event (4.57 average rating) and its content (4.71 average rating), while the keynotes and the core theme sessions also received high ratings (4.86 and 4.57, respectively).

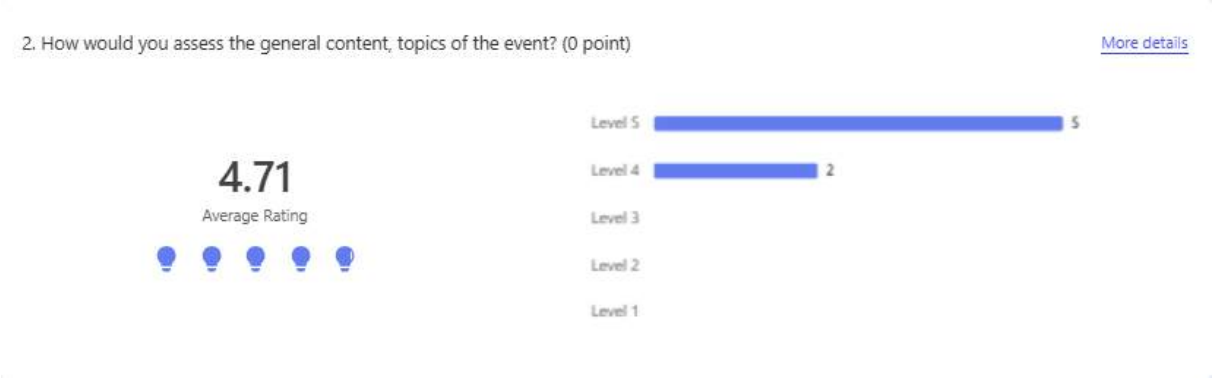



**Figure 3: General content assessment**

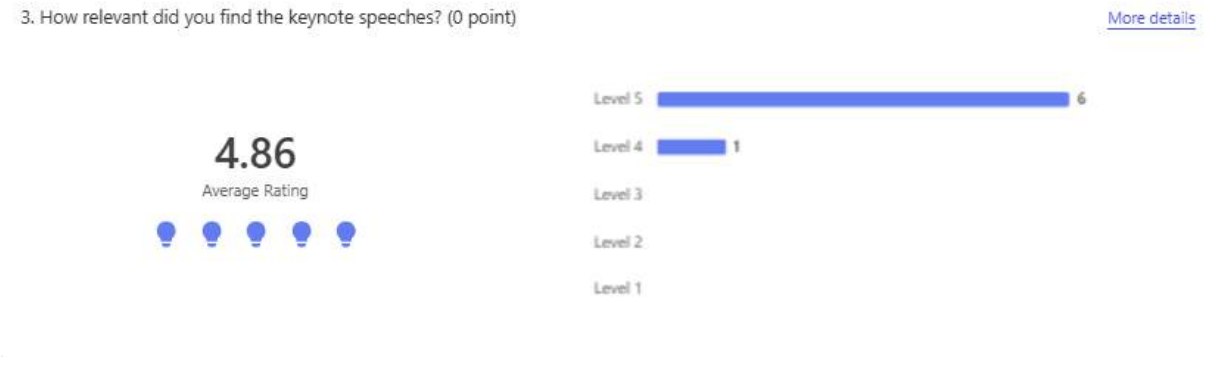



**Figure 4: Keynote speeches assessment**

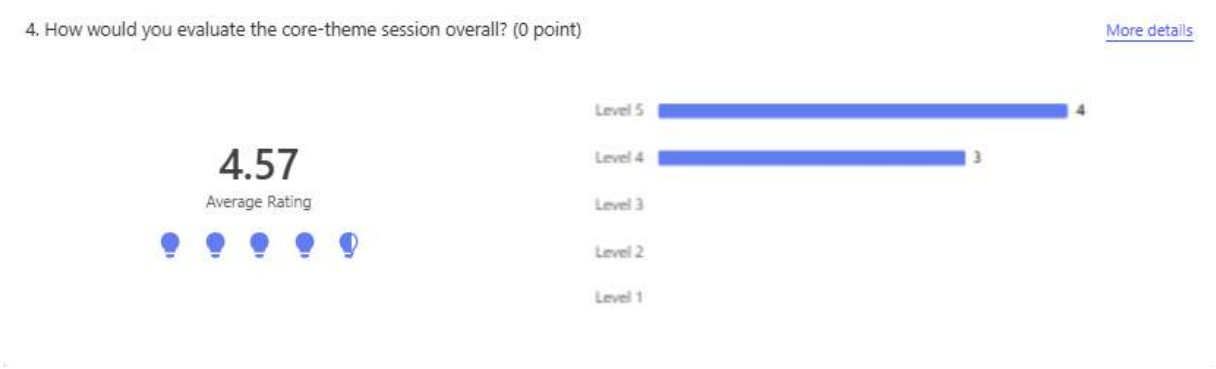



**Figure 4: Core theme sessions assessment**

Participants were also satisfied with the event arrangements (4,86 average rating), and time dedicated to it (4.47 average rating); and the event organisers were found very helpful (4.83 avarage rating).


**Figure 5: Event arrangements assessment**


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

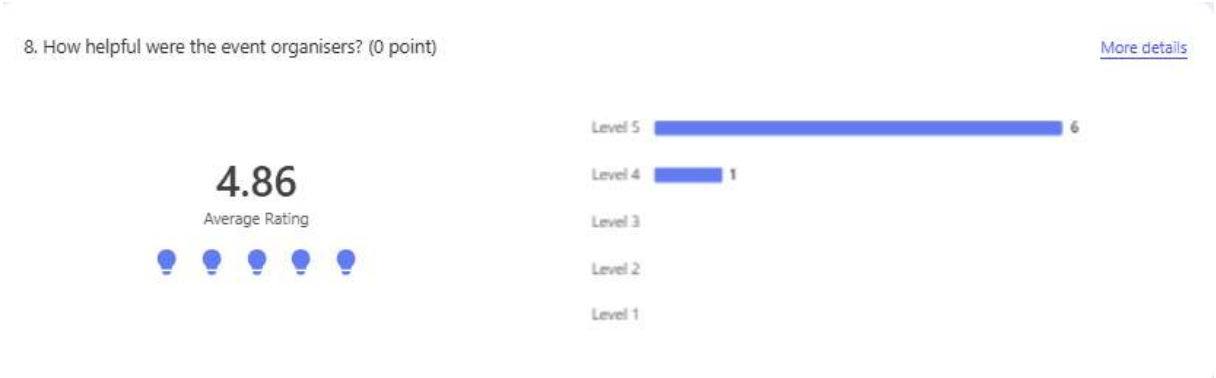



**Figure 7: Perception of the helpfulness from the organisers**

The favourite part of the FTW are presented in the figure below.

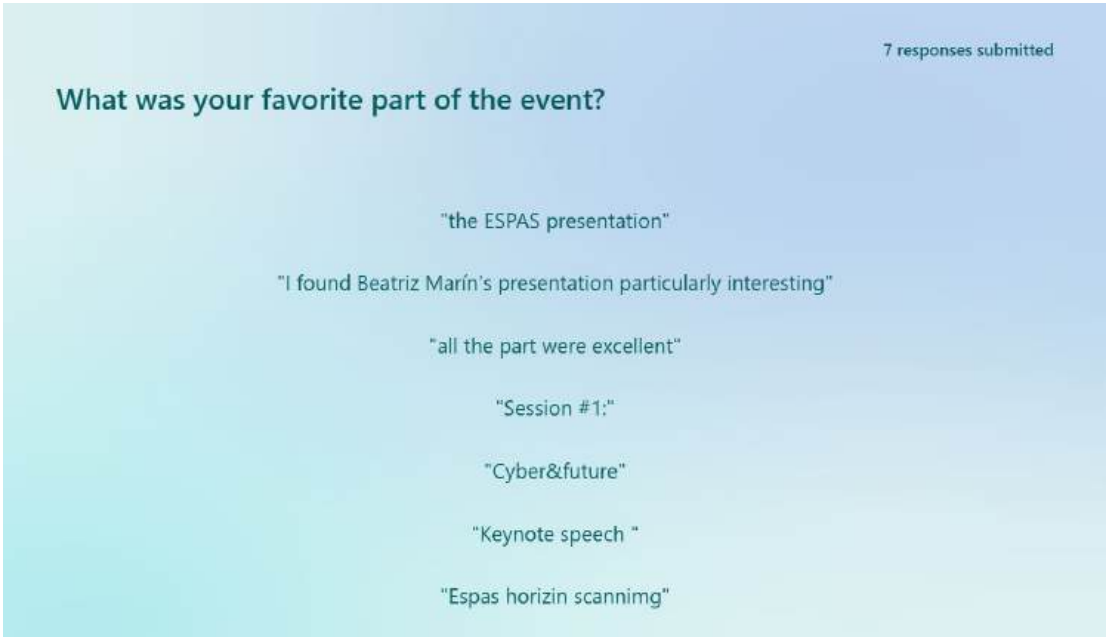



**Figure 8: Favourite part of the event**

# 6. CONCLUSIONS

The fifth and final Future Trends Workshop proved to be a successful event. It facilitated valuable connections between European practitioners, industry, SMEs, and academics, all working together to identify crucial future trends and potential solutions for analysing and countering hybrid threats. The speeches and 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 and bilateral exchanges; the topics discussed, receiving a positive return from the participants, have demonstrated to offer 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, speakers and content of the event.

In particular, the original ambitions can be considered as fulfilled:

- Keep gathering scholars, industry, practitioners and policymakers. The diversity of the audience has been conformed to the will of the organisers, and has been remarked through the exchanges with the speakers in the Q&A sessions, the breaks and the social event. The value of such a diversity has been once again remark.

- Offer a space and slots for transdisciplinary and cross-professional exchanges. The format allowed a clear social space for fertile exchanges and further cooperation between the participants.

- Deliver high quality analysis of future trends. The various interventions revealed high quality analyses from both speakers and participants, not only regarding their understanding of the topics and stakes, but also regarding the prisms of analysis and the interrogations or remarks emitted. Cumulated to interprofessional belongings and transdisciplinary approaches, the technical level of analysis was one of the factors of success of the event.

- Offer an in-depth workshop on anticipation. The JRC mobilised its Unit dedicated to foresight and proposed a participative presentation of ESPAS methodology. The direct participation, the Q&A session, the presentation of foresight training material and further comments during and after the event indicated that participants have been vividly interested in this session.

- Invite high-level representatives. With officials of European Commission's DG JRC and DG HOME, the European External Action Service and the Polish presidency of the Council of the European Union, the aim to have high-level representatives marking the final EU-HYBNET workshop has been fulfilled.

Identifying future trends serves is a key of hybrid threats. Indeed, hybrid attacks fundamentally operate through innovations, to deceive and surprise democracies and overflow their defences. The Future Trends Workshop operates therefore as an essential part of EU-HYBNET in developing solutions against hybrid threats. The interconnection of the future trends reflects the interconnections between the different threats. In this respect, future trends offer a unique insight into the possibilities to

counter future attacks, through both technical and non-technical solutions in a world where the technological tools and the threat landscape evolve more and more quickly.

# ANNEX I. GLOSSARY AND ACRONYMS

**Table 3: Glossary and Acronyms**

| Term | Definition / Description[TH1] [U2] |
|---|---|
| **JRC** | Joint Research Centre – European Commission |
| **EOS** | European Organization for Security |
| **LAUREA** | Laurea University of Applied Sciences |
| **DSB** | Direktoratet for samfunnssikkerhet og beredskap |
| **EU-HYBNET** | Empowering a pan-European Network to Counter Hybrid Threats –project |
| **UCSC** | Catholic University of the Sacred Heart of Rome |
| **Hybrid CoE** | European Centre of Excellence for Countering Hybrid Threats |
| **FTW** | Future Trends Workshop |
| **EU MS** | European Union Member State |
| **Q/A** | Questions and answers |
| **ESPAS** | The European Strategy and Policy Analysis System |
| **EU** | European Union |
| **OB** | Objective |
| **SME** | Small and medium-sized enterprise |
| **L3CE** | Lithuanian Cybercrime Center of Excellence for Training, Research and Education |
| **UiT** | The Arctic University of Norway |
| **URJC** | King Juan Carlos University |

| | |
|---|---|
| **SATWAYS** | Satways Ltd. |
| **WP** | Work package |
| **KPI** | Key performance indicator |
| **IA** | Innovation Arena |
| **EAB** | External Advisory Board |
| **NGO** | Non-governmental organization |
| **FIMI** | Foreign Information Manipulation Interference |
| **EEAS** | European Union External Action Service |
| **DG HOME** | The Directorate-General for Migration and Home Affairs |
| **AI** | Artificial Intelligence |
| **LLM** | Large Language Model |
| **IBD** | Identity-based disinformation |

# ANNEX II: PARTICIPANT ORGANISATIONS AND COUNTRIES

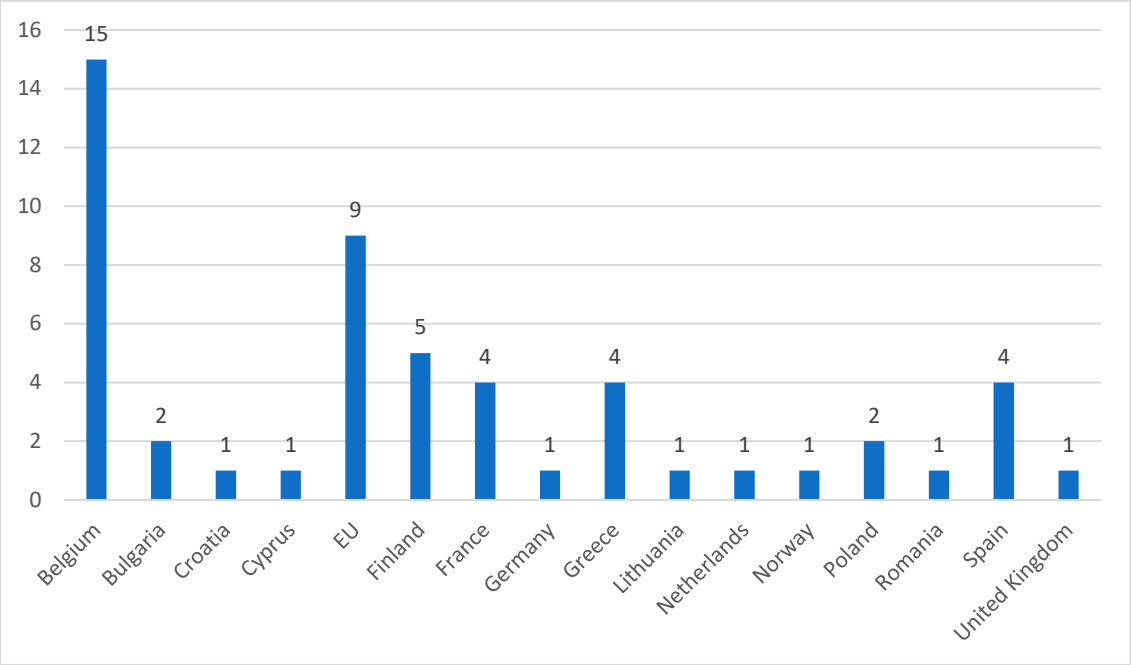



**Figure 9: Distribution per countries**

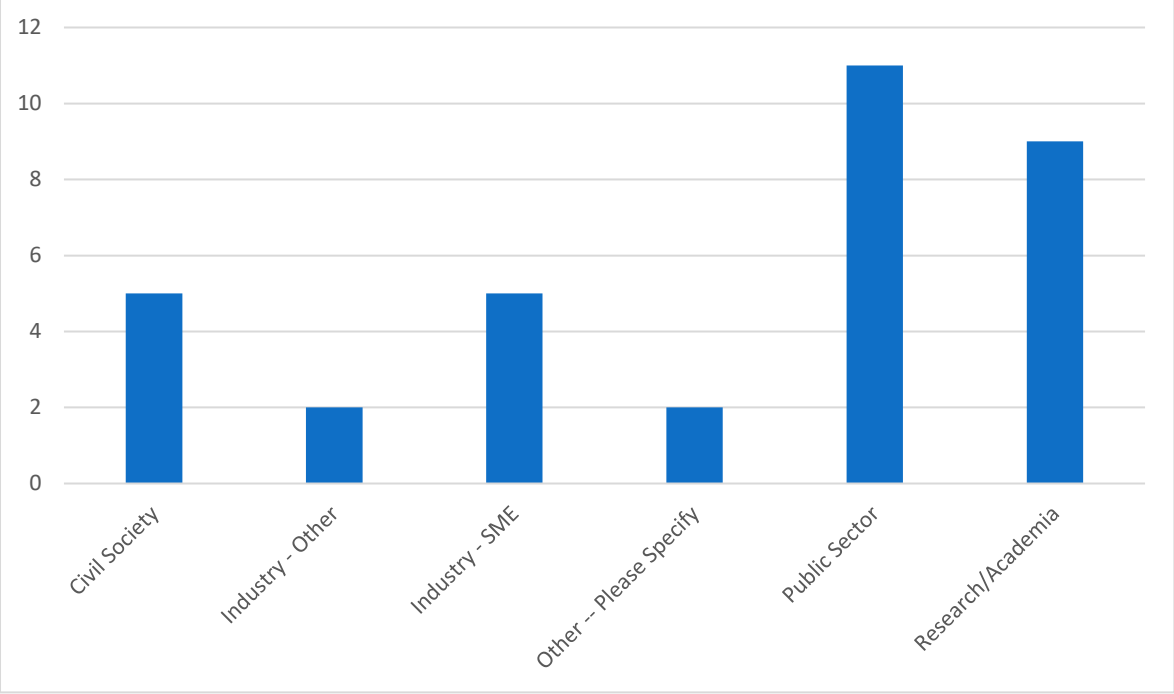
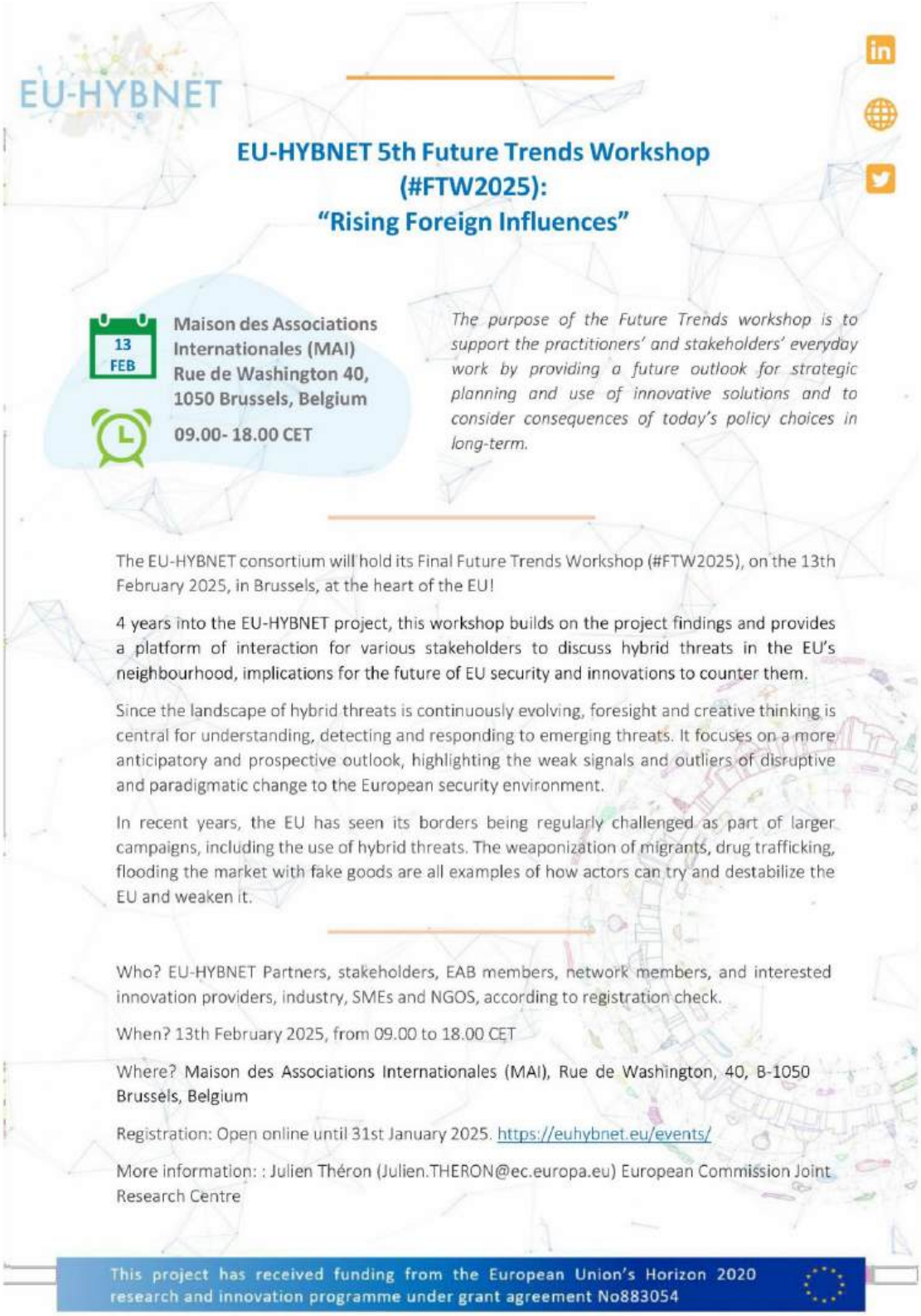



**Figure 10: Distribution of number of participant organisations per type of organization**

**Table 4: Distribution of number of participant organisations per type of organisation and country**

| | Civil Society / NGO | Industry - Other | Industry - SME | Other -- Please Specify | Public Sector | Research/Academia | Grand total |
|---|---|---|---|---|---|---|---|
| Belgium | 2 | 1 | 1 | 1 | 2 | 1 | 8 |
| Bulgaria | | | | | 1 | 1 | 2 |
| Croatia | 1 | | | | | | 1 |
| Cyprus | | | 1 | | | | 1 |
| EU | | | | | 2 | 1 | 3 |
| Finland | | | | 1 | | 1 | 2 |
| France | | 1 | 1 | | 2 | | 4 |
| Germany | | | | | | 1 | 1 |
| Greece | 1 | | 1 | | | 1 | 3 |
| Lithuania | | | | | | 1 | 1 |
| Netherlands | | | | | 1 | | 1 |
| Norway | | | | | | 1 | 1 |
| Poland | | | | | 2 | | 2 |
| Romania | | | | | | 1 | 1 |
| Spain | 1 | | | | 1 | | 2 |
| United Kindom | | | 1 | | | | 1 |
| **Total** | **5** | **2** | **5** | **2** | **11** | **9** | **34** |

## ANNEX III: WORKSHOP AGENDA



EU-HYBNET

**EU-HYBNET 5th Future Trends Workshop (#FTW2025): "Rising Foreign Influences"**

13 FEB

**Maison des Associations Internationales (MAI) Rue de Washington 40, 1050 Brussels, Belgium**

**09.00- 18.00 CET**

*The purpose of the Future Trends workshop is to support the practitioners' and stakeholders' everyday work by providing a future outlook for strategic planning and use of innovative solutions and to consider consequences of today's policy choices in long-term.*

The EU-HYBNET consortium will hold its Final Future Trends Workshop (#FTW2025), on the 13th February 2025, in Brussels, at the heart of the EU!

4 years into the EU-HYBNET project, this workshop builds on the project findings and provides a platform of interaction for various stakeholders to discuss hybrid threats in the EU's neighbourhood, implications for the future of EU security and innovations to counter them.

Since the landscape of hybrid threats is continuously evolving, foresight and creative thinking is central for understanding, detecting and responding to emerging threats. It focuses on a more anticipatory and prospective outlook, highlighting the weak signals and outliers of disruptive and paradigmatic change to the European security environment.

In recent years, the EU has seen its borders being regularly challenged as part of larger campaigns, including the use of hybrid threats. The weaponization of migrants, drug trafficking, flooding the market with fake goods are all examples of how actors can try and destabilize the EU and weaken it.

Who? EU-HYBNET Partners, stakeholders, EAB members, network members, and interested innovation providers, industry, SMEs and NGOS, according to registration check.

When? 13th February 2025, from 09.00 to 18.00 CET

Where? Maison des Associations Internationales (MAI), Rue de Washington, 40, B-1050 Brussels, Belgium

Registration: Open online until 31st January 2025. https://euhybnet.eu/events/

More information: : Julien Théron (Julien.THERON@ec.europa.eu) European Commission Joint Research Centre

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

EU-HYBNET

## Agenda

| Time CET | Topic | Speaker |
|---|---|---|
| 09.00-09.30 | Registration | |
| 09.30-09.45 | Official Introductory Speech | Georgios Giannopoulos, Deputy Director, EC DG Joint Research Centre |
| 09.45-10.00 | Welcome & Practical Information | Julien Théron, Researcher, EC DG Joint Research Centre<br>Isto Mattila, EU-HYBNET Coordinator, Laurea University of Applied Sciences |
| 10:00-10:15 | Keynote Speech | Jacob Tamm, Deputy Head of Division, European External Action Service |
| 10:15-10:30 | Audience Q&A | Moderator: Julien Théron, Researcher, EC DG Joint Research Centre |
| 10:30-10:45 | Coffee Break | |
| 10:45-12:15 | How foresight can increase preparedness and disaster resilience – Presentation of the European Strategy and Policy Analysis System's (ESPAS) horizon scanning process and the Risks on the Horizon foresight report with the Polycrisis exploration workshop toolkit. | Maija Knutti, Policy Analyst, EC DG Joint Research Centre<br>Tommi Asikainen, Policy Officer, EC DG Joint Research Centre |
| 12:15-13:15 | Lunch Break | |
| 13:15-15:15 | Session #1: Cyber & Future Technologies & Resilient Civilians, Local Level and National Administration<br>Topic: Future Trends in Cyber and Future Technologies | Co-Chair: Evaldas Bružė, Lithuanian Cybercrime Center of Excellence for Training, Research, and Education<br>Co-Chair: Gunhild Hoogensen Gjørv, UiT The Arctic University of Norway |
| 15:15-15:30 | Coffee Break | |
| 15:30-16:30 | Session #2: Information & Strategic Communication Topic: Trends and emerging issues in disinformation/FIMI: anticipatory analysis and identity-based disinformation/FIMI | Chair: Rubén Arcos Martin, Rey Juan Carlos University<br>Beatriz Marin Garcia, Data analyst, European External Action Service |
| 16:30-17:00 | Session #3: Wrap-up session - Future Trends of Hybrid Threats | Chair: Maxime Lebrun, European Centre of Excellence for Countering Hybrid Threats |
| 17:00-17:30 | Ending keynote<br>Closing Remarks | Nicolas Bessot, EC DG HOME<br>Tomasz Tokarski, Polish presidency |

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

EU-HYBNET

## Core theme Sessions

### CORE THEME SESSION 1

**Core theme:** Cyber and Future Technologies & Resilient Civilians, Local Level and National Administration

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

**Led by:** Evaldas Bružė, L3CE & Gunhild Hoogensen Gjørv, UIT

**Description:** This theme will focus on how the interplay between technological advancements and security dynamics increasingly defines the vulnerabilities of democracies, critical infrastructures, and societal resilience, and how recent (as well predicted for near future) application of next generation technologies changes risks through their potential misuse for disinformation, sabotage, and targeted disruption of essential services. Dynamically evolving domains like Generative AI, Cognitive AI, LLMs, quantum computing, edge AI, autonomous systems and neurotechnology are particularly topical, as they represent the cutting edge of innovation and areas where hybrid threats are likely to manifest through weaponization of tech economy, exploitation of digital arena and development of digital cognitive warfare. The workshop will address broader societal impacts, such as the influence of synthetic media on public trust, the fragility of global supply chains, and the rising threats to shared cultural and natural resources. By anticipating the convergence of technological, social, and geopolitical drivers, this FTW session seeks to discuss strategies that can mitigate risks and foster innovation in countering hybrid threats, including threats to democratic processes, economies, cultural and historical heritage, rise of offensive AI and AI defence models, cybersecurity in autonomous systems, weaponization of open-source intelligence, LLMs and GenAI based systems and global digital environments.

Key points:

- Next generation AI
- Global shifts in technological supremacy
- Speed of next generation technologies adoption
- Societal and Policy resilience to new types and scales of hybrid threats
- New era of dual use technologies and solutions
- Increased societal tiredness and apathy

### CORE THEME SESSION 2

**Core theme:** Information & Strategic Communication

**Title:** Trends and emerging issues in disinformation/FIMI: anticipatory analysis and identity-based disinformation/FIMI

**Led by:** Rubén Arcos Martín, URJC

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

EU-HYBNET

**Supported by:** Beatriz Marin, EEAS

**Description:** Anticipatory analysis and identity-based disinformation/FIMI

**CORE THEME SESSION 3**

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

**Title:** Wrap-up session – Future trends of hybrid threats

**Led by:** Maxime Lebrun, Hybrid CoE

**Description:** Wrap-up session – Future trends of hybrid threats

## Speakers

### Rubén Arcos Martín

Dr. Rubén Arcos is a senior lecturer in communication sciences at University Rey Juan Carlos (URJC) in Madrid, Spain, and researcher of Cyberimaginario research group. He serves as program co-chair of the Intelligence Studies Section at the International Studies Association. He is a cofounder and codirector of IntelHub—International Online Intelligence Hub, a joint initiative between the American Public University System (APUS), the University of Leicester in the UK, and URJC. Dr. Arcos is currently a researcher and core theme leader (information and strategic communications) in the EU-HYBNET project—Empowering a Pan-European Network to Counter Hybrid Threats (a five year-long project funded by the European Commission's Horizon 2020 Programme).

### Tommi Asikainen

Tommi Asikainen works as a Policy Officer at the European Commission EU Policy Lab's Competence Centre on foresight. He holds a Master of philosophy in mathematical statistics with focus on modelling of pandemics. He has a long experience in pandemic planning and use of foresight in public health. He worked before at the European Centre for Disease Prevention and Control as a mathematical modeller. Currently leading the Future Risk project at the EU Policy Lab, developing quantitative tools for use in foresights. Leading the project on the use of AI in foresight and using foresight methods to identify future risks and their impact on policy making.

### Nicolas Bessot

Nicolas Bessot is the Head of Unit for Innovation and Security Research in the European Commission's Directorate General for Migration and Home Affairs. In his current functions, Nicolas is responsible for the management of the Security Research part (Cluster 3) of the EU Framework Programme for Research and Innovation, by setting the research agenda, in cooperation with the Member States, in the areas of Fighting Crime and Terrorism, Border Security, Disaster Resilient Societies and Infrastructure Protection. Nicolas is also co-chair of the EU Innovation Hub of EU Agencies in the field of Justice and Home Affairs since 2022. Nicolas Bessot has been working in the European Commission since 2006. He joined the Directorate-General for Migration and Home Affairs early 2015 to prepare the Commission's Internal Security Strategy for the period 2015-2020, and then coordinated its implementation within the Commission.

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

EU-HYBNET

### Evaldas Bružė

Evaldas Bružė is an experienced coordinator, project manager, WP leader, researcher and contributor to several national and EU-wide research, evaluation and technology projects focused on cyber security issues, cyber-crime, hybrid threats, radicalization, violent extremism and organized crime. Mr. Bružė has been the main architect for national information and hybrids threats methodology development (project ECOPOL and further). Have been coordinator of few H2020&Horizon projects, Research Programme Manager in SPARTA project, Core Team Leader for Cyber and Future technologies in EU-Hybnet project, Development Manager in STARLIGHT. He has created innovation uptake methodology for security domain practitioner and managing national project NAAS for innovations ecosystem development to counter information and hybrid threats. He is an IT expert with a strong technical background as a solution architect & with operational skills in process management, including 15- year experience in IT systems development projects (incl. various certifications in project management, business analysis, system architecture, professional development, software quality engineering and testing). Recently he has been focusing on OSINT, AI, DLT, Quantum innovations' transformative aspects and their uptake opportunities into LEA, security and defense end-user organizations. He played a significant role in the establishment of MRU's security LAB as a competence gateway for Cyber Security experts, R&D centres and security practitioners, and international networks of academia, as well as LEA in the cybercrime domain. Actively contributing to security domain communities being Board Member of Lithuanian Cybersecurity Experts' Association, Crypto Economy Organization (LT), EACTDA Technical Board and independent innovation strategy advisory to Security and Defense Institutions.

### Georgios Giannopoulos

Dr. Georgios Giannopoulos holds a degree in Mechanical and Aeronautical Engineering, a PhD in Engineering from Vrije Universiteit Brussel and the Royal Military Academy of Belgium, and a Management degree from Solvay Brussels School of Economics and Management. He currently serves as the Head of the Space, Connectivity, and Economic Security Unit and Deputy Director of the Societal Resilience and Security Directorate at the Joint Research Centre (DG JRC) of the European Commission. His areas of expertise and research activities involve security-related topics such as critical infrastructure risk and resilience, CBRNE, Hybrid Threats, Positioning, Navigation, and Timing with a focus on Galileo, 5G applications, Satellite Communications and analysis of critical technologies through the Observatory of Critical Technologies (OCT). This research is aimed at providing scientific advice for policy-making to promote the European Union's Economic Security and Technological Sovereignty. Dr. Giannopoulos has authored over 50 scientific publications and book chapters and has trained officials in several European countries to enhance the protection of their technological systems and critical infrastructures including countering Hybrid Threats.

### Gunhild Hoogensen Gjørv

Gunhild Hoogensen Gjørv is Professor in Critical Peace and Conflict Studies (Security and Geopolitics) at the UiT- The Arctic University of Norway, and Arctic 5 Chair in Security Studies (arcticfive.org). Hoogensen Gjørv's research examines comprehensive security dynamics in the context of hybrid threats and warfare, civil-military interaction (out of area operations, and Norwegian total defence), and Arctic perceptions of security focusing on "bottom-up" and intersectional approaches. She leads a variety of projects regarding hybrid threats and civilians. UiT profile page: https://uit.no/ansatte/gunhild.hoogensen.gjorv

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

EU-HYBNET

### Maija Knutti

Maija Knutti works as a Policy Analyst in the EU Policy Lab's Competence Centre on Foresight, which is part of European Commission Joint Research Centre. She has the master's degree on Futures Studies from the University of Turku and master's degree on Education form the University of Helsinki. She has a long experience in the field of education, mainly versatile roles in the vocational education as teacher, developer and education manager. Her current task in the Policy Lab is bringing futures thinking into the policy making. She is organising the horizon scanning process of the inter-institutional European Strategy and Policy Analysis System (ESPAS) and managing various foresight communities of the Competence Centre on Foresight.

### Maxime Lebrun

Prior to taking up his post as Deputy Director R&A 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.

### Isto Mattila

Professor Isto Mattila works for international security research in the University of Turku, Finland in the Department of Information Technology. Prof. Mattila has wide working experience covering diverse assignments in different organisations national and international level. He is a Captain Navy, Finnish Border Guard. As from 2008 to 2014 he has worked for the European Commission, DG MARE. He was a second penholder for Maritime Security Strategy and designed new information sharing mechanism (CISE) between maritime authorities in EU, which is now hosted by EMSA. He has held the position of R&D Director at Laurea UAS and he was the project coordinator of the AI-ARC Horizon 2020 project, which aims to build information sharing and anomaly detection to Arctic stakeholders.

### Jacob Tamm

Jacob is an EEAS official and EU diplomat who joined the Information Integrity and Countering Foreign Information Manipulation and Interference Division in September 2023. Prior to that, Jacob served in different services at the EEAS HQ, including as Deputy Head of the US and Canada and the Regional Affairs Divisions. He has done several postings abroad, including in the EU Delegation in Nigeria, where he led the democratic governance/counter-terrorism team, and also served as a political advisor in the EU Delegation in Bolivia. Before joining the EU institutions, Jacob was posted in Swedish Embassies in Bolivia and Guatemala, where he was engaged on Sweden's bilateral cooperation on issues related to peace, security and democratic governance, and was also working for the UNDP/UNV in Brazil and various civil society organisations. Jacob is a graduate from London School of Economics and Political Science and the University of Sussex.

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

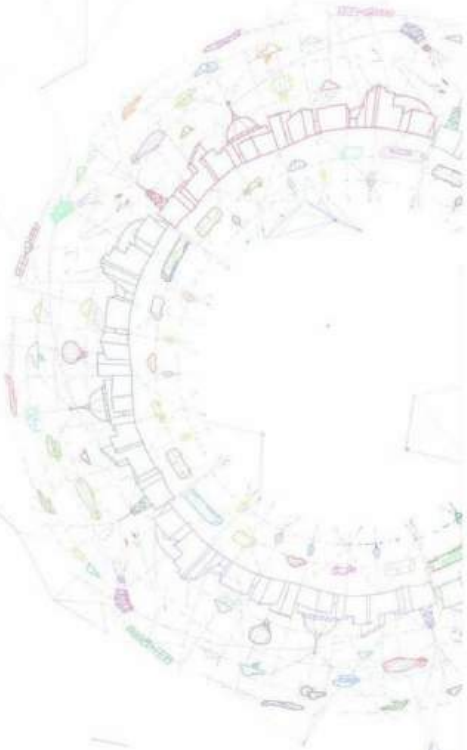
EU-HYBNET

Julien Théron

Political scientist, Dr Julien Théron taught at the universities of Budapest (BME), Beirut (USJ, USEK), Paris (Nanterre, Versailles, Panthéon-Assas). He collaborated with the French Institute of International Relations (IFRI) and the International Institute for Strategic Studies (IISS), and is a former Senior Fellow of the Norwegian Institute for Defence Studies (IFS). In policy, he worked for the French government (MFA, MoD, INSP), European Union's projects (EU) and the United Nations (UN). Specialized in complex conflicts and international security, he conducted field research in Bosnia-Herzegovina, Serbia, Kosovo, Egypt, West Bank, Lebanon, Syria, Iraq, Georgia, and Ukraine. He is a lecturer in War Studies at Sciences Po's Paris School of International Affairs (PSIA) and a researcher in Hybrid Threats at the European Commission Joint Research Centre (DG JRC).

Tomasz Tokarski

Tomasz Tokarski is a diplomat based at the Permanent Representation of Poland to the EU. Currently, as Poland holds the rotating Presidency of the Council of the EU, he chairs the Horizontal Working Party for Enhancing Resilience and Countering Hybrid Threats. This group is responsible for supporting the strategic and horizontal coordination of efforts to strengthen the preparedness and the resilience of the EU and its Members States, as well as enhance their ability to respond collectively, raise awareness and promote coherence in EU policies related to hybrid threats and FIMI. Previously, Tomasz served at Poland's MFA as well as Permanent Missions to the UN in Geneva and New York, where he worked on various aspects of security policy, with a particular focus on arms control and non-proliferation.



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

## ANNEX V: FUTURE TRENDS WORKSHOP PROMOTIONAL MATERIAL


**Figure 11: 5th FTW Invitation**

## ANNEX 6: EVALUATION FORM AND ANSWERS


1. Overall, how satisfied were you with the event? *

2. How would you assess the general content, topics of the event? *

3. How relevant did you find the keynote speeches? *

4. How would you evaluate the core-theme session overall? *

5. Please feel free to add any comments regarding your core-theme session.

Enter your answer

6. How would you assess the event arrangements? *

7. How would you assess the time invested to the event participation? *

8. How helpful were the event organisers? *

9. What was your favorite part of the event? *

Enter your answer

10. What was your favorite topic of the event? *

Enter your answer

11. What was your least favorite part of the event? *

Enter your answer

12. Any other comments?

Enter your answer




5. Please feel free to add any comments regarding your core-theme session.

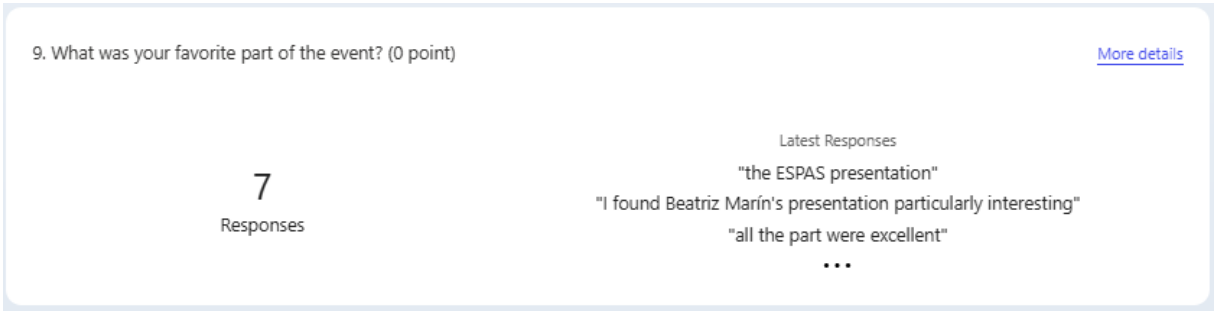
1 Responses

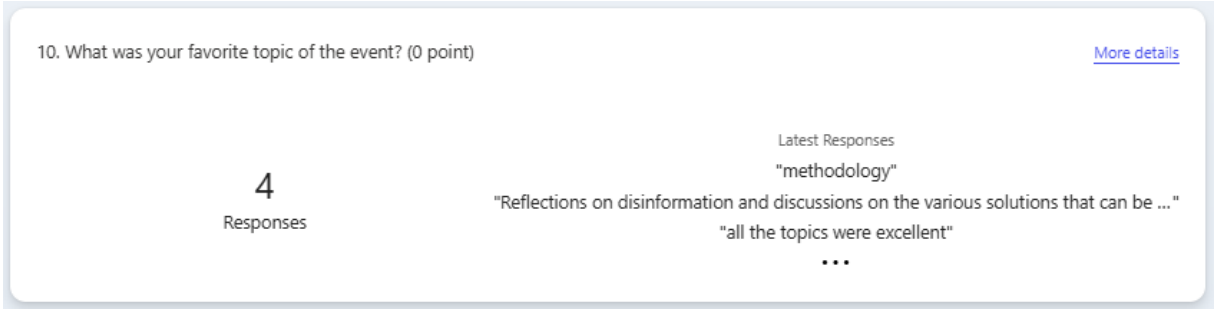
| ID ↑ | Name | Responses |
|---|---|---|
| 1 | anonymous | It was very interesting but perhaps too much time was assigned to the part on Cyber & Future Technologies & Resilient Civilians, Local Level and National Administration |

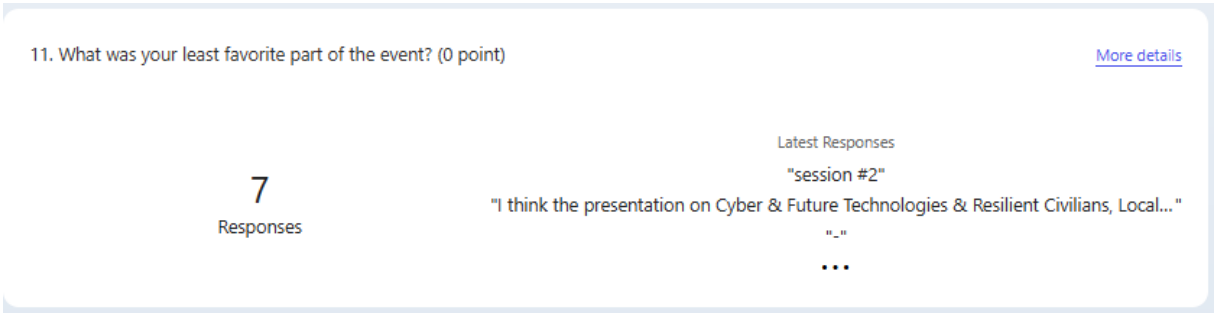

6. How would you assess the event arrangements? (0 point)
More details
4.86
Average Rating
Level 5
6
Level 4
1
Level 3
Level 2
Level 1

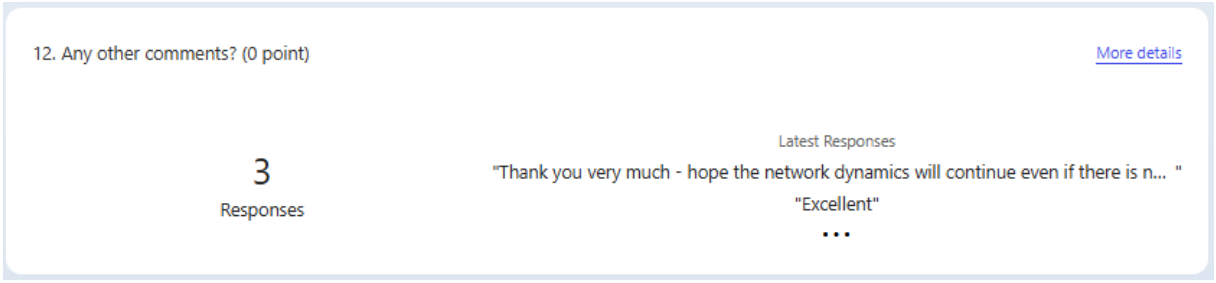

7. How would you assess the time invested to the event participation? (0 point)
More details
4.43
Average Rating
Level 5
4
Level 4
2
Level 3
1
Level 2
Level 1


8. How helpful were the event organisers? (0 point)
More details
4.86
Average Rating
Level 5
6
Level 4
1
Level 3
Level 2
Level 1


9. What was your favorite part of the event? (0 point)
More details
7
Responses
Latest Responses
"the ESPAS presentation"
"I found Beatriz Marín's presentation particularly interesting"
"all the part were excellent"
...


10. What was your favorite topic of the event? (0 point)
More details
4
Responses
Latest Responses
"methodology"
"Reflections on disinformation and discussions on the various solutions that can be ..."
"all the topics were excellent"


11. What was your least favorite part of the event? (0 point)
More details
7
Responses
Latest Responses
"session #2"
"I think the presentation on Cyber & Future Technologies & Resilient Civilians, Local..."
"-"


12. Any other comments? (0 point)
More details
3
Responses
Latest Responses
"Thank you very much - hope the network dynamics will continue even if there is n... "
"Excellent"