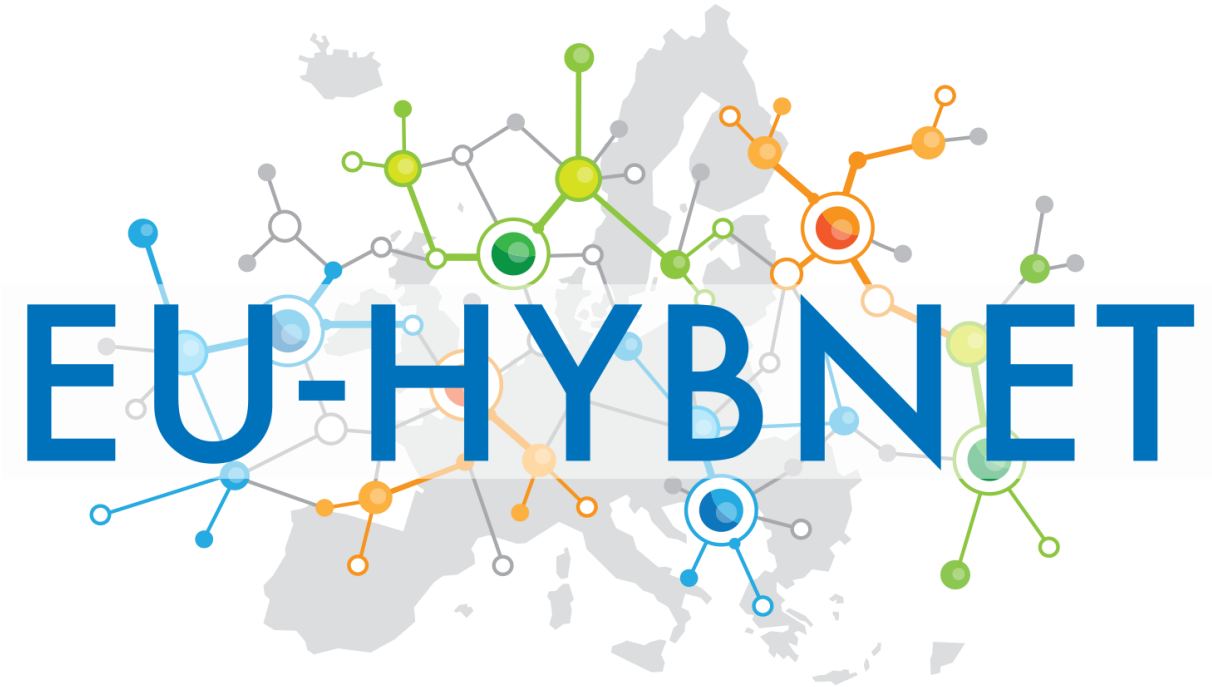

REPORT ON KICK OFF MEETING

DELIVERABLE 1.1

Lead Author : Laurea

Contributors : EOS
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

DX.X NAME OF THE DELIVERABLE

Deliverable number	**1.1**	
Version:	**03**	
Delivery date:	**31/5/2020**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Final**	
Nature:	**Report**	
Main author(s):	**Päivi Mattila, Artmir Galica, Janel Coburn, Tuomas Tammilehto, Tiina Haapanen, Isto Mattila**	**Laurea**
Contributor(s):	**Maria Chiara Properzi, Elodie Reuge**	**EOS**

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
01	27/5/2020	Laurea	Initial text
02	28/05/2020	EOS	Reviewing version 01
03	31/05/2020	Laurea	Final version

DISCLAIMER

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

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

TABLE OF CONTENT

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The Description of Action (DoA) describes this deliverable (D) as a report on the Kick Off meeting from Work Package (WP) 1 in project month (M) 1. D1.1 is a public deliverable. The Kick-Off (KO) represents also the first Milestone (MS) of the Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project. Therefore, the MS1 is now reached with the organization of the KO event.

The main objective of this document (D1.1) is to describe how the KO meeting implements the project plan and contributes to the project proceeding. In addition, the document describes how the KO meeting full fills the project objectives (OB) and Key Performance Indicators (KPI).

The KO which was originally planned to take place in Laurea University of Applied Sciences (Vantaa, Finland) from 12th-13th May 2020 had to be rescheduled due to the current Covid-19 situation. The Consortium decided not to postpone the event, but to organise it in the form of a virtual meeting that took place on 12th May at 9.00 – 16.20 CEST.

1.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 2: In this section the Kick Off meeting content, participants and arrangements are described in general;
- Section 3: In this section Kick Off presentations content and input to the project implementation and proceeding is highlighted;
- Section 4: In this section Kick Off's input to full fill project Objectives and KPIs is described;
- Section 5: In this section the D1.1 is concluded and way forward explained.

2. KICK OFF MEETING – OVERVIEW

2.1 ARRANGEMENTS OF THE MEETING AND THE PROGRAMME

The EU-HYBNET (Empowering a Pan-European Network to Counter Hybrid Threats) project Kick Off (KO) meeting took place on Tuesday 12th of May 2020 at 9.00 – 16.20 CEST. The KO was arranged by Laurea university of Applied Sciences, which acts as the coordinator of the EU-HYBNET, and the KO officially started the five-year project activities.

The KO was planned to be a two-day event and to take place in Helsinki metropolitan region, in Laurea Tikkurila Campus premises (address: Ratatie 22, 01300 Vantaa, Finland). However, due to the Covid-19 the KO was arranged as a day telco meeting.

The aforementioned change was well in advance communicated to Consortium partners, EU-HYBNET Stakeholder Group and Advisory Board members, as well as being agreed also with the Project Officer (PO) of EU-HYBNET. The original invitation to the KO was sent via email to participants already during March as "save the date" and this was followed by continuous update on the KO preparations and final event programme, and eventually the Zoom telco link was always sent to participant as part of the KO programme (Zoom telco link https://laurea.zoom.us/j/167680874). Invitation emails to the Kick Off Teleconference, see ANNEX III.

The KO meeting was not an open event, but it was restricted to Consortium partners, EU-HYBNET Stakeholder Group and Advisory Board members, EU-HYBNET related European Commission Officers. The KO programme was as depicted in the Figure 1. More precise description of the KO programme presentations is given in chapter 3.


Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
EU-HYBNET
KICK-OFF
12th May 2020 at 09.00 – 16.30 CET
Videoconference link https://laurea.zoom.us/j/167680874
09:00 – 09:15 Welcoming Words
- Dr. Mari Vuolteenaho, R&D Vice President Laurea
- Dr. Päivi Mattila, the Director of Security Research Program Laurea, EU-HYBNET Coordinator (agenda today)
09:15 – 09:30 Keynote Speech
- Dr. Teija Tiilikainen, Director of the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE)
09:30 – 09:50 Intervention on the EU policy framework on hybrid threats
- Mr. Max Brandt, Policy Officer, DG HOME, The European Commission
09:50 –10:30 Presentation on the EU-HYBNET main administrative phases
- Mr. Markus Walter, Research Programme Officer, the European Commission
10:30 – 10:45 Break
10:45 –11:15 Partners round the table
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

11:15 –11:30 Presentation on the project content

- Mr. Isto Mattila, RDI director Laurea, EU-HYBNET Innovation Manager

11:30 – 12:40 Presentation on the project Work Packages 1-6 — 10 Minutes each

- WP1 Coordination and Project Management. Dr. Päivi Mattila (WP leader) and Task leaders

- WP2 Gaps and Needs of European Actors against Hybrid Threats. Dr. Hanna Smith, Director of Research and Analysis, Hybrid CoE (WP leader) and Task leaders

- WP3 Surveys to Technology, Research and Innovations Dr. Souzanna Sofou, Senior Research Engineer and Innovation Manager, Satways (WP Leader) and Task Leaders

- WP4 Recommendations for Innovations Uptake and Standardization. Ms. Maria Kampa, Research Associate, Kentro Meleton Asfaleias (KEMEA) (WP leader) and Task leaders

- WP5 Communication, Dissemination and Exploitation Activities. Ms. Maria Chiara, Policy Manager, European Organization for Security (EOS) (WP leader) and Task leaders

- WP6 Ethics Requirements. Mr. Tuomas Tammilehto, Head of RDI in Leppävaara Campus Laurea

12:40 – 13:40 Break

13:40 – 14:15 Presentation on the project four core themes — 5 Minutes each

- EU-HYBNET research focus. Dr. Georgios Giannopoulos, Scientific Officer, Joint Research Centre European Commission (JRC)

- Future Trends of Hybrid Threats. Mr. Maxime Lebrun, Senior Analyst, Hybrid CoE

- Cyber and Future Technologies. Mr. Evaldas Bruže, deputy director of Lithuanian Cybercrime Center of Excellence for Training Research & Education (L3CE)

- Resilient Civilians, Local Level and National Administration. Dr. Gunhild Hoogensen Gjorv, Professor, The Arctic University of Norway, University of Tromso (UiT)

- Information and Strategic Communication. Dr. Rubén Arcos, Professor, Universidad Rey Juan Carlos URJC.

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

Figure 1 EU-HYBNET KO Programme

2.2 PARTICIPANTS

The KO participants were invited to the event via email and the participants consisted on following entities:

EU-HYBNET consortium partners:

1. Laurea University of applied Sciences (LAU)
2. Polish Platform for Homeland security (PPHS)
3. University of Tromso (UiT)

4. Research institutes of Sweden (RISE)
5. Kentro Meleton Asfaleias (KEMEA)
6. Lietuvos Kibernetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras (L3CE)
7. Universidad Rey Juan Carlo (URJC)
8. French Ministry of Ecological and Solidarity Transitition (MTES)
9. European organization for security (EOS)
10. TNO (TNO)
11. SATWAYS (SATWAYS)
12. City of Espoo (Espoo)
13. Universita Cattolica del Sacro Cuore (USCS)
14. Joint Research Centre European Commission (JRC)
15. National Intelligence academy M. Viteazul (MVNIA)
16. The European Centre of Excellence for Countering Hybrid Threats (HCoE)
17. Netherlands Ministry of Defense (MoD NL)
18. International Centre for Defence and Security (ICDS)
19. Valencia Local Police (PLV)
20. Polish Internal Security Agency (ABW)
21. Norwegian Directorate for civil protection (DSB)
22. Estonian Information System Authority (RIA)
23. Maldita (Maldita)
24. German Central Office for Information Technology in the Security Sector (ZITiS)
25. Bundeswehr University (COMTESSA)

The European Commission, DG HOME representatives who are working with the EU-HYBNET:

- Max Brandt, Policy Officer, DG HOME, The European Commission
- Markus Walter, Research Programme Officer, the European Commission

EU-HYBNET Stakeholder Group (SG)/ EU-HYBNET Network members:

Practitioners

- Ministry of Justice and Security – Law and justice (NL)
- Finnish Border Guard - Border and maritime security, internal and external security (FI)
- Ministry of the Interior Finland, Dep. for Rescue Services - Internal security, CBRN, Civil Protection and emergency response (FI)
- Tromso Police District – Law enforcement (NO)

EU Agencies and Offices

- European Security and Defence College - Crises management (EU, BE)

Industry, SME

- Soprasteria - Information technology, digital services (FR)
- Systematic - Critical infrastructure (FR)

- Expertsystem - Critical infrastructure (FR)
- Ardanti!Defence- Information technology, digital services (FR)

RTO, research association, organisations

- European Health Management Association - Health care (EU, BE)
- Fraunhofer-IVI - Critical infrastructure, electricity grids (DE)
- Institute for Public Goods and Policies; Spanish National Research Council - Fake news and strategic communication (ES)
- Ukrainian Association of Scholars and Experts in Field of Criminal Intelligence - Law enforcement (UA)
- CE.S.I. Istituto di Analisi di Politica Internazionale - International Politics (IT)
- Tecnoaliamenti - Food security (IT)
- SafeCluster - Security technology (FR)

EU-HYBNET Advisory Board (AB) members

- EEAST StratCom/ MS Anneli Kimber
- European Network of Law Enforcement Technology Services (ENLETS)/ Mr. Patric Padding
- Secretariat-General for National Defence and Security (SGDSN)/ Mr. Francois Murgadella
- Centre for Security and Defence Management in Bulgaria/ Mr. Todor Tagarev
- NATO/ Dr. Antonio Missiroli

EU Agencies who have been interested in joining to the EU-HYBNET Network

- The European Defence Agency (EDA)
- The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)
- The European Union Agency for Cybersecurity (ENISA)

The peak of KO participants was reached at 87 participants and this took place at the beginning of the KO. After this peak, the average of participants to the KO spammed between 73-80. These figures highlight that more than a participant from each involved EU-HYBNET consortium partner was present in KO.

During the KO virtual meeting it was also possible to take a picture of some of the KO participants, and especially those that have willingly agreed to leave their webcam open for the previously mentioned purpose. At the moment (c. noon CEST) when the picture was taken, please refer to figure 2, 80 participants actively participating to the KO:

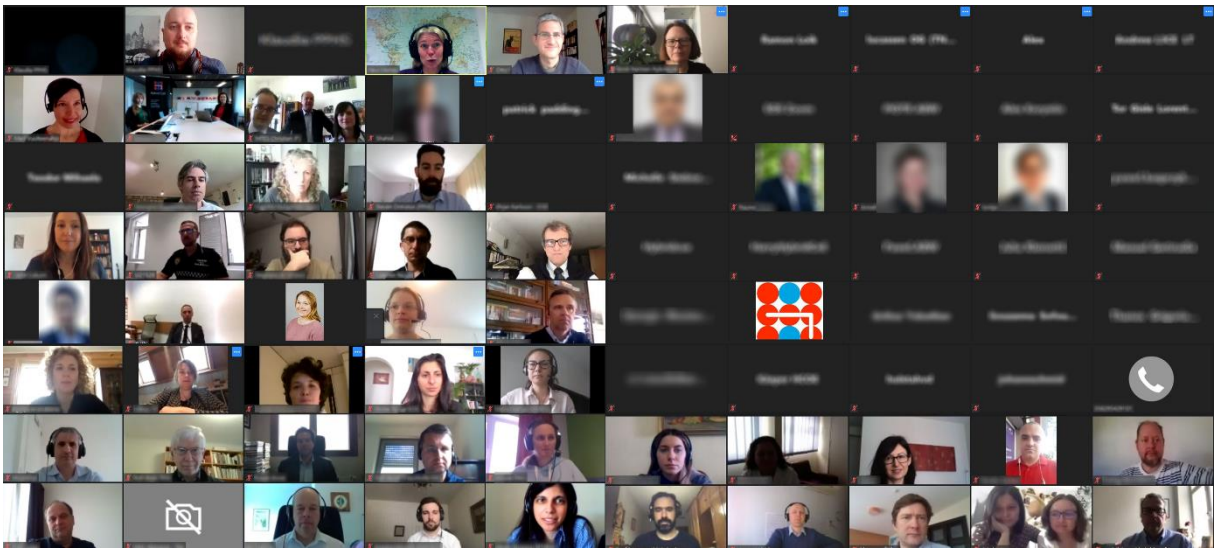

Figure 2 EU-HYBNET KO participants group picture

2.3 KICK OFF – ROLE AND MEANING IN THE EU-HYBNET

The KO is set as the first Milestone (MS) of the EU-HYBNET project (M1) and it stands for the official start of the project and its activities. The KO is part of EU-HYBNET Work Package (WP) 1 "Coordination and Project Management" activities, and specifically it pertains to Task 1.1 "Administrative and Financial Planning and Coordination".

The WP1 aims to manage and to ensure the coordination of efforts among all Consortium partners in order to guarantee an effective and smooth operations and functioning of the project and timely delivery of the expected milestones, as well as managing in a coordinated way Consortium relation with the European Commission. The influence of WP1 is highlighted in the Figure 3 below:

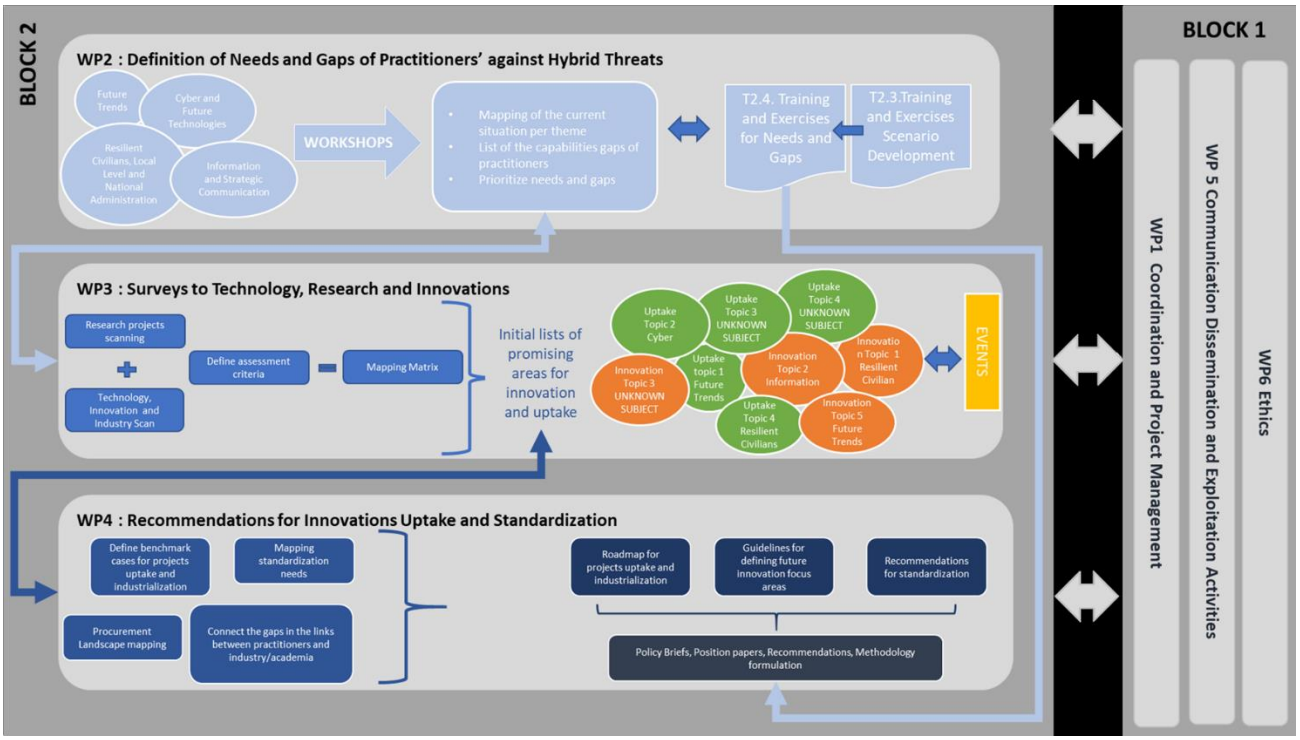

Figure 3 EU-HYBNET Structure of Work Packages and Main Activities

The importance of the KO was for the first time to bring all EU-HYBNET consortium partners, Stakeholder Group and Advisory Board members together and highlight the importance of future cooperation. In other words, KO was the first project event to support the overall goal of the EU-HYBNET to empower the network by proliferating knowledge and facilitating cooperation.

2.4 DISSEMINATION ACTIVITIES

The official project kick-off dissemination has been marked with a publication of a press release from Hybrid CoE on the day of the event, publishing key message of the project such as the official kick-off, project idea, participating organizations and countries as well as few words on current and upcoming research activities. As the project at the time did not have own website, the press release was published on the social media LinkedIn.

The document can be found here: https://www.linkedin.com/posts/eu-hybnet_eu-hybnet-kick-off-press-release-activity-6665873365221330944-XT1u. As soon as the project website is finalized, currently scheduled for M3, the document will be moved to its own publications section.

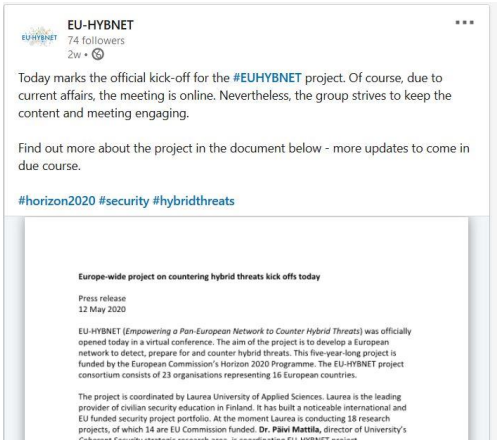

Figure 4 Official press release on LinkedIn

The project kick-off event has been well disseminated in advance via preparations, agenda discussions, guest speaker invitations and so on. As the meeting went on, the social media accounts were updated live with latest proceedings by the WP5 leader EOS. More than 23 tweets were posted on the official EU-HYBNET Twitter account during the KO, excluding the posts made from individual partners using the same hashtag. As a result from the 7-th to 12-th May the project got more than 75 followers.

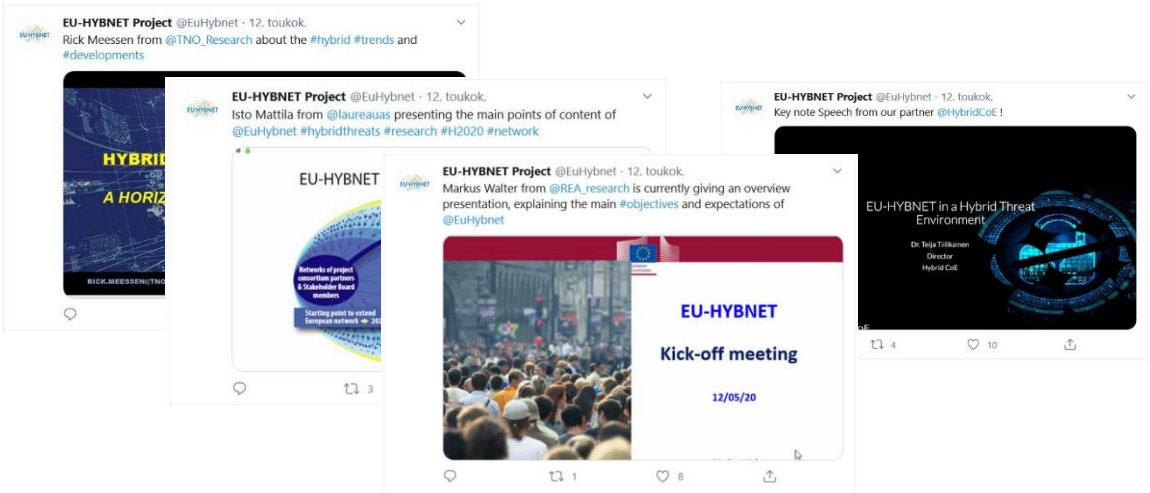

Figure 5 Social media posts during the project kick-off

3. KICK OFF PRESENTATIONS

The KO presentations that are listed in the KO agenda are described with details in the following sub-chapters. All KO presentation are saved and can be found from EU-HYBNET consortium internal working platform called eDuuni – link to the eDuuni and KO presentations, please see below. The

coordinator, Laurea hosts eDuuni and hence permission to log-in to eDuuni can be requested from Laurea/ EU-HYBNET coordinator Päivi Mattila paivi.mattila@laurea.fi

https://tt.eduuni.fi/sites/laurea-EU-HYBNET/Dissemination%20material/Forms/AllItems.aspx?RootFolder=%2Fsites%2Flaurea%2DEU%2DHYBNET%2FDissemination%20material%2FKick%2Doff%20Presentations&FolderCTID=0x01200081DAAC33BB00C5468A4884620EE5F61C&View=%7B3CCEAE31%2D3BB4%2D4811%2DAAB6%2D8ABF52A129D7%7D

3.1 WELCOMING WORDS AND AGENDA

RDI and Vice President of Laurea University of Applied Science, Ms. Mari Vuolteenaho, provided the welcoming speech to EU-HYBNET Consortium Partners and other participants joining the KO. Ms. Vuolteenaho highlighted the importance of the project for European security and safety and Laurea's strong commitment to make its best for its project coordination. Moreover, Ms. Vuolteenaho gave a short overall presentation of Laurea, in order to display the varied ways in which Laurea could provide a fruitful coordination of project's activities and its activities.

Ms. Päivi Mattila/ Laurea, and EU-HYBNET Coordinator, followed by providing an overview of the agenda. The purpose of this presentation was to tell about the practicalities of the KO and to summarize the KO programme and its expected proceeding. This was to ensure the proceeding of the KO without delays and challenges.

3.2 KEYNOTE SPEECH

The Keynote Speech was given by the Director of the European Centre of Excellence for Countering Hybrid Threats (HCoE) Dr. Teija Tiilikainen.

Her 15 minutes presentation started on a brief introduction to the world of hybrid threats and description of the historical background of hybrid threats. The transition of global power highlighted how the power struggle between Russia, China, U.S and the EU has resulted in an increase of hybrid threats, challenged international rules resulting in instability, by favouring new forms of power struggle in international relations.

Moreover, Tiilikainen highlighted difficulties to identify hybrid threats. In short, she explained that origin of unconventional means is often challenging to solve alike influence that the means tricker and cause. Furthermore, it was pointed out that the general goal of hybrid attacks is to create confusion and generate instability and to affect societies by attacking decision making in local, municipal, national level by influencing, as a direct reflex, international policy making as well. At the end of the presentation Dr. Tiilikainen described how hybrid threats are tailored to harm EU in a way that European basic values (e.g. freedom of expression) and democracy have been taken as key vulnerabilities for external influencing. This underlines the need to raise awareness of the nature of hybrid threats and influencing between the EU Member States (EU MS) and to empower cooperation between EU MS – this is seen the most fruitful way to find responses to decrease the vulnerabilities.

In general, Dr. Tiilikainen's Key Note speech highlighted the topicality of EU-HYBNET in the context of ever changing environment of hybrid threats. This was also underlined a KO participant, the French Ministry of Ecological and Solidarity Transition (MTES) who shared notion of covid-19 being used as an opportunity to create fake news and cyber-attacks in EU.

Lastly, Dr. Tiilikainen expressed the importance of network building in EU in order to enhance information sharing on hybrid threats and establish proper counter measures to these threats. Therefore, Hybrid CoE was also expressing their strong interest to contribute to the EU-HYBNET project work and its related network building. This was important aspect for the KO participants to hear because the Hybrid CoE is the leading European Centre focusing on hybrid threats and hence their strong support to the project and its sustainability is crucial.

3.3 PRESENTATIONS FORM THE COMMISSION

The European Comission, and specifically two representatives from DG HOME, provided presentations to describe the expectations of the Commission of the EU-HYBNET project progress and implementation. In addition, it was highlighted that the EU-HYBNET is expected to have a contribution to a general European policy development in the field of hybrid security and resilience which demands high level results from the project, but also open communication between the Commission representatives and the project key partners.

3.3.1 INTERVENTION ON THE EU POLICY FRAMEWORK ON HYBRID THREATS

The presentation was given by Mr. Max Brandt, Policy Officer, DG HOME, the European Commission.

While discussing the EU policy framework, Mr. Brandt emphasized the growing importance and relevance of Hybrid Threats worldwide citing recent EU and NATO activities such as the Zagreb Declaration[1], which also mentions hybrid threats as one area of its concentration.

Mr. Brandt emphasized, throughout the presentation, that there has been a growing need for a hybrid network to effectively address and counter, current and unforeseen hybrid threats. Similarly, he expressed that the idea of the EU-HYBNET project is not as much a classic research project or a Practitioners' network, but it requires a strategic yet flexible approach from practitioners to bring together all the knowledge, to identify the gaps and needs, and to develop targeted policy recommendation that will eventually provide guidance on how to approach decision-making.

Mr. Brandt wanted also to highlight that, notwithstanding that Framework Programme 8 (Horizon 2020) provides financing to civilian security research programs, this will not hamper any expected relation and cooperation with the Defence sector within the scopes and means of EU-HYBNET, taking into account the nature itself of hybrid threats.

The presentation was a high importance to the EU-HYBNET project because it underlined the strong expectations form the Commission side to the project to provide an input to different European policy discussions in the context of hybrid threats.

3.3.2 PRESENTATION ON THE EU-HYBNET MAIN ADMINISTRATIVE PHASES

The presentation was given by Mr. Markus Walter, Research Programme Officer, European Commission; who is the Project Officer (PO) of EU-HYBNET project.

Mr. Walter provided a background introduction to Horizon 2020 Secure Societies (H2020 SEC) funded projects implementation from the EC point of view. In addition, Mr. Walter addressed all legal and procedural questions regarding the project for the next five years and addressed payment and guidelines on reporting. The roles and responsibilities of the Project Coordinator were also highlighted, alike the general practise that all issues should go through the Project Coordinator whom would be responsible to report the issue back to the PO. Furthermore, the PO requests an open, timely, and clear communication with the Consortium and specifically with the Project Coordinator.

Mr. Walter also explained all the importance of technical coordination, timely submission of reports, knowledge of the key elements and rules of the Grant Agreement. The recommendation to the project consortium partners was to get familiar with the AMGA document, which explains the grant agreement in details. In addition, a brief outline of the project was provided to the KO participants.

The project, which consists of sixty (60) months like EU-HYBNET will include four reporting periods, and one review after each reporting period. The first fifteen months is the first reporting period. Concluding the first reporting period the first review occurs. The review focuses on results and summaries, not on how results were achieved. All consortium partners were asked to remind to plan enough time and be concise. The same was requested in the case of periodic reporting that occurs in two parts: technical and financial reporting.

Lastly the payment schedule was summarized alike the research ethics. Special focus was given to the ethical issues in the project and their profound implementation in the project from the early phase to the very end of the project.

The presentation was very important for all partners, especially for those partners who participate the first time to a H2020 funded project. In addition, the presentation summarized profoundly the key points to focus on in the project implementation. Lastly, it was highly important for all partners to meet the PO in person because this supports the five-year cooperation.

3.4 PARTNERS ROUND THE TABLE

All EU-HYBNET consortium partners gave a short presentation on their role and main contribution to the EU-HYBNET project. The presentations were given according to partner numbers. The figure below describes the variety of EU-HYBNET consortium partners EU MS background:

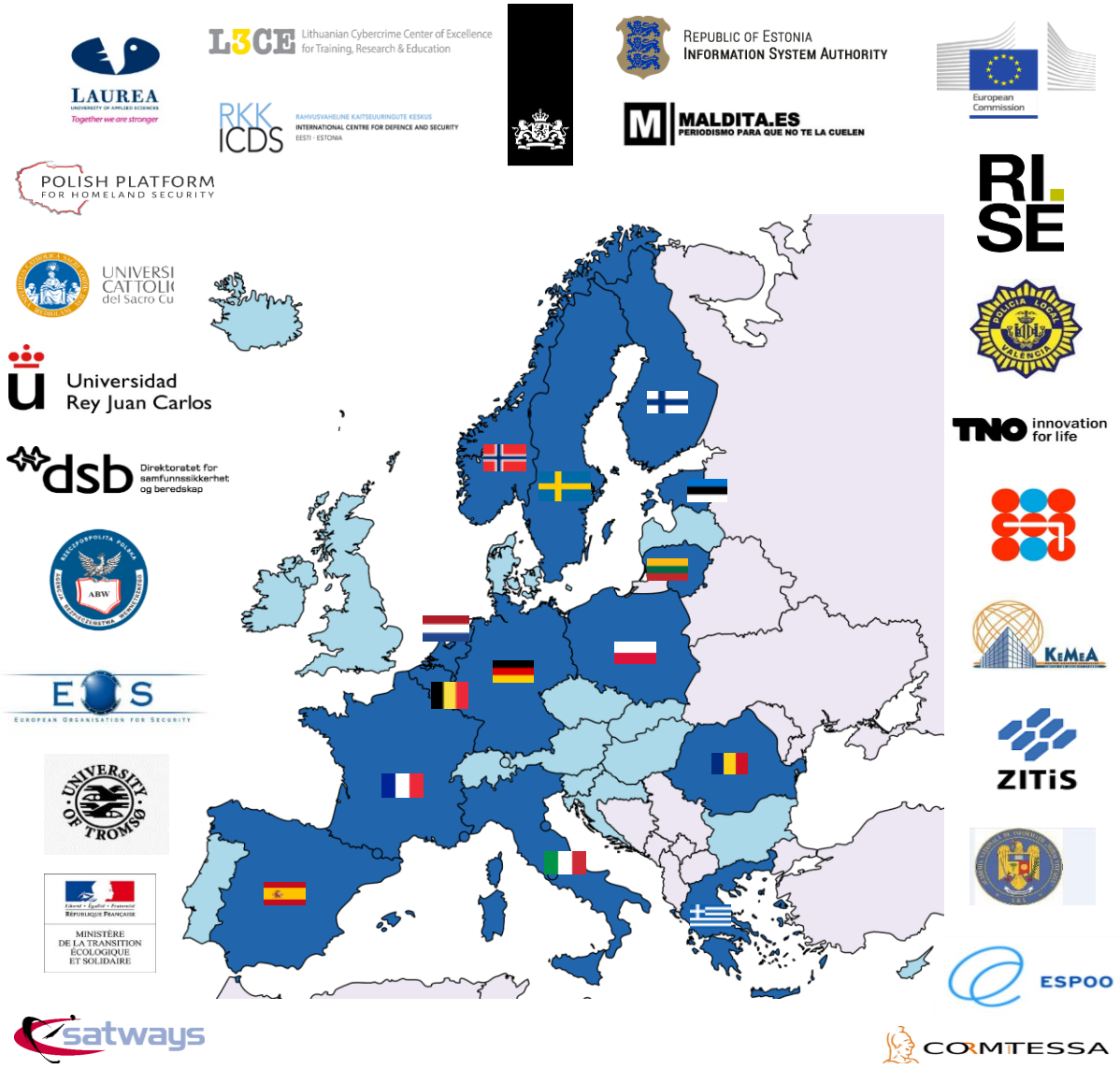

Figure 6 EU-HYBNET Consortium partners

Laurea University of Applied Sciences (Finland). Project Coordinator. Work Package 1 leader, providing coordination and support and Work Package 6 leader providing the ethical requirements. Task Leader for tasks: WP1/ T1.1, WP1/ T1.2, WP5/ T5.3. Contributions in addition to project management include leading the projects Ethical Advisory Group.

Team:

- Päivi Mattila- Project Coordinator;
- Artmir Galica- Project Manager;
- Janel Coburn- Project Assistant;
- Tiina Haapanen- Project Finance Manager;
- Rauno Pirinen- Network Manager;
- Tuomas Tammilehto- Ethics Manager; and
- Isto Mattila- Innovation Manager.

The Arctic University of Norway (University of Tromso)- UiT (Norway), as the 3rd largest university in Norway and the northern most university in the world, will be participating to tasks WP 1/ all Tasks. WP 2/ T2.1, T2.2, T2.4. WP 5/ T5.2 & T5.3. They are a project leader for one of the four project core themes, "Resilient Civilians" and will also participate as a member to the project's Scientific Advisory Group.

Team:

- Gunhild Hoogensen;
- Tor Gisle Lorentzen; and
- Bjørg Hunstad.

Research Institutes of Sweden - RISE (Sweden) The largest public-sector research institute in Sweden heavily focused in cybersecurity research. RISE contribute as Task Leader for WP4/ T4.2 and participate to WP 1/ T1.1, T1.3, WP 2/ T2.1, T2.2 & T2.4. WP3/ T3.1 & T3.3. WP4/ T4.4. WP 5/ T5.2 & T5.3. Rise will primarily work with the core theme 2 area, mapping Cyber and Future Technologies. In WP3 and WP4 RISE will contribute to the survey of available cyber security solutions and their standardization and uptake by practitioners and participate to the innovation uptake and tandardization of innovative solutions in order to close identified gaps.

Team:

- Rolf Blom; and
- Shahid Raza.

Kentro Meleton Asfaleias- KEMEA (Greece) is the research entity of the Hellenic Ministry of Citizen Protection, established in 2005. The R&D mission of KEMEA includes; technology and research watch on security and civil protection issues worldwide and transfer of knowledge to the relevant Greek public services; facilitate Greek law enforcement agencies with their participation in R&D activities and initiatives and link them with the International R&D community; consulting and technological support for the modernization of the operational services of the Hellenic Police and of Ministry dependent organizations. This dedicated approach to exploring synergies, establishing communication links and working together to produce end-user driven research on all fronts of the Security Sector during the last decade, has earned KEMEA its participation in numerous National and EC R&D projects. KEMEA will act as work package leader for WP4 coordinating the formulation of the final strategy for the innovation uptake and industrialization, the standardization activities and the publication of the relevant policy briefs and recommendations. As task leader for WP2/T2.3 & WP4/ T4.1. Elsewhere KEMEA will participate to WP1/all tasks, WP2/T2.1, T2.3 & T2.4, WP3/ T3.2, WP4/all tasks, WP5/all Tasks. In addition, KEMEA will participate as a member to the project' Steering Committee and a member to the project's Ethical Advisory Group.

Team:

- Pantelis Michalis;
- Maria Kampa;
- Ilias Gkotsis;
- George Eftychidis;

- Mirela Rosgova;
- Athanasios Grigoriadis;
- Aggelos Vassileiou;
- Vasiliki Zomenou;
- Dimitra Papadaki; and
- Christina Pavlou.

Lithuanian Cybercrime Center of Excellence for Training Research & Education - L3CE (Lithuania) will focus on one of the four project core themes, "Cyber and Future Technologies". Focusing on research and applications in cybercrime; complex, sophisticated, full-spectrum cyber related hybrid threats, developing hybrid methodologies for early identification and prevention of threats, and delivering cyber capability management and inclusive innovations' governance models. Contributing as a task leader for WP2/ T2.4 and WP3/ T3.3 and participating to WP 1 all tasks, WP 2/ T2.1 & T2.2. WP 3/ T3.2. WP 4/ T4.2. WP 5/ T5.2, and generally helping and assisting organizations and addressing hybrid threats by focusing on innovations, cyber, and future technologies.

Team:

- Egidja Versinskiene;
- dmundas Piesarskas;
- Evaldas Bruze; and
- Rimantas Žylius.

Universidad Rey Juan Carlos - URJC (Spain) Focusing on such themes as hybrid threats, security threats, intelligence, and strategic communication, URJC is contributing as a leader of one of the four project core themes, "Information and Strategic Communication" and participating to tasks: WP1/all tasks, WP2/ T2.1, T2.2, & T2.4, WP3/ T3.4. WP4/ T4.4. WP5/ T5.2. URJC will also participate as a member to the project's Ethical Advisory Group.

Team:

- Ruben Arcos Martin;
- Manuel Gértrudix Barrio;
- Mario Rajas;
- Carmen Gálvez;
- Carmen Gertrudis;
- Victoria Campos;
- Rosa Mesa; and
- Bernandino Muñoz.

Ministère de la transition écologique et solidaire/The Ministry of Ecological and Solidarity Transition –SHFDS (France) As a partner, SHFDS is interested to contribute services which support a hybrid threat network across Europe. By collaborating with industry, academia, and practitioners to identify capability and operational gaps, monitor research and innovation, indicate priorities for standardization and policy recommendations, and disseminate results and interact with other related networks. They are participating to tasks WP1/ all tasks, WP 2/ T2.1, T2.2 & T2.4. WP3/ T3.1. WP4/ T4.1. WP 5/ all tasks and will participate as a member to the project's Ethical Advisory Group.

Team:

- Antoine Tristan Mocilnikar;
- Yves Rougier ;
- Christian Desprès ; and
- Pierre Dumontet.

European Organization for Security - EOS (Belgium) is the voice of the European Security Community consisting of SMEs, universities, and research centres whose main goal is to create a harmonized European security market. Contributing as the Work Package Leader for WP5 Communication, Dissemination and Exploitation Activities and Task leader in WP3/ T3.4, WP5/ T5.1. EOS is also participating to tasks WP1/ T1.1 & T1.3, WP2/T2.1 & T2.4, WP3/ T3.3, WP4/ T4.1 & T4.4, WP5/ all Tasks and also participating as a member to the project' Steering Committee.

Team:

- Maria Chiara Properzi;
- Elodie Reuge;
- Paolo Venturoni;
- Alberto Curatolo; and
- James Philpot.

Nederlandse Organisatie voor Toegepast Natuurweten Schappelijk Onderzoek - TNO (Netherlands) One of the major research and technology organisations in Europe with approximately 3,000 scientists carrying out research impacting the domains of industry, healthy living, defence safety & security, energy and living environment. Worked for the Programme 'Resilience against hybrid threats' for Dutch ministries and is a stakeholder with the Ministry of Foreign Affairs. TNO is contributing as a task leader in for WP3/ T3.1 and participating to WP1/ all Tasks, WP2/ T2.1, T2.2, & T2.4, WP3/ T3.4, WP5/ T5.2 & T5.3. TNO will also participate as Innovation Manager in the project's Project Management Board and as a member to the project's Scientific Advisory Group.

Team:

- Rick Meessen;
- Angela Kwaijtaal;
- Anja van der Hulst;
- Okke Lucassen; and
- Carolina Van Weerd.

SATWAYS Ltd. (Greece)- Mainly works to develop integrated Geospatial command and control and situation awareness solutions for Security and Public Safety applications. The goal is to provide effective decision support, to simplify operations, to provide a Common Operational Picture (COP) and collaboration tools across organizations, to collect and disseminate data in the field and to coordinate response units and system users. SATWAYs will contribute as a Work Package Leader for WP3 and participate to WP1/ all Tasks, WP2/ T2.1, and WP5/ all tasks and as a member of the Project Management Board as WP3 Leader.

Team:

- Souzanna Sofou;,
- Dimitris Diagourtas;
- Antonis Kostaridis;
- Katerina Kadena; and
- Georgia Moutsou.

City of Espoo, ESPOO- (Finland) Speaker not Present, Coordinator Päivi Mattila presents)- Espoo is the second biggest city in Finland located next to the capital city Helsinki. Espoo is one of the European forerunners in innovation, its modular city structure and the city's commitment to develop City as a Service forms the basis for Espoo's approach in promoting innovation and building a networked and multi-stakeholder cooperation. The city of Espoo will participating to WP1/ T1.1 & T1.3, WP2/T2.1, T2.2 & T2.4, WP4/T4.1, and WP5/ all tasks.

Team:

- Petri Häkkinen;
- Satu Laukkanen; and
- Jasmin Repo.

Università Cattolica del Sacro Cuore, - UCSC (Italy), located in Rome, specializes in hospital and healthcare knowledge with 5 campuses. Their extensive research program closely collaborates with 16 internal colleges, 62 departments and 93 research centres. The School of Medicine, established in Rome in 1961, covers all modern medical disciplines as well as some of the most considered medical scholars in the world. UCSC will participate to WP1/ all Tasks, WP2/ T2.1 &T2.4, WP3/ T3.1 & T3.4, WP 4/ T4.1, and WP 5/all tasks. Additionally, UCSC will contribute to the ethics and societal impact assessment activities in the project and participate as a member to the project's Ethical Advisory Group.

Team:

- Sabina Magalini;
- Rachele Brancaleoni;
- Daniele Gui;
- Saverio Caruso;
- Lorenzo Marchesi;
- Monica Bernassola; and
- Camilla Pilotti.

Joint Research Center-European Commission (JRC)- The Joint Research Center is the European Commission's science and knowledge service whose mission is to support EU policies with independent evidence throughout the whole policy cycle. There are 6 locations in 5 member states, an estimated 1500 staff and 42 large facilities. The JRC will contribute to the project as the overall leader of the four project core themes, act as task leader for WP2/ Gaps and Needs of European Actors against Hybrid Threats and participate to WP1/ all tasks, WP2/ T2.1 & T2.4, WP3/ T3.4, WP4/ T4.3 & T4.4 and WP5/ all tasks. The JRC is mainly involved in WP2 leading task 2.2 which focuses on the research to support increase of knowledge and performance. JRC will also organize the 3rd Annual Workshop of the network and will participate as a member to the project's Scientific Advisory Group.

Team:

- Georgios Giannopoulos;
- Georgios Marios Karagiannis; and
- Georgios Theodoridis.

National Intelligence Academy Mihan Viteazul- MVNIA (Romania)- The National Intelligence Academy serves as the only intel and security expert training and education facility in Romania, specializing in the training of intelligence officers, the promotion of security culture for the civil society and conducting research in the fields of intelligence and security studies. These studies include security risk emerging trends, security culture, terrorism/counterterrorism, decision-making in homeland defence, innovation needed in local, regional and global security policies and strategies, early warning indicators of terrorism, cyber-crime or extremist violence, community and institutional resilience to crisis situations, security culture development, new tools for intelligence analysis, intelligence flows and support to strategic decision making. MVNIA will participate to WP1/ all tasks, WP2/ T2.1, T2.2, & T2.4, WP 3/T3.4, WP4/ T4.1, and WP5/ all tasks as well as acting as Security Manager in the project's Security Advisory Groups.

Team:

- Cristina Ivan;
- Irena Chiru;
- Ileana Surdu;
- Valentin Stoian; and
- Dana Sirbu.

European Centre of Excellence for Countering Hybrid Threats- Hybrid CoE (Finland)- Established in 2017 it acts as an intel hub for practitioners and experts enhancing EU & NATO cooperation. The task of the Centre is to support the participating governments' efforts to enhance their awareness and preparedness, civil-military capabilities and resilience to counter hybrid threats, with a special focus on European security. HCoE will lead of one of the four project core themes, "Future Trends", act as a Work Package Leader for WP2 Gaps and Needs and as a Task leader in WP1/ T1.3, WP2/ T2.1, WP4/ T4.4 and participate to WP1/ all tasks, WP2/ all tasks, WP3/ T3.1 and T3.4, WP5/ all tasks. HCoE will also act as Network Manager in the project's Project Management Board, as a Scientific Manager in the project's Scientific Advisory Group and moreover, will participate as a member of the project' Steering Committee and Security Advisory Group. Additionally it is currently foreseen that Hybrid COE will continue to coordinate the EU HYBNET when the Horizon funding will been discontinued.

Team:

- Teija Tiilikainen;
- Hanna Smith;
- Käsper Kivisoo;
- Emma Lappalainen;
- Maxime Lebrun;
- Päivi Tampere;
- Paul Dickson; and

- Ulla-Marja Wilenius.

Ministry of Defense Netherlands- MOD (Netherlands) The MOD will act as a practitioner at ministry level (administration) in the EU HYBNET project. The MOD has a legal mandate to plan and take measures against hybrid threats. According to the latest Defence White Paper of 2018, 'Hybrid Warfare' is identified as one of the major current threats. Consequently, in 2018 a Counter Hybrid Unit was formed that falls under the Directorate-General of Policy of MOD. The MOD is also a member of the Steering Board of the Centre of Excellence on Hybrid Threats in Helsinki. The MOD will participate to WP1/ T1.1, WP2/ T2.1, T2.3, & T2.4, WP3/ T3.1 & T3.4, and WP4/ T4.4.

Team:

- Margriet Drent;
- Hans van Leeuwe; and
- Gwenda Nielen.

International Centre for Defence and Security- ICDS Estonia (Estonia)- Located in Tallinn, ICDS is the leading think-tank in Estonia specialising in foreign policy, defence, security and resilience issues. The aim of the ICDS is to be the regional knowledge hub of first choice for the security and defence communities of Estonia, its allies and partners. Participating to WP1/ T1.1 & T1.3. WP2/T2.1, T2.2, & T2.4, WP3/T3.2, WP4/T4.4, WP5/5.2 & 5.3.

Team:

- Ramon Loik;
- Ivo Juurvee; and
- Tomas Jermalavicius.

Valencia Local Police -PLV (Spain)- More than 1,600 police officers and 8 districts form the Valencia Local Police. The R&D department has participated in 24 successful European projects from different Programmes (H2020, 7th FP of R+D in Security, Lifelong Learning Programme, Prevention and Fight against Crime, Daphne III, Civil Protection Financial Instrument, Criminal Justice, etc. PLV will participate to WP1/ all tasks, WP2/ T2.1 & T2.4, WP3/ T3.4, WP4 T4.1 & T4.3, and WP5/ all tasks. As end-user PLV will contribute to defining needs and gaps, requirements definition, and testing and validation. PLV is also responsible for arranging WP3 and WP4 events of the project.

Team:

- José L. Diego Orozco;
- Carmen Castro Garcés;
- Susana Sola Zurriaga;
- Rubén Fernández; and
- Iván Luis Martínez Villanueva.

The Internal Security Agency/ Agencja Bezpieczenstwa Wewnetrznego-ABW/ISA (Poland) – The ABW is a special service agency and government institution which protects the internal security of the Republic of Poland and its citizens. Its primary objective is to effectively neutralise threats to the State's internal security, it efforts focus on terrorism prevention, counter intel, counter terrorism, IT security,

WMD counter proliferation, and to protect classified information. In part, ABW will focus efforts to enrich existing networks against Hybrid threats with academics, practitioners and indicate priorities for standardization and recommendations for innovations uptake. ABW will participate to WP1/ T1.1 & T1.3, WP2/ T2.1 & T2.4, WP4/ T4.1, WP5/ all tasks.

Team:

- Anna Kańciak;
- Jakub Rodzeń;
- Małgorzata Leszczyńska;
- Piotr Kosieradzki; and
- Paweł Sapiecha.

Norwegian Directorate for Civil Protection/ Direktoratet for samfunnssikkerhet og beredskap – DSB (Norway) The DSB is a directorate under the Ministry of Justice and Public Security. As practitioners and researchers with hybrid threats, we are heavily involved in the national Total Defence Program, where hybrid, and issues such as cognitive resilience are central topics. We also engage in scenario development and international cooperation in this field and act as an interface between civilian and military in society. The BSB will be participating to WP1/ T1.1 & T1.3, WP2/ T2.1 & T2.4, WP4/ T4.1, and WP5/ all tasks.

Team:

- Ørjan Nordhus Karlsson; and
- Hege Støtvig.

Estonian Information System Authority/Riigi Infosüsteemi Amet – ISA/RIA (Estonia)- Estonia's State-owned cybersecurity agency (RIA) is Estonia's cybersecurity competence centre that develops Estonia's e-governance services (eID and Trust Services) and assures cybersecurity standards that are the core of the safe use of Estonia's information system. RIA coordinates the development and administration of the Estonian state information system, organises activities related to information and cybersecurity, and handles the security incidents that have occurred in Estonian computer networks. RIA advises the providers of public services on how to manage their information systems as per requirements and monitors them. RIA will participate to WP1/ T1.1 &T1.3, WP2/ T2.1, WP 5/T5.2 & T5.3.

Team:

- Uku Särekanno;
- Märt Hiietamm.

Maldita, Asociación Maldita Contra La Desinformación- Maldita.es (Spain) is a platform that consists of independent journalists focused on the control of mis- and dis-information in public and political discourse through fact-checking and data journalism techniques. Promoting transparency in public and private institutions and promoting media literacy and technological tools in order to create an aware community that can defend itself from disinformation and lies in all areas. This is their 1st EU Commission project, they are 'High Level Group' experts on Fake News debunking more than 1500 cases in the last two years. Maldita will participate as a member to the project' Security Advisory Group and will participate to WP1/ T1.1 & T1.3, WP 2/ T2.1, T2.2, & T2.4, WP4/ T4.4, WP5/ T5.2 & T5.3.

Team:

- Stéphane M. Grueso;
- Clara Jiménez Cruz;
- David Fernández; and
- Andrés Jiménez Bryden.

Central Office for Information Technology in the Security Sector- ZITis (Germany)- Newly created in 2017, the Federal Ministry of the Interior, Building and Community established the Central Office for Information Technology in the Security Sector (ZITiS) to meet the German need for a Cyber Security Strategy. As service provider for the German security authorities, ZITiS pools technical expertise in the cyber domain and support security authorities through research, development, and consultancy. In addition to sharing information on Law enforcement agency's needs and requirements in order to support definition of innovation to identified gaps and needs, ZITiS will also focus on distribution of the results. ZITis will contribute its expertise in the fields of digital forensics and lawful interception to the EU-HYBNET project and assist in gathering requirements from federal and state police and distributing standards, knowledge, tools and best-practices in the field. ZITiS will participate as a member to the project' security advisory group and also to WP1/ T1.1 & T1.3, WP2/ all tasks, WP3/ T3.1 & T3.2, WP4 T4.1 & T4.3 and WP5/ all tasks.

Team:

- Jessica Steinberger;
- Klara Dolos; and
- Andreas Steinberger.

Bundeswehr University of Munchen - COMTESSA (Germany) The Competence Center COMTESSA, based in the Bundeswehr University Munich, is an interdisciplinary research group with focus on Operations Research, Strategic Management and Safety & Security, especially in the context of Civil Security, it is not a military academy but has strong connections to the national government. COMTESSA- Core Competence Center for Ops Research Management, Strategic Planning, Safety & Security, Alliance, specializes in predictive and prescriptive analytics expertise. Bundeswehr University will have practitioner partner role and exclusive civilian security focus in the project activities. Based on experience COMTESSA will participate to WP1/ all tasks, WP2/ T2.1 & T2.2 & T2.4, WP3/ T3.3, WP 4/ T4.1, and WP 5/ all tasks.

Team:

- Stefan Pickl;
- Maximilian Moll;
- Truong Son Pham;
- Leonhard Kunczik; and
- Gonzalo Barbeito.

3.5 PRESENTATION ON THE PROJECT CONTENT

A presentation on the EU-HYBNET project general content was given by R&D Director Isto Mattila, Laurea. The goal was to highlight EU-HYBNET project's key elements which to deliver project's expected results.

In the beginning of the presentation it was reminded that the EU-HYBNET is to empower European network to counter against 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. Moreover, the presentation highlighted that EU-HYBNET will encompass future innovations and solutions in the domain of technical and social research, and deliver results to the identified European actors' gaps and needs to counter hybrid threats. This will lead to innovation uptake and standardizations recommendations. The core building blocks of the project are presented in the figure below:

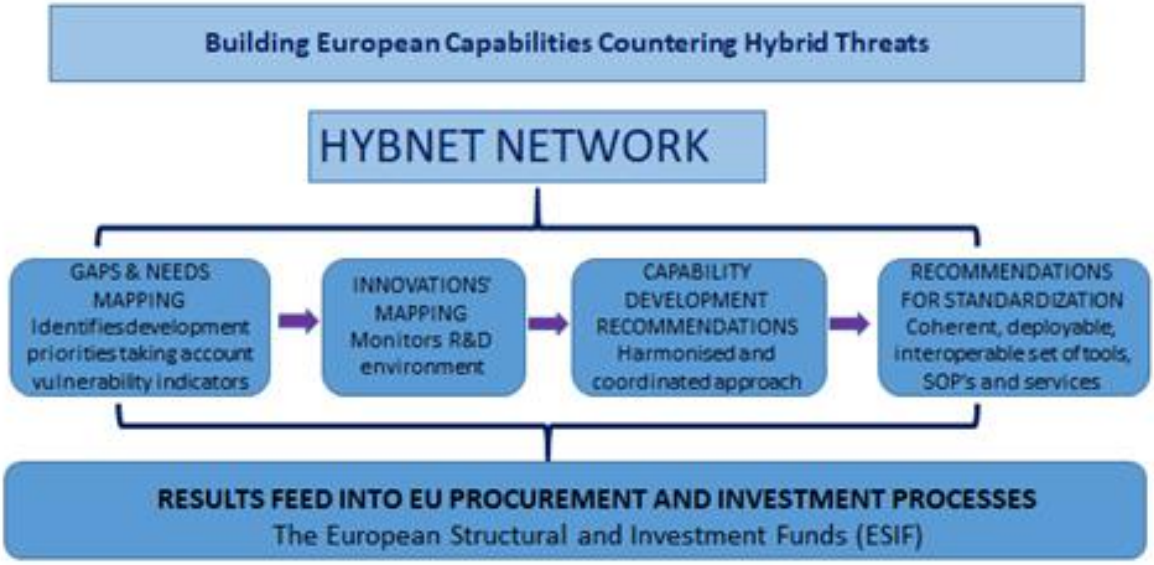

Figure 7 EU-HYBNET key building blocks

Moreover, Mattila explained that the project objectives have a crucial role in the project's implementation, and he reminded that the EU-HYBNET has seven objectives (OB) – the OB. are:

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

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

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

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

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

OB7. To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners, especially those whose daily work primarily involves coordination of operations

After the explanation of the OB, Mattila gave a short introduction to the EU-HYBNET project process and content. The EU-HYBNET has an iterative approach, consisting of three full scale project cycles in three core activity areas: i) research (incl. training), ii) innovation monitoring, and iii) recommendations for standardisation and innovation uptake (including industrialisation). Additionally, in a concluding fourth cycle, the project will collect results from each of the previous three cycles, draw conclusions, and make suitable recommendations. The figure below depicts the structure of the principal activities of EU-HYBNET. Each cycle will employ measures of high quality that will allow for agile responses to the proliferation of hybrid threats by continually increasing the network's membership with professionals that will be trained to deal with hybrid threats and have the potential to enhance European capabilities along the same lines.

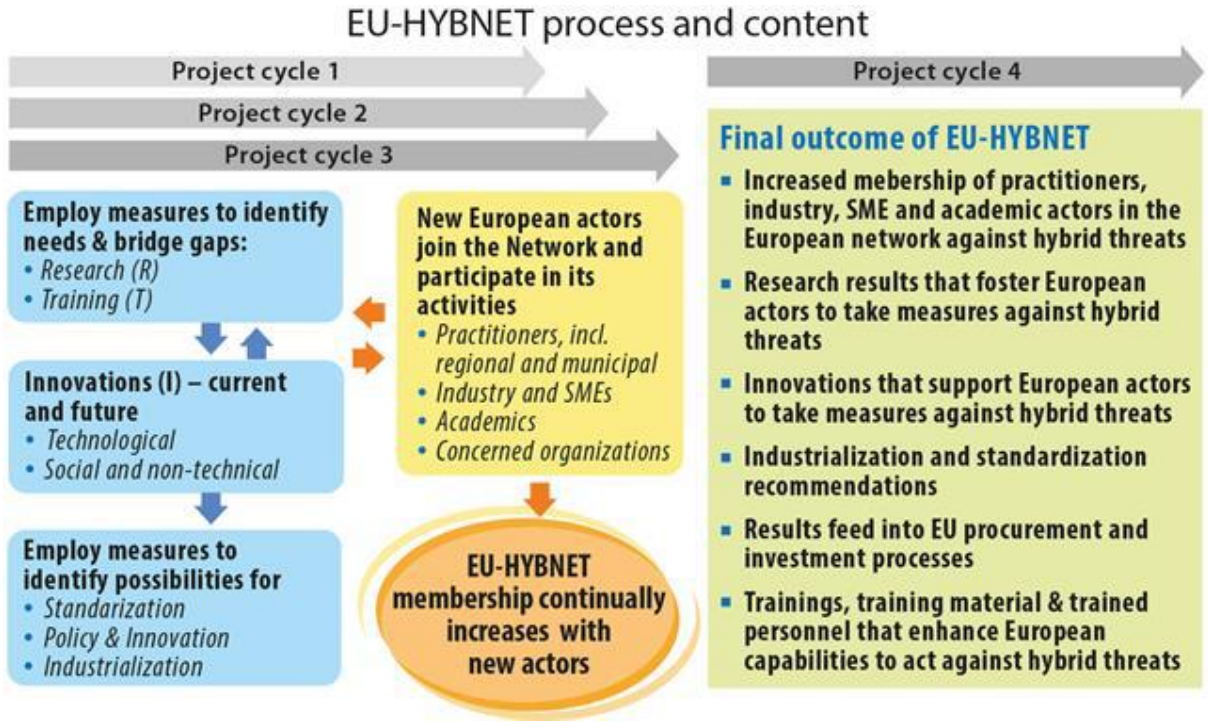

Figure 8 EU-HYBNET process and key content

The presentation also summarized the main short and long term impacts set to the EU-HYBNET.

The EU-HYBNET has defined three short term impact to the project. The first impact is related to the innovations definition and recommendations. In short, EU-HYBNET is to deliver definitions of most promising innovations to counter hybrid threats and to provide a common understanding of innovation potential. This will be done by creating and hosting interaction and discussions between practitioners, industry/ SMEs and academia. The discussion and dialogue is to bring mutual understanding on the most relevant innovations for European practitioners to counter hybrid threats. This will finally contribute to an expression of innovation uptake and standardization recommendations.

The second short term impact to the EU-HYBNET is a greater involvement from public procurement bodies upstream in the innovation cycle. For greater involvement from public procurement bodies EU-HYBNET provides a 2-level approach. The first level includes the practitioners involved in EU-HYBNET. In short, the project starts with its 12 practitioner partner organizations from 10 countries and stakeholder group's 8 more practitioner organisations from 3 other countries (total 20 practitioners and 13 countries), which will extend every year with new practitioners during the 5-year run of the EU-HYBNET network project. In addition, the HybridCoE and JRC as a project partners provide link to all EU MSs. The practitioners will feed the innovative solutions identified and prioritised in EU-HYBNET into their own organisation, and especially into their national and in-house procurement agencies and departments. The second level includes the mapping of the current processes in the European procurement landscape with special attention to procurement of innovative products and services. This activity will not only be undertaken at the research task, but also by actively reaching out to procurement experts (and groups) such as the Procure2Innovate network. The connections to procurement experts and networks are in special focus in the project dissemination and communication activities.

Lastly, the third short term impact is defined to be more efficient use of investments made across Europe in demonstration, testing, and training facilities. Here EU-HYBNET's main contribution to the efficient use of demonstration, testing and training facilities is the extensive network itself. By bringing together a large variety of stakeholders (industry, SME, practitioners, academia, research and technology organisations, think tanks) from all regions throughout Europe, information exchange about national and private facilities, both existing and in-development, will lead at least to a clearer picture of a large part of Europe's landscape of facilities relevant for hybrid threats. Sharing facilities in the short or medium term will of course be a national or private responsibility (i.e. up to the partners.

The EU-HYBNET has only one expected long term Impact - creation of synergies with European, national and sub-national networks of practitioners. The activities to deliver this impact are imbedded to all project activities. In short, all project activities are planned to base on extensive interaction and information sharing between not only the project partners, but also additional European actors, esp. practitioner networks - The interactions between European actors on a large scale will tempt European actors from different backgrounds and with shared interests joining the EU-HYBNET network. This will, of course, over the long term, increase 'synergies with already established European, national and sub-national networks of practitioners in the field of hybrid threats,' and will give rise to a comprehensive extension of the European network against hybrid threats. In addition, the project dissemination and communication measures will ensure that new actors may become aware of the network's activities and by their own initiative. The sustainability if the EU-HYBNET network and its' connections to other Networks of Practitioners (NoP) is ensured by the fact that HCoE will continue to host the EU-HYBNET Network after the project duration.

The last part of the presentation summarized the project Work Package structure and its building blocks, Work Packages (WP). The WPs are presented in more details in the next chapter.

3.6 PRESENTATIONS ON THE PROJECT WORK PACKAGES 1-6

The KO included presentations of EU-HYBNET project WP 1-6. The goal of the presentations was to describe the planned project activities, milestones (MS) and deliverables (D). In addition, the focus in the presentations was to tell about the concrete actions that will support to achieve the WP Task results. The EU-HYBNET Gant Chart is highlighted in the Figure below:

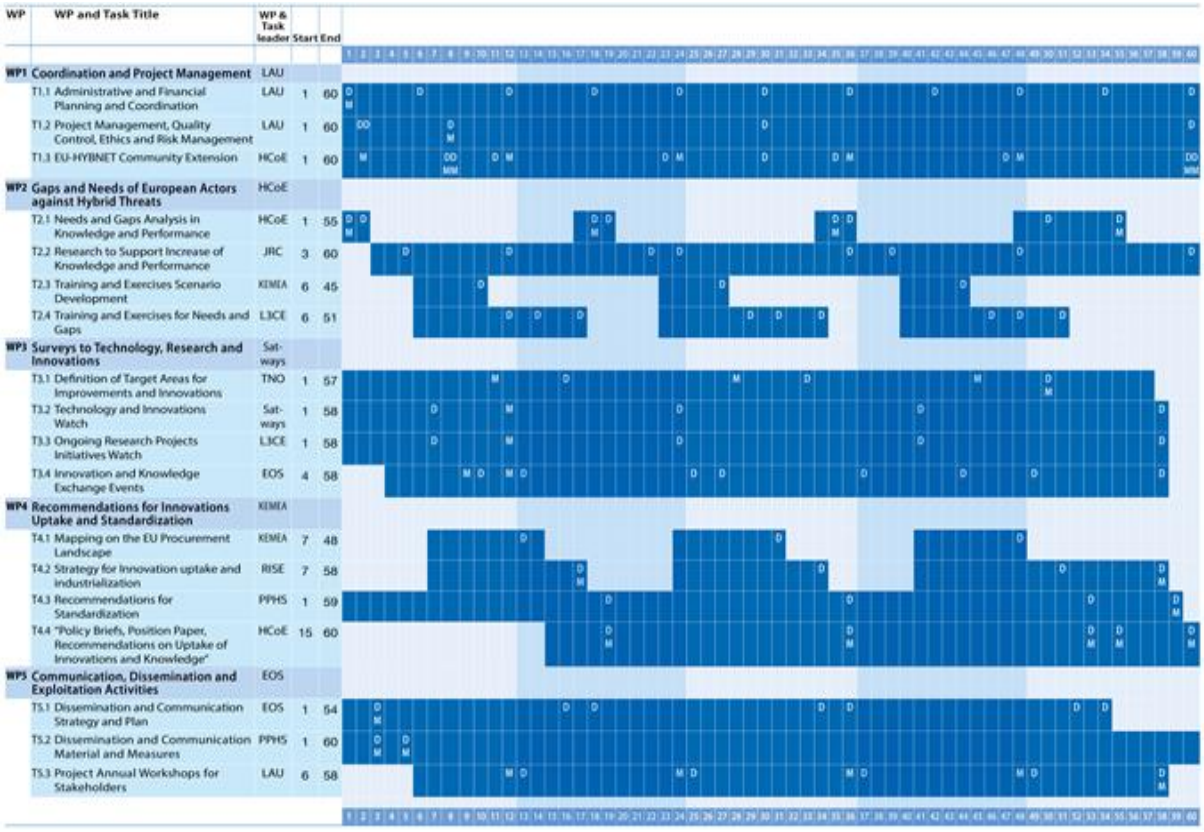

Figure 9 EU-HYBNET Gant Chart

3.6.1 WP1 - COORDINATION AND PROJECT MANAGEMENT

WP1 is led by Laurea and its duration is from M1 to M60. It has 25 D and eleven MS. The first MS is the Kick Off meeting. All partners contribute to the WP1 activities.

The purpose of WP1 is to manage and to ensure the coordination of efforts among all partners in order to guarantee effective operation of the project and timely delivery of the expected milestones as well as the management of project relations with the European Commission. In WP1 input is needed from all partners and the outputs concern all partners and all WPs since everyone is obliged to conduct activities related to project management and network extension in their own organization.

WP1 has five Task related objectives (OB.) - they are:

- OB. 1. To coordinate and manage all administrative and financial project activities and to ensure that consortium partners will conduct project administration well on time and with high-quality;
- OB. 2.To ensure that all project ethical, legal and quality aspects of the project are thoroughly addressed and conducted;
- OB. 3. To run project Boards (Scientific, Security Ethics, Security Advisory Board) activities:
- OB. 4. To identify, join and increase the amount new European expert actors to be involved with the EU-HYBNET network activities;
- OB. 5. to ensure sustainability of the EU-HYBNET network activities and existence also after the project.

The goal of the WP1 is also to contribute to the overall Project Objectives (OB.) 1, 5 and 7 – the OB. are:

- OB.1 -To enrich the existing network countering hybrid threats and ensure long term sustainability
- OB.5 - To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network
- 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 defined concrete actions in the WP1 Task will also deliver results to the named project general objectives.

The concrete actions to reach the WP1 and the project general objectives are conducted in the WP1 Tasks (T) – the Tasks are:

- *T1.1. Administrative and Financial Planning and Coordination (M1-M60) – lead by Laurea*
- *T1.2 Project Management, Quality Control, Ethics and Risk Management (M1-M60) – lead by Laurea*
- *T1.3 EU-HYBNET Community Extension (M1-M60) – lead by HCoE*

The concrete and most urgent actions in the implementation of the WP1 Tasks were described in KO to be as follows:

Task 1.1

- **Creation of deliverables (D) and milestones (M) lists with guidance** to plan forthcoming activities assists project progress and partners to proceed without challenges
- **Creation of project follow-up process** (e.g. includes set telcos and meetings) assists project execution and partners to proceed according to GA, CA, DoA
- **Creation of process** that support consortium in project reporting (incl. admin and finance issues) to the Comission on time and with quality
- Follow up and **guidance** that project reporting templates are created so that they include own section to describe the project's input to the three lines of actions
- **Guidance** that the project reports highlight findings related to the three lines of action (if applicable): 1) Recommendations of results for uptake or industrialization 2) Requirements

defined for innovations that fill gaps& needs 3)Knowledge and performance priorities set and standardization needs expressed

- Three lines of actions reporting results and findings are delivered to dissemination activities

Task 1.2

- **Set project internal meeting's agenda(s)**. They ensure information sharing and decision making and the actions points coherent uptake to project execution
- WP and Task leaders deliver together with Task contributing partners quarterly project internal report(s) that support project execution and management so that possible challenges are solved on time and proceeding with quality ensured
- **Eduuni** (for partners) & e.g. **TUOVI** (for Network members) **Platforms** are **taken into use** to for project information sharing and to support project execution and project management
- **Created processes and set agendas** to *Project Management-, Advisory-, Security Advisory Board and Stakeholder- , Security Advisory-, Ethical Advisory- and Scientific Advisory* group to work and to solve possible specific challenges in WPs& Task**.** This supports project execution's sound proceeding
- **Process and guidelines** to risk, conflict and delay follow-up and control are set in order to notice them on time and solve them in the early phase
- **Ethics & Societal Impact Assessment (SIA) procedures, guidelines and templates** are **created** and shared with partners in order to ensure that project notices all necessary ethical and SIA aspects in project execution. N.B. overlapping work with WP6/ Ethics will be avoided

Task 1.3

- **To provide a sound basis for extension** of the EU HYBNET
- Essential KPIs of 30 new members yearly at least and 3 events of over 100 actors represented engaging in information sharing from diverse fields.
- This action foresees therefore the **selection and validation of eligibility criteria** for new members to join the EU HYBNET network – organisations, projects, networks, associations and other stakeholders.
- Those **criteria** will serve as **a basis for network extension** towards new members with a view to benefit the overall purpose of EU-HYBNET
- **To ensure network sustainability; Fostering** European capacities of detection, reaction and response through increased arenas of collaborative work and information sharing.
- The **definition and validation of eligibility criteria** shall therefore take a longer term view as to ensure long term sustainability of the network in order to enhance the work accomplished throughout the project time-span. Key points:- New potential members to have demonstrated **concern and appreciation** for hybrid threats; New potential members to have a capacity to entice further partners into joining the network; **attraction capacity**
- Highlight central role of the Hybrid CoE as **essential driver** of the network's sustained work
- The initial and final sustainability **reports** will therefore aim at **providing a solid basis** of understanding in order to **push the work of the network forward** in the longer term.

3.6.2 WP2 - GAPS AND NEEDS OF EUROPEAN ACTORS AGAINST HYBRID THREATS

WP2 is led by the European Centre of Excellence for Countering Hybrid Threats (HCoE) and its duration is from M1 to M60. It has 28 Deliverables (D) and 4 Milestones (MS). The first MS is the start of the project 1. Cycle (M1). All partners contribute to the WP2 activities.

The purpose of WP2 is to identify gaps and needs of the European practitioners to counter hybrid threats. This will follow research activities to identified key gaps and needs in order to deliver solutions to the challnges. Moreover, WP2 will eventually arrange training where to test identified solutions (from WP3), incl. technical and non-technical innivations to cover the gaps and needs. This will feed into WP4 where innovation update and standardization recommendations will be compiled.

In WP2 input is needed from all partners and the outputs concern all partners and all WPs since everyone is obliged to conduct activities related to project gaps and needs definition.

WP2 has five Task related objectives (OB.) - they are:

- OB. 1. To identify critical gaps and needs of practitioners, industry and academic actors in knowledge, performance and innovations in the measures against hybrid threats;
- OB. 2, To increase European stakeholders' knowledge of the hybrid threats via research (focus on the four core project theme and their variations) and hence to enhance European actors' performance and measures against hybrid threats;
- OB. 3. To facilitate knowledge transfer on present and future cases through dedicated training and exercises and lectures;
- OB. 4. to test innovations that are seen likely to enhance European stakeholders measures against hybrid threats and provide material that supports to consider their possible uptake;
- OB. 5. To support the extension of actors in the European Network against hybrid threats via EU-HYBNET project four core themes' research activities and focus on new key actors in the network.

The goal of the WP2 is also to contribute to the overall Project Objectives (OB.) 2, 5 and 6 – the OB. are

- OB.2 - To define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats
- 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

The concrete actions to reach the WP2 and the project general objectives are conducted in the WP2 Tasks (T) – the Tasks are:

- *T2.1 Needs and Gaps Analysis in Capability and Knowledge (M1 – M55) - Lead by HCoE*
- *T2.2 Research to Support Increase of Capacity and Knowledge (M3-M60) - Lead by JRC*
- *T2.3 Training and Exercises Scenario Development (M6-M45) - Lead by KEMEA*
- *T2.4 Training and Exercises for Needs and Solutions for Gaps (M6-M51) - Lead by L3CE*

The concrete and most urgent actions in the implementation of the WP2 Tasks were described in KO to be as follows:

Task 2.1

- **Gather information** from partners about vulnerabilities, gaps and needs.
- Vulnerabilities **idenified**
- Needs **identified**
- Gaps **identified and sorted** with focus on the four project core themes (joint effort with 2.2). **Trends tracked**.
- Delivery of overall evaluation and conclusion of task 2.1.
- Delivery of an evaluation document ”What were the results and lessons learned”

Task 2.2

- Delivery of key gaps and needs of European actors’ measures against hybrid threats – **short list**
- **Selection** of research topics for the four project core themes
- **Injects for the scenarios** that foresee combinations of adversarial activities
- **Recommendations and guidelines** for practitioners and policy makers and other EU-HYBNET stakeholders

Task 2.3

- Training and Exercise **Scenario delivery and material for trainings** and/or exercises to be conducted under T2.4
- **Testing of innovative solutions** (recommended by WP3) to enhance European stakeholders’ measures against hybrid threats
- **Description of desired impact** under the objective of filling and fulfilling gaps and needs to tackle hybrid threats
- **Development of methodology** to measure the achieved impact
- **Delivery** of Lessons learnt for T2.4

Task 2.4

- **Identification and classification** of available materials:
- **Request** to Project partners about the available resources (Training modules available, Tools available, Methodologies in application).
- Open source simple **scan** of available relevant trainings outside the Project
- **Compilation** of training and training structure (purpose, structure, content, etc.)
- **Managing** the requests and alignment with relevant vendors and research initiatives to align to Scenario and Training structure
- **Delivery** of training and exercises (knowledge exchange event)
- **Preparation** for delivery of training and exercises (agenda, invitations, site, logistics, video...)
- **Deliver** training and exercises (knowledge exchange event)

- **Develop and deliver** training in lecture format
- **Execute** training evaluation process (evaluation questioners, feedback loop, etc.)
- **Evaluation** of Scenario used during the trainings
- **Evaluation** of tested innovations in order to provide information for WP3 and WP4 to define the innovations potential, needs for standardization and to compile recommendations of innovations uptake (incl. industrialization).

3.6.3 WP3 - SURVEYS TO TECHNOLOGY, RESEARCH AND INNOVATIONS

WP3 is led by SATWAYS and its duration is from M1 to M58. It has 18 Deliverables (D) and 7 Milestones (MS). The first MS is the start of the First project cycle of Innovation and Knowledge exchange events (M9). Majority of partners contribute to the WP3 activities.

The purpose of WP3 is to get from WP2 a longlist and shortlist of current (and if possible also future) gaps and needs as identified by the practitioners and the WP 2 team. WP3 will then use this as input to scan and monitor potential research and innovations that can cover the gaps, needs and requirements. This can range from existing and available research and innovations to future research and innovations. In the latter case this means that WP3 will identify and describe the type of research and innovations that is needed. The level of detail of these descriptions must be in such a manner that we can make a selection and prioritisation of the most promising ones, and that WP4 can define requirements for uptaking and standards for the prioritised research topics and innovations...

In WP3 input is needed from majority of partners and the outputs concern esp. WP4 and WP2 partners since they are obliged to conduct activities related to the relevant innovation testing (WP2) and innovation uptake recommendations and standardization (WP4).

WP3 has three Task related objectives (OB.) - they are:

- OB. 1. To map current and future needs for innovations across the different operational areas, focusing on practitioners and relevant actors; results will be populated via the innovation arena;
- OB. 2. To monitor and select currently available innovative solutions for measures against hybrid threats also with a view of possible standardisation;
- OB. 3. To arrange events where project partners will meet innovation (technical and Social, non-technical) providers that are invited outside of the project consortium to explain and demonstrate innovative solutions that match with the event theme and to interact with practitioners. The events will highlight what kind of innovations (existing or future) are needed and exists already

The goal of the WP3 is also to contribute to the overall Project Objectives (OB.) 3. and 5. – the OB. are:

- OB. 3. – To monitor developments in research and innovation activities as applied to hybrid threats
- OB.5 - To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network

The concrete actions to reach the WP3 and the project general objectives are conducted in the WP3 Tasks (T) – the Tasks are:

- *Task 3.1 Definition of Target Areas for Improvement and Innovations (M1- M57) – Lead by TNO*
- *Task 3.2 Technology and Innovations Watch (M1-58) – Lead by Satways*
- *Task 3.3 Ongoing Research Projects Initiatives Watch (M1-58)- Lead by L3CE*
- *Task 3.4 Innovation and Knowledge Exchange Events (M4-58) – Lead by EOS*

The concrete and most urgent actions in the implementation of the WP3 Tasks were described in KO to be as follows:

Task 3.1

- **Mapping gaps and needs onto solutions** (research, technologies and innovations in the area of hybrid threats)
- **Assessment of mappings** (e.i. black spots)
- **Prioritization** (clustering and feedback-loop)

Task 3.2

- **Assess** the relative technology innovations developed from the private sector (European companies)
- **Investigate** related innovative products from countries outside Europe
- **Analyze** the needs and gaps findings of Wp2 and the future needs assessment of T3.1

Task 3.3

- **Identify and select available techniques and tools** to perform the scanning and monitoring. Selection of sources. **Making an inventory of sources** that need to be scanned and monitored: partner accessible resources; Open sources, Internet, databases, other sources; Recent available technology and horizon scan reports; Closed/Personalized sources and databases like EU SCOPUS.
- Using the hybrid threats taxonomy (defined proposal Section1-3) and the selected techniques, methods, tools – this includes (1.) **Run surveys& gathering** of the information on the project partners' innovations& researches portfolio; Run surveys& gathering of the information on the extended partners innovations&researches portfolio on the topic; Perform available tools based scanning / monitoring perform scanning/monitoring; (2) Experts will **scan** sources using source specific search tools and develop long list of the research; (3)Experts will **review** long list and will make a short list of most relevant research, detalizing relevance to identified gaps&needs
- **Run** a workshop to conceptualize findings and **align** identified results to Needs&Gaps

Task 3.4

- **Organisation** of three "Innovation and Knowledge exchange " events
- **Organisation** of five "Future Trends" 5 Workshops.

3.6.4 WP4 - RECOMMENDATIONS FOR INNOVATIONS UPTAKE AND STANDARDIZATION

WP4 is led by KEMEA and its duration is from M1 to M60. It has 16 Deliverables (D) and 8 Milestones (MS). The first MS is the start for innovation uptake and industrialization strategy compilation (M17). Majority of partners contribute to the WP4 activites.

The purpose of WP4 is to build a strategy for achieving the uptake and industrialisation as well as the standardization of the most promising innovations to counter hybrid threats.

In WP4 input is needed from partners representing esp. WP3 and the outputs concern whole project since the WP4 delivers recommendations on innovation uptake and standardization and policy briefs on the key project findings.

WP4 has six Task related objectives (OB.) - they are:

- OB. 1. Analysis of the current standardisation and procurement landscape
- OB. 2. Develop benchmark cases in order to define the cornerstones of on innovation uptake and industrialisation methodologies followed up to now.
- OB. 3. To uptake the results of WP2 and WP3 and select feasible innovations areas and projects of European actors against hybrid threats in order to foster the hybrid threat situational awareness;
- OB. 4. To build a concrete roadmap on innovation uptake
- OB. 5. To compile recommendations for standardisation activities
- OB 6. To deliver Policy Briefs, Position Paper and Recommendations on key innovation and knowledge areas of European actors against hybrid threats

The goal of the WP4 is also to contribute to the overall Project Objectives (OB.) 4:

- OB. 4. - To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats

The concrete actions to reach the WP4 and the project general objectives are conducted in the WP4 Tasks (T) – the Tasks are:

- *Task 4.1 Mapping on the EU Procurement Landscape (M7 – M48) - Lead by KEMEA*
- *Task 4.2 Strategy for Innovation uptake and industrialisation (M7– M58) – Lead by RISE*
- *Task 4.3 Recommendations for Standardization (M1 – M59) – Lead by PPHS*
- *Task 4.4 Policy Briefs, Position Papers, Recommendations on Uptake of Innovations and Knowledge (M15 – M60) – Lead by HCoE*

The concrete and most urgent actions in the implementation of the WP4 Tasks were described in KO to be as follows:

Task 4.1

- **Preparations** for source scanning: Questionnaires preparation; Links to stakeholders for material and information collection; Defining a criteria set enabling the procurement procedures and current practices assessment
- **Collect** material: Collect answers to the questionnaires; Collect and Review material

- **Analyze** material collected & **draw results**: Analyse answers and material based on the criteria defined, Production of results, Detection 'grey spots' (e.i. problems in procurement activities) that do require extra attention and recommendations)

Task 4.2

- **Preparation** for the analysis/ **Collect** material for activities of the other WPs and T4.1.; **Identify** the methodological framework for the strategy creation
- **Analysis** of the material: Identification and assessment of good practices and possible pitfalls in innovation uptake procedures and processes for innovation uptake; Identification and assessment of good practices and possible pitfalls in innovation uptake procedures and processes for industrialisation of solutions; Selection of the areas that the strategy will comprise
- Stategy **preparation: Select** feasible innovation areas and projects; Concrete strategic approach for innovation uptake and industrialisation will be **defined**.

Task 4.3

- **Preparatory** actions: Select methodology; Collect feedback from WP2-4; Identify and opportunities needs for standardisation; Map current Status; Conduct 3 workshops where a standardisation focus be discussed on a given theme
- **Compile recommendations** for standardisation: Analyze the material collected, Analyze which stakeholders are suitable for the outcomes, Barriers to standardization will be assessed, Prepare standardisation recommendations

Task 4.4

- **Preparatory** actions: Mapping results from all WPs ; Analyze material; Identification of priorities; Coordination of producing
- **Prepare** policy briefs , recomendations , papers: Policy brief possible focuses for innovation uptake and building resilience to hybrid threats: less attractive areas for uptake and industrialisation, recommendation in changes on national and EU policies, best practice & new concepts, standardisation, future innovation needs, needs for training activities and needs not yet addressed; Provide recommendations on future focus research areas

3.6.5 WP5 - COMMUNICATION, DISSEMINATION AND EXPLOITATION ACTIVITIES

WP5 is led by European Organization for Security (EOS) and its duration is from M1 to M60. It has 14 Deliverables (D) and 4 Milestones (MS). The first MSs are MS31 "Dissemination, Communication and Exploitation Plan" and MS32 "Website" both are delivered in M3. All of partners contribute to the WP5 activities.

The purpose of WP5 is to disseminate results and interact with other relevant networks; create conditions for better interactions with Industry, Research and Academia; finally to enrich existing network against Hybrid threats with Academics, Practitioners, Stakeholder and Industry Actors across Europe.

In WP5 input is needed from all partners and the outputs concern all partners and all WPs since everyone is obliged to conduct dissemination, communication and exploitation activities.

WP5 has three Task related objectives (OB.) - they are:

- OB. 1. to disseminate results and interact with other related networks; ,
- OB. 2. to create conditions for better interaction with industry, research and academia;
- OB. 3. to enrich existing network against Hybrid threats with academics, practitioners, stakeholders and industry actors across Europe

The goal of the WP5 is also to contribute to the overall Project Objectives (OB.) 1, 5 and 7 – the OB. are:

- OB.1 -To enrich the existing network countering hybrid threats and ensure long term sustainability
- OB.5 - To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network
- 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 concrete actions to reach the WP5 and the project general objectives are conducted in the WP5 Tasks (T) – the Tasks are:

- *Task 5.1 Dissemination, Communication and exploitation Plan (M1-M54)– Lead by EOS*
- *Task 5.2 Dissemination and Communication Material and Measures (M1-M60) – Lead by PPHS*
- *Task 5.3 5.3 Project Annual Workshops for Stakeholders (M6-M58) – Lead by Laurea*

The concrete and most urgent actions in the implementation of the WP4 Tasks were described in KO to be as follows:

Task 5.1

- **Development of operational dissemination procedure**. By defining how to cooperate with other funded projects and initiative. This will be an useful toolto extend the membership of the EU-HYBNET Platform. It will provide also a definition of targeted audiences and tailored messages, thanks also to the support of all Partners.
- **To develop dissemination protocols for news**, and communication material in general.

Task 5.2

- **Introduction of Social Media Channels**, with a continuous engagement with interested stakeholders and a consistent visual and written representation of the Project actions and related results;
- **Development of the website**, which will be engaging and user-friendly website providing all users with the relevant information about the project, its objectives and expected results. As well as representing a hub for all outbound content relevant to the audience, to include: news, partner information, events, project deliverables, etc.
- **Development of initial dissemination materials.** A selection of materials to be used electronically and in print by all Partners to share information about EU-HYBNET (like logo,

leaflet, roll-up, newsletter, etc.). this will be done through means of a cohesive design and content, by keeping in mind the vision and project communication plan and strategy.

- **Innovation Arena.** A place to collect the hybrid threat innovations needs of partners and external stakleholders. An environment to display and explain solutions tailored to the specific needs elicited from users. An area to foster discussion and interactions between the parties raising challenges, and the actors providing the solutions.
- **Analytics and measurement for KPIs.** To ascertain how users interact with EU-HYBNET and its various platforms. To gather data and information that allows the team to alter their strategic plan towards communication and dissemination activities. To understand the effective channels for communication and dissemination, helping to maximise reach and impact of project efforts.

Task 5.3

- **Arrange yearly project Annual Workshop.** By raising awareness of the project, support dissemination of project findings and assess their feasibility. Ensuring a vivid interaction with Industry and Academi, and other providers of innovation solutions outside of the Consortium. By ensuring sustainability of the project activities. By fostering network activities and to increase members in the network.

3.6.6 WP6 - ETHICS REQUIREMENTS

This WP6 is led by Laurea, and its duration is from the first month until the very last, i.e. M1-M60. WP6 has four Deliverables and no Milestones.

The objectives of this WP6 are:

- to ensure that all actions of EU-HYBNET are in compliance with the ethics & security requirements set out in this WP.
- WP TO set out the ethics requirements that the project must comply with.

Laurea is the sole responsible for WP6 all Tasks, still input is needed from all partners. Also, the outputs concern all partners and all WPs since everyone is obliged to follow the ethical requirements.

This WP does not have specific tasks *per se*. The action of this WP is around two things:

- identifying the pertinent and needed information and requesting them from all partners; and
- formulating the gathered information into forms, templates and into deliverables.

The WP6 deliverables (D) will be submitted all on M6 and hence the work for the Ds has been started. The Ds are the following:

D6.1 Humans Involvement – Requirement No. 1
D6.2 Protection of Personal Data – Requirement No. 2
D6.3 Non EU-countries, Third countries – Requirement No. 4
D6.4 Potential Misuse – Requirement No. 5

The content of these deliverables will cover ethical issues on:

- Process and criteria to identify/recruit research participants;
- Appointment of the DPOs, information of all the DPOs (and if not, the detailed data protection policies);
- Description of security measures to prevent unauthorised access to personal data, equipment use to processing; Descriptions of anonymization/pseudonymisation techniques; Confirmation that the personal data transferred to and from EU country and non-EU country is done in accordance with Chapter V of the GDPR and national law; Legal basis for further processing of personal data; Information on informing data subjects that are tracked;
- Ethical standards and guidelines of H2020;
- Risk assessment and details to prevent misuse of the research findings;
- Consent forms, information sheets and other templates;
- Report on the DPOs;
- Confirmation on the rigorous following of the ethical standards and guidelines;
- Risk assessment and report on the misuse of EY-HYBNET research results.

3.7 PRESENTATIONS ON THE PROJECT FOUR CORE THEMES

The EU-HYBNET project has a selected a Conceptual Model approach (developed by the Hybrid CoE and the Joint Research Centre (JRC)) to characterise hybrid threats and to line the EU-HYBNET research focus. The conceptual model integrates all relevant parameters, such as actors, tools, domains and timeline, with a view to furnishing an extensive landscape of hybrid threats and thereby helping experts to adequately assess crisis incidents and to design counter-measures. This model will be the basis for understanding hybrid threats in the contemporary security environment. Indeed, it is the conceptual cornerstone of the EU-HYBNET project, which demonstrates a strong commitment to operate in accordance and in support of the European Comission (EC) JOIN (2016) and SWD (2019) communications. The Conceptual Model approach is described in figure below:

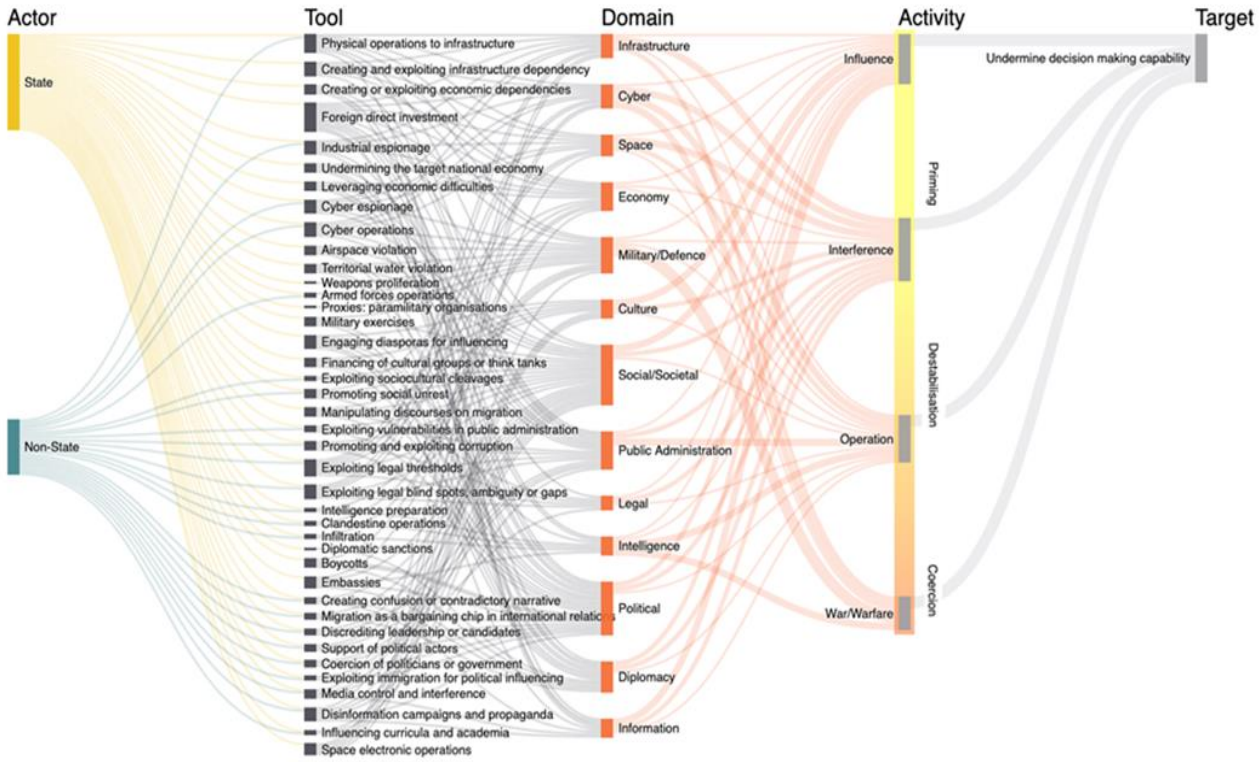

Figure 10 EU-HYBNET research methodology - Conceptual Model

The conceptual model defines that hybrid threats can arise in any of 13 different domains. This means also a new approach to find countering solutions. EU-HYBNET has selected four project core themes to ensure coherence with the Conceptual Model approach and the project's results – the four core themes are: *1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 4) Resilient Civilians, Local Level and National Administration, 4) Information and Strategic Communication*. These four core themes will create an opportunity to focus on all hybrid threat domains, including interfaces between the domains, and will ensure that the project delivers coherent results in relation to the model. In addition the selected approach is seen to provide a solid foundation for European actors to carry out EU-HYBNET project activities. The activities are: research and innovation monitoring, defining new measures for countering hybrid threats , expressing common requirements as regards innovations that could enhance capabilities, bridge gaps and improve future performance, identifying priorities in areas requiring increased standardization.

3.7.1 EU-HYBNET RESEARCH FOCUS

The overview of the EU-HYBNET guiding approach, the Conceptual Model was given by the European Commission Joint Research Centre (JRC), Mr. Georgios Giannopoulos who is also the EU-HYBNET Task 2.2 "Research to Support Increase of Capacity and Knowledge" leader.

In the beginning of the presentation Giannopoulos gave a general presentation on the Conceptual Model and explaned how hybrid threats are seen to arise in 13 different domains. Furthermore, Giannopuolos described that the four project core themes (Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communication) are expected to focus to all 13 domains, including interfaces between the

domains. and hence the project is able to deliver coherent results in relation to the model. The 13 domains in the conceptual model are described in the figure below:

Figure 11 EU-HYBNET research focus on 13 identified hybrid threats domains

Furthermore, Giannopoulos described that when European practitioners' gaps and needs to counter hybrid threats are mapped and defined (in the beginning of the each project cycle), the research focus will be on vulnerabilities. In short, the vulnerability assessment is seen as a novel and incisive approach compared to the common risk assessment in the context of hybrid threats. The figure below highlights the selected focus:

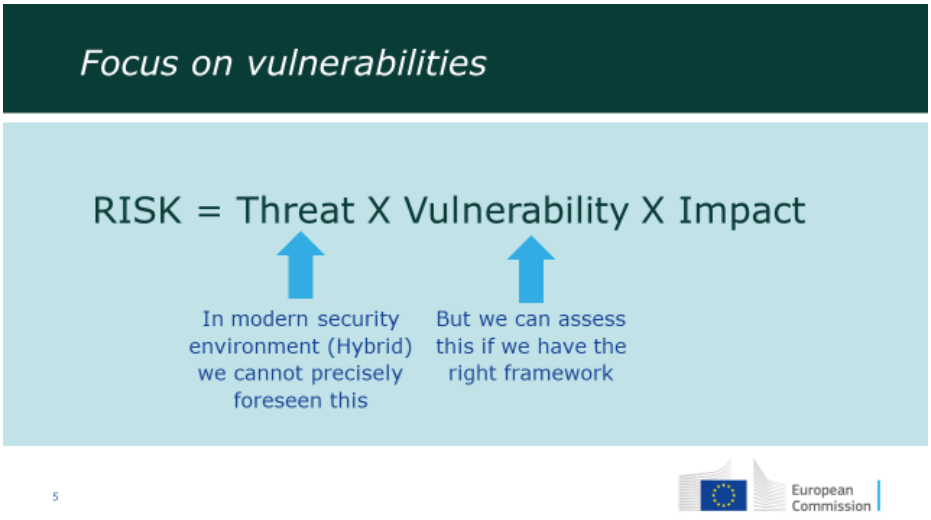

Figure 12 EU-HYBNET rationale to use vulnerability assessment

In the end of the presentation it was summarized how the Conceptual Model, 13 domains, the four core themes and the vulnerability assessment complete each other and ensure sound basis for the project to build on its assessment on European practioners' gaps and needs to counter hybrid threats and potential innovations to fill the gaps and needs.

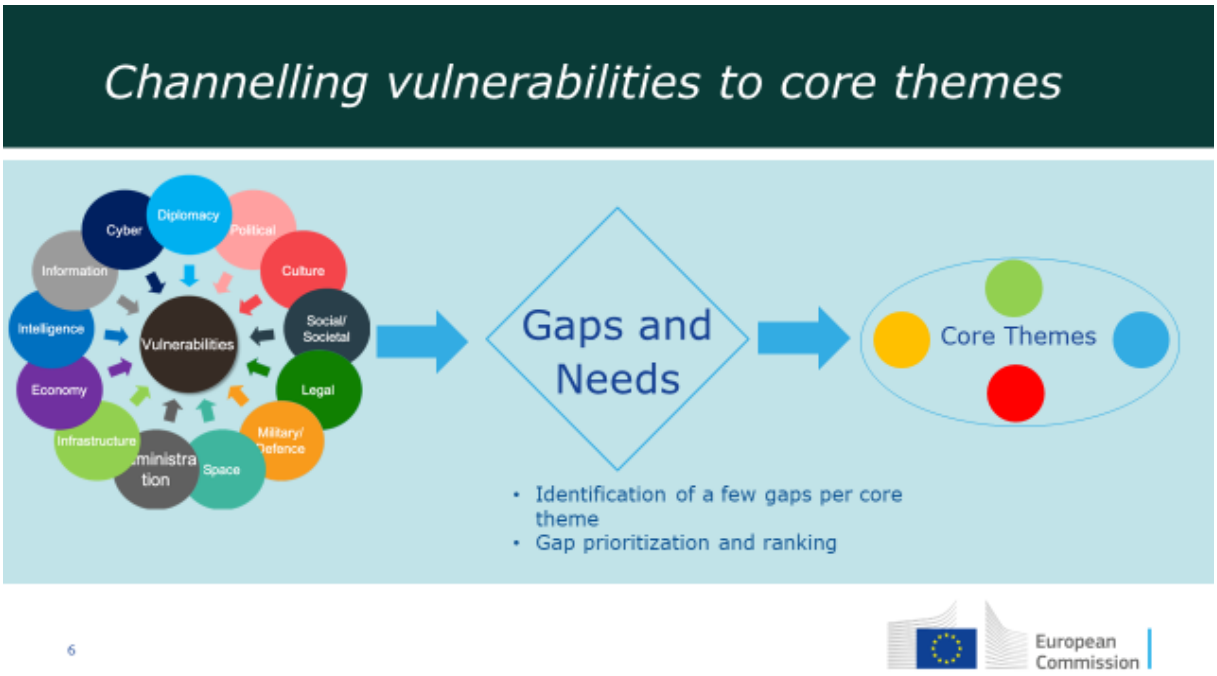

Figure 13 EU-HYBNET research focus and its core elements

The presentation was followed more through presentation on the each EU-HYBNET four project core themes.

3.7.2 FUTURE TRENDS OF HYBRID THREATS

The EU-HYBNET project core theme "Future Trends of Hybrid Threats" (Theme 1.) is led by Hybrid CoE and a presentation of theme was given by Mr. Maxime Lebrun from Hybrid CoE.

The essence of the Theme 1. is to produce foresight in order to address the indetermination of hybrid threats as much as possible in imagining and paring for a greater range of eventualities. In short, it is seen that trends are paradigms in order to characterize the dynamics of the security environment of hybrid threats. Furthermore, the logic in Theme 1. is to mapp a greater range of practitioners' vulnerabilities, capability gaps and needs. This is done according to the project research focus, esp. focusing on the 13 domains of hybrid threats and how they interface. In general the Contribution of the Theme 1. to the project is to provide a baseline and continuing dynamic for the definition of practitioners' requirements, identification of knowledge gaps and needs. In this work the focus is on cross-domains span, foresight orientation and the findings and proceedings within the Core Theme 1. will innerve the research, innovation and training endeavours. Lastly, the Theme 1. will have a strong Interrelation to the other project four core themes through the corresponding KPIs and deliverables, the trends mapping should inspire the other Core Themes. Moreover, the possible overlaps with other Core Themes will be taken care of by active communication and collaboration with the other Themes and the Theme1. goal is to provide ground for reflection in the other Core Themes by proposing and testing a series of overarching trends of hybrid threats. The Theme1. has defined a 4-steps circular working method – from data collection to deduction of capability needs:

1. crowdsourced data collection: consortium members' vulnerabilities, gaps and needs assessments

2. induction of explanatory trends: characterizing the threat perceptions and the determinants of the security environment of hybrid threats
3. identification of supporting variables to the trends: variables working as indicators of the trends' heuristic value
4. Deduction of critical capability needs to be adressed: based on the security trends and corresponding capability gaps identified

The importance of the Theme1. is to ensure that the attention is paid to changing nature of hybrid threats over time, and the focus of the EU-HYBNET project will be up to date to the European actors needs to counter hybrid threats.

3.7.3 CYBER AND FUTURE TECHNOLOGIES

The EU-HYBNET project core theme "Cyber and Future Technologies" (Theme 2.) is led by L3CE and a presentation of theme was given by Mr. Evaldas Bruze/ L3CE.

In the beginning of the presentation Bruze explained a logic and definition of Theme 2. In short, the theme 2. focuses on cyber and cyber mediated threats and potential attack vectors, based on following three aspects:

- Emerging future cyber related technologies
- Radically new uses of new technologies
- Understanding of new perpetrators' methods

Furthermore, Bruze explained method and focus to be two-fold in the EU-HYBNET Theme 2.:

- To focus the research and provide common narrative, the complex, "hybrid-threat friendly" subject of "Election Interference" will be applied
- Cyber and Cyber related emerging threats and threat vectors will be discussed and analyzed, further broadening them for wider application.

In addition, Bruze explained that the Theme 2. will use a 4-steps circular working method to deliver expected results in the EU-HYBNET project. The method includes following 4 steps:

- Self-governing volunteers' group (experts in the field)
- Facilitate crowdsourced data collection
- Induction of explanatory trends
- Prioritization and focusing of cross WP work in the scope of selected topicality

The importance of the Theme 2. to the EU-HYBNET project is that EU pays a lot of attention to analyzing the trends in cyber issues and cyber security can be characterized as a frontline field of concern for any hybrid activity. In short, adversaries often use cyber attacks and hence the cyber security and future

technologies theme is pertinent to address seriously in all aspects in the EU-HYBNET project and its results.

3.7.4 RESILIENT CIVILIANS, LOCAL LEVEL AND NATIONAL ADMINISTRATION

The EU-HYBNET project core theme "Resilient Civilians, Local Level and National Administration" (Theme 3.) is led by the University I Tromso (UiT) and a presentation of theme was given by professor Gunhild Hoogensen Gjorv/ UiT.

In the beginning of the presentation the importance of the Theme 3. was highlighted. In short, knowledge about civilian agency actions during crisis or conflict is very limited and hence this requires further research in order to enhance resilience in socities. In general, there are only some assumptions what might be the role of civilians during the crises – the main assumptions are:

1. conflict carried out and managed «from above» (agencies, organisations like militaries, governments)
2. Conflict happens to civilians
3. Civilians are passive elements?

However, Hoogensen-Gjorv also explained that at least some key elements on civilians role in crises are known. First, civilians are engaged and second they are active depending on their ability (full agency, controlled agency, restricted or no agency), thirdly civilians seek human and societal security. Even so, Hoogensen-Gjorv emphasized that there is still need to focus more to general population behaviour and reactions during crisis, in relation to preparations made by civilian and military authorities. For this reason, the Theme 3. sees that its theme, the role of populations, intersects with all the other EU-HYBNET project four core themes. Therefore, the Theme 3. seeks strong cooperaiton with other four project core theems and esp. data collection will be coordinated with the other themes in order to prevent overlap. However, the Theme 3. focus the following aspects in data collection:

- Media types and methods (including algorithmic approaches)
- potentially vulnerable or susceptible groups
- Surveys on trust
- Case studies
- Overview of national/local crisis management plans - where do civilians fit in and how?

In the end of the presentation the Theme 3. listed its' theoretical analytical approaches to consist on: Civilian agency, Societal trust, Resilience, Populism/Nationalism, Societal security; the key is that when Connected to civilian agency we will explore linkages with assumptions about the role of societal trust between people and authorities.

The Theme 3. is important to the EU-HYBNET project because the theme serves as a framework to assess whether EU level activities really do reach the grass roots level. Due to subsidiary considerations, EU policies will trickle down through a long chain of transformations on national, regional and local levels. Through our gaps and needs analysis, practitioners will be able to assess the

effectiveness of policies, and whether the recent steps taken have actually addressed the most critical issues in a practical manner.

3.6.5 INFORMATION AND STRATEGIC COMMUNICATION

The EU-HYBNET project core theme "Information and Strategic Communication" (Theme 4.) is led by the University of Rey Juan Carlos (URJC) and a presentation of theme was given by professor Rubén Arcos/ URJC.

In the beginning of the presentation Arcos explained the framework of the Theme 4. In short, Arcos highlighted that communication is to be seen as a process (models, elements of the process) and combination of symbolic communication and behavioral communication (signaling through behaviour or absence of behaviour). Furthemore, Arcos emphasized that a key is the actor, "Who" (State, non-state, state-affiliated) says or delivers a certain message "what" (information, disinformation, misinformation, malinformation – product perspective). Furthermore, according to Arcos the other relevant questions in the framework are:

- On behalf of whom (or on its own behalf) something is said?
- Attribution challenges (gaps and needs)
- With what intentions? (intelligence assessment)
- In what situations? (situational vulnerabilities of the target)
- With what assets? (capability assessment – intelligence perspective; owned, shared, and paid media; technologies) Ecosystem of media for information influencing and patterns of behavior
- Using what strategies (key messages and channels)?
- To which audiences? (audience perspective, target vulnerabilities)
- Producing what kind of effects? (evidence-based outputs, outtakes, outcomes – cognitive, affective, behavioral effects) Laboratory through SimDeck an Internet (and Social Media) simulator (consent from participants; feed with Maldita's database of cases)

With reference to the selected framework Theme 4., Arcos explained that following issues will be addressed in the research conducted in the EU-HYBNET project:

- Malicious Information influencing; Manipulative interference; Narratives (exploiting target's vulnerabilities: social, historical, economic…) and conspiracy theories
- Ecosystem of media for information influencing and patterns of behavior, Owned/affiliated/covertly sponsored media assests and shared media used and likely to be used. Ad-hoc alliances; Generative medias (articles, pictures, video, sounds) and audiovisual forgeries (new trends). E.g. G&N for detection and analysis, and training
- Case studies: country specific; big hits; replays; Trends and scenarios
- Communication effects: measurement and evaluation methods and techniques; Propaganda analysis techniques; Social media listening platforms; Content likelihood to be shared; Attribution
- Counter communication strategies and tactics; Planning and implementation issues; Mitigation and deterrence by denial; Indications and warning perspective on malicious information influencing/reflexive control. E.g. Hybrid information influencing indicator list,

Indications of hybrid information influencing activities Information-Intelligence G&N analysis, Open source collection for target audience segmentation in information influencing.

The importance of the Theme 4. to the EU-HYBNET project is that EU pays a lot of attention to analyzing the trends in *strategic communications* and the theme can be characterized as a frontline field of concern for any hybrid activity. In short, adversaries often use media as a target and hence the Theme 4. is having an important role in the EU-HYBNET project focus and results.

3.8 PRESENTATION ON EU-HYBNET DISSEMINATION ACTIVITIES, INCL. INNOVATION ARENA

3.8.1. DISSEMINATION AND COMMUNICATION ACTIVITIES

The presentation on project dissemination activities including innovation arena has been characterised with current and upcoming planned activities and their objectives in order to support communication and disseminate results of the project to the wider audience, as well as to support the network extension.

The presentation was started by the WP5 Dissmeinaiton and Exploitation leader EOS on foundations of dissemination ctivities and their objectives. Dissemination of results will ultimately contribute to the progress of the project findings and of science in general:

- To **link EU-HYBNET to the policy context** of the call for proposal and to current items;
- To **prepare the exploitation and dissemination plan carefully**. Initially this will have first steps and the final goal. This plan will be updated during the project, in order to make it more detailed.
- To **involve potential end-users and stakeholders** (this through linking with other funded projects, as well as through the means of the innovation arena)
- To **implement open access to some of the data produced during the project activities** (such as communication material and some of the deliverables that may be useful to share in order to increase the participation to the Innovation arena).
- To **provide recommendations as results of the activities** of the several events we will organize;
- To **understand what are the potential barriers to any application of EU-HYBNET's results** and how the Consortium plans to tackle them.

Furthermore, the presenters from EOS revealed concrete actions with regards to dissemination and communication of project activities to wider multiple audiences.

The first and most important activity is to draft a comprehensive communication plan that defines clear objectives and supporting KPIs, as well as messages adapted to the relevant target audiences, setting-out also a description and timing for each activity.

Activities within the dissemination and communication plan that will take place during the project are as follows:

- **Website**, which will be mainly addressed to Practitioners, Academia, Industry, Policy Makers and the wider public
- **Social media channels** (starting with LinkedIn; Twitter and YouTube), which will mainly address the wider public; as well as Practitioners, Academia, Industry, Policy Makers when it comes to LinkedIn and Twitter.
- **Innovation Arena**, which will be mainly addressed to Practitioners;
- **Annual Workshops, Gaps and Needs events, and other face-to-face activities**, which will be mainly addressed to Practitioners, Academia, Industry and Policy Makers.

Communication activities will also be done through means of:

- **Flyers, Brochures, Posters**, and other traditional campaign tools as needed, which will be uploaded on the EU-HYBNET website, in a specific section, ready to be downloaded;
    - These documents will be updated from time to time, as new milestones in the projects will be reached;
- **Newsletter**, every 6 months EU-HYBNET will issue a newsletter for its subscribers and members of the Consortium that will comprise all important information related to the core themes of the Project; as well as advertising Project results, events, etc.

3.8.2. INNOVATION ARENA

The project dissemination and communication plan also includes the creation of the Innovation Arena (IA) platform, planned to be carried out by Laurea UAS in M5 and will continue running until M60. Since this deliverable is still on the design phase, a brief presentation was given on the main use case scenarios, logic of content relations, the added value to the project by the IA and the security and data protection related information.

The core usefulness of the IA platform is that it will enable project partners and other network members to provide input to identified challenges (gaps & needs), that will ultimately support WP3 and WP2 and eventually WP4 to deliver the recommendations of the most promising innovations uptake (incl. industrialisation).

The IA will be a social Idea management platform as it will have also social elements integrated into it such as; Members, Votes, Likes, Discussions, Sharing of content, private messages between members, e-mail notifications and more.

The main use cases of the IA will be as illustrated in the figure (IA use cases) below:

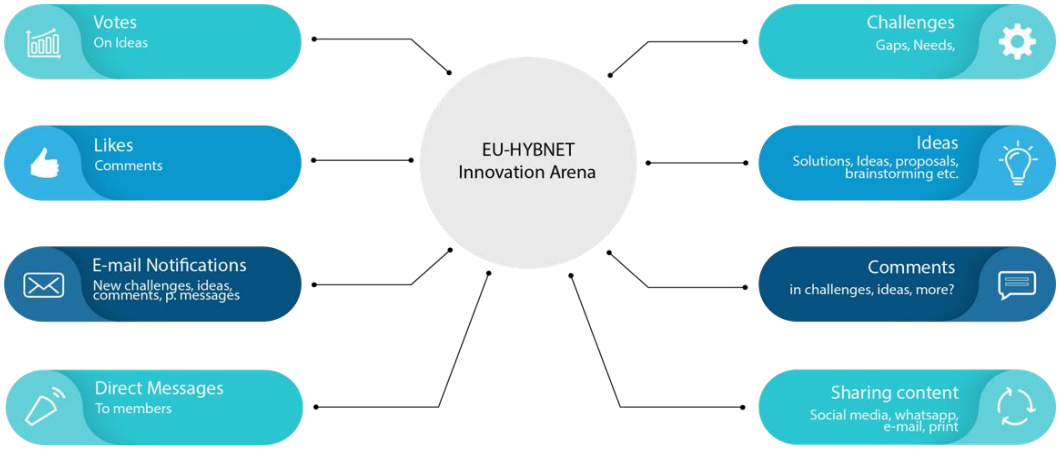

Figure 14 IA use cases

The two main contents of the Innovation Arena will be Challenges and Ideas. These content types will work interlinked with one another. I.e. Ideas can exist within challenges or on their own as standalone solutions to unidentified challenges. Here with Challenges we will be referring to issues such as gaps and needs while with ideas we will refer to solutions to challenges (gaps and needs) i.e. ideas for improvement, new technologies and so on. Furthermore both content types will have possibility to contain illustrative images, documents, active time, discussions and so on.

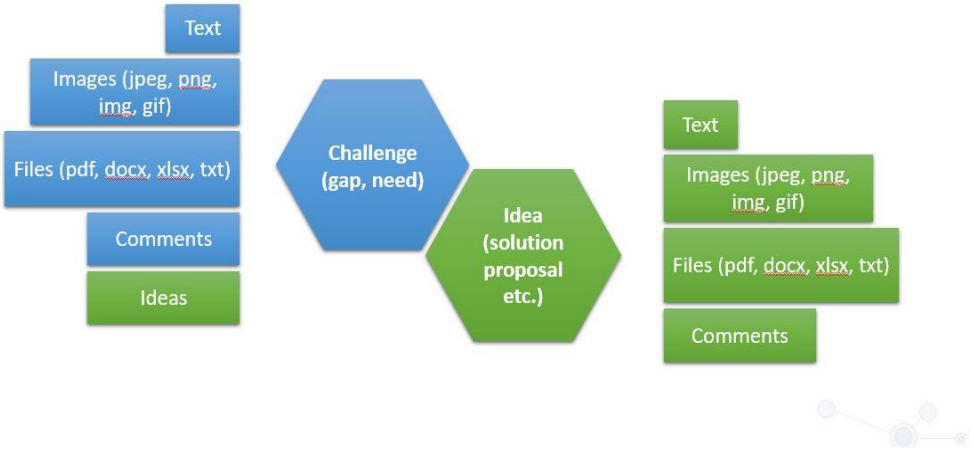

Figure 15 IA content types

The IA will have a central role in the EU-HYBNET innovation mapping. In short, by building an on-line Innovation Arena (IA) Platform the project provides an arena for project partners (esp. practitoners) and those who will join via the project to the European Network against Hybrid Threats to announce their needs for new innovations. In addition, in IA those project and network members (esp. industry, SMEs, academics) who may provide possible solutions to announced innovation needs may tell about their solutions and what is reasonably expected, and according to which timetable. The project will use the IA discussion between those who need and those who may deliver innovations (technical and social) in Work Package (WP) 3 and WP2 for their research and analysis activities in order to find the

most promising and potential innovations that answer to practitioners needs and can be recommended to the standardisations process.

3.9 HORIZON SCAN OF TRENDS AND DEVELOPMENTS IN HYBRID CONFLICTS SET TO SHAPE 2020 AND BEYOND

A presentation of trends and developments in hybrid conflicts was given by the Netherlands Organisation for applied scientific research, TNO. This presentation is based on the co-authored booklet by TNO and the Hague centre for Strategic Studies, HCSS, published here : https://hcss.nl/sites/default/files/files/reports/Horizon%20scan%20Hybrid%20Trends%20and%20Developments%20%282002%29.pdf

The presentation gave an overall review of how hybrid threats are being used by state and non-state actors to gain influence on others. The risks associated from materialisation of different types of threats and how they affect societies and shift political powers and negotiation tables. Similarly a review of emerging technologies and future threats was highlighted and that there is still to be learned and done. Hybrid conflict is spreading to new frontiers with smaller states acting as both the perpetrators and victims of hybrid tactics and that they always evolve, taking new forms and making it challenging to identify. Overall, hybrid tactics will remain a dominant shaper of competition and conflict for at least the next five to ten years, and will continue to add complexity to world affairs.

During the presentation, 12 examples of hybrid campaigns were presented. Among the examples were: Globalization of Hybrid Threats, Private sector: target and channel, Special Ops Operatives, Psychological warfare, Rise of Lawfare, Hiding behind Proxies, Political machinations, Shifting Realities, Economic coercion and seduction, Formation of Digital Islands, Cyberspace, society's fragile underbelly and Emerging technologies & new capabilities.

These were further elaborated to show that the hybrid threats are becoming more and more globalized with the help of technology, internet, social media and so on. As of 2019, at least seventy states had executed some form of (foreign or domestic) disinformation campaign—a substantial increase from 2018 (48 states) and 2017 (28 states). We see that the private sector is playing also an increasing role in the realm of hybrid conflict – as a target and channel for spreading (dis)information and influence elections and so on.

A worrisome hybrid threat currently is also the Special Ops Operatives assassinations such as the Skripal case in UK, clearly in violation of international laws and an indication that these types of acts are back on the table. And the so called Sleeper Cells, who remain dormant and undetected for extended periods of time untill they are called from the home country to act, mostly a tactic employed by the Russian (Soviet) military intelligence, Iran and Iran-backed Hesbollah.

The presenter also explained an observed increase in psychological warfare such as claims of posessing unprecedented military power & technology by state actors that are used to create fear, gain influence and possibly shift negotiation tables. Similarly also increase in unanounced military exercises, violation of territorial aerial space that leaves defense in question how to react, are a thin line between preparedness and provocation that could lead to escalation of situation into war.

Among the current hybrid threats we see a rise of Lawfare. Use or misuse of international law agencies for personal gain is on the rise, creating distrust on the institutions and the agencies. One example of Lawfare is weaponizing Interpol using fake accusations and charges to paint individuals and then call Interpol to act.

Proxies, are increasingly used by states to engage in conflict. The key value in this is that they can't be attributed to the state legally. These include i.e. private armies, mafias and so on, such as the case in Yugoslav wars, where local football hooligans were used as proxies to engage in conflict, or the more recent Ukraine conflict where Russia uses local gangs to destabilize the country. Political machinations is also a means of states influencing internal affairs of other states through interference in elections and so on. I.e. the Brexit referendum and the US presidential election proved that this was not the result of one single attack but rather a combination of tactics disinformaiton, campaigns, corruption and so on. Also a rise in Shifting realities is that now social media can influence masses like never before. I.e. fake news is rising in occurrence, scope and impact deep fakes and cheap fakes are going to be very problematic as the technologies become more sophisticated. These can undermine the trust in experts, politicians, institutions, governments and so on. States use economic coercion and seduction by introducing economic sanctions, manipulating trade flows, blocking trade institutions, interdiction of people, seduction through investment for leverage and influence and so on. Another hybrid threat is the rise of digital islands i.e. Increase of national governance of the internet, to some extent even for a national internet such as the RUnet and the great firewall of China. These make it easier to threaten or attack others' internet infrastructure. Cyberspace and cyberattacks are becoming a defining factor in future hybrid conflicts. More so the emerging technologies bringing in new capabilities i.e. quantum computing, internet of things, 5G network technology, satellite jamming and spoofing technologies, advanced offensive cyber tools and so on can cause serious damage to i.e. power plants, causing them to explode and risk human casualties or financial disruptions to banking systems and so on.

3.10 PRESENTATION ON THE ROLE OF THE EU-HYBNET STAKEHOLDER GROUP AND ADVISORY BOARD

The presentation on the role of the EU-HYBNET Stakeholder Group (SG) and Advisory Board (AB) highlighted the SG's and AB's role to the project implementation. Furtermore the SG and AB members were invited to the KO (listed in chapter 2.2) and many of them were present. The participation of SG and AB members to the KO was important because the goal was to hear their wishes to the project proceeding. The role of SG and AB is shown in the figure below

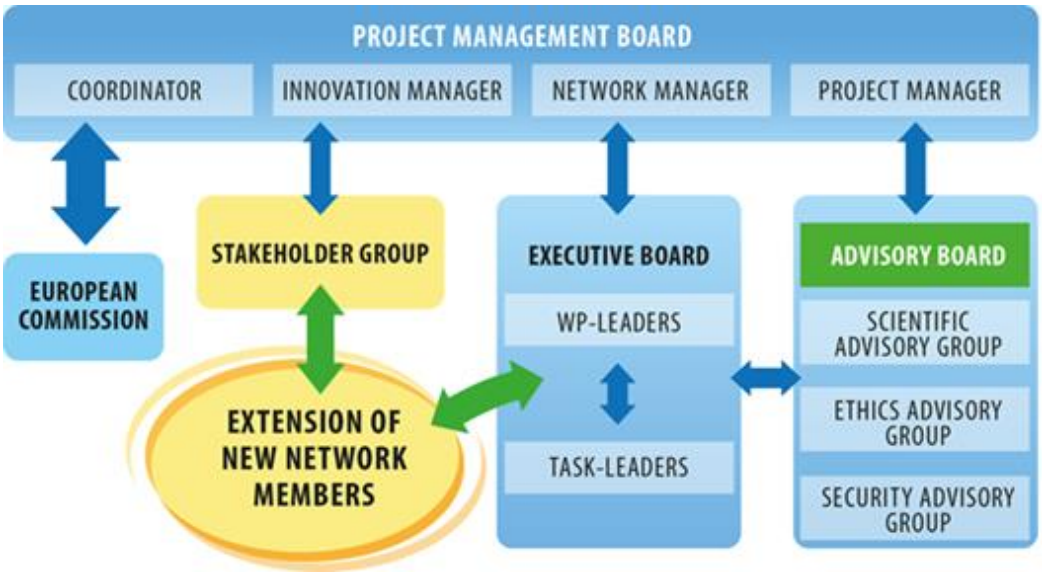

Figure 16 EU-HYBNET organisational structure

The KO presentation highlighted the importance of EU-HYBNET SG because they form, together with the consortium partners, the core team of the EU-HYBNET Network and are the starting point to the project Network extension. Because the EU-HYBNET is a five-year project it is crucial that the project will be able to include new SG/ Network members every year from different fields because this ensures that the network is able to share relevant present information how to counter hybrid threats. Furthermore, the KO presentation highlighted how the SG may participate and contribute to the project activities. In short, each SG member is expected to bring new relevant members to the network on their side. It is expected that the EU-HYBNET network will have 30+ new members yearly. The new network members are to ensure that the network extension is covering many different and relevant fields of hybrid threats.

The EU-HYBNET Advisory Board (AB) role to the project success was highlighted in the presentation. The AB is expected to advise on strategic directions of the project with reference to objectives and goals, impacts, key research areas, most promising innovations and recommendations as regards bridging gaps and fulfilling needs; assessing recommendations regarding innovation uptake and standardisation, or reviewing the conclusions arising from discussions around ethical and societal considerations. In addition, the AB is expected to provide critical feedback to the project proceeding. Moreover, it was reminded that AB may act as arbiter to resolve disputes, if they cannot be resolved by Project Management Board. In general the AB and the coordinator is aimed to have close cooperation. The AB will meet the coordinator and the consortium partners at least once a year when AB is invited to have a project AB meeting. However, AB members are invited to all project events while they present the high expertise in the field countering hybrid threats. Therefore, strong and active cooperation with AB members will be pursued and facilitated by frequent interaction in order to ensure high quality results within the EU-HYBNET project

After the presentation there was time for KO participants to provide comments or address questions. The European Security and Defence College (ESDC) representative as a SG member expressed their strong interest to continue and deepen the cooperation with the EU-HYBNET project. In addition, ESDC highlighted the importance of the project network to disseminate project results and to bring new relevant members to the network. The ESDC's comment well summarized the importance of the

Network and underlined that the extension of the network and the cooperation with the network members is crucial.

3.11 PRESENTATION AND DISCUSSION ON THE EU-HYBNET NETWORK AND ITS EXTENSION

The focus of the presentation was to describe the key features in the EU-HYBNET network extension and to inspire the KO participants to have a discussion on the network extension process and possibilities issue after the presentation. The general plan of the EU-HYBNET network extension is described in the figure below

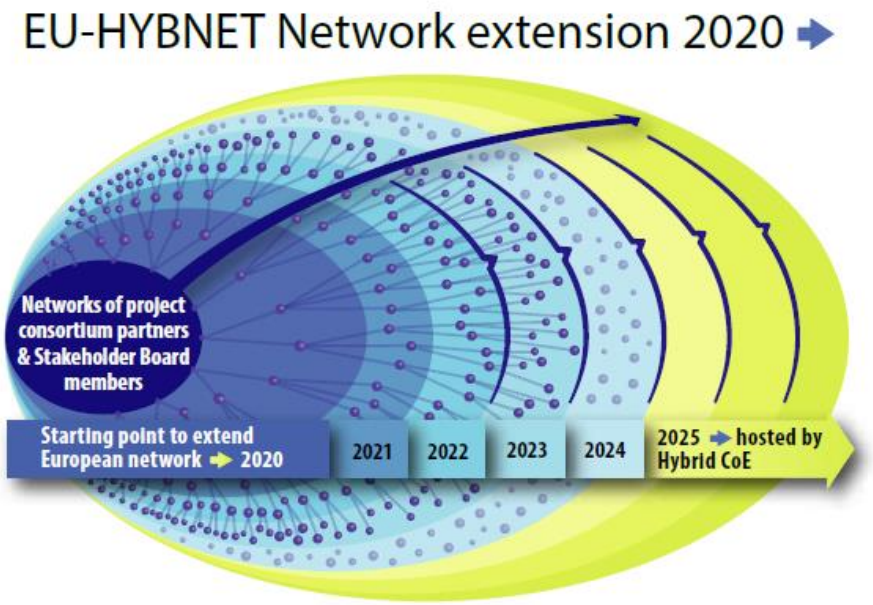

Figure 17 EU-HYBNET Network extension

First the presentation described how all project activities will be planned and conducted in a manner that they support to attract new relevant European actors to the EU-HYBNET Network. Furthermore, the project dissemination and communication measures will be tailored new actors to become aware of the network's activities and hence by their own initiative may request to become members. It was highlighted that there are many different actors and entities who are identified as relevant EU-HYBNET Network members - they are:

- Relevant EU projects and already established Network of Practitioner (GM-01) projects e.g. *MEDEA, NO-FEAR, ARCSAR, I-LEAD, ILEANET, SAY-SO, FIRE-IN, EXETER, INCLUDING*
- EU Agencies and Offices (discussion already established with ENISA, EU-LiSA, EDA) e.g. FRONTEX, EUROPOL
- Practitioners as defined in the EU-HYBNET project: I) *ministry level* (administration), II) *local level* (cities and regions), III) *support functions to ministry and local levels* (incl. Europe's third sector)
- actors central to EU-HYBNET Four core themes (subjects) and representing industry/SME, academia, NGOs

In addition, the presentation shortly summarized the selection process of the new network members and the networks' sustainability plan:

- The project management board (PMB) will select new members on a yearly basis which will allow for cooperation and information sharing with other network members in forthcoming years
- the extension of the network and its sustainable existence is grounded in the fact that after the project's completion HCoE will continue to host the Network and make use of its various platforms, which will ensure that network activities will be able to sustain a long lasting impact

In the end of the presentation the importance of the new network members was highlighted because they are seen the key to empower European resilience against the hybrid threat. After this the KO partners asked to present questions and comments. An EU-HYBNET member, the Valencia Local Police highlighted the importance to accept new network member candidates immediately to the network and not on a a yearly basis as it is now planned in the project. The faster acceptance process ensures that the benefit of the project to European stakeholders can be maximized. This was agreed by many KO participants with the chat comments and hence the view was taken as a relevant action point to the project's future execution.

3.12 PROJECT ADMIN AND FINANCE ISSUES

Presentation on project admin and finance issues was given by Tiina Haapanen, Laurea. The goal of the presentation was to describe for the consortium partners the general Commission H2020 rules and guidance to admin and finance issues that to follow in the EU-HYBNET implementation.

In the beginning of the presentation EU-HYBNET total budget and pre-financing arrangements were presented. It was highlighted that all funds received before EC has accepted final project report (M60) should be considered as pre-payments and final contribution will be calculated and paid when "Final Technical and Financial" -reports are accepted by EC. Reporting periods were presented and it was also stated that along official reporting to EC there will be internal reporting throughout the project.

General rules for cost eligibility and requirements for keeping records were described general level. It was also pointed that each partner is responsible for their own budged share and eligibility of declared costs. In addition, each partner was asked to familiarize with the Annotated Model Grant Agreement (AMGA), which is an important tool when managing H2020 –projects. In addition, it was mentioned that next to EC's guidance (eg. AMGA, H2020 Online manual[2]) there is more support available as each EU member states have National contact points (NCP) that provide guidance and support in H2020 on national level.

Lastly, at the end of the presentation it was mentioned for the partners that a separate finance and admin meeting will be arranged soon so as to provide more detailed information for the partners on admin and finance issues.

3.13 END OF THE MEETING

The KO ended with closing words given by EU-HYBNET coordinator. All partners were thanked for their participation to the KO and the presentations given, also the questions and comments said. The questions and comments were highly valuable to networking and to learning about issues that the partners wish and expect the project to focus on.

A key action point from the day was to change the process of accepting new members to the EU-HYBNET network not in the end of every project year but if possible, non-stop and immediately. The possibility to change planned processes to accept new network members was an issue that the coordinator promised to solve together with the consortium partners and the PO. The wish to extend the EU-HYBNET network as soon as possible was a pleasant action point to conclude the KO.

Lastly, the coordinator requested all KO partners not to hesitate in contacting the coordinator organization,so that the partners will get an answer to their questions and the project may proceed as expected.

Final words were to wish most fruitful cooperation between all project contributing actors and the best health for all. Hopefully covid-19 is soon over and the consortium partners can meet in person.

4. KICK OFF EVENT AND THE PROJECT OBJECTIVES AND KPIS

4.1 KICK OFF CONTRIBUTION TO THE PROJECT OBJECTIVES AND KPIS

The Kick Off event (KO) as part of WP1 is to contribute to the overall Project Objectives (OB.) 1, 5 and 7. Each of the project OB include Key Performance Indicators (KPIs) and the relevant KPIs to KO are listed below:

OB.1 -To enrich the existing network countering hybrid threats and ensure long term sustainability

- Goal 1.3. To arrange and host events where practitioners, industry, SME and academic actors can engage in information sharing
  - ➔ KPI: Events are organized to attract European actors willing to participate in professional exchanges

OB.5 - To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network

- Goal 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, standardization
  - ➔ KPI: Events for practitioners, industry/SMEs/academic actors are organised; forums established in relation to 4 core themes

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

- Goal 7.5 To interact with a wide circle of European stakeholders, share information; and explore possibilities for engaging Network synergistically
  - ➔ KPI : Events are structured to facilitate interactions among stakeholders to establish synergies

With reference to the named project objectives KPIs the KO contributed to the in many ways. First, the main importance of the KO was to highlighted for the project members the importance of networking and information sharing in order to build coherent European approach to counter hybrid treaths. In addtion, the KO was important project activity to tell for the network members about benefits of the project and network members' possibilities to contribute to the project content. Furthermore, the KO brought people together that is the key for becoming familiar with each other and finding the joint interests that eventually supports for future cooperation also outside the project activities. This all supports to empowering the Pan-European network to counter hybrid threats.

5. CONCLUSION

5.1 SUMMARY

In this document the EU-HYBNET KO event and its content and way forward was described.KO was the first project Milestone that is now set. In addition, the KO gathered over 80 participants that highlights the strong interest of the consortium partners, Stakeholder Group members and Advisory Board members to the project activities. This is supposed to indicate the project participants' high activity in the project activities. Furthermore, the Commission, DG HOME representatives (Mr. Max Brandt/ Policy Officer and Mr. Markus Walter/ Research Programme Officer) joined the meeting that highlighted the importance of the project for the commission and expectations of high results of the project. Lastly, it was important to hear that many KO participant expressed their interest to invite and have new network members in the project asap. This is taken as an important action point to the project future activities especially because the network extension and empowerment is in the heart of the EU-HYBNET project.

In Section 2. KO was described, as well as clarifying its participants and their role. Moreover, the numerous dissemination activities related to the KO have been highlighted.

In Section 3. the content of the KO presentations and their input to the project implementation was presented.

5.2 FUTURE WORK

The KO was an official start to the EU-HYBNET project activities planning and implementation. All KO presentations highlighted the next concrete actions in the project implementation and how they answer to the project Objectives and KPIs. The project coordinator will ensure that the work in the project will continue as expressed in the presentations. Furthermore, the comments from the KO participants are taken into notice, especially the wish to accept new EU-HYBNET network members immediately and not in a yearly basis. In addition, the wish of ESDC to contribute to the project proceeding is well noted and the discussion on concrete actions to do the cooperation will be continued. Lastly, KO was important EU-HYBNET event for project dissemination and the dissemination activity during the KO was high. Therefore, the high level of KO dissemination activities will be highlighted as a set level for future EU-HYBNET events as well.

ANNEX I GLOSSARY AND ACRONYMS

Term	Definition / Description
H2020	Horizon 2020 Programme
SEC	Secure Socities Progamme in H2020
EC	European Commission
DG HOME	Directorate General for Migration and Home Affairs
EU MS	European Union Member State
PO	Project Officer
CoU	Community of Users, hosted by DG HOME
NoP	Network of Practitioners project, funded by H2020 Secure Socities Programmw
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats -project
KO	Kick Off
OB	Objectives set to the EU-HYBNET project
KPI	Key performance Indicator set to the EU-HYBNET project
WP	Work Package
T	Task
D	Deliverables
M	Milestone. In some cases it indicates project month
SG	Stakeholder Group/ EU-HYBNET Network. EU-HYBNET includes from the project proposal preparations phase 16 SG members who are the starting point to the EU-HYBNET network extension together with the project consortium partners
AB	Advisory board of the EU-HYBNET project
NATO	The North Atlantic Treaty Organization, also called the North Atlantic Alliance, is an intergovernmental military alliance between 30 North American and European countries
EAST STRATCOM	The East StratCom Task Force is a part of the administration of the European External Action Service, focused on proactive communication of European Union policies and activities in the Eastern neighbourhood and beyond
ENLETS	European Network of Law Enforcement Technology Services
SGDSN	Secretariat-General for National Defence and Security
LAUREA	Laurea-ammattikorkeakoulu Oy
RTO	University of Turku, Department of Future Technologies, Finland - third linked party to Laurea
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
EOS	European Organisation for Security Scrl

TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
SATWAYS	SATWAYS
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
UCSC (UNICAT)	Universita Cattolica del Sacro Cuore
JRC	JRC - Joint Research Centre - European Commission
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
HCoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NLD MoD	Ministry of Defence/NL
ICDS	International Centre for Defence and Security, Estonia
PLV	Ayuntamiento de Valencia / Valencia Local Police
ABW	Polish Internal Security Agency
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
UniBW	Universitaet der Bundeswehr München

ANNEX II REFERENCES

[1] Zagreb Declaration, 6th May 2020, available here: https://www.consilium.europa.eu/media/43776/zagreb-declaration-en-06052020.pdf.

[2] Annotated Model Grant Agreement – H2020 Programme available here https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf

ANNEX III INVITATION EMAILS TO THE KICK OFF

Invitation to the EU-HYBNET consortium partners to the EU-HYBNET Kick Off (incl. final programme and the last updates of the Kick Off)

From: Päivi Mattila <Paivi.Mattila@laurea.fi>
Sent: Wednesday, May 6, 2020 6:29 PM
To: Tiina Haapanen <Tiina.Haapanen@laurea.fi>; Meessen, W.R.M.J. (Rick) <rick.meessen@tno.nl>; Käsper Kivisoo <kasper.kivisoo@hybridcoe.fi>; Maria Kampa <m.kampa@kemea-research.gr>; Hanna Smith <hanna.smith@hybridcoe.fi>; Päivi Tampere <paivi.tampere@hybridcoe.fi>; Carina Öhrnberg <carina.ohrnberg@hybridcoe.fi>; Repo Jasmin <jasmin.repo@espoo.fi>; Häkkinen Petri <petri.hakkinen@espoo.fi>; José L. Diego <proyectosplv@valencia.es>; Pantelis Michalis <p.michalis@kemea-research.gr>; Klaudia Kaczmarek <klaudia.kaczmarek@ppbw.pl>; Kwaijtaal, A. (Angela) <angela.kwaijtaal@tno.nl>; Rashel Talukder <rashel.talukder@ppbw.pl>; Maria Chiara Properzi <maria.properzi@eos-eu.com>; Prof. Dr. Stefan Pickl <stefan.pickl@unibw.de>; tor.g.lorentzen@uit.no; Egidija Versinskiene <egidija@l3ce.eu>; Natalia Jarmuzek <natalia.jarmuzek@ppbw.pl>; ramon.loik@icds.ee; Proyectos Europeos <proyectosplv@valencia.es>; Klara.Dolos@ZITiS.bund.de; R Andrew Paskauskas <andrew.paskauskas@gmail.com>; Evaldas Bruze (L3CE) <evaldas@l3ce.eu>; Saverio Caruso <saverio.caruso@chirurgia-urgenza.it>; bjorg.hunstad@uit.no; Gunhild Hoogensen Gjørv <gunhild.hoogensen.gjorv@uit.no>; Ivo Juurvee <ivo.juurvee@icds.ee>; Shahid Raza <shahid.raza@ri.se>; Rolf Blom <rolf.blom@ri.se>; cristina.ivan@animv.ro; 'Rubén Arcos Martín' <ruben.arcos@urjc.es>; Elodie Reuge <elodie.reuge@eos-eu.com>; Irena Chiru <irena.chiru@animv.ro>; Stéphane Grueso <steph@maldita.es>; Magalini Sabina <Sabina.Magalini@unicatt.it>; rachele.brancaleoni@unicatt.it; Jessica.Steinberger@ZITiS.bund.de; MOCILNIKAR Antoine-Tristan - SG/SDSIE/DIEPI <antoine-tristan.mocilnikar@developpement-durable.gouv.fr>; Georgios.GIANNOPOULOS@ec.europa.eu; Dimitris Diagourtas <d.diagourtas@satways.net>; ileana.surdu@animv.ro; s.sofou@satways.net; g.moutsou@satways.net; Michal Rataj <michal.rataj@abw.gov.pl>; Dimitra Papadaki <d.papadaki@kemea-research.gr>; Rūta Ziberkienė <rutzib@mruni.eu>; Georgia Melenikou <g.melenikou@kemea-research.gr>; Odd Morten Pettersen <morten.pettersen@politiet.no>; Son Pham <son.pham@unibw.de>; Marchesi Lorenzo <lorenzo.marchesi@unicatt.it>; Lucassen, O.G. (Okke) <okke.lucassen@tno.nl>; Mart.Hiietamm@ria.ee; ME.Drent@mindef.nl; andreas.attenberger@ZITiS.bund.de; Klara.Dolos@ZITiS.bund.de; rimantas@l3ce.eu; andreas.attenberger@ZITiS.bund.de; Christian.Despres@developpement-durable.gouv.fr; Dominykas Versinskas <dominykas@l3ce.eu>; Carmen Castro Garcés <proyectosplv@valencia.es>; Christian.Huck@ZITiS.bund.de; Orjan.Karlsson@dsb.no; DUCOS Géraldine (Chargée d'études) - CGDD/SEEIDD/MA1 <geraldine.ducos@developpement-durable.gouv.fr>; Carina Öhrnberg <carina.ohrnberg@hybridcoe.fi>; Emma Lappalainen <emma.lappalainen@hybridcoe.fi>; ivan.cristina@animv.eu; nicula.valentin@animv.eu; Isto Mattila <isto.mattila@laurea.fi>; Rauno Pirinen <Rauno.Pirinen@laurea.fi>; Tuomas Tammilehto <Tuomas.Tammilehto@laurea.fi>; Artmir Galica <artmir.galica@laurea.fi>; a.kanciak <a.kanciak@abw.gov.pl>; 'Jakub Rodzeń' <j.rodzen@abw.gov.pl>; Dmitri Teperik <dmitri.teperik@icds.ee>; Paul Dickson <paul.dickson@hybridcoe.fi>; p.kosieradzki@abw.gov.pl; Valentin NICULA <valentin.nicula@animv.ro>; m.leszczynska.cpt@abw.gov.pl; p.sapiecha.cpt@abw.gov.pl; ileana.surdu@animv.ro; m.rosgova@kemea-research.gr; a.grigoriadis@kemea-research.gr; Steven Ormston <steven.ormston@ppbw.pl>; Maxime Lebrun <maxime.lebrun@hybridcoe.fi>; Ulla-Maria Wilenius <ulla-maria.wilenius@hybridcoe.fi>
Subject: EU-HYBNET_Kick Off_Final and Updated Programme_12/5/2020 (9.00-16.20 CEST)

Dear EU-HYBNET partners,

I wish my email finds you well.

The EU-HYBNET Kick Off (KO) will take place in few days, on Tuesday 12/5 at 9.00-16.20 CEST. It is great pleasure to start the project officially with you!

I kindly send updated Kick Off Programme for you, please see attachment. As you may notice also the Commission Policy Officer, Mr. Max Brandt who is responsible for the hybrid threat related policy issues at DG HOME will join the KO. Tomorrow we will go the KO programme shortly through together in the consortium meeting and questions are most welcome.

Now wishing you a pleasant late afternoon!

With best regards,

Päivi

Päivi Mattila

Director of Security Research Program

Laurea University of Applied Sciences

Vanha Maantie 9, 02650 Espoo, Finland

Tel. +358 40 640 2253

www.laurea.fi

Invitation to the EU-HYBNET Stakeholder Group partners to the EU-HYBNET Kick Off

From: Päivi Mattila
Sent: keskiviikko 6. toukokuuta 2020 19.45
To: sari.lindblom@raja.fi; Rodrigue.GERMANY@systematic-paris-region.org; isabelle.desutter@systematic-paris-region.org; sara.degli.esposti@csic.es; david.arroyo@csic.es; Marios.THOMA@eeas.europa.eu; arthur.tokatlian@soprasteria.com; iacovino@cesi-italia.org; marco.gerevini@tecnoalimenti.com; Honkanen Jari SM <Jari.Honkanen@intermin.fi>; janne.koivukoski@intermin.fi; tarja.ferm@intermin.fi; mikko.jaaskelainen@intermin.fi; alex@korystin.pro; michele.calabro@ehma.org; ralf.hedel@ivi.fraunhofer.de; gsensidoni@expertsystem.com; jmgomez@expertsystem.com; morten.pettersen@politiet.no; francois.ardant@ardanti.com; Jean-Michel.DUMAZ@safecluster.com; laura.carel@safecluster.com
Cc: Artmir Galica <artmir.galica@laurea.fi>
Subject: EU-HYBNET_Kick Off Event_Invitation and link_Updated programme

Dear EU-HYBNET Stakeholder group members,

I wish my email finds you well and in good health.

The EU-HYBNET Kick Off (KO) will take place in few days, on Tuesday 12/5 at 9.00-16.20 CEST (teleconference, link in the attachment). It is great pleasure to start the project officially with you.

I kindly send updated Kick Off Programme for you, please see attachment. As you may notice also the Commission Policy Officer, Mr. Max Brandt who is responsible for the hybrid threat related policy issues at DG HOME will join the KO. This means that next the to EU-HYBNET project content you will learn more on Commission perspectives to the hybrid threats. We are looking forward to having a fruitful start for our cooperation with you.

See you soon and wishing you a good health and all the best to the spring!

With best regards,

Päivi

From: Päivi Mattila
Sent: torstai 9. huhtikuuta 2020 13.45
To: 'sari.lindblom@raja.fi' <sari.lindblom@raja.fi>; 'Rodrigue.GERMANY@systematic-paris-region.org' <Rodrigue.GERMANY@systematic-paris-region.org>; 'isabelle.desutter@systematic-paris-region.org' <isabelle.desutter@systematic-paris-region.org>; 'sara.degli.esposti@csic.es' <sara.degli.esposti@csic.es>; 'david.arroyo@csic.es' <david.arroyo@csic.es>; 'Marios.THOMA@eeas.europa.eu' <Marios.THOMA@eeas.europa.eu>; 'arthur.tokatlian@soprasteria.com' <arthur.tokatlian@soprasteria.com>; 'iacovino@cesi-italia.org' <iacovino@cesi-italia.org>; 'marco.gerevini@tecnoalimenti.com' <marco.gerevini@tecnoalimenti.com>; 'Honkanen Jari SM' <Jari.Honkanen@intermin.fi>; 'janne.koivukoski@intermin.fi' <janne.koivukoski@intermin.fi>; 'tarja.ferm@intermin.fi' <tarja.ferm@intermin.fi>; 'mikko.jaaskelainen@intermin.fi' <mikko.jaaskelainen@intermin.fi>; 'alex@korystin.pro' <alex@korystin.pro>; 'michele.calabro@ehma.org' <michele.calabro@ehma.org>; 'ralf.hedel@ivi.fraunhofer.de' <ralf.hedel@ivi.fraunhofer.de>; 'gsensidoni@expertsystem.com' <gsensidoni@expertsystem.com>; 'jmgomez@expertsystem.com' <jmgomez@expertsystem.com>; 'morten.pettersen@politiet.no' <morten.pettersen@politiet.no>; 'francois.ardant@ardanti.com' <francois.ardant@ardanti.com>; 'Jean-Michel.DUMAZ@safecluster.com' <Jean-Michel.DUMAZ@safecluster.com>; 'laura.carel@safecluster.com' <laura.carel@safecluster.com>
Cc: Artmir Galica <artmir.galica@laurea.fi>
Subject: EU-HYBNET_Kick Off Event_Invitation and link
Importance: High

Dear EU-HYBNET Stakeholder Group members,

I wish my email finds you well and in good health.

It is pleasure to send the *official Kick-Off program and a link to the Kick-Off videoconference on 12th of May 2020 at 9.00-16.20 CET* for you, please see the Program attached and the link below.

I see that Stakeholder Group members may join to the Kick Off for whole day but there are certain program slots where we wish you especially to participate - the slots are *from 14.35 until 15.30* or a slot *from 13.30 until 1530*.

If you have any questions, pleasure to answer together with the EU-HYBNET project Manager Mr. Artmir Galica/Laurea who will also work with you during the project (Cc.).

Looking forward to starting the project with you on May 2020 and we are looking forward to having the most fruitful cooperation with you!

Wishing you most pleasant Eastern despite of the challenging times.

With best regards,

Päivi

Kick-Off videoconference link: Join Zoom Meeting https://laurea.zoom.us/j/167680874

Meeting ID: 167 680 874 - Find your local number: https://laurea.zoom.us/u/cvVf0SQpF

Päivi Mattila

Director of Security Research Program

Laurea University of Applied Sciences

Vanha Maantie 9, 02650 Espoo, Finland

Tel. +358 40 640 2253

www.laurea.fi

Invitation to the EU-HYBNET Advisory Board to the EU-HYBNET Kick Off

From: Päivi Mattila
Sent: keskiviikko 15. huhtikuuta 2020 17.11
To: missiroli.antonio@hq.nato.int; Anneli.Kimber@eeas.europe.eu; francois.murgadella@sgdsn.gouv.fr; patrick.padding@politie.nl; tagarev@gmail.com
Cc: Hanna Smith <hanna.smith@hybridcoe.fi>; Käsper Kivisoo <kasper.kivisoo@hybridcoe.fi>; Emma Lappalainen <emma.lappalainen@hybridcoe.fi>; Artmir Galica <artmir.galica@laurea.fi>; Käsper Kivisoo <kasper.kivisoo@riigikantselei.ee>
Subject: H2020_project_ Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)_Advisory Board_Kick Off

Dear EU-HYBNET Advisory Board members,

CC. the European Center of Excellence for Countering Hybrid Threats (HCoE)/ Hanna Smith, Käsper Kivisoo, Emma Lappalainen; Laurea/ Artmir Galica (EU-HYBNET Project Manager)

I wish my email finds you well and in good health.

It is a pleasure to tell that the Commission has granted funding (Horizon2020 Programme) for the project "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) that was prepared last year

together with the Hybrid CoE and 23 European partners. Thank you once more on your interest to participate to the EU-HYBNET Advisory Board as member.

The EU-HYBNET project will start on May 2020 and hence I now kindly send for you the *official Kick-Off program and a link to the Kick-Off videoconference on 12th of May 2020 at 9.00-16.20 CET*, please see the Program attached and the link below.

I see that Advisory Board members may join to the Kick Off for whole day but there are certain program slots where we wish you especially to participate - the slots are *from 14.35 until 15.30* or a slot *from 13.30 until 1530*.

If you have any questions, pleasure to answer together with the EU-HYBNET Project Manager Mr. Artmir Galica/Laurea who will also work with you during the project (Cc.).

Looking forward to starting the project with you on May 2020 and we are looking forward to having the most fruitful cooperation with you!

Wishing you most pleasant spring despite of the covid-19.

With best regards,

Dr. Päivi Mattila, EU-HYBNET coordinator

Kick-Off videoconference link: Join Zoom Meeting https://laurea.zoom.us/j/167680874

Meeting ID: 167 680 874 - Find your local number: https://laurea.zoom.us/u/cvVf0SQpF

Päivi Mattila

Director of Security Research Program

Laurea University of Applied Sciences

Vanha Maantie 9, 02650 Espoo, Finland

Tel. +358 40 640 2253

www.laurea.fi