EU-HYBNET

TRAINING AND EXERCISES SCENARIO AND TRAINING MATERIAL

DELIVERABLE 2.28

Lead Author: KEMEA

Contributors: Laurea, L3CE, URJC, ICDS

Deliverable classification: PUBLIC

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

D2.27 TRAINING AND EXERCISES SCENARIO AND TRAINING MATERIAL

Deliverable number	**D2.28**	
Version:	**1.0**	
Delivery date:	**28/06/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Delivered**	
Nature:	**Report**	
Main authors:	**Vanessa Papakosta**	**KEMEA**
Other contributors:	**Edmundas Piesarkas**	**L3CE**
	Päivi Mattila	**LAUREA**
	Marek Kohv	**ICDS**
	Ruben Arcos	**URJC**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	05/04/2024	Edmundas Piesarkas /L3CE	Material produced
0.2	06/05/2024	Vanessa Papakosta/ KEMEA	Table of Contents
0.3	13/05/2024	Vanessa Papakosta/ KEMEA	Update on content
0.4	20/05/2024	Vanessa Papakosta/ KEMEA	Update on content
0.5	03/06/2024	Päivi Mattila/ LAUREA	Making comments and Review
0.6	10/06/2024	Vanessa Papakosta/ KEMEA	Update on content
0.7	17/06/2024	Edmundas Piesarkas/ L3CE	Update on content
0.8	18/06/2024	Vanessa Papakosta/ KEMEA	Ready for review
0.9	26/6/2024	Päivi Mattila/ LAUREA	Review and text editing
0.91	28/6/2024	Ruben Arcos/ URJC	Review
0.92	28/6/2024	Marek Kohv/ ICDS	Review
0.93	28/6/2024	Vanessa Papakosta KEMEA	Final review
1.0	28/6/2024	Päivi Mattila LAUREA	Final review and submission of the document to the EC

DISCLAIMER

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

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

TABLE OF CONTENTS

TABLES

FIGURES

EXECUTIVE SUMMARY

The purpose of this deliverables (D2.28) is to present the material used for the “Empowering a Pan-European Network to Countering Hybrid Threats” (EU-HYBNET) project training effort and includes guides and content both for the trainees as well as for the trainers. This deliverable serves as a supporting document, aiming to provide insights to the training material which was developed as part of the associated Task 2.4 “*Training and Exercises for Needs and Gaps*” whose main objective was to deliver EU-HYBNET training event, based on the results of Work Package (WP2) “*Gaps and Needs of European Actors against Hybrid Threats*” and WP3 “*Surveys to Technology, Research and Innovations*”.

The developed material allowed practitioners and stakeholders to leverage the full spectrum of capabilities, expertise and experience related to hybrid threats and promoted knowledge over the aforementioned topic as well as over the relevant innovations, technical and non-technical ones.

As part of an iterative design strategy, the training material was also evaluated by the participants during the training event; following this evaluation, the material will be further enhanced to provide more efficient and useful content on the 3rd working cycle of the project. The training activities, as well as the evaluation of the overall training are described in more detail in Deliverables 2.22 and 2.25. However, this deliverable (D2.28) will deliver the training material used in the training.

The content of the current document can support various training activities for all relevant models, tools and methods selected and it is intended for the overall hybrid threats community. It is important to highlight that the training material was prepared by the EU-HYBNET Consortium and more specifically by L3CE in Task 2.4 “*Training and Exercises for Needs and Gaps*”. However the scenario and the innovations suggested to be tested in the training were delivered by KEMEA in Task 2.3 “*Training and Exercises Scenario Development*”. The content of the current document will be published eventually in CORDIS and hence it will be publicly available to all. Naturally EU-HYBNET WP5 “Communication, Dissemination and Exploitation Activities” may advertise D2.28 that it is ready for pan-European stakeholders to benefit in their own trainings.

1. INTRODUCTION

1.1 OVERVIEW

The EU-HYBNET project aims to create a pan-European network of security practitioners and relevant stakeholders which through their collaboration and interaction will strengthen the capacity responses against hybrid threats. In this context and to achieve the project main objective, the Consortium organized and delivered 3rd EU-HYBNET training event on 18-19/01/2024 in Vilnius, Lithuania in order to create and/or strengthen the capacities of European practitioners, industry, SME and academic actors to counter Hybrid Threats.

Figure 1. shows EU-HYBNET WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.4 "*Training and Exercises for Needs and Gaps*" training activities in relation to the other WPs and to the overall EU-HYBNET project.

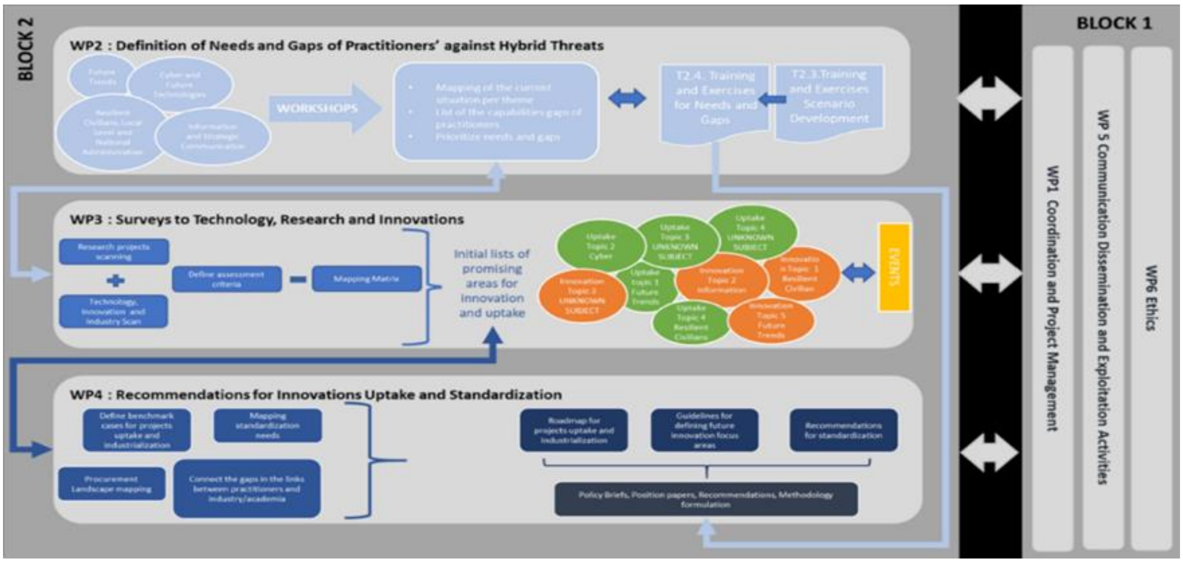

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

Figure 1 EU-HYBNET structure of Work Packages and Main Activities

As presented in EU-HYBNET Description of Action (DoA), the overall objective of the EU-HYBNET training is to create and strengthen the capacities of European practitioners, industry, SME and academic actors to counter Hybrid Threats. Furthermore, EU-HYBNET Training event and D2.28 strongly supports the achievement of the EU-HYBNET objective OB 6.4 : *To empower European practitioners, industry, SME and academic actors' capacity to counter hybrid threats by offering relevant trainings and materials*. Moreover, D2.28 is linked and delivers results to the EU-HYBNET's three Lines of Action, namely : "*priorities as regards of increasing knowledge and performance requiring standardization*".

In order to reach the named objectives, the training event agenda (ANNEX III) covered the introduction session with a brief overview of the training flow and introduction to Scenario helping the participants grasp and retain the information. This was followed by breakout sessions, focused on interactive discussions involved participants to share their experience and plan response campaigns to hybrid threats and attacks. Hearing different voices also supported to keep the sessions varied and interesting. In order to ensure that the project may learn how useful the training was seen by the training participants, each participant was asked to fill an assessment form and to give their structured feedback as well comments and other reflections. The training participants also were asked to provide relevant improvement points or additional expectations they would see relevant and important for the future EU-HYBNET trainings. The feedback was gained to the training format, scenario and tested innovations that all form the three key building blocks of the EU-HYBNET Training. The Training material for stakeholders is also introduced and delivered according to these building blocks in the following chapters.

1.2 STRUCTURE OF THE DELIVERABLE

This deliverable includes following sections:

- Section 1. introduces the objectives of this report and describes the deliverable in general
- Section 2. provides an overview of the EU-HYBNET training three key building blocks: (i) training approach used (DTAG), (ii) scenario and vignettes created, (iii) innovations selected and tested
- Section 3. includes the training scenario material produced
- Section 4. presents the innovations to consider as possible solutions to the challenges presented during the training
- Section 5. provides training Lessons Learned for future similar events
- Section 6. outlines the conclusions of the current document

2. EU-HYBNET TRAINING OVERVIEW

The 3rd EU-HYBNET Training consists of three key building blocks: (i) the training format, (ii) scenario and (iii) innovations tested. They all are shortly introduced below.

Training format

A Disruptive Technology Assessment Game (DTAG) was used to test the technical/social/human/organizational solutions and their impact on an operating environment during the 1st and 2nd cycle EU-HYBNET Training and Exercising Event. For the 3rd cycle DTAG methodology was adjusted, reflecting experience, and Lessons Learned from the 2nd cycle. However, the key elements of DTAG were not modified, and hence thorough guidance to use DTAG can be familiarized from EU-HYBNET 1st and 2nd cycle "Training and Exercises Scenario and Training Material" D2.28, see CORDIS: https://cordis.europa.eu/project/id/883054/results

On the whole, the DTAG gaming format is a seminar type wargame and in EU-HYBNET DTAG is to:

- Provide a basis for understanding how to operationalize the potential use of the innovations and solutions (so-called Ideas of Systems (IoSs)) to counter hybrid threats through the analysis of the Innovations.
- Explore the potential impact of the Innovations in an operational context and hybrid threats setting (Background Scenario)
- Identify the potential vulnerabilities in (the use of) the Innovations that adversaries might exploit, thereby mitigating the intended effects of the Innovations
- Generate additional insights into how potential counter-measures against adversaries could alter our perspectives on the potential use of the suggested innovations and solutions

The DTAG provided the basis for the training execution and discussions and a fruitful use of the EU-HYBNET Training scenario.

Scenario and vignettes

The goal of the T2.3 "Training and Exercises Scenario Development" is to deliver scenario for EU-HYBNET T2.4 "Training and Exercises for Needs and Gaps" that will arrange the 3rd EU-HYBNET training event (January 18th -19th, 2024 in Vilnus, Lithuania). The goal of the training and exercises is to test identified promising innovations to EU-HYBNET 3rd project cycle (M35-M52/ March 2022 – Aug 2024) WP2 T2.1 and T2.2 identified most critical pan-European security practitioners' gaps and needs to counter Hybrid Threats under each of the EU-HYBNET Four Core Themes (1.Future Trends of Hybrid Threats; 2.Cyber and Future Technologies; 3.Resilient Civilians, Local Level and National Administration; 4. Information and Strategic Communication). The promising innovations (technical and non-technical) are identified in EU-HYBNET WP3 "Surveys to Technology, Research and Innovations"/ T3.2 "Technology and Innovations Watch" and T3.3 "Ongoing Research Projects Initiatives Watch" in their deliverables: T3.2/D3.5 "Second mid-term report Improvement and innovations" and T3.3/D3.9 "Second mid-term report Innovation and Research monitoring". The innovation testing is important so that EU-HYBNET may eventually deliver innovation uptake recommendations for pan-European security practitioners' needs and in this way support and to enhance European response to Hybrid Threats.

There is also a sub-chapter: how The EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Themes and EU-HYBNET 3rd project cycle specific gaps& needs to counter hybrid threats; the gaps and needs definition is deriving from EU-HYBNET deliverable D2.11. The Gaps and needs are mentioned as "Threats".

The aim of the training is to hold a free discussion on the challenges and dilemmas that are underlying to the scenario injects and to have discussion how the selected innovations could support the pan-European security practitioners to plan and conduct their counter measures to the challenges, Hybrid Threats. It requires participant to exercise critical thinking and a creative approach, also to analyse and suggest new features to the selected and tested innovations. In order to "test the innovations", the training event will provide an exhaustive list of innovations, research monitoring results explored under WP3 in order to provide food for thought to participants regarding the possible ways to address the problems posed by the scenario. This shall not concern the minute applicability of specific innovations to a given situation but rather an exploration and debate and to deliver research material for EU-HYBNET WP3 T3.1 "Definition of Target Areas for Improvements and Innovations" and WP4 "Recommendations for Innovations Uptake and Standardization" to provide recommendations for most promising innovations uptake for pan-European security practitioners' needs.

In order to support training participants to be well familiar with the scenario and vignettes, relevant sections of the scenario and vignettes were distributed to the training participants as pre-reading material.

Innovations

The DTAG has been designed to assess innovations and innovative solutions to presented challenges and hence the format is optimal to EU-HYBNET training goals. After all, the main focus in the EU-HYBNET is to support EU-HYBNET to identify and to deliver recommendations of most promising innovations to the EU-HYBNET's identified pan-European security practitioners' and other relevant actors gaps and needs to counter Hybrid Threats and further innovation analysis in the EU-HYBNET project.

To test the innovations during the training, list of innovations (technological and non-technological, incl. research monitoring results) was provided as food for thought to participants regarding the possible ways to address the problems posed by the scenario. This shall not concern the minute applicability of specific innovations to a given situation but rather an exploration and debate to provide recommendations for most promising innovations uptake for pan-European security practitioners' needs. The innovation analysis and discussion on the innovations was formulated according to the four Core Themes and the training participants were forming analysis and training teams according to the Four Core Themes.

During all training events participants in teams were asked to freely assess the overall situation and to test the innovations presented for them as possible promising solutions. The aim during all 3 cycle remained the same - to hold a free discussion on the challenges and dilemmas that are underlying to the scenario Vignettes and to have discussion how the selected innovations could support them to plan and conduct counter measures to the challenges, Hybrid Threats. This requires participant to exercise critical thinking and a creative approach, also to analyse and suggest new features to the selected and tested innovations.

The training participants had possibility to familiarize with majority of the selected innovations before the training event from the delivered pre-reading material.

For the 3rd cycle 15 different innovative solutions were proposed for discussions in Core Theme based groups.

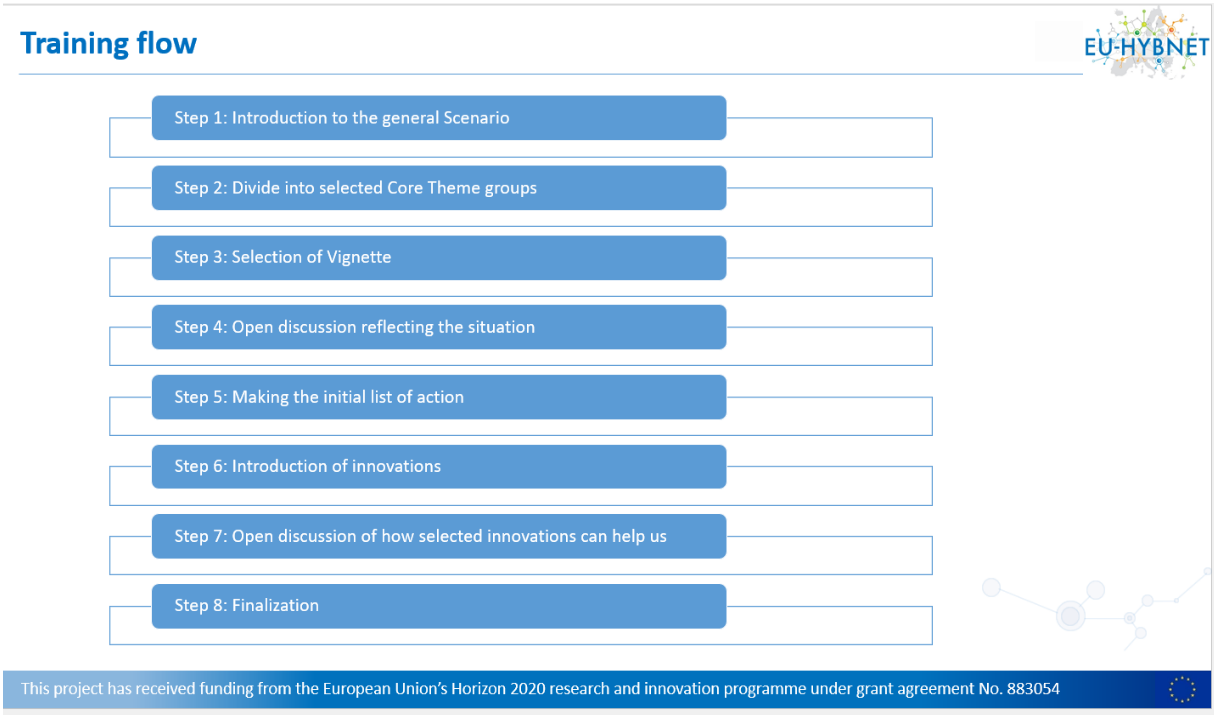
Core themes	Innovative solution
Future Trends of Hybrid Threats	Mobile application to pinpoint acts of harassment/violence on the street and online SMIDGE WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories DesinfoEND
Cyber and Future Technologies	Advanced Surveillance Systems with Perimeter security Code of Practice on Disinformation ENGAGE (Engage Society for Risk Awareness and Resilience)
Resilient Civilians, Local Level, National Administration	AI-enhanced disaster emergency communications -innovation The Countering Foreign Interference (CFI) project 'Antidote' to hostile messaging delivered by private messaging apps EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threat
Information and Strategic Communication	Blockchain -based verification -innovation Media Pluralism Monitor (MPM) ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE

Eventually, EU-HYBNET Four Core Theme based training teams were formulating how the solutions could improve response to different challenges described in scenario and given vignettes. Teams have been asked to develop initial campaigns plans to structure the reaction to the situations described in the Vignettes in the context of the general Scenario. In the next stage innovative solutions were introduced and teams continue discussions is search for the most feasible innovative solution for selected vignette and to envision how it could be operationalized. It resulted in updated response campaigns, plans giving the basis to learn how innovations could be helpful in Hybrid Threat scenarios, similar to the ones provided in the exercise. During the 3rd round special attention was given for the Red team component. Red team, in the form of “devils advocate” is included in the methodology, but in previous cycles it was not used enough. During the 3rd event there were strong Red teams formed to challenge presentations of planed campaigns at each stage.

All of the above have been captured into solutions assessments during the training by the EU-HYBNET Four Core Theme leaders who were the moderators of the sessions.

3. TRAINING SET UP

The Training Agenda that was shared for participants (ANNEX III) formed the proceeding plan for the Training event. The plan was formulated as "Training Flow" so that the participants could easily understand the needed steps to go the training successfully through. The "Training Flow" plan also supports any organization to arrange similar training as it was done during the 3rd EU-HYBNET training event. The "Training Flow" is following:



Training flow

EU-HYBNET

Step 1: Introduction to the general Scenario

Step 2: Divide into selected Core Theme groups

Step 3: Selection of Vignette

Step 4: Open discussion reflecting the situation

Step 5: Making the initial list of action

Step 6: Introduction of innovations

Step 7: Open discussion of how selected innovations can help us

Step 8: Finalization

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

As described in the "Training Flow" the first step was to provide a brief overview, introduction (Step 1.) of the training day and to go the Scenario through helping the participants to grasp and to retain the information. This was followed participants division into training teams according to the EU-HYBNET Four Core Themes (*Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communication*) (Step 2.). Next step (Step3.) was to select in the team Vignette that to focus on and then have an open discussion on the situation at hand. The interactive discussions (Step 4.) involved participants to share their experience and plan response campaigns. Hearing different voices also keeps the sessions varied and interesting. According to the discussion, the teams were encouraged to make a priority list of actions to counter the hybrid threat and hybrid attacks in the situation (Step 5.). This was followed an introduction to pre-selected innovations that to consider to deliver support for the counter measures or ease to react and to solve the situation (Step 6.). An important part (Step 7) was to have analysis of the innovations and have discussion how the selected innovations may support in the actions. Last step (Step 8.) in the training is to provide final conclusion what else should be taken into account in the possible similar situation in the future and how the innovations may support necessary actions.

The support the teams to proceed according to the "Training Flow" following documents were provided:

- Scenario and Vignettes. The material includes detailed description of background scenario and all proposed vignettes describing the general situation in more details. The material originates from EU-HYBNET D2.19 "*Training and Exercise, Scenario delivery*"" in CORDIS https://cordis.europa.eu/project/id/883054/results
- Innovations proposed for discussions. The material includes description of innovative solutions and suggested aspects to be discussed during the training. Document also provided linking of innovations to Vignettes and Core Themes. The material originates from EU-HYBNET D2.19 "*Training and Exercise, Scenario delivery*"" in CORDIS https://cordis.europa.eu/project/id/883054/results
- PowerPoint –slide set to each training team formed according to the project Four Core Themes. The PP was to support the discussion to proceed in all needed "Training Flow" steps and the team to finalize their proceeding plans and to analyse the usability of the innovations in order to reach the wanted goals in solving the situation.

All above mentioned Steps in the training teams and evaluation of the whole "Training Flow" according to training participants feedback have been captured by the team moderators (four Core Theme leaders) into solutions assessments. The outcomes of the whole training event and the innovations' validation and assessment are elaborated further in this document chapter 5. and chapter 6. The next subchapters present the Training material used during the training so that interested organization may arrange similar training on their own.

3.1. TRAINING SCENARIO

The ultimate goal of building scenarios, whether they originate from models, stakeholder participation, or as it is often the case both, is to assess outcomes from alternative future trajectories, through model analysis and planning with stakeholders, to inform decision making. A more specific goal is to assess the response of the involved practitioners to alternative future trajectories, based on model analysis or expert knowledge. The scenarios should include the different views of the stakeholders on possible alternative future developments that are hard to predict and the assumptions behind the scenarios must be made transparent. The scenarios need to represent different kind of challenges and alternatives to deal with them.

The EU-HYBNET scenario and vignettes portray a crisis situation, giving opportunities to hybrid threat actors in leveraging societal and other vulnerabilities in order to further their strategic objectives while acting under the threshold of detection and circumventing political attribution, using a variety of means that have the characteristic to offset and upend anticipations and predictions of policymaking, crisis management and contingency management.

3.1.1 SCENARIO - MAIN ACTORS AND SITUATIONAL MAP

The main actors in the EU-HYBNET training and exercise scenario are:

a. STEPLAND is a militarily strong country, exporting hydrocarbons and financially stable, with a rather autocratic regime.

b. POLDONIA is a republic, financially strong in confrontation with STEPLAND, that on many occasions led to major border incidents.

c. The LATARUM Republic is an independent country, formerly part of POLDONIA, with many Poldonians residing, commercially and culturally linked to STEPLAND.

d. BAKVERIA is a strong oil producing republic, with many ports and LNG offshore facilities.

e. SILVERITANIA is a newly established independent country under military, diplomatic and financial pressure from STEPLAND who wishes to incorporate it.

f. FREEWICK is a republic in alliance and financial partnership with BAKVERIA

The situational setup in the EU-HYBNET training and exercise scenario is following:

- STEPLAND is spreading online disinformation targeting incitement of POLDONIAN minority residing in LATARUM.

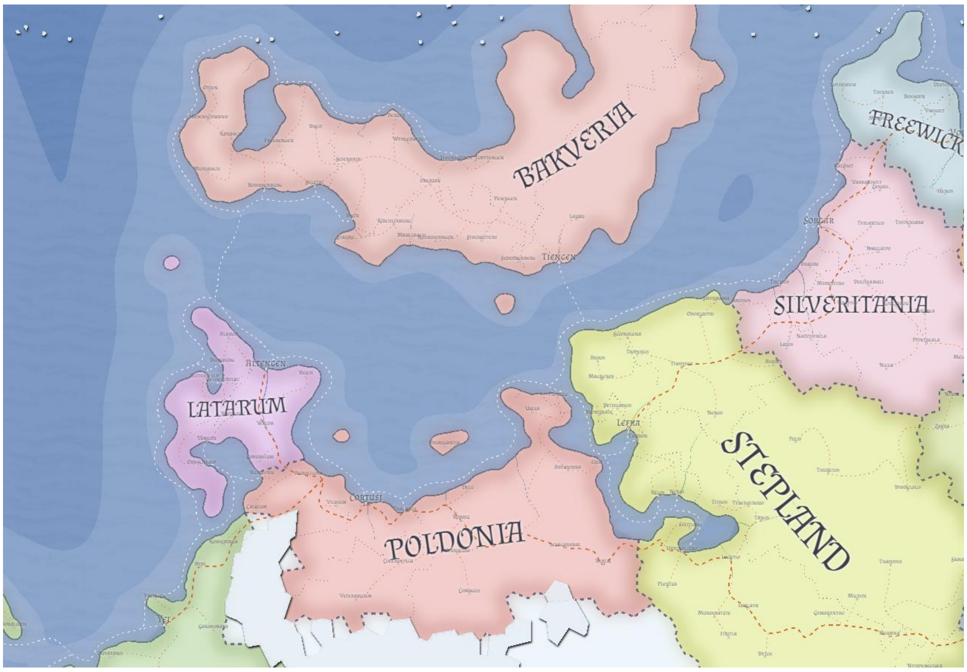
- Disinformation in LATARUM includes fake news and fake videos

- Critical infrastructure in BAKVERIA is attacked, public safety is also at risk with bombing attacks. Physical attacks on important infrastructure lead to social unrest and fear. Compromising access to basic needs such as emergency and health services can increase population insecurity and hardship.

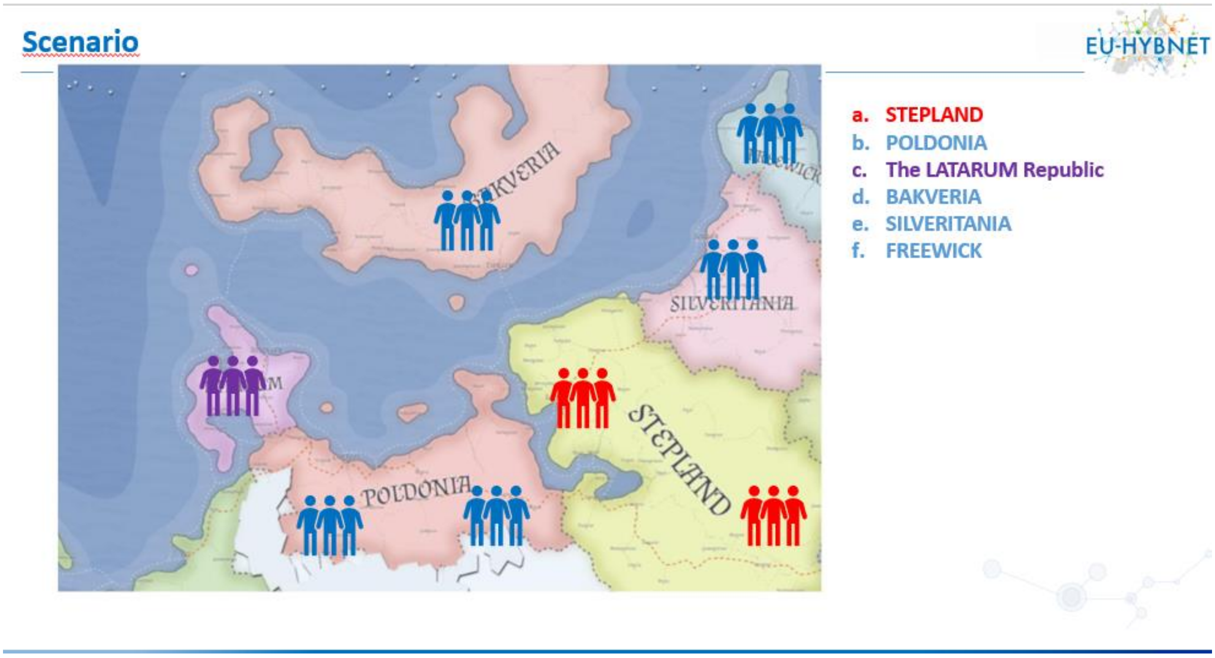
- A Mega Forest Fire in SILVERITANIA is challenging the ability of the state to handle the incident. It is attributed probably to malignant arsons and is causing a huge number of victims to be dispatched in hospitals. Hospitals efficiency and effectiveness is challenged.

- STEPLANDs Airforce is constantly violating the Bakverian Airspace while its navy is violating Bakveria’s territorial waters. STEPLAND denies all allegations presenting videos to support its grounds.

The above mentioned scenario activities and actors are taking place in the region and context described in the map below:



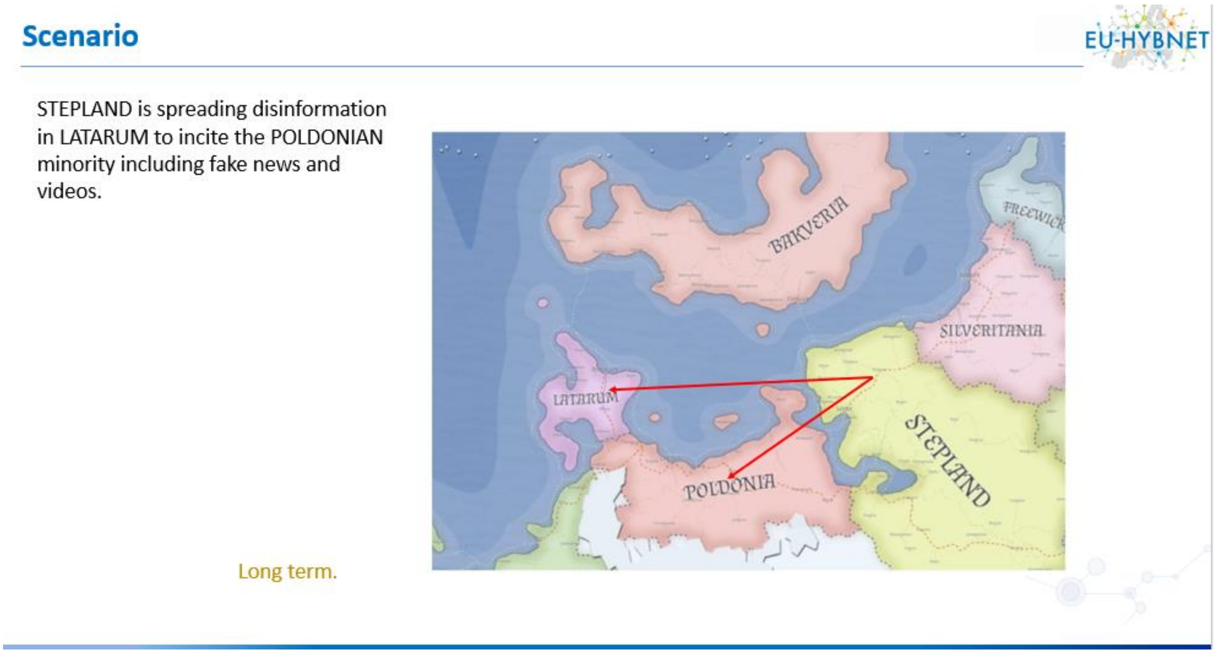
The map above present the location of the actors.



Scenario

a. STEPLAND
b. POLDONIA
c. The LATARUM Republic
d. BAKVERIA
e. SILVERITANIA
f. FREEWICK

The map above present the tension between the actors and provides understanding to forthcoming scenario actions and tensions.

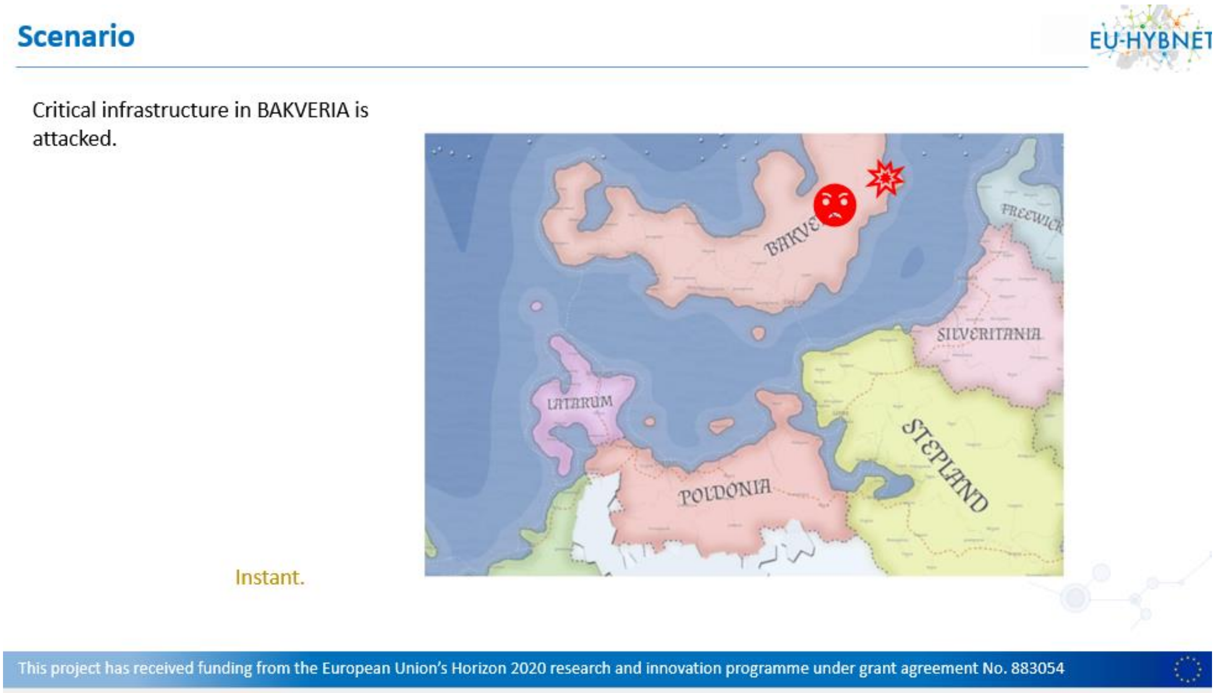


Scenario

EU-HYBNET

STEPLAND is spreading disinformation in LATARUM to incite the POLDONIAN minority including fake news and videos.

Long term.



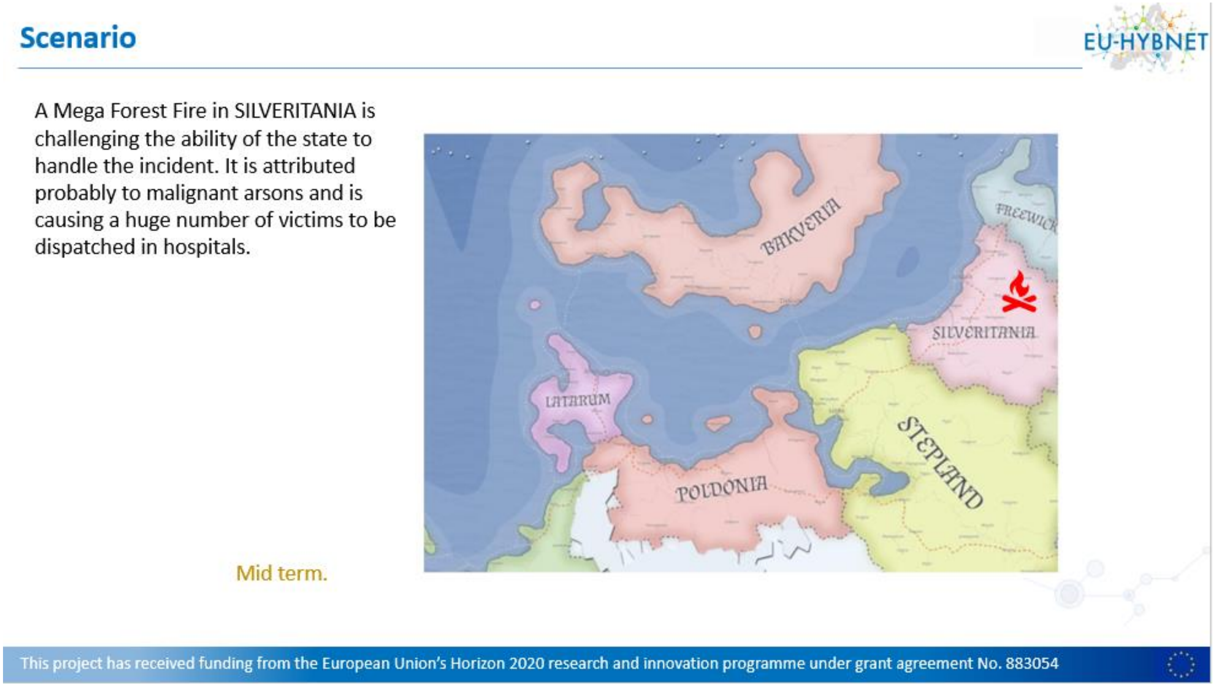
Scenario

EU-HYBNET

Critical infrastructure in BAKVERIA is attacked.

Instant.

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



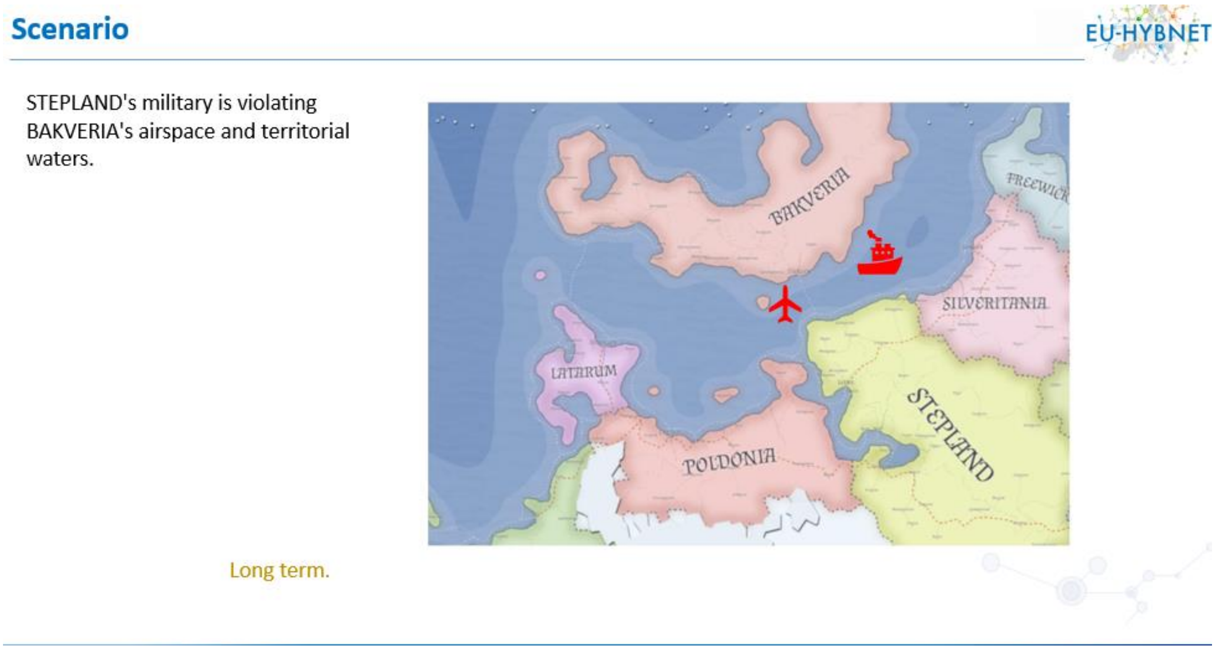
Scenario

EU-HYBNET

A Mega Forest Fire in SILVERITANIA is challenging the ability of the state to handle the incident. It is attributed probably to malignant arsons and is causing a huge number of victims to be dispatched in hospitals.

Mid term.

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



Scenario

EU-HYBNET

STEPLAND's military is violating BAKVERIA's airspace and territorial waters.

Long term.

3.1.2 SCENARIO – VIGNETTES

Scenario walk-through was followed by introduction to the scenario vignettes to the training participants according the participants selected interest to belong to a certain training team formed according the project four core themes. The following Vignettes supported training participants in way to keep well track in the training flow.

The training was designed to include assessment of innovations by discussing which of these might be considered for formal uptake by practitioner organizations. During the 1st project cycle prioritization and evaluation of innovations was made at the end of the Training Event. Survey, using specifically designed questionary was organized. Due to a very limited response rate, different approach was applied during the 2nd project cycle. Assessment was done during discussion. In the last cycle assessment was done in a similar manner, bus also supported by Mentimeter tool. This provided possibilities to grasp priorities in a more structured way during the training event.

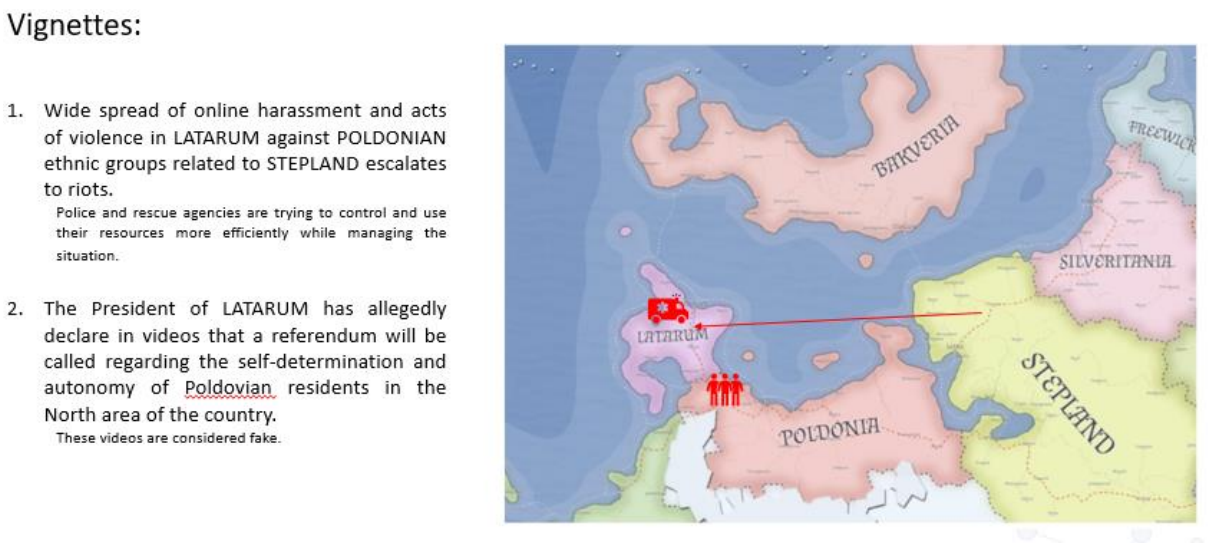
During the preparation phase different Vignettes were linked to Core Themes. Innovative solutions were linked to the Vignettes, assuming that they can provide additional value in the situation bound by it.

Each Core Theme group discussed attributed Vignettes. After the first phase (situation assessment) participants were introduced to relevant innovations. List of innovations varied according to Vignette. Participants were asked to discuss all innovations presented and select the most relevant (1 or 2) for the given situation. Such prioritization does not provide a proper quantitative indication of their ranking but should be considered as qualitative indication of preference of a given group of participants. Dissemination level of this deliverable is Public, so details of discussion within groups are not provided. Those can be requested by trusted partners and will be delivered as inputs for the further 3rd cycle work in WP4.

The Vignettes according to the each Fore Core theme are following:

Core Theme: Future Trends of Hybrid Threats

There were 2 Vignettes attributed to this Core theme.



Vignettes:

1. Wide spread of online harassment and acts of violence in LATARUM against POLDONIAN ethnic groups related to STEPLAND escalates to riots.
   Police and rescue agencies are trying to control and use their resources more efficiently while managing the situation.

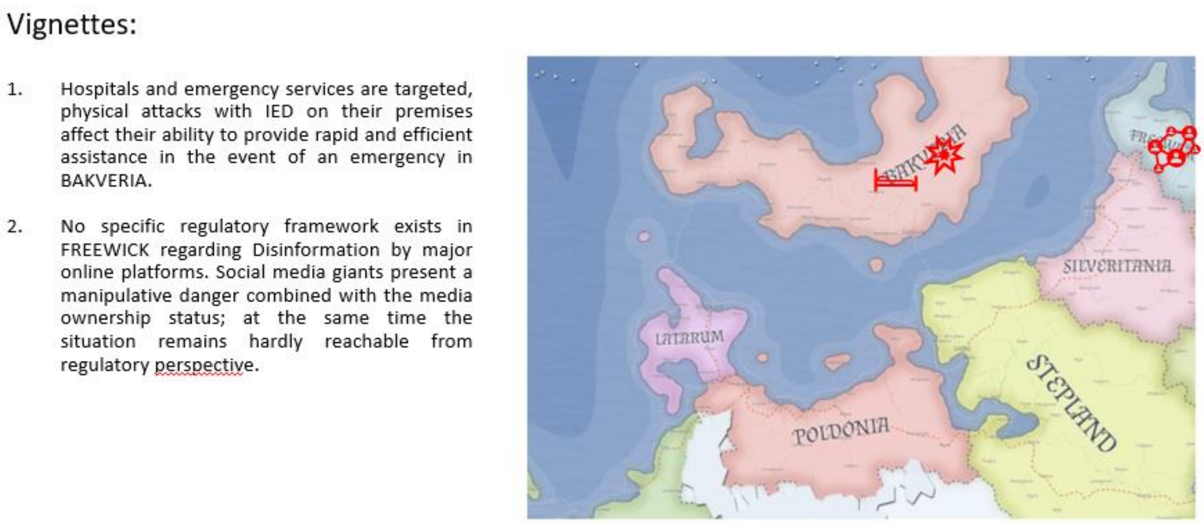
2. The President of LATARUM has allegedly declare in videos that a referendum will be called regarding the self-determination and autonomy of Poldovian residents in the North area of the country.
   These videos are considered fake.

Respective innovations presented were:

Vignette 2	Vignette 2
Mobile application to pinpoint acts of harassment/violence on the street and online	We Verify, a video plugin to debunk fake videos on social media that spread conspiracy theories
SMIDGE	DesinfoEND

Core Theme: Cyber & Future Technologies

There were 2 Vignettes attributed to this Core theme.



Vignettes:

1. Hospitals and emergency services are targeted, physical attacks with IED on their premises affect their ability to provide rapid and efficient assistance in the event of an emergency in BAKVERIA.

2. No specific regulatory framework exists in FREEWICK regarding Disinformation by major online platforms. Social media giants present a manipulative danger combined with the media ownership status; at the same time the situation remains hardly reachable from regulatory perspective.

Respective innovations presented were:

Vignette 2	Vignette 2
Advanced Surveillance Systems with Perimeter security	Starlight Disinformation-Misinformation Toolset

Code of Practice on Disinformation	Innovative Cluster for Radiological and Nuclear Emergencies, INCLUDING
ENGAGE (Engage Society for Risk Awareness and Resilience)	

After innovations were presented, prioritization discussion was held. Priorities from both groups are summarised in the figure below.

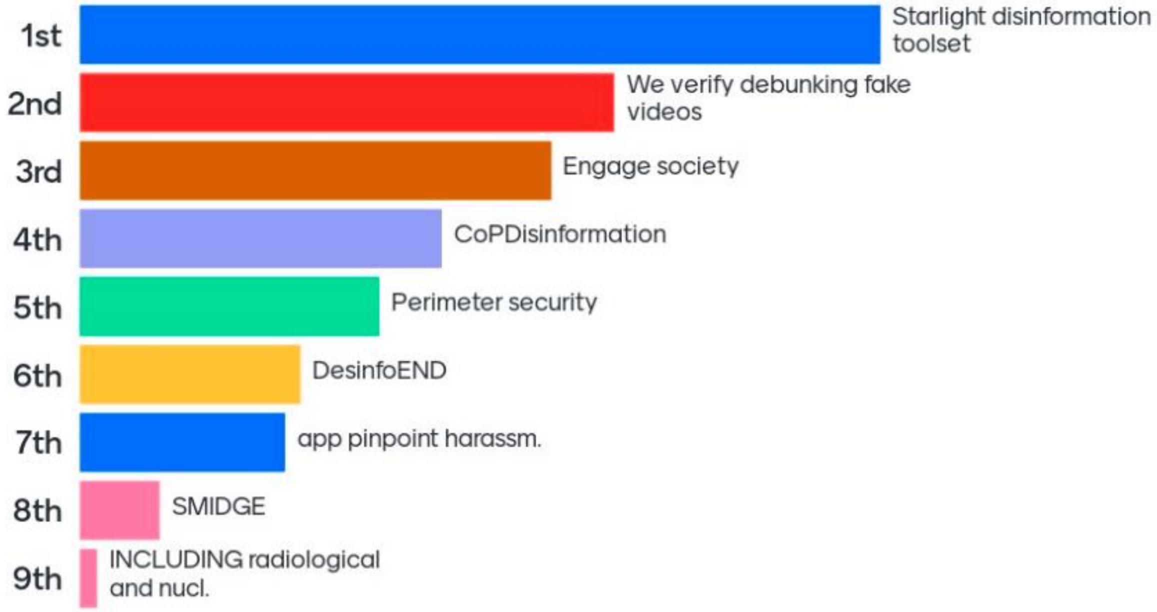
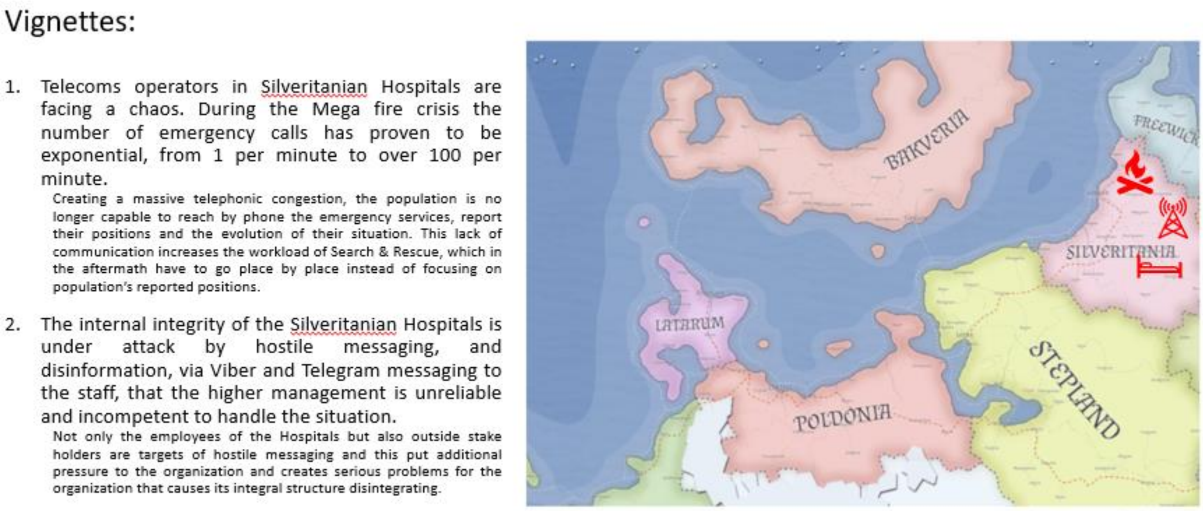


Figure 2 Response to the question “Which innovations were most useful for the given situation?”.

Core Theme: Resilient Civilians, Local Level National Administration

There were 2 Vignettes attributed to this Core theme.


Vignettes:

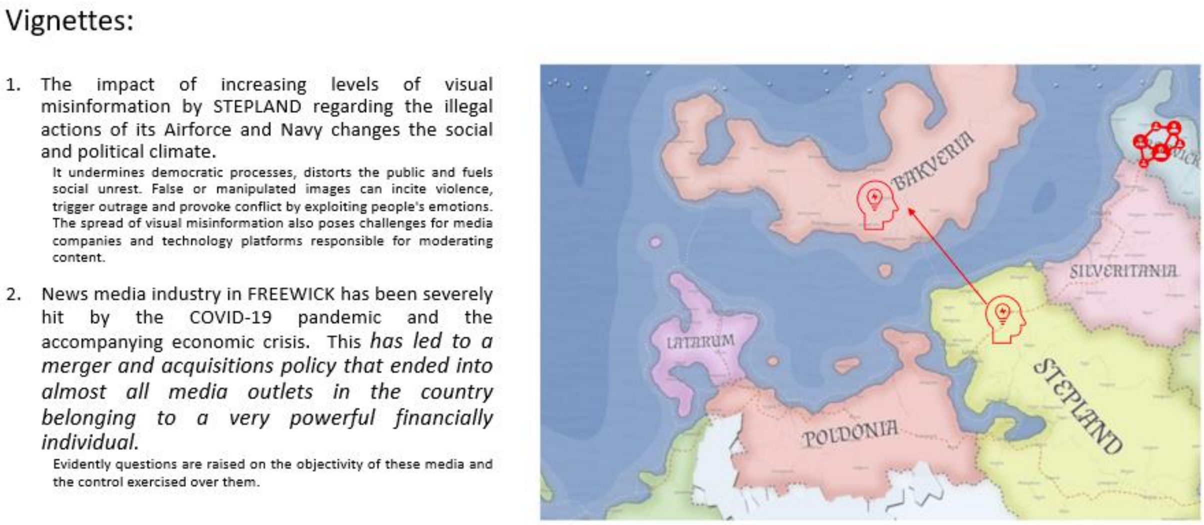
1. Telecoms operators in Silveritanian Hospitals are facing a chaos. During the Mega fire crisis the number of emergency calls has proven to be exponential, from 1 per minute to over 100 per minute.
   Creating a massive telephonic congestion, the population is no longer capable to reach by phone the emergency services, report their positions and the evolution of their situation. This lack of communication increases the workload of Search & Rescue, which in the aftermath have to go place by place instead of focusing on population's reported positions.
2. The internal integrity of the Silveritanian Hospitals is under attack by hostile messaging, and disinformation, via Viber and Telegram messaging to the staff, that the higher management is unreliable and incompetent to handle the situation.
   Not only the employees of the Hospitals but also outside stake holders are targets of hostile messaging and this put additional pressure to the organization and creates serious problems for the organization that causes its integral structure disintegrating.

Respective innovations presented were:

Vignette 1	Vignette 2
AI-enhanced disaster emergency communications - innovation	'Antidote' to hostile messaging delivered by private messaging apps
The Countering Foreign Interference (CFI) project	EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective
	STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats

Core Theme: Information and Strategic Communication

There were 2 Vignettes attributed to this Core theme.



Vignettes:

1. The impact of increasing levels of visual misinformation by STEPLAND regarding the illegal actions of its Airforce and Navy changes the social and political climate.
   It undermines democratic processes, distorts the public and fuels social unrest. False or manipulated images can incite violence, trigger outrage and provoke conflict by exploiting people's emotions. The spread of visual misinformation also poses challenges for media companies and technology platforms responsible for moderating content.
2. News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This *has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual.*
   Evidently questions are raised on the objectivity of these media and the control exercised over them.

4. TRAINING AND INNOVATION ANALYSIS

The EU-HYBNET training was designed to assess innovations discussing which of these might be considered for formal uptake by EU-HYBNET stakeholders, especially pan-European security practitioner organizations in the future.

In order to provide a coherent ground for the innovation analysis, different scenario **vignettes were linked to project Four Core Themes, and the preselected, EU-HYBNET's identified innovative solutions were linked to the vignettes,** assuming that the innovations may provide additional value in the situation bound by it..

Each training team based on the project's Four Core Themes started their discussion with preparation of the initial campaign – how they would respond to the given situation. After this so-called situation assessment participants were introduced to relevant innovations. List of innovations varied according to Vignette and training team/Four Core Themes. Core Theme leaders, also moderators of the discussions, prioritized innovations presented and select the most appropriate (one or two) for their topic.

At the end of discussions the priorities of the whole group were made. Such prioritization does not provide a proper quantitative indication of their ranking but should be considered as qualitative indication of preference of a given group of participants on the most promising innovation for future use. This is to support organizations to discover promising solutions to counter hybrid threats.

4.1. INNOVATIONS TO CORE THEME: FUTURE TRENDS OF HYBRID THREATS

This sub-chapter presented how The EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Theme "Future Trends of Hybrid Threats" and the promising innovations to be tested as identified in WP3 T3.2/D3.5 and T3.3/D3.9 under the named Core Theme.

Vignette 1. *Wide spread of online harassment and acts of violence in LATARUM against POLDONIAN ethnic groups related to STEPLAND escalates to riots. Police and rescue agencies are trying to control and use their resources more efficiently while managing the situation.*

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.1 "Political Deficiency"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Mobile application to pinpoint acts of harassment/violence on the street and online**	Countering online harassment and acts of violence requires to link the victims or witnesses of these actions and the dedicated law enforcement agencies. This requires the solution to cover a larger surveillance area, to be fast and avoid the situation to enter into a spiral of

		kinetic violence such as riots. Such a detrimental situation would indeed require more police and rescue resources, with a reduced ability to control the situation. It also promotes a whole-of-society approach. The proposed solution has a dual interest for the violence occurring in LATARUM against POLDONIAN ethnic groups related to STEPLAND: not only it can detect and regulated online situations, but also physical violence if the online behaviours spill over the streets. This solutions should therefore have a double impact to restore the rule of law.
3.9	**SMIDGE**	Online extremism can result being extremely destabilizing, even if a short amount of activists are propelled into action. Attempts to overthrow democratic government regularly occur from reduced and clandestine cells praising extremist ideologies. The solution proposes to provide a dual effect. The first one concerns the promotion of a sane information through counter-narrative and reliable resources for professionals dealing with information. The second one deals with policy- and decision-makers through guidelines and recommendation.

Vignette 2. *The President of LATARUM has allegedly declare in videos that a referendum will be called regarding the self determination and autonomy of Poldovian residents in the North area of the country. These videos are considered fake.*

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.3 "Substitutive Reality"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**We Verify, a video plugin to debunk fake videos on social media that spread conspiracy theories**	Debunking became an imperative necessity in all democracy as spiral of violence could be easily triggered from disinformation. Dividing society, groups against group is a way to undermine the unity of a country, and social media contribute even more to the polarisation, isolation and antagonisation of social groups. General conspiracy theories and fake news spread more easily than the solutions to counter them. It seems therefore compulsory to spread debunking solutions that are able to tackle the phenomenon. Easily usable through plug-in and applicable to social networks, this solution aims at preventing viral fake videos to intoxicate the citizens by reaching metadata, copyright, transformations to analyse the authenticity of the video. As videos are easily shared, this tool can participate to contain the phenomenon.
3.9	DesinfoEND	As people can be vortexed into a spiral of online disinformation, it is necessary to both prevent such

		actions and protect from its negative effects. Cutting short the conspiracies disinformation permits to protect the informational scene and favour a safe access to reliable news to the population. The tool proposed here aims to focus on vulnerable groups, promoting critical thinking against antagonizing disinformation. Immediate critical thinking is also accompany through this solution with a more long-term education to responsible behaviour regarding information and online communication.

4.2. INNOVATIONS TO CORE THEME: CYBER AND FUTURE TECHNOLOGIES

This sub-chapter presented how the EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Theme no 2. "Cyber and Future Technologies" and the promising innovations to be tested as identified in WP3 T3.2/D3.5 and T3.3/D3.9 under the named Core Theme.

Vignette 3. *Hospitals and emergency services are targeted, physical attacks with IED on their premises affect their ability to provide rapid and efficient assistance in the event of an emergency in BAKVERIA.*

Core theme 2. "Cyber and Future Technologies"

- Threat No 2.3 "Attack on Services"
- Threat No. 2.1 "Stealing Data, Attacking individuals"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Advanced Surveillance Systems with Perimeter security**	Attacks on the critical infrastructure such as health care deprive people from urgent needs of care, endanger staff working conditions and undermine the whole infrastructure system. The Advanced Surveillance Systems (ASS) and Perimeter security is built to protect the critical infrastructure from physical threats. The ASS and Perimeter security tools could be used to mitigate physical threats to the critical infrastructure reinforcing the protection. A central monitoring station with trained personnel continuously monitors the real-time camera images transmitted via redundant channels and enables and ensures an immediate response to suspicious activities. This innovation relates especially to physical threat No. 2.1. "Stealing Data, attacking individuals" and to the

		scenario case where the critical infrastructure in BAKVERIA is attacked and public safety is at risk.
3.5	**Code of Practice on Disinformation**	Disinformation is widespread across different social media channels making it difficult to mitigate. The Code of Practice on Disinformation, which is a self-regulatory tool aims to counter disinformation worldwide in multiple domains. The Code of Practice contains total of 44 commitments and 128 measures to mitigate disinformation on several areas. Operated voluntarily by VOST Europe, the Code of Practice can be activated to perform selected measures in support of affected organizations and jurisdictions. The size of VOST Europe teams is not specified. The Code of Practice on Disinformation could be harnessed to mitigate the spread of disinformation and misinformation targeting hospitals and emergency services accessibility in social media platforms. However, it should be notified that this innovation relies on the voluntary based work and that this innovation must be validated by each MS individually. To make this solution work well, the internal procedures should be clear enough for each actor. As this solution is running with voluntary-based work, appropriate time should be allocated to the monitoring activities.
3.9	ENGAGE **(Engage Society for Risk Awareness and Resilience)**	Civil society has an important role to play in the societal preparedness against natural and man-made disasters. This innovative project aims are to find ways how individuals and local practices could interrelate with planned preparedness and response, practitioners, and technology. The project focuses on aspects that can be directly enhanced such as risk awareness, communication, social media, citizens' as well as authorities' and first responders' involvement. Solutions will aim at bridging the gap between formal and informal approaches to risk and emergency management, increasing the ability of communities to adapt before, during and after disaster. In this project, the prototyped solutions are validated via 3 social emergency simulations that threaten the security of EU societies. The outcomes of this project can be used to enhance and strengthen the collaborative efforts between citizens, first aid responders and emergency workers during a period of a crisis. Strengthened collaboration would at best increase the risk awareness and societal resilience.

Vignette 8. *No specific regulatory framework exists in FREEWICK regarding Disinformation by major online platforms. Social media giants present a manipulative danger combined with the media ownership status, at the same time the situation remains hardly reachable from regulatory perspective.*

Core theme 2. "Cyber and Future Technologies"

- Threat No 2.2 "On-line Manipulation/ Attacking democrazy"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Starlight Disinformation-Misinformation Toolset**	STARLIGHT project (https://www.starlight-h2020.eu/) is one of the flagship projects dedicated to deliver easy deployable toolset to address various need of LEA and other security practitioners driven by constantly changing tech driven crimes modus operandi. In particular, STARLIGHT has one direction dedicated for disinformation and misinformation related threats. This direction is composed of several organisations developing different tooling enabling deep access of information in social platforms and tools to detect different misleading aspects of the information. There are tools dedicated to access information on general internet, communication platforms such as Telegram or X (Twitter) platforms, but majority are focused on detection of fault or forbidden content. Majority of them can work on different languages. All of Starlight tools listed are planned to be integrated in one interface, making them easier to use. At this point of time Starlight project is developing solutions for LEA, but it can be developed further for different target groups and serves as a good example of what is needed to handle artificial amplification complexity. In the context of the vignette Starlight could provide support for LEAs to discover manipulation in information and also have material to prove the manipulation. This could ease the citizens to gain trusted informaiton from LEAs that the citizens are under influencing. Furthermore, this could support the regime to develop new legistlation that will ask media giants to check the possible false information and to prevent spreading the information.

3.9	**Innovative Cluster for Radiological and Nuclear Emergencies,** INCLUDING https://cordis.europa.eu/project/id/833573	The EU-funded INCLUDING project will build a dynamic cluster of 15 partners from 10 EU Member States acting in the INCLUDING Federation. An advanced web platform will shape a map of cooperation between governmental, security and medical institutions, industrial services and others. Partners will provide multidisciplinary knowledge, research, new technologies and infrastructure. Procedures will be formed for joint actions: field exercises, training and simulations. The project will be a base for a modern flexible network for better security in the RN field in Europe. In the context of the vignette, INCLUDING could be an example how information sharing from authorities side will remain crucial in society even though Media Outlets would be bought by malicious actors.

4.3. INNOVATIONS TO CORE THEME: RESILIEN CIVILIANS, LOCAL LEVEL, NATIONAL ADMINISTRATION

This sub-chapter presented how The EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Theme “Future Trends of Hybrid Threats” and the promising innovations to be tested as identified in WP3 T3.2/D3.5 and T3.3/D3.9 under the named Core Theme.

Vignette 4. *Telecoms operators in Silveritanian Hospitals are facing a chaos. During the Mega fire crisis the number of emergency calls has proven to be exponential, from 1 per minute to over 100 per minute, becoming impossible to sort out by emergency dispatchers, especially with the average emergency call lasting from 3 to 15 minutes dealt by just a few emergency dispatchers. Creating a massive telephonic congestion, the population is no longer capable to reach by phone the emergency services, report their positions and the evolution of their situation. This lack of communication increases the workload of Search & Rescue, which in the aftermath have to go place by place instead of focusing on population’s reported positions.*

Core theme 3. “Resilient Civilians, Local Level, National Administration”

- Threat No 3.2. “Attack on Social Structures”

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**AI-enhanced disaster emergency communications -innovation**	The starting point for the selected innovation is that the technology can be applied to enhance the resilience of social structures in the face of hybrid threats. The company HighWind has developed and patented the first Artificial Intelligence that can assess a patient's emergency priority level in less 100 millisecond thanks to Computer Vision and Deep learning using a crossed analysis on traumatology (nature of the wounds), emotions (pain, fears, etc.) and contextual elements (fire, smoke, etc.). Applied to major disasters, and encompassed within an smartphone "Disaster Mode" app for the population (downloaded or emulated by text-message link), it gives the emergency responders the ability to immediately visualize who are the persons most at risks on a map, prioritize search & rescue efforts to the most vulnerable persons, avoid the emergency calls congestion and facilitate patient referrals to hospitals based on the severity of their injures, thereby mitigating the potential influx of patients in hospitals. Instead of taking one by one, lengthy emergency calls due to stressed persons, the emergency dispatch centre can perform several actions at once: send a "Disaster Mode" notification to the population, receive an accurate view on the emergency requests critical levels and positions on a map in few seconds, to better coordinate SAR efforts. Leveraging on basic smartphone features, the AI is capable to immediately sort out victims, saving hours for the SAR teams and significantly increasing chances of survival. The "Disaster Mode" is also capable to take decisions to optimize communication based on available networks quality (no data, 2G to 5G). On the whole, the solution can be used to protect the social infrastructure to potential attacks and increase resilience of health sector during the crisis situations. The solution is specifically

		designed to enable an early assessment of the crisis. Initial triage at the crisis scene serves the purpose of enabling hospitals and all involved stakeholders better understand the severity of crisis and prepare appropriately. N.B. The innovation primary pertains to technical aspects. However, to make the solution operational ready there is a need to develop a framework of utilization of the "Disaster Mode" solution and its AI-enhanced Safety Check ensuring compliance to EU General Data Protection Rules (GDPR), considering level of risks of a given disaster for the safety and health of the persons and ensure compliance of the prototype toward EU main guidelines: AI Act, Data Act and GDPR.
3.9	**The Countering Foreign Interference (CFI) project** https://www.iss.europa.eu/content/euiss-launches-eu-funded-project-countering-foreign-interference	The FCI project focuses on improving understanding of potential threats in the information space. It will utilize accumulating knowledge for developing improved tools and methods to identify, monitor and counter those threats. Often adversaries aim to amplify the present crises by increasing disinformation in the information flow. Therefore, in a case of crises, it is important for the authorities that their guidance and information can be well reached so that the crises will not escalate further on the basis of false information. Therefore, it is important for the authorities to have the improved tools and methods to identify, monitor and counter disinformation in early phase.

Vignette 5. *The internal integrity of the Silveritanian Hospitals is under attack by hostile messaging, and disinformation, via Viber and Telegram messaging to the staff, that the higher management is unreliable and incompetent to handle the situation. Not only the employees of the Hospitals but also outside stake holders are targets of hostile messaging and this put additional pressure to the organization and creates serious problems for the organization that causes its integral structure disintegrating.*

Core theme 3. "Resilient Civilians, Local Level, National Administration"

- Threat No 3.3. "Undermining institutions' internal organization"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**'Antidote' to hostile messaging delivered by private messaging apps**	The starting point and goal of the solution is very straight forward: to improve people's resilience to hostile messaging and hence fostering the integrity of organizations. The starting point in the suggested solution is that information is to be shared in order to raise awareness and standard of critical thinking. I.e. messages like "this is not true" may not be the most efficient, but rather the games attracting attention to the problem may be used. Technically most simple solutions are sharing the link to freely available and already existing games but games takes time and 'Antidote' can be shared in other ways too. For an example the simplest, but also much more expensive way, is to buy "antidote" as advertisement. The more complex, but much cheaper and more efficient way, would be to collaborate with the owners of the private messaging apps in order to sort out the target groups to be immunized and share the content for free. Although the best 'antidote' could be chosen by the organization which integrity needs protection, the communication and dealing with private messaging app owners should be handled centrally. This asks time but is still seen as a sound and well recommended solution. Furthermore, the technical solution – private messaging apps – is already there. There is only a need to start using them more efficiently in the fight countering disinformation and getting the owners of the app on board.
3.9	**EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective** https://cordis.europa.eu/project/id/608385	It is expected that information sharing platforms for strategic security institutions would provide not only needed tools for information sharing inside the organization but also between the institutions. The platforms are also to increase cooperation between actors and to increase traceability and trust alike motivation for the cooperation due to enhanced results. The gained trust in cooperation builds resilience to adversaries possible attempts to harm the trust and to paralyze joint proceeding in critical cases and in crises.

		A successful project to increase cooperation in information sharing and cooperation has been EUCISE2020 project in European maritime domain. The project has lead to development of Common Information Sharing Environment (CISE) to pan-European and national maritime authorities. On the whole, CISE is not only to support various pan-European security authorities to increase their cooperation, but it also empowers the cooperation in national level due to the development of national nodes. In short, without the cooperation between the national security institutions and authorities in the specific security domain (e.g. in maritime domain/ border guards, navy, police, customs) development of the solution/CISE national node would not have been possible. In short, the pan-European CISE has pushed national security authorities and institutions to find and definite new ways of cooperation and information sharing reducing partly also the culture of secrecy between institutions and inside the institutions. An example of increased cooperation between national *strategic security institutions* is a FINCISE project from Finland **FINCISE 2.0 Project** CISE | The Finnish Border Guard (raja.fi) (Duration: 2022 -2024) where all Finnish Maritime Cooperation (FIMAC) authorities joined to CISE development and finding new ways for future cooperation. On the whole, the takeaway from the above mentioned CISE projects' is that the approach seems to work in various security domains and hence also hybrid threats related security authorities could consider to develop CISE for their purposes. Furthermore, CISE seems to support cooperation between strategic security institutions and diminish culture of secrecy between institutions, also in the institution.
3.9	**STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats** https://cordis.europa.eu/project/id/740610	Also solutions that have trained actors in organizations, or between organizations, to work together during crises (e.g. during malicious influencing campaigns to cooperation) are much needed in order to ensure critical institutions solid work flow. With reference to this, STOP-IT project has developed a solution that ensures training for organization to face future severe cases in a manner that trust and knowledge how to proceed without severe challenges will be maintained.

		STOP-IT has delivered an integrated, modular platform that supports strategic/tactical planning, real time operational decision making and post-action assessment for the key parts of the water infrastructure. The focus in the platform can be in any other infrastructure too. The STOP-IT platform is scalable (scaling from small utilities to large ones); adaptable (including various modules addressing different needs, with expandability for future modules); and flexible (the utility managers can decide how to use it and it will be usable by experts, novices, and even non-technical staff). The categories in the platform are: Decision Makers; Risk Officers and Modellers; Real Time Operators and Maintenance Managers. Even though the platform has been developed to three different user categories in organizations, it can also host multi-agency/ institutions discussion and planning. On the whole, the STOP-IT platform supports to enhance cooperation skills and trust between the users because its use provides exercise(s) that may then ease the cooperation in the future in real cases.

4.4. INNOVATIONS TO CORE THEME: INFORMATION AND STRATEGIC COMMUNICATION

This sub-chapter presented how The EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Theme “Future Trends of Hybrid Threats” and the promising innovations to be tested as identified in WP3 T3.2/D3.5 and T3.3/D3.9 under the named Core Theme.

Vignette 6. *The impact of increasing levels of visual misinformation by STEPLAND regarding the illegal actions of its Airforce and Navy changes the social and political climate. It undermines democratic processes, distorts the public and fuels social unrest. False or manipulated images can incite violence, trigger outrage and provoke conflict by exploiting people's emotions. The spread of visual misinformation also poses challenges for media companies and technology platforms responsible for moderating content.*

Core theme 4. “Information and Strategic Communication”

- Threat No 4.3. “Attack on information”
- Threat No 4.2 “Antagonizing victimization narratives in the informational space.”

Vignette 7. *News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual. Evidently questions are raised on the objectivity of these media and the control exercised over them.*

Core theme 4. "Information and Strategic Communication"

- Threat No 4.3. "Attack on information"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Blockchain -based verification -innovation**	Blockchain technology can play a crucial role in the fight against the increasing use of visual misinformation. By leveraging the inherent security and transparency of blockchain, a robust system can be established to verify the authenticity of images and videos. Blockchain allows us to timestamp visual content at the time of creation. Each medium is linked to a unique cryptographic hash and recorded on the blockchain, creating an immutable record of its provenance. This timestamp ensures that the authenticity of the content can be easily verified, thus helping to identify real footage and distinguish it from manipulated images. Fact-checking organizations are integrating this blockchain technology into their processes by recording their findings and conclusions on the blockchain. This creates an immutable record of verified information, increasing confidence in their reviews. Collaborating with content creators is essential. Encouraging professionals and journalists represents a sign of trustworthiness to certify the authenticity of their work on the blockchain. This also increases trustworthiness in a time plagued by misinformation. Public blockchain visual content verification databases managed by a consortium of organizations can further improve transparency and accountability. Furthermore recognizing blockchain as evidence in court cases related to

		misinformation is an incentive to use this technology to verify content.
3.5	**Media Pluralism Monitor (MPM)** https://cmpf.eui.eu/media-pluralism-monitor/	Media Pluralism Monitor (MPM) is a tool developed by the Centre for Media Pluralism and Media Freedom (CMPF) of the European University Institute (EUI) to assess the potential weaknesses in national media systems that may hinder media pluralism. Based on 20 indicators, summarizing 200 variables, it covers four areas: 1. Fundamental protection 2. Market plurality 3. Political independence 4. Social inclusiveness. The news media industry has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. Although the shock was largely foreseeable due to the extraordinary circumstances, its depth and the diverging effect between different countries has to be investigated.
3.9	**ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE (Grant agreement ID: 101094742)** **Website:** https://resilientmedia.eu/ **Cordis:** https://cordis.europa.eu/project/id/101094742	Resilient Media for Democracy in the Digital Age (ReMeD) responds to the European Commission's call HORIZON-CL2-2022-DEMOCRACY-01-06: "Media for democracy – democratic media" and will tackle existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the

		creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. ReMeD could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, in the same way project MeDeMAP can. By gathering, analysing, comparing and contrasting data regarding professional journalists, alternative media content producers and citizens which operate in technologically mediated configurations, as well as the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape, ReMeD could, as a biproduct identify trends and qualitative indicators which could help better understand the demand of and thus the sustainability of quality journalistic media.

Vignette 7. *News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual. Evidently questions are raised on the objectivity of these media and the control exercised over them.*

Core theme 4. "Information and Strategic Communication"

- Threat No 4.1. "Media Conundrum"

Proposed innovations to be tested in the training event according to D3.5 and D3.9 are following:

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**The Media Pluralism Monitor (MPM) tool**	The Media Pluralism Monitor (MPM) is a tool developed by the Centre for Media Pluralism and Media Freedom (CMPF) of the European University Institute (EUI) to assess the

		potential weaknesses in national media systems that may hinder media pluralism. Based on 20 indicators, summarizing 200 variables, it covers four areas: 1.Fundamental protection, 2.Market plurality, 3.Political independence, 4.Social inclusiveness. The solution can be used to prevent the deprivation of market shares from quality journalistic media by ensuring that sufficient investment in investigative journalism is not sacrificed in the face of journalistic competitiveness, by identifying and sharing best practices for journalistic media economic sustainability. In the context of the vignette, Media outlets, journalists, publishers, broadcasters, editors and other related stakeholders are the end-users of the idea. Media Pluralism Monitor (MPM) assesses the potential weaknesses in national media systems that may hinder media pluralism and covers the areas of fundamental protection, market plurality, political independence and social inclusiveness.
3.9	**Resilient Media for Democracy in the Digital Age (ReMeD) project** https://resilientmedia.eu/	Resilient Media for Democracy in the Digital Age (ReMeD) tackles existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. In the context of the vignette ReMeD could contribute to the identification and sharing of

		best practices for economic sustainability of journalistic media.
D3.9	**INJECT Innovative Journalism: Enhanced Creativity Tools -project** https://cordis.europa.eu/project/id/732278	INJECT's objective was to transfer new digital technologies to news organisations to improve the creativity and the productivity of journalists, to increase the competitiveness of European news and media organisations. To achieve this objective, INJECT extended and aggregated new digital services and tools already developed by consortium members to support journalist creativity and efficiency, and integrated the services and tools with current CMSs and journalist work tools in order to facilitate their uptake and use in newsrooms. The services undertook new forms of automated creative search on behalf of journalists, using public sources (e.g. social media) and private digital resources (e.g. digital libraries of political cartoons) to generate sources of inspiration for journalists who were seeking new angles on stories. The tools provide new interactive support for journalists to think creatively about new stories and reuse news content in new ways to increase productivity. To transfer the new services and tools to Europe's news and media organisations, INJECT established a new INJECT spin-off business, built up and expanded multiple vibrant ecosystems of providers and users of new digital technologies, and exploited its position at the heart of Europe's journalism industry to raise market awareness and take-up on the services and tools. With respect to Call ICT21, INJECT increased the competitiveness of one of Europe's most important creative industries – journalism - by stimulating ICT innovation in SMEs, by effectively building up and expanding vibrant EU technological ecosystems that met the emerging needs of Europe's new and existing news and media organisations. In the context of the vignette, INJECT could deliver new ideas on ways how small scale media outlets may compete against giant Media outlets and have their news feed also heard by the citizens.

.

5.TRAINING LESSONS LEARNED COCNLUSIONS

The Lessons Learned report (D2.25 Training and exercises Lesson Learned report) has assessed the third cycle event with the aim of providing suggestions especially for future T&E as a project outcome. The report also recognises the improved work carried out since the first event with simplified scenario play, clarifying the type of situation, inviting innovation providers to demonstrate the added value, and organising the events both on site and online.

If consortium partners are to run T&E events in the future after the project ends, it is suggested that they:

- Have a clear understanding of the objectives and nature of the event at the onset: a training event, a lecture event, or, for example, an innovation assessment event.
- Provide a clear description of training and exercise objectives, scenarios, and selected innovations, with at least one key takeaway.
- Define the target audiences very clearly. One option could be to organise several types of T&E for targeted groups.
- Simplify the scenario setting without vignettes and project structure pillars such as core themes.
- Choose max. 1-2 innovations that are at the core of the training instead of scenarios.

6.CONCLUSIONS

In this document, the training material produced under Task 2.4 has been presented. Under the scope of the document and its relevant task, a set of documentation has been prepared in order to be circulated to all EU-HYBENT training participants, moderators and trainees.

Many EU-HYBNET consortium partners and network members are training providers, covering subject of Hybrid Threats. In order to avoid delivery of overlapping scenarios and training delivery EU-HYBNET T2.4 initiated a survey that aimed to identify and analyse other available trainings. Analysis results are described in EU-HYBNET D2.22 «Training and exercises delivery on up-to-date topics« . Furthermore, EU-HYBNET training has no overlapping issues to the identified, existing training.

In order to address unique aspects of prioritized gaps training has been redesigned with unique Hybrid scenarios Vignettes (types of events and attacks) as well incorporating EU-HYBNET identified innovations.

The training methodology was especially designed to cover subject of innovation role in countering hybrid threats. It is worth noting that similar methodology (DTAG) was applied in all three cycles. This made trainings more familiar for participants and eventually more effective.

Materials provided before and during the training events were gradually reduced in complexity to avoid time spend on clarification of initial setup.

Also videos from all training events are/will be made available in EU-HYBNET TUOVI Platform to support project partners and Network Members if similar approach is used in other training occasions.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / description
DTAG	Disruptive Technology Assessment Game
D	Deliverables
OB	Objective
T	Task
WP	Work Package
EU	European Union
EC	The European Commission
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats -project
IoS	Ideas of Systems
MS	Member States
RTO	Research And Technology Organisation
OB	Objectives
T&E	Training and Exercises

ANNEX II. REFERENCES

[1] EU-HYBENT Deliverable 2.19 Training and Exercise, Scenario delivery

[2] EU-HYBENT Deliverable 2.22 Training And Exercises Delivery On Up-To-Date Topics

[3] EU-HYBENT Deliverable 2.25 Training And Exercises Lessons Learned Report

ANNEX III. ADENDA OF THE EVENT

EU-HYBNET 3rd Training and Exercise Event
18-19 January, 2024, Vilnius Didlaukio g. 55, Lithuania

Agenda

Day 1, January 18 (Thursday)

Link for on-line participants in MS Teams platform:

LIN K

Meeting ID: 385 942 426 504

Passcode: jN2PkC

Time	Item	Room
12:00 - 12:20	Welcome and Introduction	102
12:20 - 13:00	Description of the event flow	
13:00 – 14:00	“Mind setting” plenary session: • Julien Théron, EC Joint Research Center, CORE model (fresh look at hybrid threats) • Jorge Gomes, VOST Europe, Content moderation on media platforms (how this can be handled)	
14:00-14:20	**Break**	
14:20-14:45	Introduction to Scenario	
14:45-15:00	Q & A and **Logistics to Breakout rooms**	
	Breakout rooms: 1. “Future trends of Hybrid Threats” LINK 2. ”Cyber & Future Technologies” LINK 3. ”Information and Strategic Communication” LINK 4. ”Resilient Civilians, Local Level National Administration” LINK	104 102 101 407
15:00-16:15	Breakout rooms: • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
16:15-16:30	**Break**	
16:30-17:30	Presentation of results of Core Themes	102
17:30-17:45	Closing remarks	102

Day 2, January 19 (Friday)

Link for on-line participants in MS Teams platform:

LINK

Meeting ID: 385 942 426 504
Passcode: jN2PkC

Time	Item	Room
10:00-10:15	Welcome and Introduction	102
	Breakout rooms: 1. “Future trends of Hybrid Threats” LINK 2. ”Cyber & Future Technologies” LINK 3. ”Information and Strategic Communication” LINK 4. ”Resilient Civilians, Local Level National Administration” LINK	104 102 101 407
10:15-11:30	Breakout rooms (Session I for the 1st vignette): - Introduction to innovations - Campaign planning - Presentation of the campaign plan	101, 102, 104, 407
11:30-11:45	**Break**	
11:45-13:00	Breakout rooms (Session II for the 2nd vignette): - Introduction to innovations - Campaign planning - Presentation of the campaign plan	101, 102, 104, 407
13:00-13:20	**Break**	
13:20-14:20	Presentation of results of Core Themes	102
14:20-15:00	Feedback session and closing remarks	102