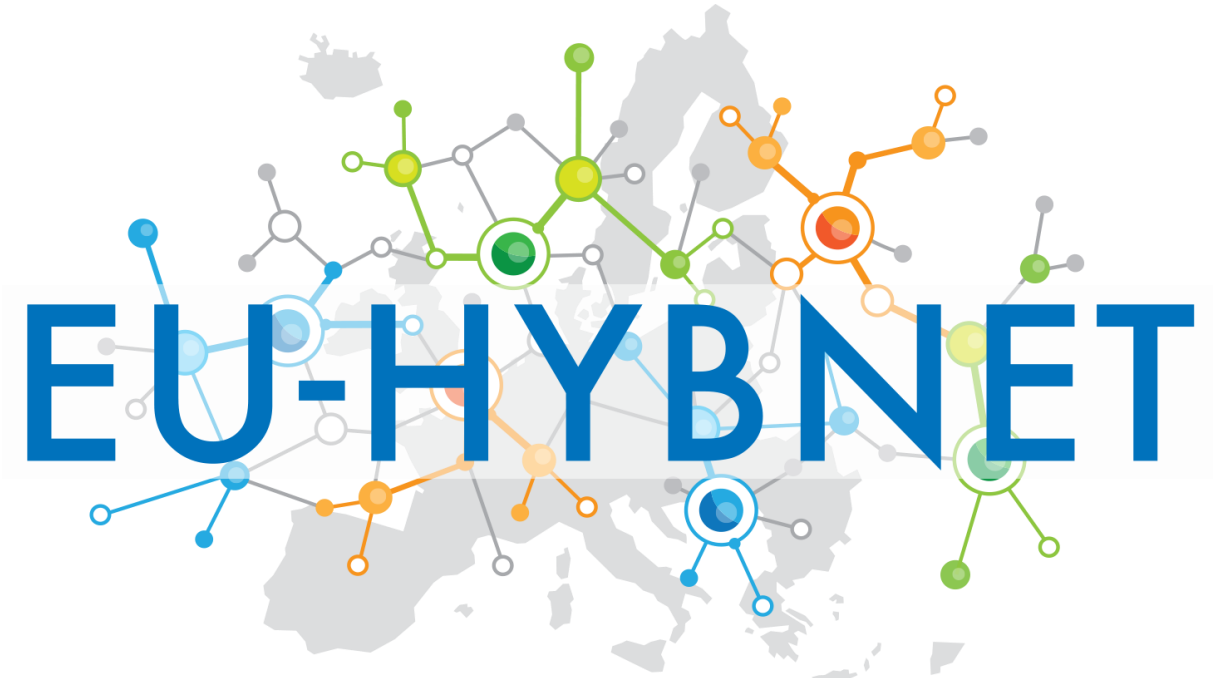


# FIRST INNOVATION AND KNOWLEDGE EXCHANGE EVENT REPORT

DELIVERABLE 3.11

Lead Author : European Organisation for Security (EOS)

Contributors : All

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

# D3.11 FIRST INNOVATION AND KNOWLEDGE EXCHANGE EVENT REPORT

| | | |
|---|---|---|
| **Deliverable number** | **D3.11** | |
| **Version:** | **V 0.7** | |
| **Delivery date:** | **M10** | |
| **Dissemination level:** | **Public (PU)** | |
| **Classification level:** | **PU** | |
| **Status** | **Ready** | |
| **Nature:** | **Report** | |
| **Main authors:** | **Elodie Reuge, Maria Chiara Properzi** | **EOS** |
| **Contributors:** | **Rick Meessen** | **TNO** |
| | **Souzana Sola** | **Satways** |
| | **Isto Mattila, Päivi Mattila** | **Laurea** |

## DOCUMENT CONTROL

| Version | Date | Authors | Changes |
|---|---|---|---|
| V0.1 | 29/01/2021 | EOS/ Elodie Reuge, Maria Chiara Properzi | First document draft |
| V0.2 | 08/02/2021 | TNO/ Rick Meessen | Review and text editing |
| V0.3 | 08/02/2021 | LAUREA/ Päivi Mattila | Review and text editing |
| V0.4 | 10/02/2021 | Satways/ Souzana Sola | Review |
| V0.5 | 09/02/2021 | EOS/ Elodie Reuge, Maria Chiara Properzi | Text editing and final draft |
| V0.6 | 15/02/2021 | Laurea/ Isto Mattila, EU-HYBNET Innovation Manager | Review |
| V0.7 | 16/02/2021 | Laurea/ Päivi Mattila | Final review and final editing, document submission to EC |

## DISCLAIMER

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

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

© Copyright in this document remains vested in the Project Partners

## TABLE OF CONTENT



## TABLES

## FIGURES

# 1. INTRODUCTION

## 1.1 OVERVIEW

EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) project aims at enriching the existing European networks countering hybrid threats and at ensuring long term sustainability, by identifying European practitioners' and other relevant actors in the field of hybrid threats common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities or research, innovation and training endeavours concerning hybrid threats.

Deliverable D3.11 provides a general overview of the First Innovation and Knowledge Exchange Workshop, #IKEW, which was held virtually on the 19th of January 2021.

This first #IKEW introduced participants to the EU-HYBNET project, its existing network and the European Commission's interest to extend the network as a Pan-European hybrid platform for Member States' needs. It aimed to provide practitioners, industry, SMEs, and academia an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to answer them.

The event focused on the EU-HYBNET core themes which are:

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

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

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

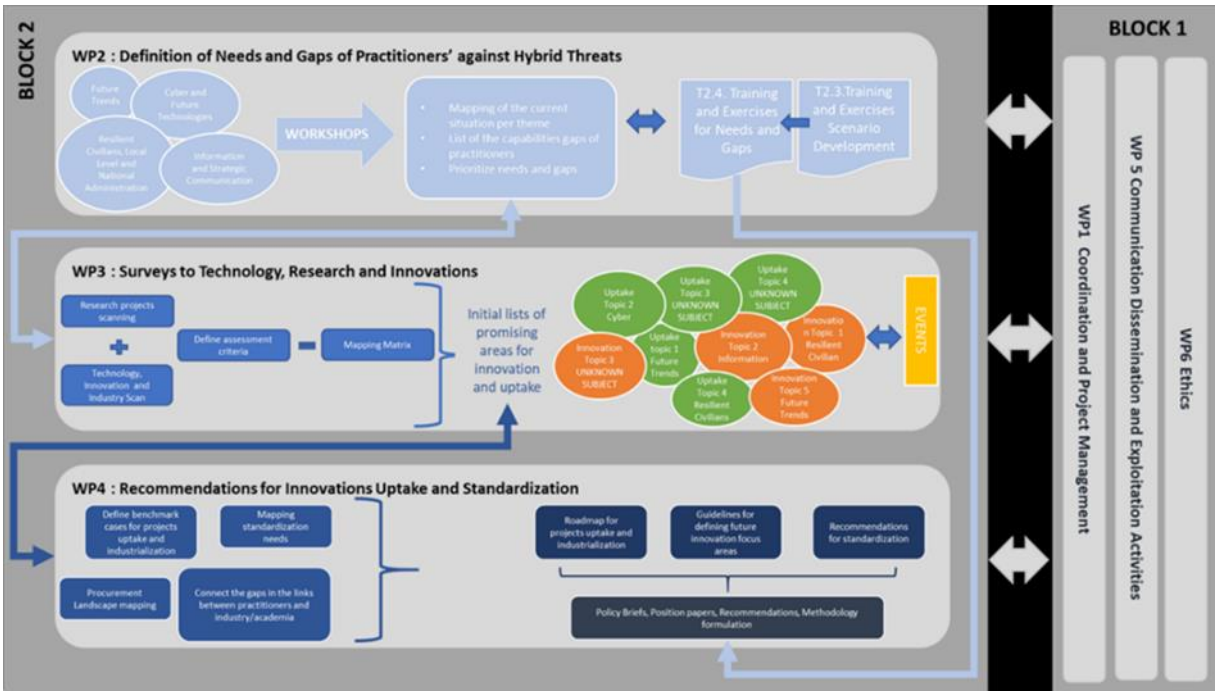


**Figure 1 : EU-HYBNET Structure of Work Packages and Main Activities**

The organisation of the IKEWs are directly linked to **project Objective (OB) 1**: *To enrich existing network for countering hybrid threats and ensure long term sustainability,* and supports project **OB 5**: *To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network*, **OB 6**: *To foster capacity building and knowledge exchange on countering hybrid threats* and **OB 7:** *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 amount of events organised, which was set to a minimum 3 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<br>-Innovation arena (IA) and Web site are in use by at least 4 forums (see KPI for Goal 5.1) |
| **OB6: To foster capacity building and knowledge exchange on countering hybrid threats** | | | |
| **Goal** | | **KPI description** | **KPI target value** |
| 6.1 | To arrange dialogue sessions for EU practitioners, industry, SME and academic actors to strengthen capacity and hybrid threat knowledge exchange | Events are organised to communicate the new hybrid threat knowledge; and on latest best practices | -At least three yearly events are executed with a minimum of 100 participants each time |
| **OB7. To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats** | | | |
| **Goal** | | **KPI description** | **KPI target value** |
| 7.2 | To empower European practitioners, industry, SME and academic actors to recognise important innovations/trends | Events are organised on innovations and future trends | -At least 2 events yearly where information on innovations and future trends is shared |
| 7.5 | To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically | Events are structured to facilitate interactions among stakeholders to establish synergies | -At least 2 events yearly where over 100 actors will meet<br>- Newsletter, published every 6 months w. 60 new readers yearly |

In terms of Milestones (MS), the MS 11 (below) is also directly linked to the organization of the cycle of IKEWs.

**Table 2 : EU-HYBNET MS 21**

| Milestone No. | Milestone name | Related WPs | Due project month | Means of verification | Progress |
|---|---|---|---|---|---|
| 21 | Cycle of Innovation and Knowledge exchange events is started | all | 9 | Cycle of Innovation and Knowledge exchange events is started | 1 |

## 1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 2: Overview of the event
- Section 3: Content of the workshop
- Section 4: Assessment of the event and global outcome
- Section 5: Registration and attendance
- Section 6: Logistics and organisation
- Section 7: Conclusion
- Section 8: Annexes

# 2. OVERVIEW OF THE EVENT

## 2.1 OBJECTIVES OF THE INNOVATION KNOWLEDGE AND EXCHANGE WORKSHOPS

The objective of the Innovation Knowledge and Exchange Workshops (#IKEW) is to facilitate the exchange of knowledge and of information about innovations to increase the likelihood of future uptake.

It allows practitioners to become aware of innovation possibilities via the EU-HYBNET project and network activities. For the first event organised, the following outputs will be used to create a mapping matrix of gaps/needs and research/innovations:

- Definition of target areas for improvement and innovations.
- Technology and innovation watch.
- Ongoing research project initiatives watch.

Each of the three 'Innovation and Knowledge Exchange' events will have different themes. However, all #IKEW will maintain adherence to the project's four core themes and will facilitate the continuous mapping of needs, monitoring of solutions, and providing a forum where practitioners can engage with innovation providers.

Innovation providers are invited to explain and demonstrate their innovative solutions that align with the event theme and to interact with practitioners. Meetings will involve key personnel from organisations involved in countering hybrid threats.

Knowledge transfer will be incorporated in several ways: peer-to-peer practitioners learning, learning from EU MS national actors, and through workshops. Meetings will involve key personnel within organisations involved in measures against hybrid threats.

During each event organized, EU-HYBNET partners will organize time for interaction between industry, academia, and relevant participants outside of the consortium, to objectively assess the feasibility of the projects activities and findings.

## 2.2 WORKSHOP AGENDA

Initially planned in physical presence, the 1st Innovation workshop of EU-HYBNET project has been held as a full day online event, on the 19th of January, due to the consequences of COVID-19 travel restrictions. The agenda of the day is presented below, while a better overview of the agenda is provided in the Annex I, where the final leaflet is inserted.

**Table 3 : Agenda of the 1st Innovation Knowledge and Exchange Event**

| Time | Topic | Speaker(s) |
|---|---|---|
| 10.00-10.10 | Opening remarks | Mr. Paolo Venturoni, CEO, EOS. |
| 10.10-10.20 | Welcome & Introduction | Dr. Päivi Mattila, the Director of Security Research Program Laurea, EU-HYBNET Coordinator. |
| 10.20-11.00 | Intervention on the EU policy framework on hybrid threats<br>Q&A | Mr. Maciej Szymański, Policy Officer, DG DEFIS, European Commission.<br>Mr. Max Brandt, Policy Officer, DG HOME, European Commission. |
| 11.00-11.05 | **Break** | |
| 11.05-11.45 | Towards new preparedness: comprehensive and multinational approach to counter Hybrid Threats<br>Q&A | Dr. Hanna Smith,<br>Director of Research and Analysis Hybrid CoE. |
| 11.45-12.15 | Critical gaps and needs in knowledge and performance in relation to innovations.<br>Q&A | Dr. Rick Meessen, Principal Advisor Defence, Safety and Security, TNO. |
| 12.15-13.00 | **Lunch** | |
| 13.00-14.30 | **Roundtable I**<br>*Industry view to innovations answering Pan-European practitioners and other relevant stakeholders' needs countering hybrid threats, in relation to:*<br>•*Resilient civilians, local level, and administration*<br>•*Cyber and future technologies*<br>•*Information and strategic communications*<br>•*Future trends of Hybrid Threats* | Moderators:<br>Ms. Maria Chiara Properzi, Policy Manager, EOS and Ms. Elodie Reuge, Crisis Management Project Manager.<br>Speakers :<br>• • Mr. Antoine-Tristan Mocilnikar, General Mining Engineer, (Ministère de la Transition, écologique, France).<br>• • Mr. Radu Pop, Head of Infrastructures and Frontier Security Solutions Sales, (Airbus)<br>• • Dr. Shahid Raza, Director of Cybersecurity Unit, (Research Institutes of Sweden – RISE). |
| 14.30-14.40 | **Break** | |
| 14.40-16.10 | **Roundtable II**<br>*Unknown threats and low-technology threats – status of the art, and future challenges, in relation to:*<br>•*Resilient civilians, local level, and administration*<br>•*Cyber and future technologies*<br>•*Information and strategic communications*<br>•*Future trends of Hybrid Threats* | Moderators:<br>Ms. Elodie Reuge, Crisis Management Project Manager and Ms. Maria Chiara Properzi, Policy Manager.<br>Speakers :<br>• • Mr Athanasios Grigoriadis, Senior Cyber Security Expert, Kentro Meleton Asfaleias (KEMEA).<br>• • Mr. Vito Morreale, Director of the Industry and Security Technology, Research, and Innovation (IS3), Lab, (Engineering).<br>• • Dr. Rubén Arcos Martín, Lecturer, and Researcher of Communication sciences (Universidad Rey Juan Carlos). |
| 16.10-16.20 | **Break** | |
| 16.20-17.00 | Closing remarks & Wrap Up | Mr. Isto Mattila, RDI director Laurea, EU-HYBNET Innovation Manager. |

# 3. CONTENT OF THE WORKSHOP

## 3.1 PRESENTATIONS

As clearly reflected in the agenda, the day was divided into three parts:

- Morning session with EU-HYBNET related presentations, and institutional presentations.
- Afternoon session with two roundtables discussions.
- Closing remarks and Wrap Up.

### 3.1.1 MORNING SESSION

A series of speakers were mobilized to present a selected list of topics:

- Mr. Paolo Venturoni, who is the CEO of EOS – the partner in charge of the organisation of the first IKEW, opened the day giving opening remarks.
- Dr. Päivi Mattila, Director of Security research Program in Laurea and EU-HYBNET coordinator, presented the Welcome and introductory words of this first IKEW.
- A first presentation about the "Intervention on the EU policy framework on hybrid threats" was delivered by Mr. Maciej Szymański, Policy Officer, DG DEFIS, European Commission Mr. Max Brandt, Policy Officer, DG HOME, European Commission.
- Dr.Hanna Smith, Director of Research and Analysis at Hybrid CoE, presented "The extension of the European Network against hybrid threats and its sustainability" ;
- Dr. Rick Meessen, Principal Advisor Defence, Safety and Security at TNO, gave the final presentation of the morning on the following subject: "Critical gaps and needs in knowledge and performance in relation to innovations".

Each presentation in the morning session was followed by a Q&A session where the floor was opened to the audience.

### 3.1.2 AFTERNOON SESSION

The afternoon session was organised around two roundtables discussions.

#### 3.1.1.1 FIRST ROUNDTABLE

The Roundtable I, moderated by Maria Chiara Properzi and Elodie Reuge from EOS, had as main subject: Industry view to innovations answering pan-European practitioners and other relevant stakeholders' needs countering hybrid threats, in relation to:

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

The speakers invited in the first roundtables were:

• Mr. Antoine-Tristan Mocilnikar, General Mining Engineer, (Ministère de la Transition, écologique, France).

• Mr. Radu Pop, Head of Infrastructures and Frontier Security Solutions Sales, (Airbus)

• Dr. Shahid Raza, Director of Cybersecurity Unit, (Research Institutes of Sweden – RISE).

#### 3.1.1.2 SECOND ROUNDTABLE

The Roundtable II, moderated by Maria Chiara Properzi and Elodie Reuge from EOS, has as main subject: Unknown threats and low-technology threats – status of the art, and future challenges, in relation to:

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

The speakers invited in the second roundtable were:

• Mr Athanasios Grigoriadis, Senior Cyber Security Expert, Kentro Meleton Asfaleias (KEMEA).

• Mr. Vito Morreale, Director of the Industry and Security Technology, Research, and Innovation (IS3), Lab, (Engineering).

• Dr. Rubén Arcos Martín, Lecturer, and Researcher of Communication sciences (Universidad Rey Juan Carlos).

## 3.2 MAIN RESULTS OF THE DISCUSSION

As already explained in the previous section, the day was divided into several three parts which will also be reflected in the main results of the discussion.

### 3.2.1 MORNING SESSION

#### 3.2.1.1 OPENING REMARKS AND WELCOME WORDS

#IKEW started with the opening remarks by **Mr. Paolo Venturoni**, CEO of the European Organisation for Security (EOS), who stressed the importance of cooperating to counter hybrid threats. Following the opening remarks, **Dr. Päivi Mattila**, who acts as the EU-HYBNET Coordinator.

#### 3.2.1.2 INTERVENTION ON THE EU POLICY FRAMEWORK ON HYBRID THREATS

After the project introduction, Mr. Maciej Szymański, Policy Officer at DG DEFIS, and Mr. Max Brandt, Policy Officer at DG HOME, provided relevant insights on the EU policy framework on hybrid threats.

Mr. **Szymański** presented the main principles of the EU response for countering hybrid threats (e.g., "connecting the dots" principle, promotion of the whole-of-government/whole-of-society approach), the main actors of the EU framework and the main pillars for countering hybrid threats.

During his presentation, **Mr. Brandt** underlined the importance of considering innovation as a strategic tool to counter hybrid threats and to anticipate both future risks and opportunities and presented the domains covered under the Security research programme. Mr. Brandt concluded by highlighting the importance, from the EC's perspective, of having a practitioners-network like EU-HYBNET to foster the discussion in the coming years and to have a comprehensive overview of the different dimensions to effectively decide where to allocate available funds.

Among the questions addressed to the presenters, one focused on whether the EC sees disinformation, fake-news, and critical information as a part of critical infrastructures and a possible tool for Hybrid attack.

According to Mr. Brandt, the EC has not addressed the issue of fake-news and disinformation from the research side yet. Therefore, in Horizon Europe it will be crucial to look at these issues much more since they can have devastating potential and they are low cost means for the attacker.

According to Mr. Szymański there is no link between critical infrastructures protection and fake-news or disinformation if we just look at legislation. However, if we look at the COVID-19 disinformation the link is clear. Therefore, having this awareness the EC is trying to address this kind of situation.

#### 3.2.1.3 TOWARDS NEW PREPARDNESS: COMPREHENSIVE AND MULTINATIONAL APPROACH TO COUNTER HYBRID THREATS

**Dr. Hanna Smith**, Director of Research and Analysis at the European Centre of Excellence for Countering Hybrid Threats, introduced the 21st-century security environment and underlined the need for the EU to foster its own resilience by adopting a comprehensive and multinational approach. Specifically, this means considering the whole society and all its different domains while looking at new innovations and solutions for fostering and building resilience. Secondly, in a comprehensive and multinational approach, responses are comprehensive and integrated, meaning that civil society organisations, NGOs, volunteer organisations, the private sector etc. need to be considered as being part of the resilience-building and countering activities. Dr. Smith concluded by underlying that in the context of EU-HYBNET the above-mentioned comprehensive and multinational approach is central. In fact, the project will include actors in the fields of comprehensive security at local, regional, national, and international levels across the EU.

Among the questions addressed to the presenter, one focused on how to increase the involvement in the field of security of actors from other areas to implement a holistic approach.
According to Dr. Smith, this can be done through case-studies that show how security issues pose direct challenges to different types of domains, like culture or health care.

#### 3.2.1.4 CRITICAL GAPS AND NEEDS IN KNOWLEDGE AND PERFORMANCE IN RELATION TO INNOVATIONS

**Dr. Rick Meessen**, Principal Advisor Defence, Safety and Security, TNO, began his presentation by highlighting the wide variety of domains affected by hybrid threats (e.g., diplomacy, cyber, information, economy, culture, societal, political etc.). After that, the presenter stressed the importance of identifying gaps and needs and monitoring the development in research and innovation activities and introduced the mapping-process methodology developed within the EU-HYBNET project. This methodology (push-pull methodology) is based on the interaction between two different sides: demand (pull) and supply (push). For each core theme the methodology results in identifying vulnerabilities, capability gaps and needs in the demand side, and the related ideas for solutions and innovations in the supply side. Finally, some preliminary analysis' results were presented, related to the type of solutions and innovations identified so far.

### 3.2.2 AFTERNOON SESSION

The event was followed by two compelling round-table conversations, each of them with three speakers and, respectively, with **Ms. Maria Chiara Properzi,** Policy Manager from EOS and **Ms. Elodie Reuge**, Crisis Management Project Manager, as moderators.

#### 3.2.2.1 1ST ROUNDTABLE

The core theme of the first round-table conversation was the industry view to innovations answering Pan European practitioners and other relevant stakeholders' needs countering hybrid threats in relation to four topics: resilient civilians, both local level and administration, cyber and future technologies, information and strategic communications and future trends of hybrid threats.
**Mr. Antoine-Tristan Mocilnikar**, General Mining Engineer at the French Ministry of Ecological Transition, was the first speaker. Mr. Mocilnikar firstly stressed the need not to focus exclusively on prevention within the standardization process and introduced the management of hybrid threats through active scenarios, which is based on alert, detection, and preparation of crisis management (AI models to produce different scenarios before the crisis start). In a second moment, the presenter focused on legal, ethic and conformity issues and reminded that in the EU-HYBNET project ethic needs to be at the center.

The second speaker was **Mr. Radu Pop**, Head of Infrastructures and Frontier Security Solutions Sales at Airbus, who explained why a company could feel itself as a target for hybrid threats. Airbus, for instance, feels itself as a target for hybrid threats as it is both a security, civilian and a military company, as well as both a threat and security provider in the field of hybrid threats. In a second moment, the presenter focused specifically on the ways for a company to deal with cyber-attacks. In this regard, Airbus created a cyber division, thus turning the threat into an opportunity. This experience proves that sometimes being a target may make you better react and start building capabilities that can become an opportunity.

The third speaker was **Dr. Raza**, Director of the Cybersecurity Unit at the Research Institutes of Sweden (RISE). The presenter introduced the current cybersecurity landscape and focused specifically on the three cybersecurity pillars (confidentiality, integrity, availability), as well as on the main threat and security actors and on their respective goals. The speaker also addressed the issue of emerging threats and trends, such as adversarial AI as a hybrid threat and IoT and cloud technology in critical infrastructures and emphasized the existence of two defence sides: defence and offence mechanisms. In this regard, it is important to underline that in the cyberspace offensive tools are mostly used for training and strengthening defence.

**Questions to the speakers:**

Among the questions addressed to the speakers, one focused on the potential need for more standards and legislation to protect industry against hybrid threats.
On this point, Mr. Pop believes that it does help to regulate, especially in the legislation part of what is really a threat or how to define an attack or the consequences of an attack (criminal responsibilities etc.). As regards to standards, Mr. Pop highlighted that any kind of public standard, although they make our life easier, also pose a threat because they are open to every actor, including malevolent actors.
Mr. Mocilnikar believes that in the standardization process it is important not to focus exclusively on prevention, which is of course very important, but also to reinforce ourselves concerning alert, detection, preparation and crisis management.
Finally, according to Mr. Raza what we are missing the most are available standards for sharing hybrid threats information.

A second question addressed to the speakers focused on the way not to over-securitise societies while countering hybrid threats.

On this point, Mr. Raza considers that risk analysis and assets management analysis are crucial to understand what we must protect and what we do not have to protect.
According to Mr. Mocilnikar, it is important to put ethics at the center, to have legal and conformity dynamics. In the EU-HYBNET project ethics is at the center.
Mr. Pop believes that what is an over-securitised society is very subjective. For instance, what we consider normal in terms of surveillance can be considered differently in other parts of the world. Additionally, Mr. Pop believes that cyber risks should be better communicated to EU citizens and that real investments in risk analyses and cyber units are needed at a governmental level.

#### 3.2.2.2 2ND ROUNDTABLE

The core theme of the second roundtable conversation were the unknown threats and low-technology threats – status of the art, and future challenges.

**Mr Athanasios Grigoriadis**, Senior Cyber Security Expert at Kentro Meleton Asfaleias (KEMEA) was the first speaker. He began his introduction by highlighting that, traditionally, one of the defence best practices is offense and underlined the importance of connecting the dots and of reflecting the growing need to adopt a holistic approach to deal with hybrid threats. In fact, the multi-layered and multi-faced nature of hybrid threats calls for an equally multi-pronged response, theoretically embracing the widest range of actions with a view to "building resilience" and "responding to attacks". As regards offensive technologies that could be used to counter hybrid threats, Mr. Grigoriadis mentioned offensive intelligence, preparedness, advanced reconnaissance and exploitation techniques against systems, tools and methodologies that are commonly used for offensive operations targeting with accuracy cyber-threat actors' assets. Lastly, given the increasing complex nature of hybrid attacks, the presenter underlined that the most effective way to counter hybrid threats is through a comprehensive defence system functioning both nationally and supranationally in both a defensive and offensive mode.
The second speaker was **Mr. Vito Morreale**, Director of the Industry and Security Technology, Research, and Innovation (IS3), Lab, (Engineering). Mr. Morreale began his presentation by reminding that even if countering hybrid threats is under the primary responsibility of Member States, recent events, as well as the intrinsic nature of hybrid threats, showed that it is crucial to work across geographical borders. Coordination at the EU level, therefore, is very important. To enable joint actions and cooperation, however, common and shared languages, procedures, rules and standards are needed. According to the presenter, common situational awareness is the area of the Joint Framework where there is the most pressing need for standardization and the creation of a common language and understanding. The speaker concluded his section by introducing two potential important processes that could be helpful in countering hybrid threats, namely reporting and cross-border gathering of electronic evidence.

The third speaker was **Dr. Rubén Arcos Martín**, Lecturer and Researcher of Communication sciences at Universidad Rey Juan Carlos. During his presentation, Dr. Martín stressed the importance to conduct regular intelligence collection and analysis efforts when it comes to science and technologies (e.g., assessment of vulnerabilities and of adversary capabilities and intentions). This, according to him, should be done both at the national and international level, where Member States and allies could cooperate through existing structures and whole-of-government approach. Finally, as in our

contemporary society information can be deliberately used for a malign activity to produce cognitive, affective, and behavioural effects, Dr. Martín underlined the urgent need to foster innovations assisting the democratization of image, video, audio forensic and verification.

**Questions to the speakers:**

Among the questions addressed to the speakers, one focused on whether security systems interoperability will remain a top priority to achieve a holistic approach in combating hybrid threats.
On this point, Mr. Morreale considers that machine-readable models and data-exchange models are needed to enable interoperability among heterogeneous systems and security systems working at different levels. However, it should consider that 1) we are not talking about fully automated processes and that 2) we are in the middle of a process in which national sovereignty is an important element. Therefore, the final step of the interoperability needs to consider these aspects.
According to Mr. Grigoriadis the interoperability of security systems is a top priority but there is a need to develop standardized models for this. Moreover, it also crucial to think about privacy issues.

Dr. Martín believes it would be important to share common languages concerning the exchange of information among intelligence agencies, for instance to communicate vulnerabilities and uncertainties.

A second question addressed to the speakers focused on how to cope with the rise of the internet of things (IoT) and its potential vulnerabilities against cyber-attacks.

On this point, Mr. Morreale believes the problem is not so much the cyber-attack to IoT but the cascading effects it can have on any kind of infrastructure and device connected with the IoT. In his opinion, the problem is not the specific vulnerability but the fact that this vulnerability can open the door to get access to critical infrastructures, corporate systems etc.
Mr Grigoriadis suggested some specific actions to cope with IoT and its potential vulnerabilities. In particular, the suggested actions are:

- Ensure that IoT systems assist people and do not take automated decisions.
- Need to prioritize IoT related research and development projects.
- Enhanced collaboration between society and arm forces, security and defence agencies, private sector, and academia to develop the security data culture to cope with IoT related challenges.

# 4. ASSESSMENT OF THE EVENT AND GLOBAL OUTCOME

Overall, the first EU-HYBNET Innovation Knowledge Exchange Workshop represented a valuable opportunity to exchange insightful views between speakers and participants on hybrid threats, a challenge that we will continue to face in the years to come.

## 4.1 CLOSING REMARKS AND WRAP-UP

Mr. Isto Mattila RDI director at Laurea, EU-HYBNET Innovation Manager provided the concluding remarks of #IKEW, underlying how useful it is for attendees to provide them a short introduction course to the Hybrid Threat phenomena and existing challenges and how EU-HYBNET will help our EU security society to build necessary resilience against hybrid threats.

Mr. Mattila reminded participants about both medium- and long-term impact of EU-HYBNET:

- Medium term: Common understanding of innovation potential between practitioners in the same discipline.
- Long term: EU-HYBNET seeks synergies (like standardization) with already established European, national, and sub-national networks of practitioners to coordinate of their operations.

Mr. Mattila also highlighted that the fight against Hybrid threats is under MS responsibility. However, we need EU for facilitating coordinated approach since hybrid threats do not necessary are limited to one country only. Therefore, we need to have more cross-border cooperation for pan-European solutions and connecting dots together. This means that there needs to be in the future more awareness to recognize and counter hybrid threats and to cooperate in achieving this. This is a reason EU HYBNET network is all about.

Indeed, it is important to start this practical work. As Rick Meessen informed about our approach as depicted in the figure below.

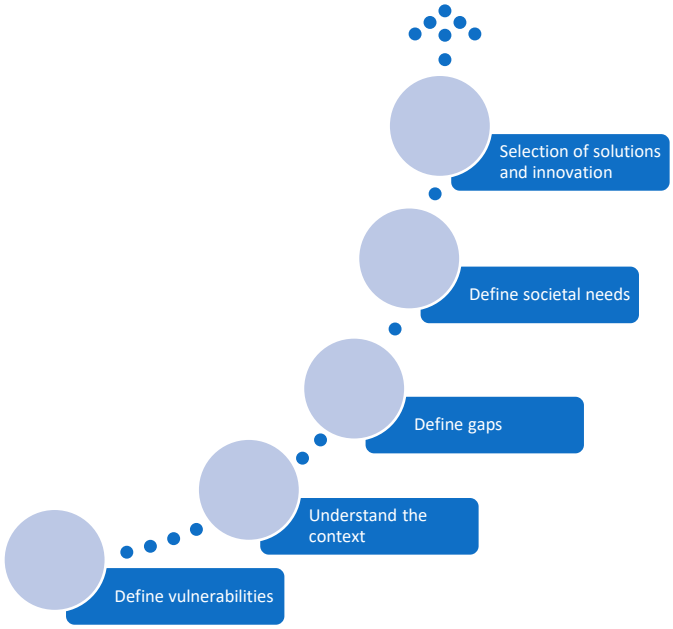


**Figure 2 EU-HYBNET Approach**

There we will find then possible solutions and innovations to develop further with e.g., some new R&D projects. This operational circle to answer our priority needs is done 3 times during our project (the 4th time being a mini cycle mainly collecting and summarizing results). During these considerations we have same time to debate with the European Commission where necessary legislative initiatives will be defined. It is important to see that hybrid threats are dangerous to many other domains such as cultural, information reliability, research, education just some to mention. Luckily, EU-HYBNET has an inbuilt approach where we can address any vulnerability possible.

Another, very important issue is also that EU-HYBNET is not bound to look for innovative solutions only within the existing legislated environment. Our four core themes answer almost all possible

considerations being them civilian or defense, public or private, national or EU level, when countering Hybrid threats.

### 4.2 IMPACT OF THE WORKSHOP ON THE EU-HYBNET NETWORK AND COMMUNITY

For the EU consortium partners the IKEW provided a very good opportunity to align the work that has to be done and to improve the shared awareness of results and ongoing activities. It was also a unique opportunity to present key questions to the invited speakers, especially with respect to standardisation and interoperability needs. The views provided highlight the importance of including all actors in the study of hybrid threats and in the study of possible solutions to address such multidimensional problems.

The presence and attendance of many individuals and organizations that are (currently) not partners in the EU HYBNET consortium confirms that the topic of hybrid threats as well as the EU HYBNET project remain very relevant (more than 170 registrations were received in total).

The IKEW also showed that there are many views on hybrid threats, its challenges and the way how to cope with these threats and challenges. It proved to be very valuable to share and exchange these different views in order to get a more profound understanding of how to proceed and how to deliver relevant knowledge and results by the EU HYBNET project.

Finally, the IKEW also identified some topics that we have not yet (or only limited) addressed in the EU HYBNET project (e.g. new domains, other types of solutions). We can and will use these for further guidance within the project.

### 4.3 LESSONS LEARNT

Project open workshops are the key to engage with a wide audience, with people having a particular interest to the topic, working on it in their own organizations. The organisation of open workshops provides the possibility to share project results, to the wider benefit of the European stakeholders.

Presenting progress and in particular results that have been produced by the EU HYBNET project is a key element in this type of (external) workshops. It gives credibility and relevance to the EU HYBNET project and provides also some focus for discussion. For the next IKEW, we even should better align the results with the (roundtable) discussions, which is also feasible since, by then, even more in-depth results can be presented with respect to the input provided.

The setup of the round tables during the afternoon proved to be a success. It enabled the exchange of different views from different stakeholders (industry, RTO, academia, SME etc.). For the next IKEW some additional elements are considered to be used in the round table discussion, like the use of some sharply defined theses, bringing together experts with very opposite views, embedding the audience in a more interactive manner (e.g. by using an electronic voting system).

## 5. REGISTRATION AND ATTENDANCE

In this section the following aspects will be treated:

- Registration process.
- Raising awareness

- Actual attendance

## 5.1 REGISTRATION PROCESS

The registration process was managed by the lead organizer, the European Organisation for Security, through the means of MS Form.


**Figure 3 MS Form used for registration purposes**

The MS Form collected information related to interested participants comprising:

- Title.
- Name.
- Surname.
- Nationality.
- Country of residence.
- Organization.

- Email address.
- Acknowledgement that the data entered is up-to-date.
- “In order to join the meeting via Zoom, you will be prompted to enter your full name and email address. By joining the meeting via the provided link, you understand that your data will be processed by Zoom. Data might be transferred to the U.S.”
- “Do you give consent for your full name, organisation, and email to be shared through a digital participation list?”
- “The meeting might be recorded. Do you authorise the organisers to take video and/or audio recording of your participation during the conference?”
- “Please note that registrations are being handled via the registration tool "Microsoft Form". By finalising your registration, you understand and agree that your information will be processed by Microsoft.”

All data were cancelled after EU-HYBNET Partners have finalised a list of authorised participants. In fact, to avoid “malevolent” actors, EOS, Laurea and Satways have performed a check of the data entered in the registration tool, to avoid unlawful actor to participate to the event.

## 5.2 RAISING AWARENESS

The event, as explained in previous section, was open to the public. For this reason, the raising awareness campaign was done in due time, reaching different audience, and not only restricted to EU-HYBNET Partners.

### 5.2.1 INTERNAL RAISING AWARENESS CAMPAIGN

The event, was first and foremost, communicated and shared to EU-HYBNET Partners and the so-called project friends. The first communication – done via email – was shared on Monday 2 November 2020, as shown in figure 5.

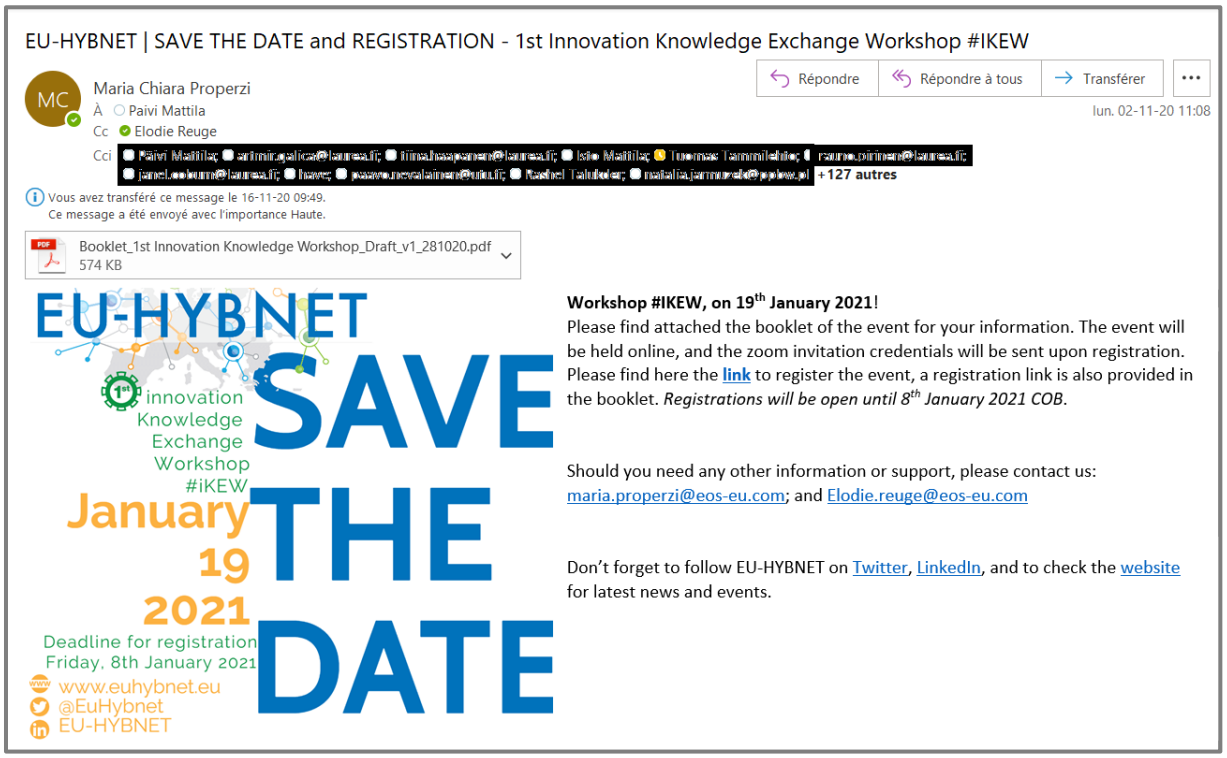


**Figure 4 First #IKEW Save the Date**

This email was shared with: EU-HYBNET Partners, EU-HYBNET Stakeholders Group, EU-HYBNET Advisory Board, EU-HYBNET Scientific Advisory Group, EU-HYBNET Ethical Advisory Group, and EU-HYBNET Security Advisory Group. The invitation was also shared with the EU-HYBNET network members via TUOVI platform. In addition, EU-HYBNET as a Commission funded Network of Practitioners –project (NoP) welcomed all other NoP-projects to join the IKEW via NoP-projects' CIRCAB platform.

The abovementioned email was sent through reminders every two weeks to the same set of contacts, until the deadline for registration was reached.

### 5.2.2 EXTERNAL RAISING AWARENESS CAMPAIGN

Likewise, EU-HYBNET Partners were invited to share the invitation with their own networks. Moreover, the external raising awareness campaign could count also on the efforts done by means of EU-HYBNET Website, EU-HYBNET Twitter, and EU-HYBNET LinkedIn profile, as shown in the following figures.


**Figure 5 First tweet related to #IKEW**

At the same time, to increase the attendance and to reach further audiences, EU-HYBNET Partners have also published, in the events' section of the EU-HYBNET profile the information of the event, so to increase the publicity of #IKEW, itself, and as shown in Figure 5.

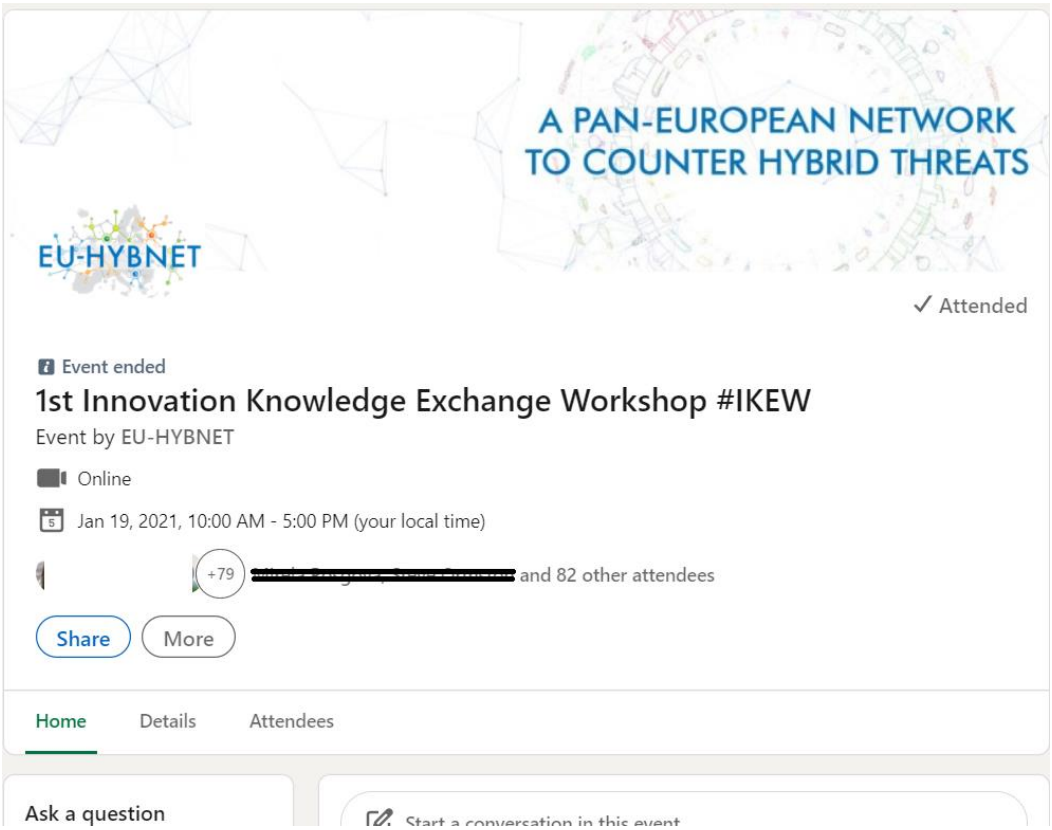


**Figure 6 #IKEW LinkedIn Event**

At the same time, the event also counted the participation of some students of, Dr. Paresh Rathod, Coordinator (Cybersecurity) and Chairman (ECSO WG5) at Laurea, that counted EU-HYBNET as part of the curriculum of its cybersecurity class.

## 5.3 ACTUAL ATTENDANCE

As explained before, the main organisers: EOS, Laurea and Satways, have performed a due background check of the registered participants. All EU-HYBNET partners were encouraged to share the IKEW invitation further in their own networks.

Moreover, during the day, Ms. Janel Coburn was the designated person to check the actual participants with those connecting online. Through the data matched between the final list of registered participants to that of attending the day of the event, #IKEW counted of more than 100 participants. Participation that fluctuated during the day and did not go below 70 participants online.

# 6. LOGISTICS AND ORGANISATION

The messages expressed in the 4th part will be displayed throughout the EU-HYBNET timeline.

## 6.1 AN EVENT HELD ONLINE

The event had to be organised online, due to the consequences of travel restrictions caused by Covid-19. However, notwithstanding this, the event was not negatively affected by the online version of it, and concrete results were met and gathered as explained in previous section.

To avoid any complications, EU-HYBNET organisers have shared the connection details and House Rules and technical instructions, to allow a proper bandwidth during the event, only after having performed the security checks that were mentioned before.

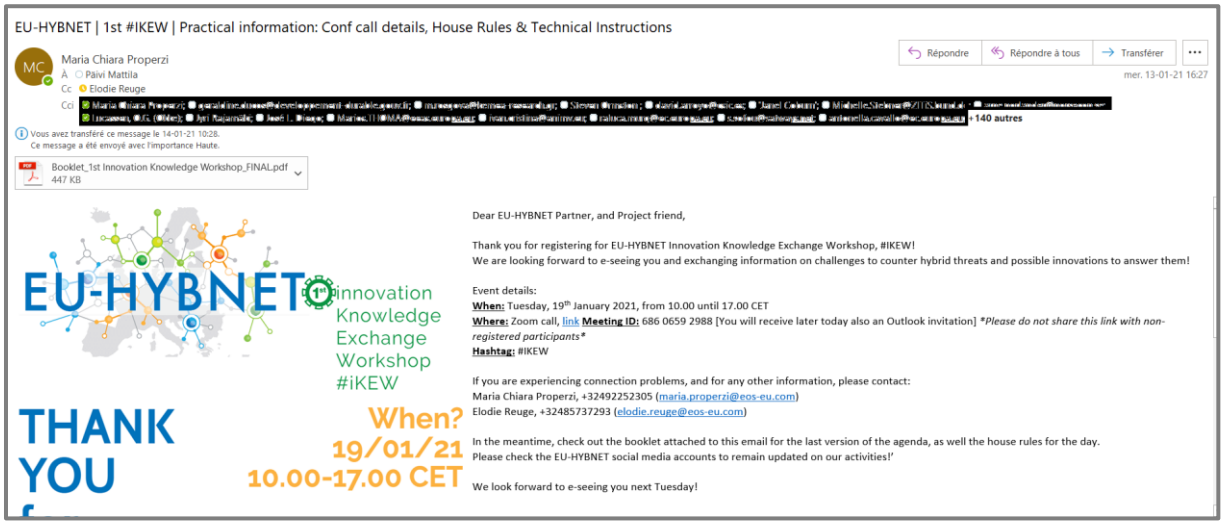


**Figure 7 #IKEW Practical Information: conf call details, house rules and technical instructions**

## 6.2 COMMUNICATION CAMPAIGN SOCIAL MEDIA COVERAGE DURING THE WORKSHOP

During the day, EU-HYBNET Partners have performed a live tweeting of the event, by means of also using the tailor-made hashtag #IKEW.


**Figure 8 Example of live tweeting during #IKEW**

In the same manner, EU-HYBNET Partners have updated members also on LinkedIn, as pictured below.


**Figure 9 Example of live coverage on LinkedIn profile**

## 6.3 COMMUNICATION AFTER THE EVENT

To complete the communication and dissemination efforts, several post event actions have been performed:

- Press release.
- Thank you email to participants, and thank you email for speakers.
- Organization of an "hot wash" session together with the coordinator, the WP leader, the Innovation Manager and the T3.1 leader.

### 6.3.1 PRESS RELEASE

The day following #IKEW, EU-HYBNET Partners have issued a press release with the main outcomes of the event, that was duly published on EU-HYBNET website, as well as being shared on Twitter and LinkedIn. A copy of the press release is available in Annex II of this deliverable.

### 6.3.2 THANK YOU EMAIL

The day following #IKEW, EU-HYBNET Partners have sent out to attendees and speakers a thank you email where the slide deck shown during the event was inserted as an attachment to the email, after having agreed to share presented slides with each of the presenters.

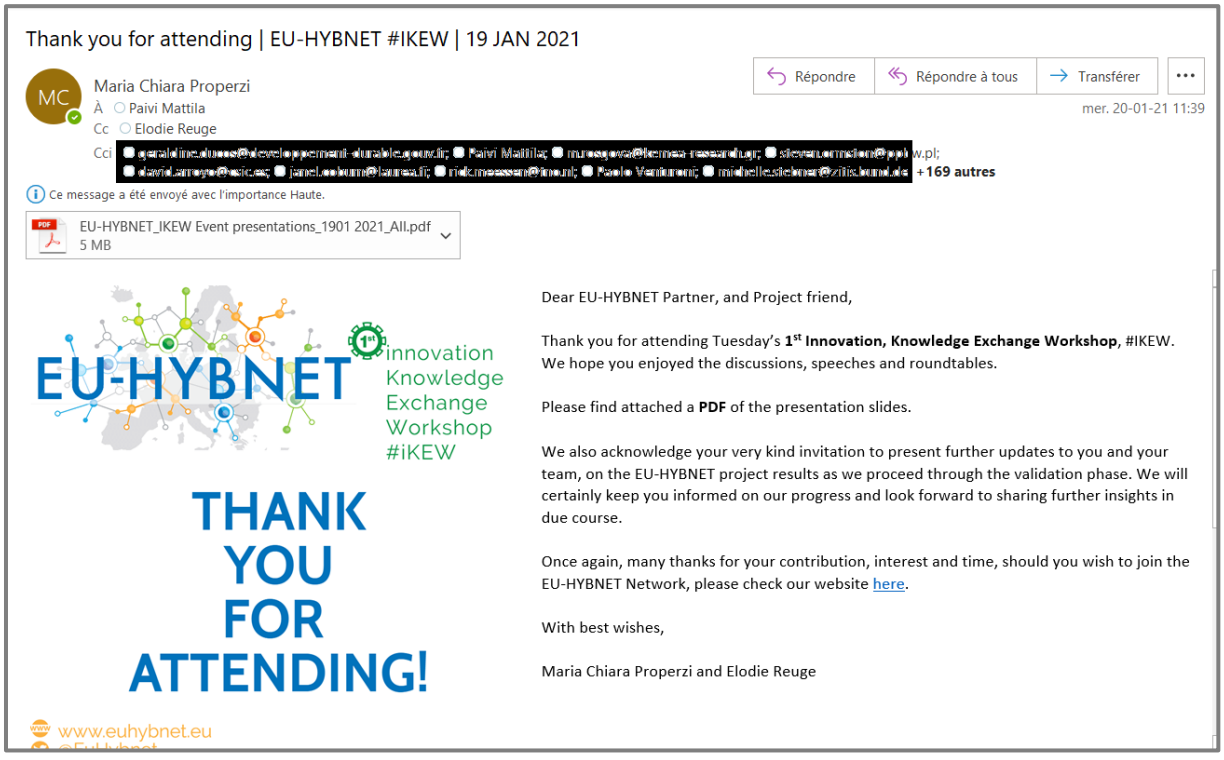


**Figure 10 'Thank you for attending' email sent to participants of the event**

### 6.3.3 HOT WASH SESSION

Following the event, #IKEW main organisers, EOS, Laurea and Satways have also organised a so-called "hot-wash session" which took place on the 27th of January and where Partners have discussed how to ameliorate participants experience for future events, enlisting all the items that could be ameliorated. The main points of the discussion are described below:

#### 6.3.3.1 EVENT SECURITY CONCERNS

Security of the event takes priority; users need to provide the requested details to be permitted to stay in the event.

How to verify attendees in the future. The people that have registered do not have the same Zoom usernames and this complicated the acceptance of these users, also cannot verify them from their registered email addresses either because these do not match their Zoom usernames.

**Action Points:**

Ask users during registration to provide their Zoom username which they will use during the event, in addition to their name, email, organization and professional title.

Provide instructions to the users how to find their username.

Reiterate to users not to share the Zoom link with anyone (even colleagues) and inform them that any unregistered participants will be checked and kicked out of the call.

#### 6.3.3.2 TECHNICAL LOGISTICS

Call hosting responsibilities.

Number of people needed to manage attendee verification and acceptance, mic muting, and timely response to emails, chats, and phone texts.

Need to use an alphabetical list of registered attendees, Ctrl+F (find) function not working.

How to handle users who have logged in with different usernames multiple times. Ex. Alex_ and Alex XX[1], was the same person.

**Action Items:**

Alphabetize registration list.

Assign 2 people for these event logistics duties and define roles for each attendee verification and acceptance, mic/video control, and timely response to emails, chats, and phone texts.

Determine how to ensure each participant receives a registration confirmation.

## 7. CONCLUSION

The first Innovation Knowledge and Exchange Workshop, #IKEW, was successfully held online. It gathered a very wide pan-European audience over 170+ registered and over 70+ participants to the end of the event staying on-line.

The main objectives of the IKEW were to facilitate the exchange of knowledge and of information about innovations and to increase the likelihood of future uptake. Both objectives were clearly met and achieved.

If several points (already identified) can be improved for the next workshop, this first IKEW can be judged successful. The organisation of the event was also praised by many.

[11] For a matter of privacy the family name of the attendee can not be disclosed here

The participants will now need to be engaged to help EU-HYBNET successfully achieve its work. They will also be invited to the several workshops of the T3.4:

IKEWs:
Workshop 2: Innovation and knowledge exchange in Hague by TNO (M26)
Workshop 3: Innovation and knowledge exchange in Valencia by PLV (M43)
Future Trends Workshops:
Workshop 1: Brussels by HCoE (M12)
Workshop 2: Rome by UCSC (M24)
Workshop 3: Bucharest by MVNIA (M36)
Workshop 4: Valencia by PLV (M48)
Workshop 5: Ispra by JRC (M58)

## ANNEX I: #IKEW LEAFLET

EU-HYBNET

## Innovation Knowledge Workshop #IKEW

Initially planned in physical presence, the 1st Innovation workshop of EU-HYBNET project will be held as a full day online event.

The objective of the Innovation Knowledge Workshops is to facilitate the exchange of knowledge and of information about innovations to increase the likelihood of future uptake.

It will allow practitioners to become aware of innovation possibilities via the EU-HYBNET project and network activities. For this first event, the following outputs will be used to create a mapping matrix of gaps/needs and research/innovations:

- Definition of target areas for improvement and innovation.
- Technology and innovations watch
- Ongoing research project initiatives watch.

Each of the three 'Innovation and Knowledge Exchange' events will have different themes. However, all will maintain adherence to the project's four core themes and will facilitate the continuous mapping of needs, monitoring of solutions, and providing a forum where practitioners can engage with innovation providers.

Innovation providers are invited to explain and demonstrate their innovative solutions that align with the event theme and to interact with practitioners. Meetings will involve key personnel from organisations involved in countering hybrid threats.

Knowledge transfer will be incorporated in several ways: peer-to-peer practitioner learning, learning from EU MS national actors, and through workshops. Meetings will involve key personnel within organisations involved in measures against hybrid threats.

During each event organized, EU-HYBNET partners will organize time for interaction between industry, academia, and other relevant participants outside of the consortium, to objectively assess the feasibility of the projects activities and findings.

> ***The objective of the Innovation Knowledge Workshops is to facilitate exchange of information on innovations and knowledge and increase the likelihood of uptake.***

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

EU-HYBNET

## Agenda

| Time | Topic | Speaker(s) |
|---|---|---|
| 10.00-10.10 | Opening remarks | Mr. Paolo Venturoni, CEO, EOS. |
| 10.10-10.20 | Welcome & Introduction | Dr. Päivi Mattila, the Director of Security Research Program Laurea, EU-HYBNET Coordinator. |
| 10.20-11.00 | Intervention on the EU policy framework on hybrid threats<br>Q&A | Mr. Maciej Szymański, Policy Officer, DG DEFIS, European Commission.<br>Mr. Max Brandt, Policy Officer, DG HOME, European Commission. |
| 11.00-11.05 | **Break** | |
| 11.05-11.45 | Towards new preparedness: comprehensive and multinational approach to counter Hybrid Threats<br>Q&A | Dr. Hanna Smith,<br>Director of Research and Analysis Hybrid CoE. |
| 11.45-12.15 | Critical gaps and needs in knowledge and performance in relation to innovations<br>Q&A | Dr. Rick Meessen, Principal Advisor Defence, Safety and Security, TNO. |
| 12.15-13.00 | **Lunch** | |
| 13.00-14.30 | **Roundtable I**<br>*Industry view to innovations answering Pan-European practitioners and other relevant stakeholders' needs countering hybrid threats, in relation to:*<br>*•Resilient civilians, local level, and administration*<br>*•Cyber and future technologies*<br>*•Information and strategic communications*<br>*•Future trends of Hybrid Threats* | Moderators:<br>Ms. Maria Chiara Properzi, Policy Manager, EOS and Ms. Elodie Reuge, Crisis Management Project Manager.<br>Speakers:<br>• Mr. Antoine-Tristan Mocilnikar, General Mining Engineer, (Ministère de la Transition, écologique, France).<br>• Mr. Radu Pop, Head of Infrastructures and Frontier Security Solutions Sales, (Airbus)<br>• Dr. Shahid Raza, Director of Cybersecurity Unit, (Research Institutes of Sweden – RISE). |
| 14.30-14.40 | **Break** | |
| 14.40-16.10 | **Roundtable II**<br>*Unknown threats and low-technology threats – status of the art, and future challenges, in relation to:*<br>*•Resilient civilians, local level, and administration*<br>*•Cyber and future technologies*<br>*•Information and strategic communications*<br>*•Future trends of Hybrid Threats* | Moderators:<br>Ms. Elodie Reuge, Crisis Management Project Manager and Ms. Maria Chiara Properzi, Policy Manager.<br>Speakers:<br>• Mr Athanasios Grigoriadis, Senior Cyber Security Expert, Kentro Meleton Asfaleias (KEMEA).<br>• Mr. Vito Morreale, Director of the Industry and Security Technology, Research, and Innovation (IS3), Lab, (Engineering).<br>• Dr. Rubén Arcos Martín, Lecturer, and Researcher of Communication sciences (Universidad Rey Juan Carlos). |
| 16.10-16.20 | **Break** | |
| 16.20-17.00 | Closing remarks & Wrap Up | Mr. Isto Mattila, RDI director Laurea, EU-HYBNET Innovation Manager. |

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

EU-HYBNET

## #IKEW House Rules

- This Innovation Knowledge Exchange Workshop (IKEW) is an event organised in the framework of the EU-HYBNET project. **Only registered participants are invited to attend.**
- The event will be recorded for the purpose of accurate minute taking. Attendance contribution will be anonymised, and the recording will be deleted once the minutes have been approved by the relevant parties.
- Please connect **15 minutes before** the event starts to allow your acceptance to virtual room and ensure the workshop can start on time. If you are a panellist, please run the Zoom audio test beforehand, not just at the beginning of the meeting.
- **Questions to panellists can be asked using the Zoom chat** anytime during the workshop. For questions, please use the Zoom chat indicating to who the question is addressed to. There will be five Q&A sessions, when the questions will be asked.

## Technical Instructions

The meeting will take place remotely using Zoom.

Ensure you have a good network connection (enough bandwidth).

**Microphone:** Please ensure your microphone is muted when joining, to avoid background noise. This should be the default option for all attendees, but please check again when entering. If you are a panellist, please check that your microphone is clear and positioned effectively, with minimal background or channel noise.

**Camera:** use of camera or vide will reduce the available bandwidth, so cameras will be kept on only by the moderators and speakers.

More info and updates on the 1st #IKEW at:

euhybnet.eu

EU-HYBNET LinkedIn Group

@EuHybnet

Don't forget to use the Innovation Knowledge Exchange Workshop hashtag: **#IKEW**

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

## ANNEX II: #IKEW PRESS RELEASE

### EU-HYBNET held its 1st Innovation Knowledge Exchange Workshop, #IKEW

On 19 January 2021, the EU-HYBNET consortium held its first virtual Innovation Knowledge Exchange Workshop, #IKEW. The first Workshop introduced participants to the EU-HYBNET project, its existing network and the EC's interest to extend the network as a Pan-European hybrid platform for Member States' needs.

In fact, the EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) project aims specifically to empower its network to counter hybrid threats by proliferating knowledge and facilitating cooperation between Industry, Practitioners, and Academia, and by providing advanced solutions for network collaboration and delivering recommendations for training, standardization, and industrialization of cutting-edge innovations.

This 1st #IKEW aimed to provide Practitioners, Industry, SMEs and academia with an opportunity to exchange information on challenges to counter hybrid threats and possible innovations to counter them. The workshop, open to project partners and external participants, focused on the EU-HYBNET core themes, which are:

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

During the event, the speakers had the opportunity to explore and present various themes related to the project and underlined the need to foster and build resilience towards a new preparedness based on a comprehensive and multinational approach, as underlined by Dr. Hanna Smith, Director of Research and Analysis in the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

The workshop was also enriched by two roundtable discussions where representatives from Industry, Academia and National Governments. Each actor provided relevant insights concerning, among others, the industry view of hybrid threats, the cybersecurity landscape (e.g., adversarial AI as a hybrid threat, IoT and cloud in critical infrastructure) and the need of common and shared languages, procedures, legislation, and standards to foster joint actions and cooperation in the field of hybrid threats.

Overall, the first EU-HYBNET #IKEW represented a valuable opportunity to exchange insightful views between speakers and participants on hybrid threats, a challenge that we will continue to face in the years to come.

If you are interested in joining EU-HYBNET's network, you can read the associated information and apply on the project's website.

For more general information on the 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