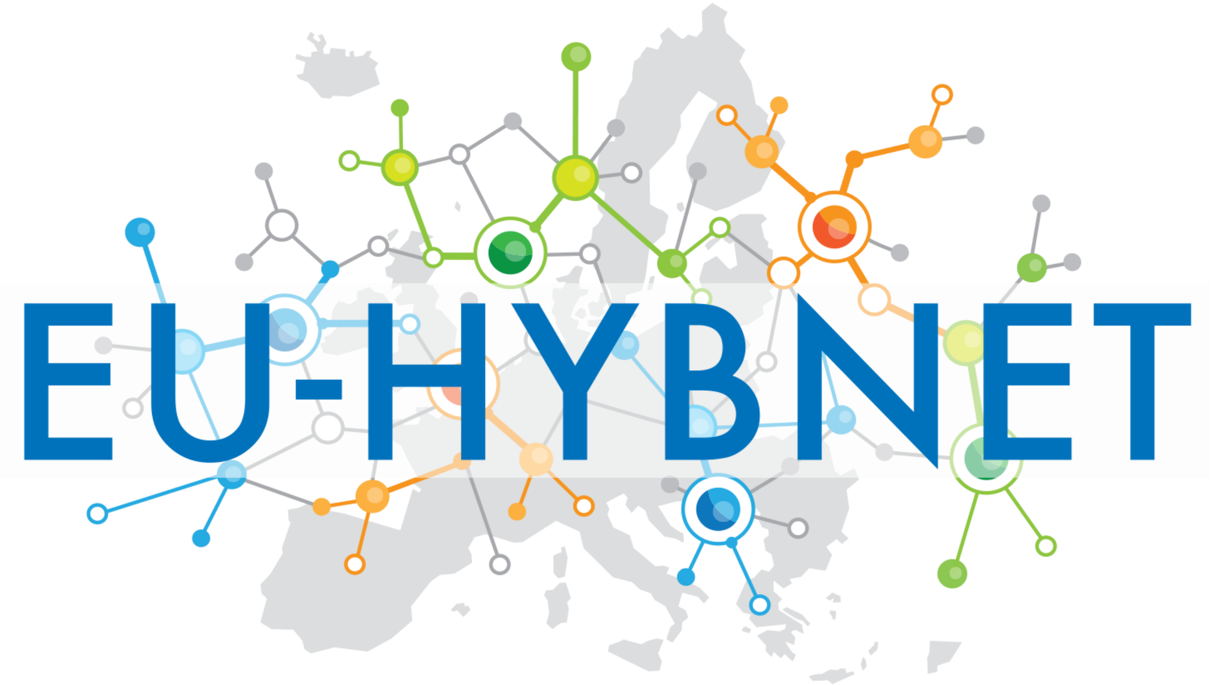


3RD FUTURE TRENDS WORKSHOP REPORT

DELIVERABLE 3.16

Lead Author: MVNIA

Contributors: EOS, Laurea, ZITiS

Deliverable classification: PUBLIC

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

D3.14 FUTURE TRENDS WORKSHOP REPORT

Deliverable number	**3.16**	
Version:	**1.0**	
Delivery date:	**10/07/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Cristina Ivan** **Mihaela Teodor**	**MVNIA**
Contributors:	**Angeliki Tsanta** **Tiina Haapanen, Päivi Mattila, Jari Räsänen** **Michael Meisinger**	**EOS** **Laurea** **ZITiS**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	28.05.2023	Mihaela Teodor/ MVNIA	First draft, text to all chapters
0.2	31.05.2023	Cristina Ivan/ MVNIA	Second draft, content input and document structure
0.3	02.06.2023	Angeliki Tsanta/ EOS	First review; Chapter 5 added
0.4		Tiina Haapanen/Laurea	Text editing
0.5	14.06.2023	Cristina Ivan/ MVNIA	Text editing and document delivery for review
0.6	14.06.2023	Päivi Mattila/ Laurea	Review and text editing
0.7	14.06.2023	Michael Meisinger/ZITiS	Review
0.8	04.07.2023	Jari Räsänen/ Laurea	Review and document editing.
0.9	07.07.2023	Tiina Haapanen/ Laurea	Text editing and final review
1.0	10.07.2023	Päivi Mattila/Laurea	Final review and submission of the document to the EC review

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.

© Copyright in this document remains vested in the Project Partners

TABLE OF CONTENTS

TABLES

FIGURES

1. INTRODUCTION

The Future Trends Workshop is an annual event organized as part of the EU-HYBNET (Pan-European Network to Counter Hybrid Threats) project. Its purpose is to address expected future manifestations of hybrid threats and their potential evolution to ensure that the project is not only looking for innovations that address existing needs but also future ones. It is one of the events arranged under EU-HYBNET Task (T) 3.4 "*Innovation and knowledge exchange events*".

The first EU-HYBNET Future Trends Workshop was organized by the Hybrid CoE, and it took place as a virtual event on 31st March, 2021. The second one was organized by the Catholic University of the Sacred Heart of Rome, Italy (UCSC), and it took place as a hybrid event (in-person and on-line) on 5th April, 2022 in Rome.

The third workshop was organised by "Mihai Viteazul" National Intelligence Academy as an in-person only event and took place on the 19th April, 2023 in Bucharest, Romania. This deliverable reports the methods and outcomes of this third workshop.

1.1 THE STRUCTURE OF THE DELIVERABLE

This document includes the following chapters:

Chapter 1: *Future trends in the EU-HYBNET project*. This chapter explains how the annual Future Trends Workshop contributes to the objectives of the project, and why the future-oriented thinking has a special role in countering hybrid threats.

Chapter 2: *Methods*. This chapter explains what kind of information was gathered in the workshop, how this was done, and how it will be used.

Chapter 3: *Outcomes of the workshop: perceptions on future of hybrid threats.* This chapter presents the three trends that the participants considered most relevant for the future of hybrid threats.

Chapter 4: *Workshop participants and feedback*. This chapter includes the main content of feedback, and the main lessons learned.

Chapter 5: *Conclusions and way ahead*. This chapter explains how the data gathered in the Future Trends Workshop will be used in the project. This is important for the EU-HYBNET Work Package (WP) 3 "Surveys to Technology, Research and Innovations" Innovation mapping to pan-European practitioners and other relevant actors (industry, academia, NGOs) gaps and needs to counter hybrid threats.

2. FUTURE TRENDS WORKSHOP AND EU-HYBNET PROJECT

The Future Trends Workshop is part of the EU-HYBNET project Task 3.4 "*Innovation and knowledge exchange events*". Its purpose is to strengthen the future-oriented thinking among participants, and to provide a platform for out-of-the-box ideas, that might open up new possibilities in countering hybrid threats. The workshop also supports project partners when looking into innovations and solutions to counter hybrid threats for today but also for tomorrow.

MVNIA was the organiser and host of this third workshop in collaboration with the European Organisation for Security (EOS), leader of EU-HYBNET's Task 3.4 and with the support of Laurea University of Applied Sciences as the coordinator of the project. All core theme leaders (L3CE, UiT, URJC, Hybrid CoE) greatly contributed to the design of the event and its break-out sessions.

As background, the figure below highlights how Future Trend Workshops in general contribute to the project content and will support each EU-HYBNET Work Packages (WP) to proceed in their work.

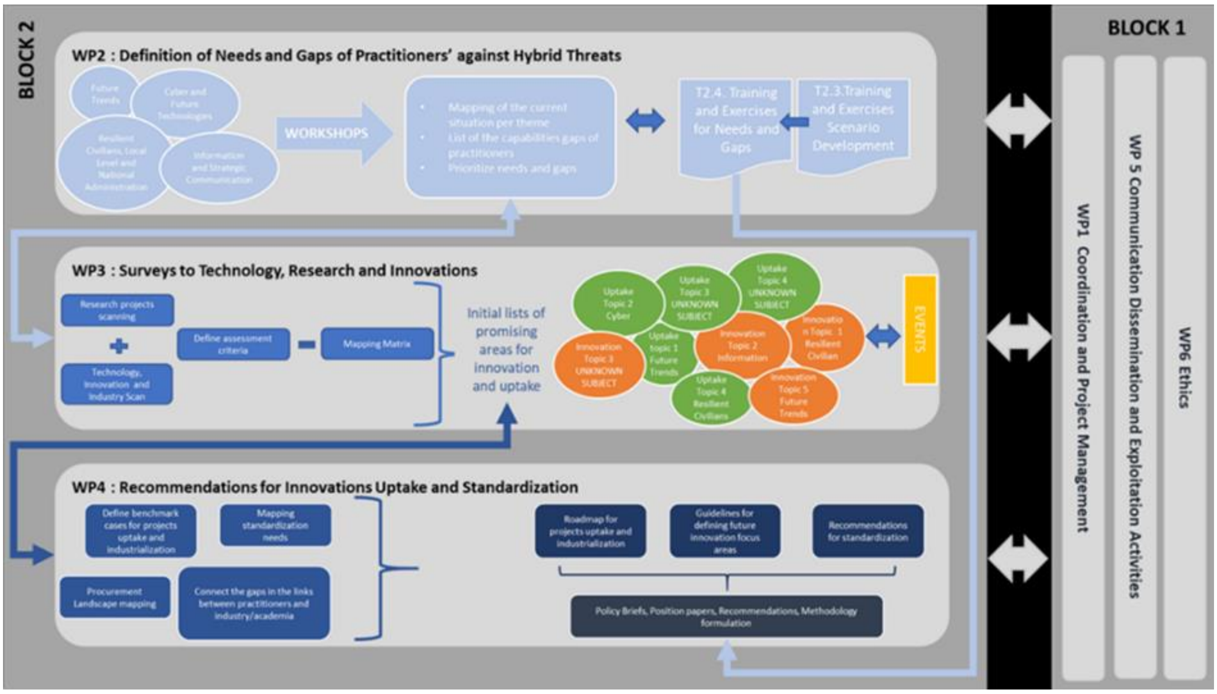

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities 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
Innovation 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 organisation of the FTWs are directly linked to **project Objective (OB) 1**: *To enrich existing network for countering hybrid threats and ensure long term sustainability,* and 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 OB Key performance indicators (KPI) for the network extension is the number of events organised, which was set to a minimum of three events every year.

The detailed connection between the project objectives and the organisation of events within EU-HYBNET KPIs are described 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 -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 - Newsletter, published every 6 months w. 60 new readers yearly

When it comes to this workshop, it should be noted that as the security environment becomes increasingly complex, so does the detection of emerging threats. Hybrid threats are by nature difficult to detect, as the hybrid threat actors operate below the threshold of open conflict, on multiple channels simultaneously, and are not always clear in relation to each other. Hybrid threats also evolve in time, due to technological advances and new ways to build resilience, and deter and counter the threats. Without detection, however, countering becomes impossible, and we would be always two steps behind, inevitably on the losing team. These complexities are managed first and foremost by building a global, dynamic overview on evolving security issues. Foresight, especially the detection and analysis of trends is a crucial capability in this regard. To understand trends of hybrid threats or those affecting their evolution, a multidisciplinary approach is needed, and signals in every domain are relevant. Therefore, we need to bring together different actors – government practitioners, local administration, non-governmental organisations, academia and private sector – to learn from each other.

Due to the central role of the core themes, foresight and trends assessment is present in every phase of the project to some extent. However, the Future Trends Workshop is the only specific event dedicated to increase this capability. The Future Trends Workshops specifically concern perspectives relevant for the next two decades and contribute especially to one of the project objectives (OB.7), which is to create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats. One of the goals under OB7. is Goal 7.2 to empower European practitioners, industry, SME and academic actors to recognise important innovations/trends.

The 3rd Future Trends Workshop event was designed to contribute to that goal, with the focus on identifying and analysing possible trends. Participants learned how megatrends could affect European security, from high-level keynote and panellist speakers. Three years into the EU-HYBNET project, this workshop built on the project findings and provided 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 has been continuously evolving, foresight and creative thinking were considered central for understanding, detecting and responding to emerging threats. Hence, the 3rd FTW focused on a more anticipatory and prospective outlook, highlighting the weak signals and outliers of disruptive and paradigmatic change to the European security environment.

The event was built around the notion that recent events in the EU neighbourhood have brought into attention a complex dynamic of adversarial tools and strategies involving weaponization of information, technology, cyberspace, critical infrastructure, energy, in an intricate pattern aimed to weaken cohesion and generate polarisation across the EU and its neighbourhood. To respond to these evolutions and in order to provide a comprehensive perspective on the expected evolution of hybrid threats trends of manifestation, the event was designed as follows:

- three keynote speeches introducing the topic from both a regional and European perspective;
- an introductory panel that set the scene by presenting existing hybrid threats (e.g., information manipulation, cyber warfare, threats to critical infrastructure etc.);
- three break-out sessions dedicated to three of the EU-HYBNET projects core themes (1) Cyber and future technologies, (2) Resilient Civilians, Local Level and National Administration, and (3) Information & Strategic Communication. The fourth core theme (Future Trends) was the overarching topic of all sessions;
- a final panel brought together the break-out session leaders to discuss the conclusions of each sessions and debate Future Trends for EU Security
- a Closing Keynote Speech on the role of the Common Information Sharing Environment (CISE) for EU Maritime Security.

While key note speeches and panel presentations aimed to give participants insight from reputed academic lecturers and central institutional stakeholders at the national and EU level on key aspects of hybrid threats detection and understanding (as detailed below), the second part of the workshop gave participants the chance to interact and debate in break-out sessions existing and future trends in the core themes (1)Cyber & Future Technologies, (2) Resilience of civilians, local and national level administration and (3) Information & Strategic Communication.

The work in small groups aimed at understanding the contexts of hybrid threats and trends as parts of megatrends, drawing a broad picture of the environment in which potential innovations could be imagined. The participants' task was to define, what they think are the most relevant trends affecting the future of hybrid threats.

The discussions concluded in a last panel that presented the findings of each break-out session and participants' insight on future trends and innovations. This panel also began to draw some first conclusions for their implications on the future of EU security.

The link of the event with the rest of the project objectives will be analyse in the following section.

3. METHOD

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

3.1 OBJECTIVE AND FOCUS

The main objective of the event was create a platform to facilitate interaction between EU-HYBNET partners, stakeholders, EAB members, network members, and interested innovation providers, industry, SMEs and NGOS so that, together they could explore the topic of Hybrid Threats emerged in the EU neighbourhood and their implications for the future of EU security.

This is because, as explained above, the Future trends workshop aims to fulfil project objective 1 (OB1), which is to enrich the existing network countering hybrid threats and to ensure long term sustainability. The public nature of the event and the efforts made by the host organisation to engage its Romanian and international network allowed EU-HYBNET to extend its reach and made the project more attractive for new members to apply. Particular attention was given by the organisers in reaching out to new organisations and presenters and offering new ideas and perspectives on the issue of hybrid threats to the consortium and the network. For example, hybrid threats in maritime security and information sharing were discussed by the European Commission’s DG MARE and EMSA.

In addition, the event provided an arena for networking and information sharing, also contributing to project objective number 5 (OB5), which is to support conditions for enhanced interaction with the network. As shown in this report, many network members not only attended the event but were also offered the opportunity to participate and present in the break-out sessions so that network and consortium members could connect and understand their individual challenges. Moreover, enabling future-oriented thinking directly supports the sustainability of all ideas and solutions that the project produces.

By defining the trends that the participants deem most important in impacting the future of hybrid threats, the workshop also fulfils the project objective two (OB2), which is to define the common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours. One specific goal (Goal 2.3) under this project objective is to gather and define insights on trends, which the event did.

The focus of the Future Trends Workshop was developed in close collaboration between the organising partners MVNIA, EOS and LAUREA while the WP 3 leader SATWAYS and all core theme leaders - notably Hybrid CoE were also consulted in this decision. The organisers aimed to take into consideration the current EU security landscape and how hybrid threats develop and will develop in its wider neighbourhood in the future. This topic is all the more relevant if we take into account the 2022 invasion of Ukraine by the Russian Federation and the subsequent war that changed to a great extent both the modus operandi and the intensity with which hybrid threats are propagated against the Western world.

The frame was set by the series of three key note lectures, one focused on resilience, delivered by Mr. Ovidiu Alexandru Raețchi, head of the Euro-Atlantic Resilience Centre in Romania, one dedicated to the technological aspects of Hybrid Threats, delivered by Mr. Dan Cîmpean, head of the National

Directorate for Cyber Security, Romania and finally the third one on the EU Maritime Security Strategy, delivered by Mr Thierry Segers, Policy Officer, Directorate-General for Maritime Affairs and Fisheries, European Commission, who attended online. This setting the frame gave insight and facilitated further discussions during the panels and break-out sessions dedicated to hybrid threats in the EU neighbourhood and the future trends of EU security.

The panel speakers were selected so as to be able to provide multiple angle perspectives; from representatives of EU and NATO institutions to diplomacy and research, not to mention the opportunity to have on board, as panel speaker, a representative of the Ukrainian Parliament, Ms. Liudmyla Buimister. Finally, discussions were opened to all participants during the break-out sessions.

These reflections will support the future assessment of EU-HYBNET results: defined gaps, needs, solutions and innovations. The purpose of bringing participants together to small working groups was to enable discussion and exchange on hybrid threats and trends in a more intimate environment and setting. The setting aimed at empowering out of the box ideas, which are needed to discuss trends and signals.

3.2 WORKSHOP STRUCTURE

The event organisers arranged a full-day in-person workshop, consisting of two parts:

a) the first part with three keynote lectures and a panel of high-level experts dedicated to the topic ***Hybrid threats in the EU's neighbourhood shaping the future of EU security*** and

b) a second, highly interactive part, where the participants were divided in break out groups that discussed: Cyber & Future Technologies, Resilient Civilians, Local Level and National Administration and last, but not least, Information & Strategic Communication

c) a third part consisting of a panel discussion on EUHYBNET findings regarding **Future Trends for EU security** and a closing note speech on the role of the Common Information Sharing Environment (CISE) for EU Maritime Security, delivered by Mr. Gianluca Luraschi, Project Officer, Department 2 - Safety, Security component and Surveillance at European Maritime Safety Agency (EMSA).

The topics of the keynote and panel were related to the topic of the event and included three keynote speeches by: Mr. Ovidiu Raetchi, President, Euro-Atlantic Resilience Centre from Romania; Mr. Dan Cîmpean, National Directorate for Cyber Security, Romania; the online intervention of Mr. Thierry Segers, Policy Officer, Directorate-General for Maritime Affairs and Fisheries, European Commission. In addition, they included a panel discussion on Hybrid threats in the EU's neighbourhood shaping the future of EU security. The panel speakers were dr. Iulian Fota, State Secretary for Strategic Affairs, Ministry of Foreign Affairs, Romania, dr. Orlando Cenciarelli, European Centre for Disease Prevention and Control and dr. Souzanna Sofou, Senior Research and Innovation Manager, SATWAYS.

The second, more interactive part consisted of three (3) breakout sessions, during which participants worked in person. The focus of the Future Trends Workshop was developed in close collaboration with all EU-HYBNET core theme leaders: UiT, L3CE, and URJC.

The topics were chosen in relation to the identified gaps and needs under each core theme: Future Trends in Cyber and Future Technologies; Resilient civilians, local level and national administration;

Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats. These were considered relevant contexts for the future manifestations of hybrid threats, in which the trends emerge. The group themes were chosen based on discussion of the most important lines of research and investigation pertaining to the project core themes. The group themes also reflected more tentative ideas by the core theme leaders which were then taken on board as a means of exploration. The topics of each session are summarised below, while the full workshop agenda can be found in Annex III.

Break-out session #1: Future Trends in Cyber and Future Technologies

Core theme: Cyber and Future Technologies
Led by: Evaldas Bružė (L3CE)
Supported by: Maltego
Description: This session looked at the current EU security environment as a whole and addressed hybrid threats arising from Cyber and Future Technologies to allow participants to identify the most pressing future trends in this field, as well as the innovations that could support the work of pan-European practitioners. The discussion was split in three building blocks:

- persistent and recurring threats already identified by practitioners in the first two cycles of the EU-HYBNET project (e.g., threats related to quantum computing);
- developing trends identified by the 3rd EU-HYBNET Gaps and Needs assessment as well as the European Commission (e.g., vulnerabilities related to space and GPS navigation infrastructure);
- new and shifting trends in the tech sector (e.g., foreign investments in social media platforms, filtering techniques applied by social media gatekeepers, social change brought by AI developments and initiatives, the metaverse, AI and ML operations, supply chain dependencies and their impact on clean tech). Participants will also have the opportunity to discuss innovative solutions and receive a demonstration of how the technology is working.

Break-out session #2: Hybrid threats in the Arctic

Core theme: Resilient civilians, local level and national administration
Led by: Gunhild Hoogensen Gjørv (UiT)
Description: This session started from the premise that the Arctic region is already (and will continue in the future) to be experiencing increased targeting via diverse non-conventional hybrid threats. This is particularly relevant given the ongoing accession talks of Finland and Sweden into NATO. The northern part of Europe is still very vulnerable due to small population concentration (compared to the south), poor infrastructure (e.g., supply lines, roads), lack of investment, vulnerability to "sympathetic" narratives etc. The region is very remote and forms a key part of the EU's external borders in the current geopolitical environment, while also being close to critical third-country-owned military bases. Third-country defence in the area is more than likely to be of a non-conventional nature than conventional, and could involve the manipulation and destabilization of the northern regions, to cut them off from their capitals if not physically (territorial capture) then by all other means necessary including cyber-attacks on infrastructure, sabotage (including water sources), mis- and disinformation, and attempts to network and build up 5th columns. This could destabilise the entire northern region of Europe.

Break-out session #3: Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats

Core theme: Information & Strategic Communication
Led by: Rubén Arcos Martín (URJC) and Irena Chiru (MVNIA)
Supported by: VOST Europe, MTES
Description: Starting with an overview of current security threats arising from disinformation as a hybrid threat, in this session participants worked towards identifying the challenges and needs of practitioners in countering this phenomenon, existing technological and non-technological solutions as well as the need to adopt a more anticipatory outlook. What trends can be identified for the future outlook of disinformation? The EU Code of Practice on Disinformation was discussed and evaluated: how does it address disinformation used by foreign actors especially given the current threat landscape, as well as emerging trends (AI-produced disinformation, ownership changes in signatories etc)? The French Ministry of Ecological Transition also presented their perspective and needs when it comes to protecting strategic assets, values and the economy against disinformation. Taking into consideration these trends, participants discussed required innovations that could assist the work of hybrid threats practitioners through an integrated and anticipatory approach.

4. OUTCOME OF THE WORKSHOP: PERCEPTIONS ON FUTURE OF HYBRID THREATS

As mentioned above, the workshop plenary aimed to set the scene and offer some initial ideas and perspectives to participants to guide the discussions and lead them to determined existing and future trends of hybrid threats.

4.1 PERCEPTIONS PRESENTED BY KEYNOTE SPEAKERS

- Mr. Ovidiu Raetchi, President, Euro-Atlantic Resilience Centre **:** „Hybrid threats in the Black Sea Region and implications for European security"
- Mr. Dan Cîmpean, National Directorate for Cyber Security, Romania: Cyber threats and their implications
- Mr Thierry Segers, Policy Officer, Directorate-General for Maritime Affairs and Fisheries, European Commission - ***online speaker:*** "EU Maritime Security Strategy"

Key take-aways:

1. the current security landscape has the ingredients for the perfect storm - -multiplication of several crisis (pandemics, energy, food, military etc.) that enter in a relation of interdependence and mutual stimulation
2. as a result, "anything can be weaponized" and the only major way forward is to enhance cybersecurity awareness, the resilience of citizens and institutions etc.
3. the next crisis will by all means imply a significant cyber component, which is low cost, high impact; however, it must be mentioned that a cyber-attack will never come alone and most likely will be accompanied by and coordinated with other types of attacks – especially in the information domain;
4. the new EU maritime strategy was also discussed, special emphasis being laid on critical infrastructure protection and changes brought forth by climate change

4.2 PANEL DEBATES AND MAIN FINDINGS

The panel discussion on *Hybrid threats in the EU's neighbourhood shaping the future of EU security* involved: Mr. Sebastian Mitrache, Ministry of Foreign Affairs, Romania; Ms. Liudmyla Buimister, Member of Parliament, Ukraine; Dr. Orlando Cenciarelli, European Centre for Disease Prevention and Control; Dr. Souzanna Sofou, Senior Research and Innovation Manager, SATWAYS.

Moderated by Dr Cristina Ivan, the session allowed participants not only to present their perceptions on hybrid threats and their future trends, but also to engage in a dialogue with each other and with workshop participants and further think of hybrid threats trends. This format led to the following conclusions:

1. Hybrid threats in Europe have the following main trends: using disinformation to lower citizen trust in state institutions, weakening purchasing chains for strategic goods and cyber operations.

2. In order to counter hybrid threats, we need an approach based on a whole of society involvement, incorporating industry, international partners and civil society, but also to develop a rapid response capacity at EU level and implementation of EU regulation at national level.
3. The use of soft power methods (e.g. political messages advanced on sports arena) to diminish trust in the Ukrainian cause, the cereal blockade enforced by Russian ships against Ukraine, the emerging disinformation campaigns in Africa (blaming the West for the lack of food stocks and prospects of famine) were other threats signalled in the hybrid spectrum against which one can only succeed in wining if and only if the response is a shared, joint and convergent one at EU level.
4. Another important domain mentioned was that of biological attacks which could become a major threat, especially when combined with online disinformation.
5. There is a distinction between hybrid threats in the North (related to critical infrastructure protection) and South of Europe (migration related).
6. As to hybrid threats attribution, speakers noted the importance of developing special AI generated algorithms that can detect recurrent aspects in seemingly unrelated events .
7. As promising evolutions in the fight against hybrid threats there were mentioned the Green Deal package and the GDPR related regulations.

4.3 TRENDS IDENTIFIED DURING BREAKOUT SESSIONS

In the second part of the FTW event, there were organised three 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	Gunhild Hoogensen Gjørv (UiT)
Breakout Session #3: Information & Strategic Communication	Rubén Arcos (URJC) Irena Chiru (MVNIA)

The breakout session # 1 - Cyber and Future Technologies, was moderated by Evaldas Bruze. Innovations discussed included:

- DLT technologies -> Financial market change (oil/gas, strategic resources, monetary power)
- AI Technologies -> content & information market change, cheap fakes, mass adoption, data economy
- Cyber offensive technologies -> EU capabilities
- Crisis of trust -> age of mass anxiety, slowdown of progress & collaboration
- Rise of decentralized businesses and infrastructures
- Quantum computation capabilities, HPC -> who first?

- Innovation maturation, uptake and operationalization speed
- Control of strategic innovation & knowledge development dissemination, access, export
- Global education and students from foreign territories
- Innovate as you go
- Adoptability by design (organization, competence, infrastructure)
- Capability to act and respond autonomously (decentralized battlefield concept)
- Future tech inclusion in primary and secondary education, issue with teachers
- Cyber attacks backed by AI, autonomous AI operations
- Cyber defence backed by AI
- Increasing collaboration with increased transparency

Participants agreed that quantum computing, cyber technologies, use of AI, social media security etc. represent instruments potentially weaponizable against democratic order and that should be approached in a security by design perspective. As features of an optimal approach, were mentioned: rapid adaptation, need to adopt emerging technologies, provide security by design formulas, digital education etc.

The breakout Session #2 was dedicated to the topic - **Resilient Civilians, Local Level and National Administration.** It was moderated by Gunhild Hoogensen Gjørv (UiT). Among the trends identified during debates, we can mention the fact that the Arctic region is likely to remain a vulnerable target for hybrid threats, due to its geographical profile which makes hybrid tactics difficult to detect (wide surface, dispersed population, severe climate conditions, limited infrastructure and reconnaissance capabilities). Northern Norway was highlighted as potentially more vulnerable due to dispersed population, low infrastructure, limited investments and Russian minority, while among the states potentially interested to expand influence in the Arctic region, most mentioned were Russia and China. Finally it was agreed that climate change, and especially melting glaciers might open a new route from China, while the new maritime route could be used to destabilize the region.

The breakout Session #3 focused on **Information and Strategic Communication.** It was moderated by Rubén Arcos (URJC) and Irena Chiru (MVNIA). During the session there was discussed the need for a multidimensional and comprehensive response to propaganda and disinformation, based on both strict regulations and self-regulatory initiatives. Among the necessary steps forward there was mentioned the need for better consolidated cooperation between state institutions and private sector, and the need to focus not only on external actors, but also those internal to democratic societies. As promising practices and regulations, participants mentioned the Digital Services Act, The Code of Practice on Disinformation Signatories, the French inter-institutional working group on the topic etc.

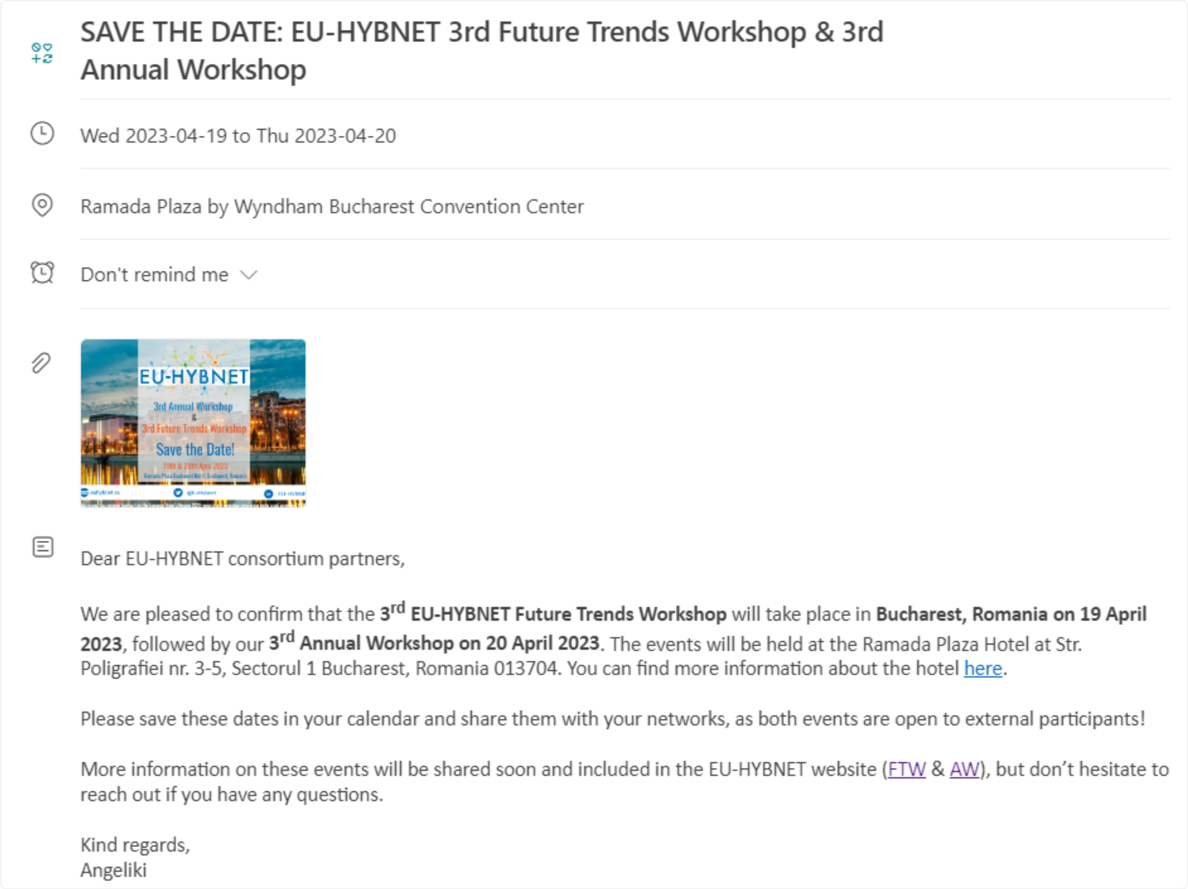
5. COMMUNICATION ACTIVITIES, PARTICIPANT'S FEEDBACK AND LESSONS LEARNT

The event was arranged as an onsite meeting taking place at the Ramada Plaza Hotel in Bucharest, Romania. The organisers determined that with Covid-19 restrictions lifted across Europe and based on the lessons learnt of previous EU-HYBNET events, a physical event was the most optimal solution that would serve the project and event objectives and allow for networking and fruitful exchanges between participants. As an exception, an option was provided for speakers to join online to be able to offer participants with several perspectives on the topic.

The event was public, and it was announced open for all interested participants from EU and Associated Countries. It was advertised on the EU-HYBNET website (https://euhybnet.eu) and social media from January 2023 onwards.

5.1 COMMUNICATION ACTIVITIES

The event planning began in September 2022. A save the date was created by EOS and shared with the EU-HYBNET consortium and network in November 2022. It was also published on the EU-HYBNET website and social media, while all partners were encouraged to share the date with their networks.



SAVE THE DATE: EU-HYBNET 3rd Future Trends Workshop & 3rd Annual Workshop

Wed 2023-04-19 to Thu 2023-04-20

Ramada Plaza by Wyndham Bucharest Convention Center

Dear EU-HYBNET consortium partners,

We are pleased to confirm that the 3rd **EU-HYBNET Future Trends Workshop** will take place in **Bucharest, Romania on 19 April 2023**, followed by our **3rd Annual Workshop on 20 April 2023**. The events will be held at the Ramada Plaza Hotel at Str. Poligrafiei nr. 3-5, Sectorul 1 Bucharest, Romania 013704. You can find more information about the hotel here.

Please save these dates in your calendar and share them with your networks, as both events are open to external participants!

More information on these events will be shared soon and included in the EU-HYBNET website (FTW & AW), but don't hesitate to reach out if you have any questions.

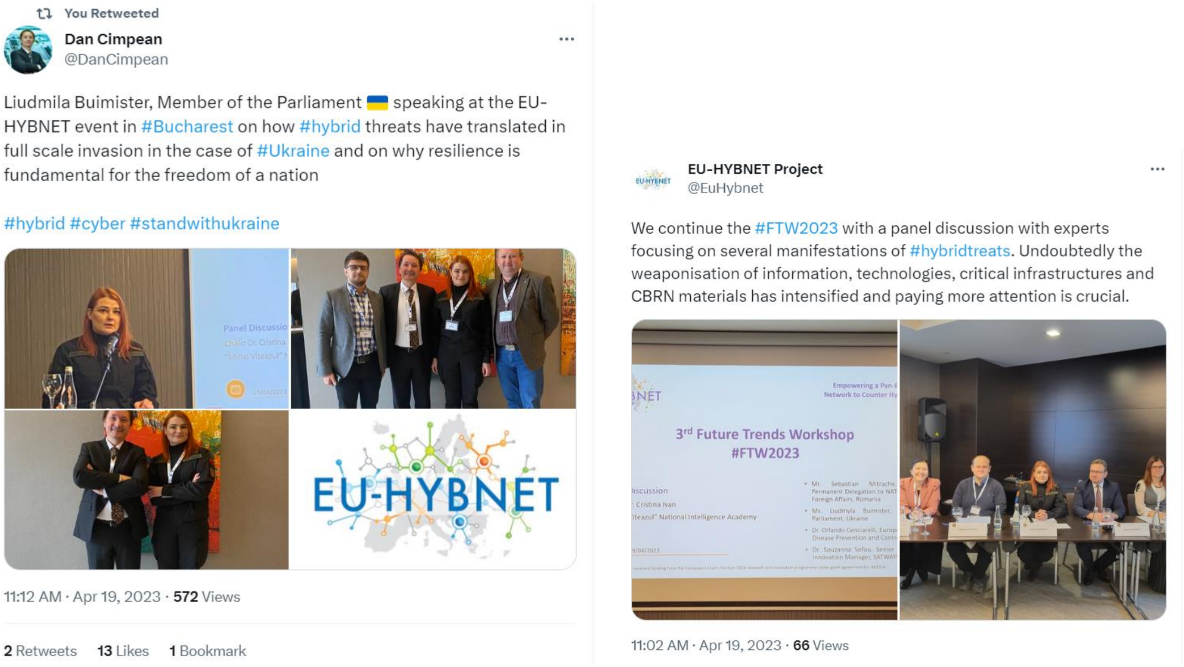
Kind regards,
Angeliki

Figure 2 3rd FTW & AW Save the date email to consortium partners

A draft agenda was created and circulated by EOS in January 2023. Registration was opened on 8 February 2023 (online through Microsoft Forms) and additional communication efforts (email, website and social media) took place at that time with an invitation being shared publicly. Continuous reminders to register were shared by EOS and other partners until the closing date of registration on 31 March 2023. The official invitation can be found in Annex IV.

Figure 3 3rd FTW Promotion Material

Communication activities continued during the event which was liveblogged by EOS on twitter. In total, 16 posts were made during the event, while all participants were encouraged to tweet about the event using the hashtag #FTW2023. After its conclusion, a first summary was shared by PPHS on Linkedin.



You Retweeted

Dan Cimpean
@DanCimpean

Liudmila Buimister, Member of the Parliament 🇺🇦 speaking at the EU-HYBNET event in #Bucharest on how #hybrid threats have translated in full scale invasion in the case of #Ukraine and on why resilience is fundamental for the freedom of a nation

#hybrid #cyber #standwithukraine

11:12 AM · Apr 19, 2023 · 572 Views

2 Retweets 13 Likes 1 Bookmark

EU-HYBNET Project
@EuHybnet

We continue the #FTW2023 with a panel discussion with experts focusing on several manifestations of #hybridtreats. Undoubtedly the weaponisation of information, technologies, critical infrastructures and CBRN materials has intensified and paying more attention is crucial.

11:02 AM · Apr 19, 2023 · 66 Views

Figure 4 Examples of 3rd FTW Twitter posts

After the event, EOS prepared a press release which was shared on the EU-HYBNET website and social media on 4 May 2023. The press release included an early overview of the key findings and trends identified during the event. It can be found in Annex IV.

Finally, EOS shared thank you emails with participants on 25 April 2023 with a reminder to fill in the satisfaction survey. The presentations given during the event were also shared with participants on 4 May 2023.

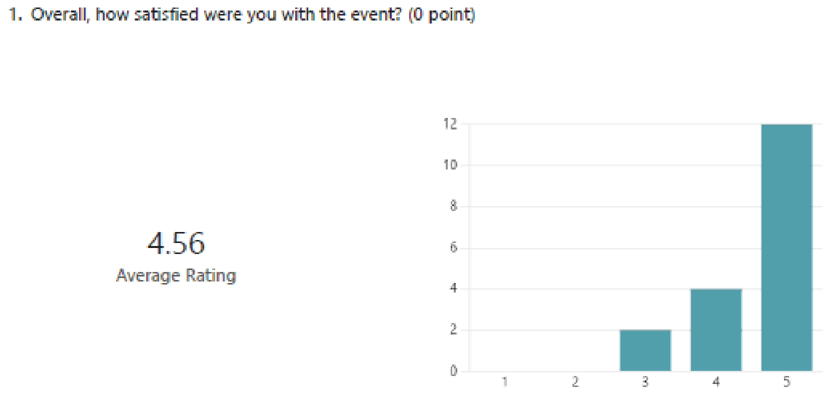
5.2 PARTICIPANTS

Participation was open to anyone, and there were no requirements for previous experience in future-oriented thinking. 87 participants from 52 organisations took part in the event. 15 EU countries were represented and 2 non-EU countries (namely Ukraine and Norway). 22 of the organization represented the academic world while 16 the practitioners' side, 9 organizations were SMEs and 5 represented NGOs. The list of participant organisations can be found in Annex II.

The participation level was deemed successful by EU-HYBNET partners, given the fact that this was the project's first event that was only held in person and not online. Additional effort will be undertaken by the network manager as a follow-up of this event to ensure that organisations new to EU-HYBNET join the network and continue their engagement and exchange with the project.

5.3 PARTICIPANTS' FEEDBACK AND LESSONS LEARNED

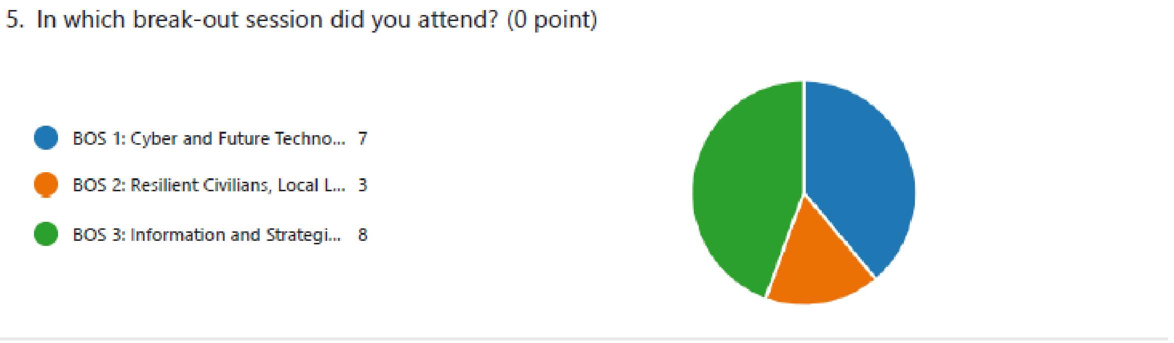
Feedback was collected immediately after the event via an anonymous online questionnaire on Microsoft Forms. QR codes linking to the questionnaires were shared with participants during the event, while a reminder was sent through email. Out of 87 participants, 18 provided feedback.



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

Figure 5 Participant satisfaction with the FTW event

Participants were overall satisfied with the event (4.56 average rating) and its content (4.39 average rating), while the keynote speeches and the panel discussions also received very high ratings (4.28 and 4.50 respectively).

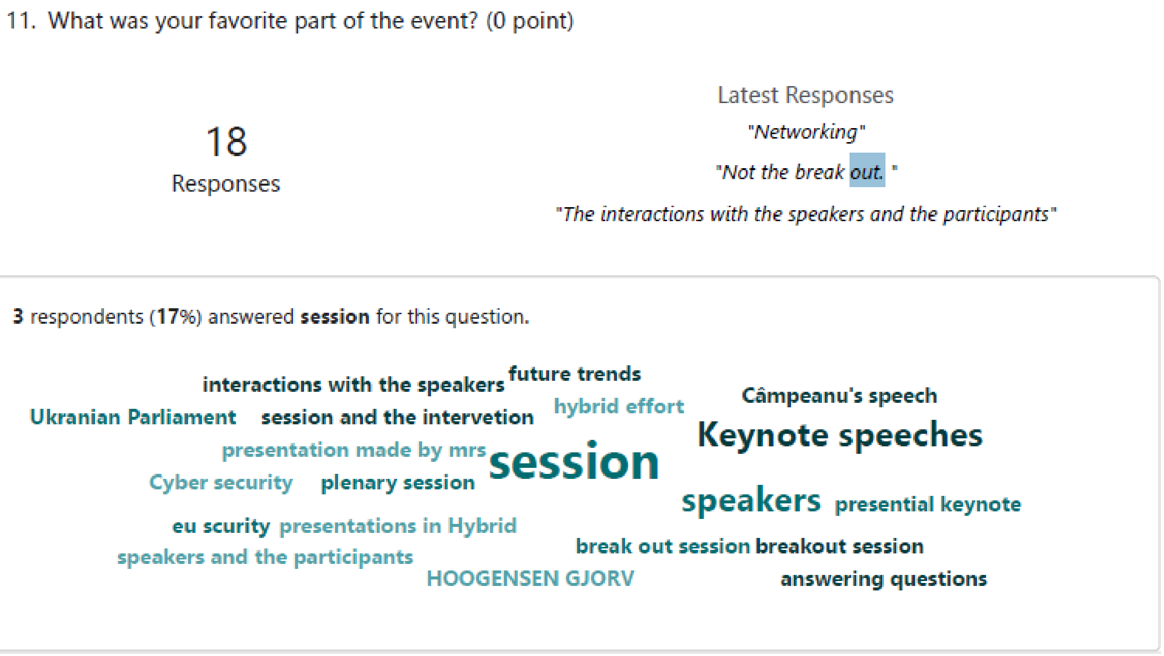


5. In which break-out session did you attend? (0 point)

Figure 6 Participation in FTW Break-out sessions

The break-out sessions received an average rating of 4.22. Participants commented the first break-out session as "Very interactive, engaging, informative and innovative", while two participants highlighted that they'd required further time for interaction and discussion. A participant in the second break-out session highlighted that more time was needed to dive into the topic and structure it better, while for the third break-out session, it was highlighted that it included "Really interesting topics with a fruitful debate. Was really good".

In general participants were also satisfied with the event arrangements (4.78 average rating), the organisation of the event (4.94 average rating) and the time dedicated to it (4.61 average rating). Based on the responses, it appears that participants were particularly satisfied with the time allowed for interaction and networking. Some respondents named the keynote speeches, some the panel and some the breakout sessions as the best parts of the event. As a result, no clear conclusion can be drawn from these responses, but it appears that impressions were in general positive.



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

18

Responses

Latest Responses

"Networking"

"Not the break out. "

"The interactions with the speakers and the participants"

3 respondents (**17**%) answered **session** for this question.

Figure 7 Word cloud depicting participants' responses regarding their favourite part of the FTW event

The weakest part for participants seemed to be the presentations made by online speakers. Some named the quality of the video, while others the lack of interaction as the reason why. There is a clear conclusion to be drawn from this: the audience seems to prefer in-person events and in-person speakers to allow for fruitful exchange of information. This comment will be taken into consideration for all EU-HYBNET future public events.

6. CONCLUSIONS AND FUTURE WORK

The 2023 EU-HYBNET Future Trends Workshop aimed to provide a platform of interaction on emerging hybrid threats in the EU's neighbourhood, their implications for the future of EU security and also potential innovations to counter them. Discussions between academics, researchers, institutional stakeholders at national and EU level, civil society representatives and practitioners were extremely useful as they allowed enhancing of awareness, shaping of new perspectives, better understanding of the interdisciplinary character of the challenges addressed while, at the same time, facilitated transfer of knowledge.

Since the landscape of hybrid threats has been continuously evolving since the beginning of the war in Ukraine, foresight and creative thinking were favoured, being considered as central for understanding, detecting and responding to emerging threats. The aim of the FTW was also to facilitate a more anticipatory and prospective outlook from the participants, to enable them collectively better understand weak signals and outliers of change in the European security environment.

The debates emphasized the pivotal importance of not only military power and detection capabilities, but also a better understanding of the adversarial tools and strategies involving weaponization of information, technology, cyberspace, critical infrastructure, energy.

Participants highlighted the role of hybrid threats in general, and of information manipulation by adversarial actors in particular, in weakening cohesion and generating polarisation across the EU and its neighbourhood. To respond to these evolutions, participants agreed there is an acute need to enhance digital and media education, foster cooperation between state and private actors, and last but not least diversify means to consolidate awareness and resilience at citizen and institutional level alike.

ANNEX I: 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

ANNEX II: LIST OF PARTICIPANT ORGANISATIONS

Nr.	Organisation	Country	Type of Organisation
1.	"Mihai Viteazul" National Intelligence Academy - MVNIA	Romania	Research/Academia
2.	University King Juan Carlos University (URJC)	Spain	Research/Academia
3.	Trust Servista	Romania	Industry – SME
4.	The University of Georgia Security Platform - UGSP	Georgia	Research/Academia
5.	RISE	Sweden	Academic/RTO
6.	National University of Political Studies and Public Administration	Romania	Research/Academia
7.	Università Cattolica del Sacro Cuore - UCSC	Italy	Research/Academia
8.	University of Dubrovnik	Croatia	Research/Academia
9.	L3CE	Lithuania	Research/Academia
10	AI – Romania	Romania	Industry – SME
11	Ukrainian Parliament	Ukraine	Public sector
12	European Centre for Disease Prevention and Control - ECDPC	EU	Research/Academia
13	National Directorate for Cyber Security	Romania	Public Sector
14	Safetech Innovations	Romania	Industry - SME
15	MET	France	Industry - SME
16	Europol Innovation Lab	EU	Public Sector
17	Helmut Schmidt University	Germany	Research/Academia
18	Mediawise Society	Romania	Civil Society
19	Polish Financial Supervision Authority PFSA	Poland	Public Sector
20	The Arctic University of Norway - UiT	Norway	Research/Academia
21	VOST Europe	EU	Civil Society
22	ABW	Poland	Practitioner
23	Laurea University of Applied Sciences	Finland	Academic/RTO
24	MALDITA	Spain	Civil Society/ NGO
25	SINTEF Digital	Norway	Research/Academia
26	MFA	Netherlands	Public sector
27	Maltego Technologies GmbH	Germany	Industry - SME
28	University of Bucharest	Romania	Research/Academia
29	Centre for Security Studies - KEMEA	Greece	Academic/RTO
30	EC-JRC	Belgium	Academic/RTO
31	EU Institute for Security Studies - EUISS	EU	Public sector
32	City of Espoo	Finland	Public sector
33	Netherlands Organisation for Applied Scientific Research - TNO	Netherland	Academic/RTO
34	Smartlink Communication	Romania	Civil Society
35	Ministry of Economy	Romania	Public Sector
36	Polish Platform for Homeland Security	Poland	Civil Society/ NGO
37	EEAS	Belgium	Public sector

38	Romanian Intelligence Service	Romania	Public sector
39	Global Initiative against Transnational Organised Crime - GI-TOC	Romania	Research/Academia
40	Satways Ltd	Greece	Industry - SME
41	Institute of Information and Communication Technologies	Bulgaria	Research/Academia
42	SDPD- EEAS	Belgium	Research/Academia
43	ANATASE COMPANY	France	Industry - SME
44	International Centre for Defence and Security - ICDS	Estonia	Research/Academia
45	European Organization for Security - EOS	Belgium	Industry - SME
46	Ministry of Defence	Netherlands	Practitioner
47	NATO JFCBS	Netherlands	Practitioner
48	UBM	Germany	Practitioner
49	Global Focus Centre	Romania	Industry - SME
50	SPP	Romania	Practitioner
51	E-ARC	Romania	Research/Academia
52	Ministry of Foreign Affair	Romania	Public Sector

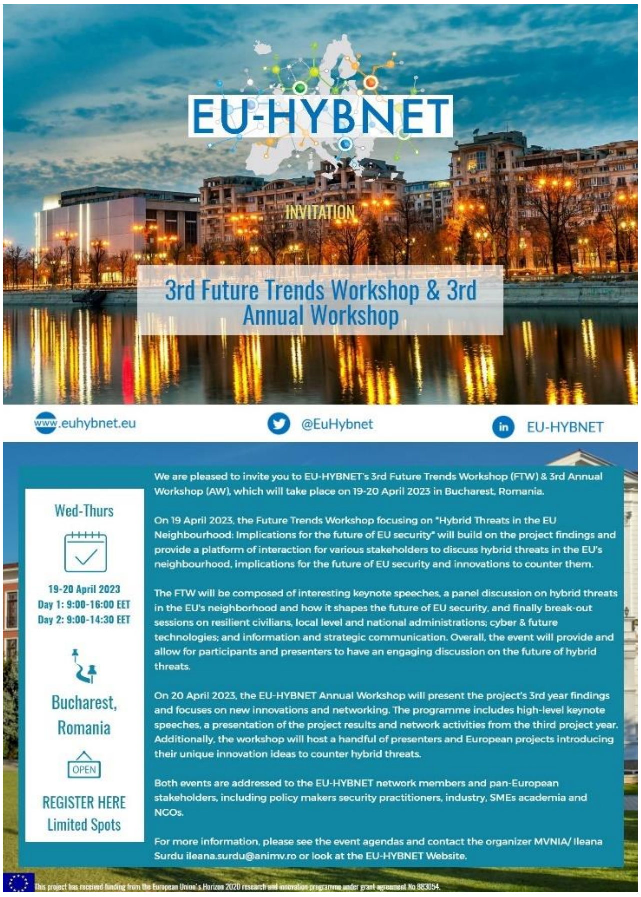
ANNEX III: WORKSHOP AGENDA

AGENDA

Time EEST	Topic	Speaker
08.30-09.00	Registration	
Plenary session (Room: Ramada Europe)		
09.00-09.15	Welcome & Practical Information	Dr. Päivi Mattila, EU-HYBNET Coordinator, Laurea Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy
09.15-09.30	**Keynote Speech #1:** „Hybrid threats in the Black Sea Region and implications for European security”	Mr. Ovidiu Raetchi, President, Euro-Atlantic Resilience Centre
09.30-09.45	**Keynote Speech #2**	Mr. Dan Cîmpean, National Directorate for Cyber Security, Romania
09:45-10:00	**Keynote Speech #3:** “EU Maritime Security Strategy”	Mr Thierry Segers, Policy Officer, Directorate-General for Maritime Affairs and Fisheries, European Commission - ***online speaker***
10:00-10:15	Audience Q&A	***Moderator:*** *Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea*
10:15-10:35	Coffee Break *(at Foyer Plaza)*	
10:35 – 12:00	**Panel Discussion:** Hybrid threats in the EU’s neighbourhood shaping the future of EU security	***Chair:*** *Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy* ***Panel speakers:*** • Mr. Sebastian Mitrache, Ministry of Foreign Affairs, Romania • Ms. Liudmyla Buimister, Member of Parliament, Ukraine • Dr. Orlando Cenciarelli, European Centre for Disease Prevention and Control • Dr. Souzanna Sofou, Senior Research and Innovation Manager, SATWAYS
12:00 – 13:15	Lunch Break *(at Red Pepper)*	
Parallel Breakout Sessions		
13:15-14:45	**Breakout Session #1:** Cyber & Future Technologies *Room: Ramada Africa*	Evaldas Bruze (L3CE)
	Breakout Session #2: Resilient Civilians, Local Level and National Administration *Room: Ramada Asia*	Gunhild Hoogensen Gjørv (UiT)
	Breakout Session #3: Information & Strategic Communication *Room: Ramada Europa*	Rubén Arcos (URJC) Irena Chiru (MVNIA)

14:45-15:00	Coffee Break *(at Foyer Plaza)*	
15:00-15:30	**Panel Discussion:** Future Trends for EU security	***Chair:*** *Mr. Isto Mattila, EU-HYBNET Innovation Manager, Laurea* ***Panel speakers:*** • Evaldas Bruze (L3CE) • Gunhild Hoogensen Gjørv (UiT) • Dr. Rubén Arcos (URJC)
15:30-15:45	Audience Q&A	
15:45 - 16.00	**Closing Keynote Speech:** The role of the Common Information Sharing Environment (CISE) for EU Maritime Security	Mr. Gianluca Luraschi, Project Officer, Department 2 - Safety, Security and Surveillance at European Maritime Safety Agency (EMSA)
16.00-16.05	Closing remarks	Dr. Cristina Ivan, Mihai Viteazul National Intelligence Academy

ANNEX IV: FUTURE TRENDS WORKSHOP PROMOTIONAL MATERIALS



EU-HYBNET

INVITATION

3rd Future Trends Workshop & 3rd Annual Workshop

www.euhybnet.eu

@EuHybnet

EU-HYBNET

Wed-Thurs

19-20 April 2023
Day 1: 9:00-16:00 EET
Day 2: 9:00-14:30 EET

Bucharest, Romania

OPEN

REGISTER HERE
Limited Spots

We are pleased to invite you to EU-HYBNET's 3rd Future Trends Workshop (FTW) & 3rd Annual Workshop (AW), which will take place on 19-20 April 2023 in Bucharest, Romania.

On 19 April 2023, the Future Trends Workshop focusing on "Hybrid Threats in the EU Neighbourhood: Implications for the future of EU security" will build on the project findings and provide 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.

The FTW will be composed of interesting keynote speeches, a panel discussion on hybrid threats in the EU's neighborhood and how it shapes the future of EU security, and finally break-out sessions on resilient civilians, local level and national administrations; cyber & future technologies; and information and strategic communication. Overall, the event will provide and allow for participants and presenters to have an engaging discussion on the future of hybrid threats.

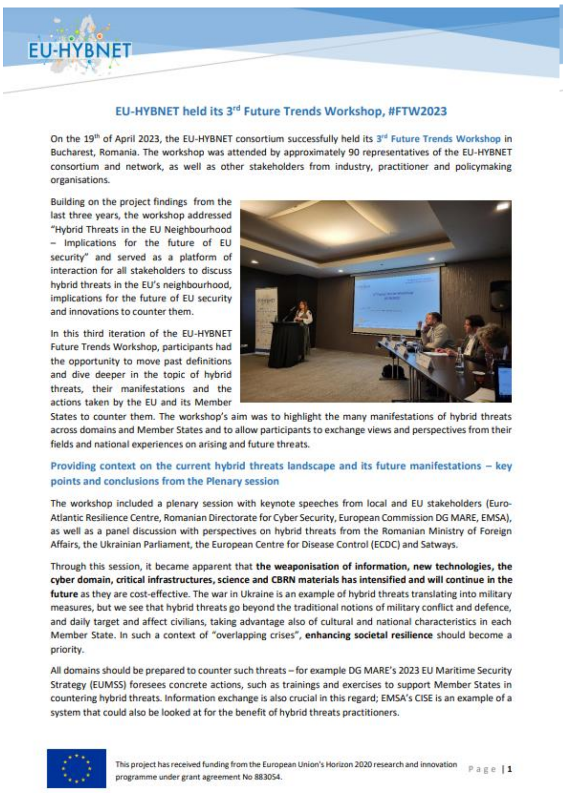
On 20 April 2023, the EU-HYBNET Annual Workshop will present the project's 3rd year findings and focuses on new innovations and networking. The programme includes high-level keynote speeches, a presentation of the project results and network activities from the third project year. Additionally, the workshop will host a handful of presenters and European projects introducing their unique innovation ideas to counter hybrid threats.

Both events are addressed to the EU-HYBNET network members and pan-European stakeholders, including policy makers security practitioners, industry, SMEs academia and NGOs.

For more information, please see the event agendas and contact the organizer MVNIA/ Ileana Surdu ileana.surdu@animv.ro or look at the EU-HYBNET Website.

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

Figure 8 3rd FTW Invitation



EU-HYBNET

EU-HYBNET held its 3rd Future Trends Workshop, #FTW2023

On the 19th of April 2023, the EU-HYBNET consortium successfully held its 3rd Future Trends Workshop in Bucharest, Romania. The workshop was attended by approximately 90 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations.

Building on the project findings from the last three years, the workshop addressed "Hybrid Threats in the EU Neighbourhood – Implications for the future of EU security" and served as a platform of interaction for all stakeholders to discuss hybrid threats in the EU's neighbourhood, implications for the future of EU security and innovations to counter them.

In this third iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and dive deeper in the topic of hybrid threats, their manifestations and the actions taken by the EU and its Member States to counter them. The workshop's aim was to highlight the many manifestations of hybrid threats across domains and Member States and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

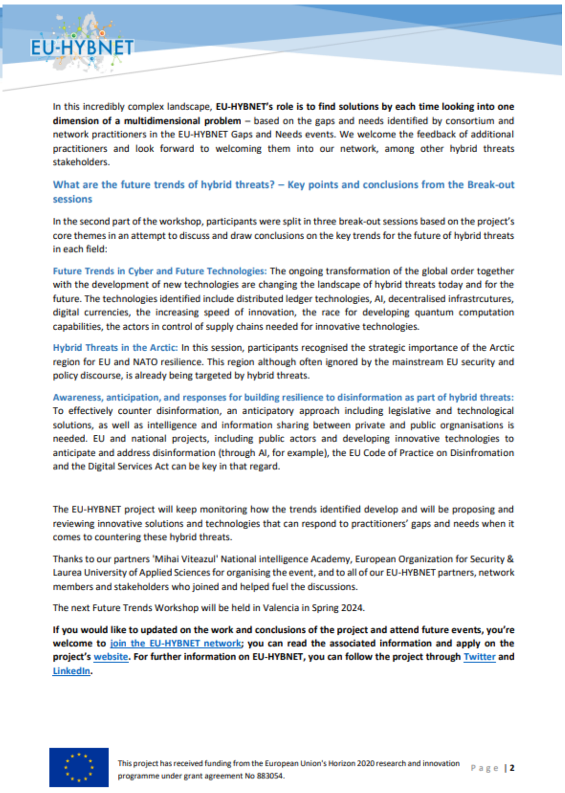
Providing context on the current hybrid threats landscape and its future manifestations – key points and conclusions from the Plenary session

The workshop included a plenary session with keynote speeches from local and EU stakeholders (Euro-Atlantic Resilience Centre, Romanian Directorate for Cyber Security, European Commission DG MARE, EMSA), as well as a panel discussion with perspectives on hybrid threats from the Romanian Ministry of Foreign Affairs, the Ukrainian Parliament, the European Centre for Disease Control (ECDC) and Satways.

Through this session, it became apparent that **the weaponisation of information, new technologies, the cyber domain, critical infrastructures, science and CBRN materials has intensified and will continue in the future** as they are cost-effective. The war in Ukraine is an example of hybrid threats translating into military measures, but we see that hybrid threats go beyond the traditional notions of military conflict and defence, and daily target and affect civilians, taking advantage also of cultural and national characteristics in each Member State. In such a context of "overlapping crises", **enhancing societal resilience** should become a priority.

All domains should be prepared to counter such threats – for example DG MARE's 2023 EU Maritime Security Strategy (EUMSS) foresees concrete actions, such as trainings and exercises to support Member States in countering hybrid threats. Information exchange is also crucial in this regard; EMSA's CISE is an example of a system that could also be looked at for the benefit of hybrid threats practitioners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054. Page | 1



EU-HYBNET

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by each time looking into one dimension of a multidimensional problem** – based on the gaps and needs identified by consortium and network practitioners in the EU-HYBNET Gaps and Needs events. 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 in three 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 hybrid threats in each field:

Future Trends in Cyber and Future Technologies: The ongoing transformation of the global order together with the development of new technologies are changing the landscape of hybrid threats today and for the future. The technologies identified include distributed ledger technologies, AI, decentralised infrastrcutures, digital currencies, the increasing speed of innovation, the race for developing quantum computation capabilities, the actors in control of supply chains needed for innovative technologies.

Hybrid Threats in the Arctic: In this session, participants recognised the strategic importance of the Arctic region for EU and NATO resilience. This region although often ignored by the mainstream EU security and policy discourse, is already being targeted by hybrid threats.

Awareness, anticipation, and responses for building resilience to disinformation as part of hybrid threats: To effectively counter disinformation, an anticipatory approach including legislative and technological solutions, as well as intelligence and information sharing between private and public orgnanisations is needed. EU and national projects, including public actors and developing innovative technologies to anticipate and address disinformation (through AI, for example), the EU Code of Practice on Disinfromation and the Digital Services Act can be key in that regard.

The EU-HYBNET project will keep monitoring how the trends identified develop and will be proposing and reviewing innovative solutions and technologies that can respond to practitioners' gaps and needs when it comes to countering these hybrid threats.

Thanks to our partners 'Mihai Viteazul' National intelligence Academy, European Organization for Security & Laurea University of Applied Sciences for organising the event, and to all of our EU-HYBNET partners, network members and stakeholders who joined and helped fuel the discussions.

The next Future Trends Workshop will be held in Valencia in Spring 2024.

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 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 | 2

Figure 9 3rd FTW Press Release