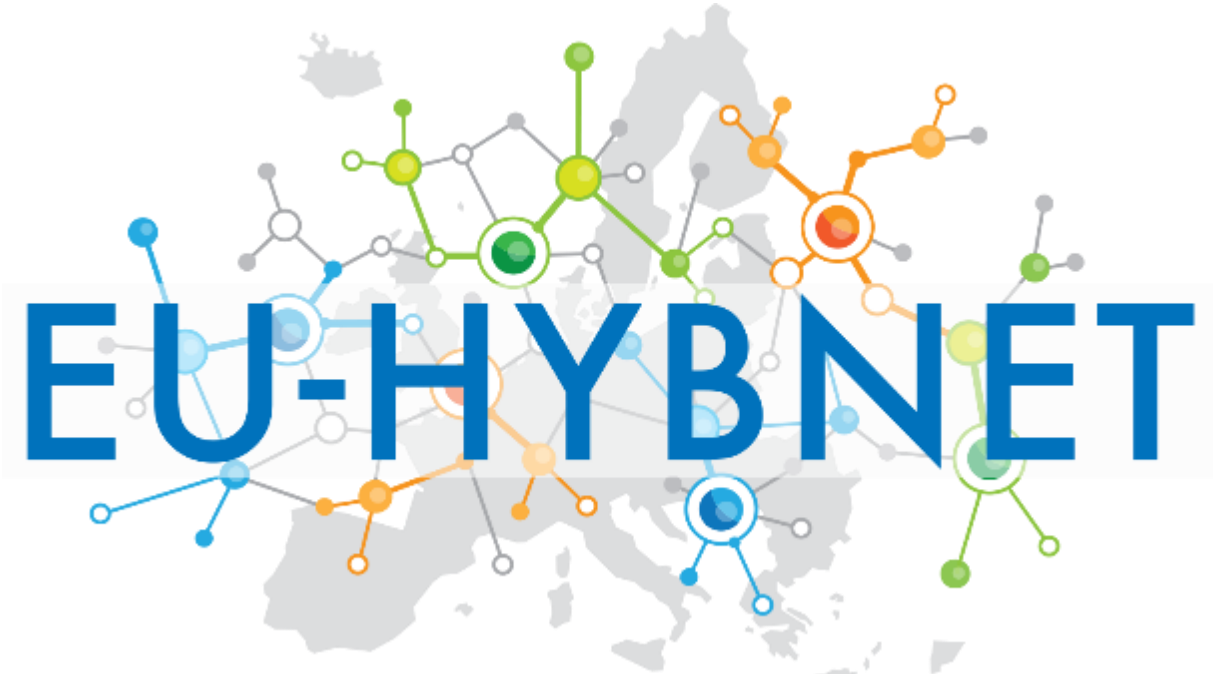


TRAINING AND EXERCISES SCENARIO AND TRAINING MATERIAL

DELIVERABLE 2.27

Lead Author: KEMEA

Contributors: L3C3, Laurea, JRC
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	**D2.27**	
Version:	**1.0**	
Delivery date:	**21/02/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Delivered**	
Nature:	**Report**	
Main authors:	**Vanessa Papakosta**	**KEMEA**
Contributors:	**Rainer Jungwirth**	**JRC**
	Edmundas Piesarkas	**L3CE**
	Päivi Mattila	**LAUREA**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	30/09/2022	Edmundas Piesarkas L3CE	Material produced
0.2	25/01/2023	Vanessa Papakosta KEMEA	Table of Contents
0.3	30/01/2023	Vanessa Papakosta KEMEA	Update on content
0.4	03/02/2023	Päivi Mattila LAUREA	Making comments
0.5	06/02/2023	Vanessa Papakosta KEMEA	Update on content
0.6	07/02/2023	Edmundas Piesarkas L3CE	Making Comments
0.7	13/02/2023	Vanessa Papakosta KEMEA	Update on content
0.8	15/02/2023	Päivi Mattila LAUREA	Review and text editing
0.9	20/02/2023	Rainer Jungwirth JRC	Review
0.91	21/02/2023	Vanessa Papakosta KEMEA	Final review
1.0	21/2/2023	Päivi Mattila LAUREA	Final review and submission of the document to the EC

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION 4
1.1 Overview 4
1.2 Structure of the deliverable 5
2. EU-HYBNET TRAINING OVERVIEW 6
3. TRAINING SET UP 9
3.1. Training Scenario 10
3.1.1 Scenario - Main Actors and Situational Map 10
3.1.2 Scenario – Vignettes 15
3.2. Training Scenario and Innovation Analysis Set Up 17
4. TRAINING AND INNOVATION ANALYSIS 20
4.1 Innovations to Analyze in the Training 20
4.1.1 Innovations to Vignettes – Core Theme: Future Trends of Hybrid Threats 20
4.1.2 Innovations to Vignettes – Core Theme: Cyber and Future Technologies 23
4.1.3 Innovations to Vignettes – Core Theme: Information and Strategic Communication 29
4.1.4 Innovations to Vignettes – Core Theme: Resilient Civilians, Local Level and National Administration 33
4.1.5 Innovations to Vignettes – three additional Presentations 43
4.2 Innovation Analysis General Remarks 44
5.TRAINING LESSONS LEARNED FOR FUTURE EVENTS 45
6.CONCLUSIONS 47
7.FUTURE WORK 48
ANNEX I. GLOSSARY AND ACRONYMS 49
ANNEX II. REFERENCES 50
ANNEX III. ADENDA of the EVENT 51

TABLES

Table 1 Glossary and Acronyms 49

FIGURES

Figure 1 EU-HYBNET structure of Work Packages and Main Activities 4

EXECUTIVE SUMMARY

The purpose of this deliverables (D2.27) 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 2nd working cycle of the project. The training activities, as well as the evaluation of the overall training are described in more detail in Deliverables 2.21 and 2.24. However, this deliverable (D2.27) 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 D2.27 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 2nd EU-HYBNET training event on 29-30/9/2022 in Vilnus, 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.

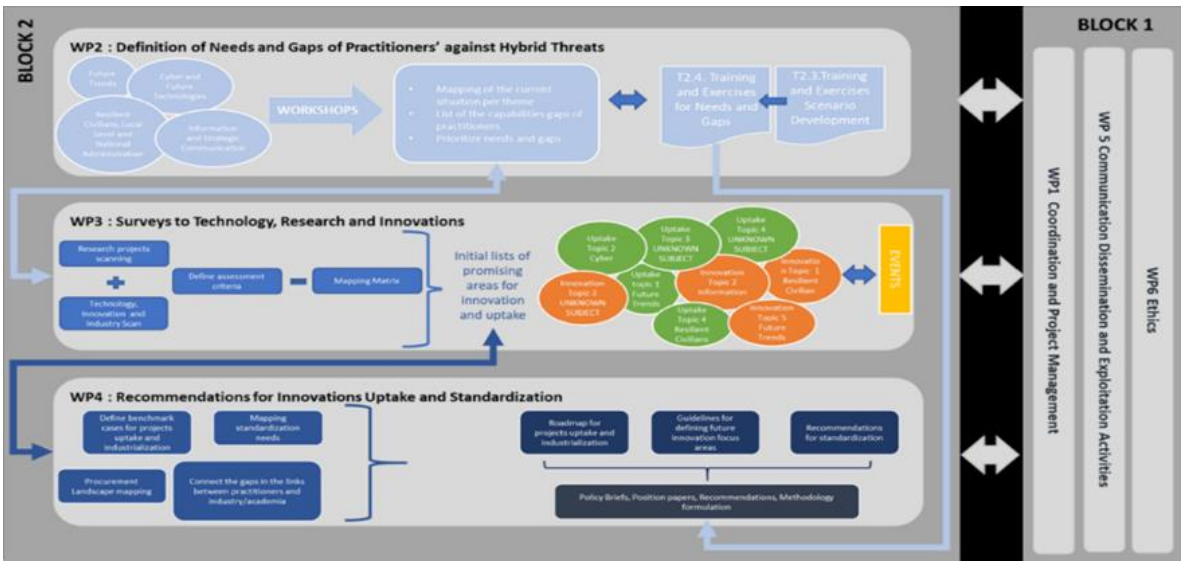


Figure 1 EU-HYBNET structure of Work Packages and Main Activities

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 D2.27 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, D2.27 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
- Section 7. presents the future work connected to deliverable 2.27.

2. EU-HYBNET TRAINING OVERVIEW

The 2nd 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 cycle EU-HYBNET Training and Exercising Event. For the 2nd cycle DTAG methodology was adjusted, reflecting experience, and Lessons Learned from the 1st cycle. However, the key elements of DTAG were not modified, and hence thorough guidance to use DTAG can be familiarized from EU-HYBNET 1st cycle "Training and Exercises Scenario and Training Material" D2.27, 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

In the 2nd EU-HYBNET training event the DTAG linked to a scenario and various vignettes developed in EU-HYBNET T2.3 "*Training and Exercises Scenario Development*"/ D2.18 "*Training and Exercise, Scenario delivery*" to sketch hybrid threats and challenges within a realistic near-future operational environment. The basis of EU-HYBNET scenario lies in six different entities that are interacting in the same geopolitical context, while different attack surfaces are developed suitable to deploy hybrid ops vectors. In the scenario various vignettes were supplemented by a selection of injects, additions to the vignette, which add new challenges, tensions and difficulty to the crisis situation. The scenario and vignettes descriptions were created to be in-line with 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*) and training teams were formulated according to the Four Core Themes. In addition, Four Core Theme supported to test possible solutions, selected innovations under each of the Four Core Themes in different situations and operational contexts. The innovations were resulting from EU-HYBNET WP3 "*Surveys to Technology, Research and Innovations*"/ D3.4 "*First mid-term report on Improvement and innovations*" and D3.8 "*First mid-term report on Innovation and Research monitoring*" results. 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 (see ANNEX I).

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 the training event participants in teams were/are asked to freely assess the overall situation and to test the innovations presented for them as possible promising solutions. The aim is 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 the pan-European security practitioners to plan and conduct their 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. However, during the event some presentations of innovative solutions with high TRL level were provided on live. The innovations were:

- EEAS, Strategic Communication Division/ DDS-Alpha tool for disinformation analysis and sharing
- HENSOLDT/ Open-source intelligence platform
- Maltego/ Information analysis platform

In addition an example of operational level use of different solutions was presented by Lithuanian Armed Forces Strategic Communications department. Live presentations were imbedded to the training in order to create a better understanding of the role of innovations.

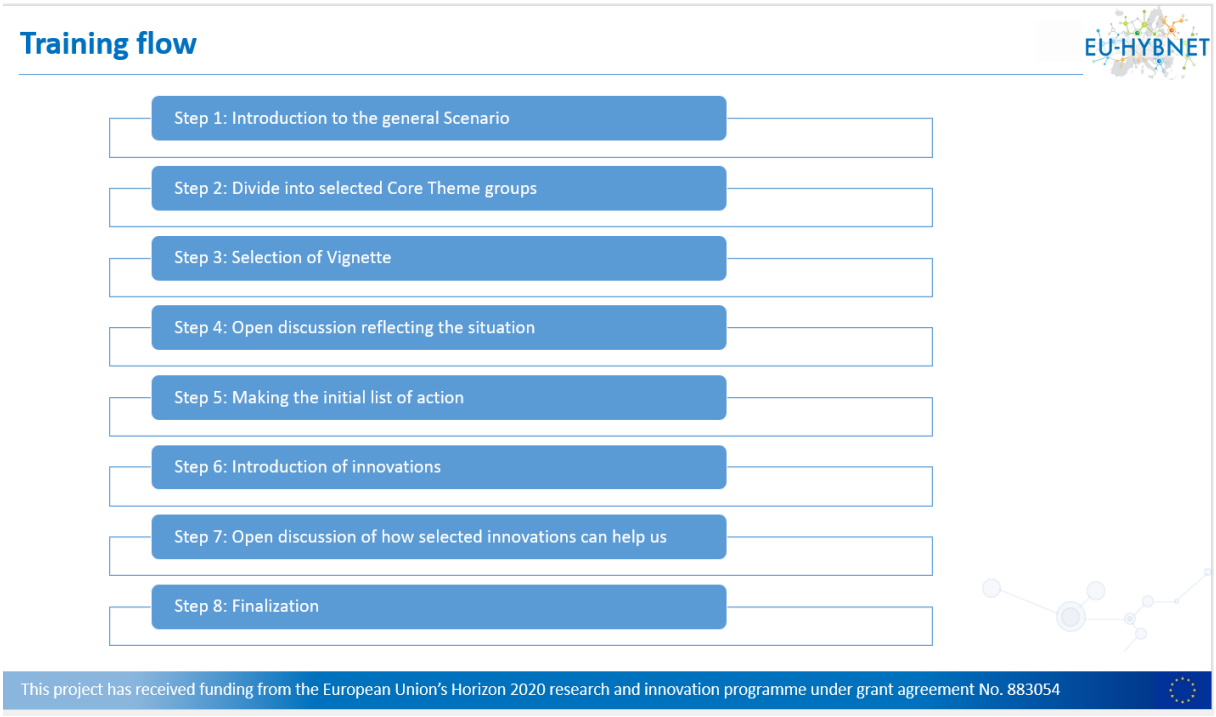
Eventually, EU-HYBNET Four Core Theme based training teams were formulating how the solutions could improve response to different challenges described in scenario and given vignettes. Teams needed to select most feasible innovative solution for selected vignette and after reaching group consensus to envision how it could be operationalized. To support this, pre-designed PowerPoint slides

were shared to the training participants to support data collection and analysis. This 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.

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. The outcomes of the innovations' validation and assessment are elaborated further in the report.

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 2nd EU-HYBNET training event. The "Training Flow" is following:



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 D2.18 "*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 D2.18 "*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 "Trianing 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

EU-HYBNET shares the general goal that 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 scenario and its' vignettes should include the different views of the stakeholders, pan-European security practitioners, on possible alternative future developments that are hard to predict and the assumptions behind the scenario and vignettes must be made transparent. The scenario and vignettes need to represent different kind of challenges and alternatives to pan-European security practitioners' 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. Berkhudian Republic, Republic of Balan and Republic of Bhic are members of the "Triple B Coalition"

b. The kingdom of Sharn is a neutral hydrocarbon producing country with important commercial ports

c. The Mugian Republic is an independent country

d. The Sandmouthian federation is a strong militarily alliance of many states, in confrontation with the "Triple B Coalition".

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

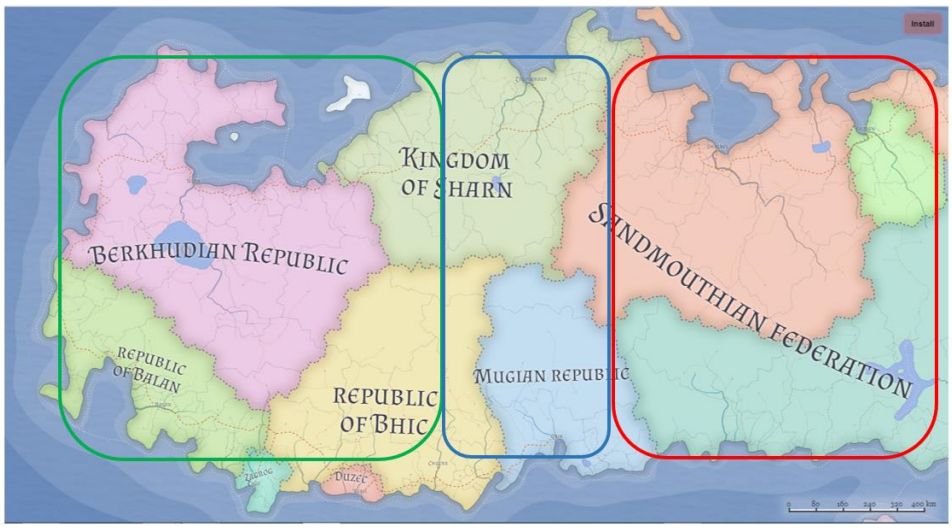
- Elections are called in the Republic of Bhic that is in close defence and diplomatic collaboration with the Republic of Balan and the Berkhudian Republic.
- In the Duzec province of Bhic Republic is active an active minority influenced by the Sandmouthian Federation, speaks Sandmouthian and has religious connections with the federation. Duzec residents are in close proximity with the federation and strongly influenced.
- The Mugian Republic desires to join the BBB coalition, while at the same time the Sandmouthian Federation is looking forward to incorporate it in the Federation, as it was a former member of it in the past.
- The kingdom of Sharn is a neutral hydrocarbon producing country supplying the BBB coalition with oil and natural gas. At the same time has commercial and trade connections with the Federation.
- The Sandmouthian federation starts large scale military exercises assembling considerable numbers of troops on the border line with Mugia. The situation seems like military offensive preparations are intended.

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

EU-HYBNET



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

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

Scenario

Elections are called in the Republic of Bhic that is in close defence and diplomatic collaboration with the Republic of Balan and the Berkhudian Republic.

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

Scenario

In the Duzec province of Bhic Republic an active minority influenced by the Sandmouthian Federationis active. Speaks Sandmouthian and has religious connections with the federation. Duzec residents are in close proximity with the federation and strongly influenced.

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

Scenario

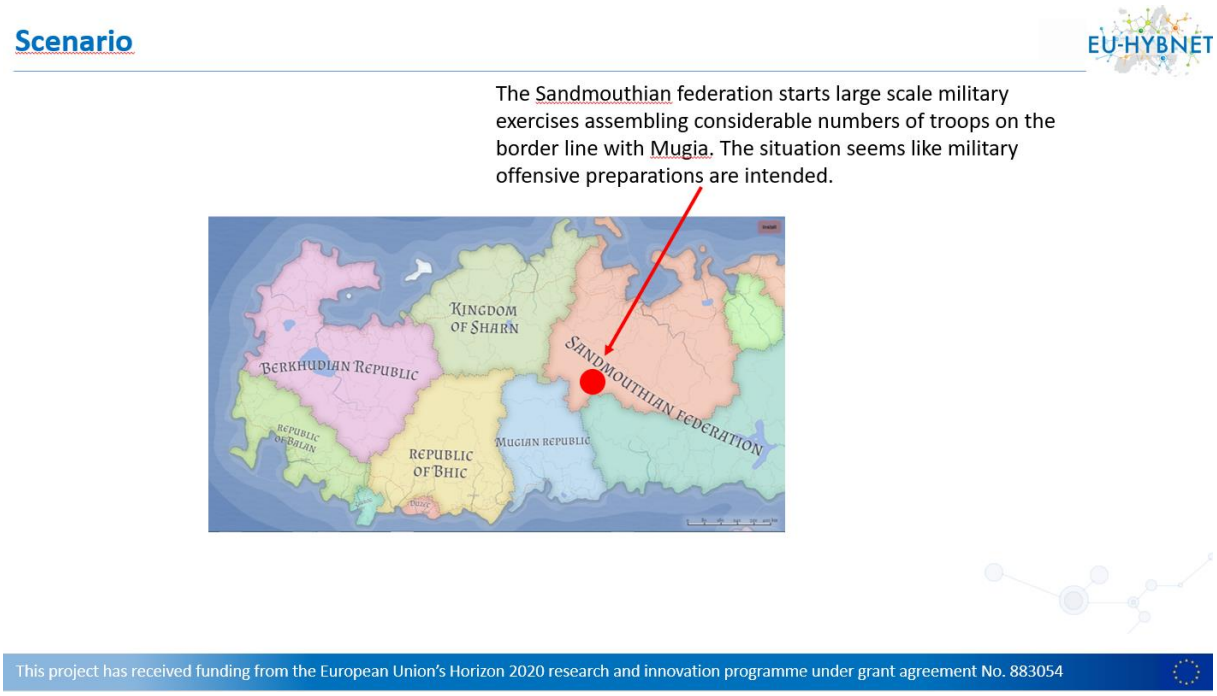
The Mugian Republic desires to join the BBB coalition, while at the same time the Sandmouthian Federation is looking forward to incorporate it in the Federation, as it was a former member of it in the past.

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

Scenario

The kingdom of Sharn is a neutral hydrocarbon producing country supplying the BBB coalition with oil and natural gas. At the same time has commercial and trade connections with the Federation.

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



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

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 following way to keep well track in the training flow:

- Vignettes were used to reduce the overall scope of the general scenario.
- Most relevant vignettes were linked to the core groups to provide situations that are relevant to the scope of the training teams/Project Four Core Themes.
- To avoid very complex contextual setting training moderators of each of the Four Core Themes were advised to select one vignette to facilitate a more narrow discussion and avoid time spend on "assessing" the situation.
- Selection of the vignettes were a starting point of discussion to set the mind on situation and understand background and interests of participants, as they were very different.

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

Core Theme: Future Trends of Hybrid Threats

Vignettes:

1. Minority groups in one area activate discussions on independence during the national elections process.
2. The irregular migrant flows are facilitated, by allowing if not escorting with its coast guard forces.
3. Air bombing attack on one of the countries. Mechanized infantry units invade. Civilian refugees are fleeing.
4. A new migrant area is created mainly by people from the adjacent majority region.

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

.

Core Theme: "Cyber & Future Technologies"

Vignettes:

1. Cyber-attacks causing major power outages. This causes serious problems on households as well as industrial control systems on a frequent basis.
2. Telecoms are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations.
3. The irregular migrant flows are facilitated, by allowing if not escorting with its coast guard forces.
4. Air bombing attack on one of the countries. Mechanized infantry units invade. Civilian refugees are fleeing.
5. A new migrant area is created mainly by people from the adjacent majority region.

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

..

Core Theme: "Information and Strategic Communication"

Vignettes:

1. Minority groups in one area activate discussions on independence during the national elections process.
2. A Fake news campaign on official media, that the electoral process is staged and premeditated is observed.
3. A new migrant area is created

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

.

Core Theme: "Resilient Civilians, Local Level National Administration"

Vignettes:

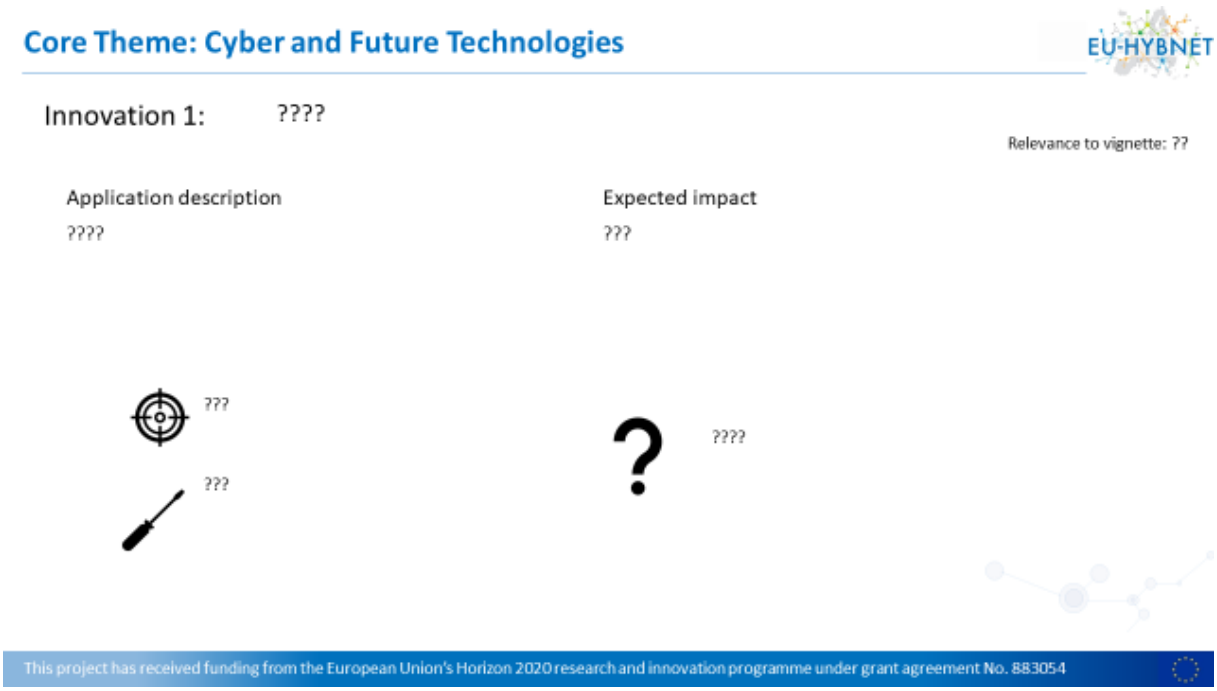
1. Minority groups in one area activate discussions on independence during the national elections process.
2. A Fake news campaign on official media, that the electoral process is staged and premeditated is observed.
3. A new migrant area is created mainly by people from the adjacent majority region.
4. Telecoms are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations,

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

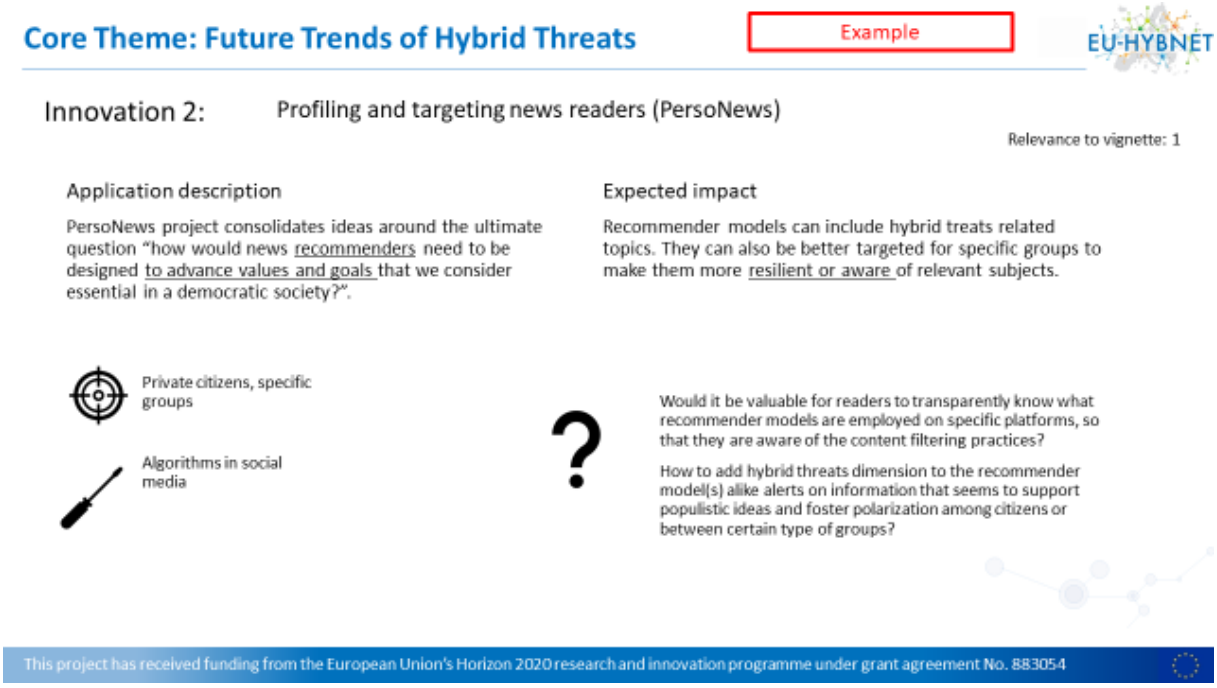
3.2. TRAINING SCENARIO AND INNOVATION ANALYSIS SET UP

Next to the scenarios and vignettes training participants and teams were shared a PowerPoint document that aims to support the situation analysis and especially to consider usability and

soundness of presented, pre-selected innovations (technological on non-technological) to each of the Core Themes. The PowerPoint template is presented below in two version: an empty version and a filled version after the training event and full scale analysis. The pictures are to highlight what is th goal of the training if arranged in any other organization.



An example of the Power Point that provides the starting point to the training to analyse the presented situation and suggested innovations as solutions.



An example of the Power Point that provides the end point to the training and highlights the usability and needs of a possible innovative solution to be used in the future.

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. In addition, and as mentioned earlier, three innovative solutions from EEAS, Maltego, HENSOLDT were also presented during the Training, and they were also included in training innovative solutions list for the training participants to concider.

Each training team based on the project's Four Core Themes started their discussion with selection of the Vignette that interests them most. 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. In each team participants were asked to prioritize innovations presented and select the most appropriate (one or two) for further discussions.

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 ANALYZE IN THE TRAINING

As mentioned above the pre-selected innovations were analysed in training teams formed according the project Four Core Themes. Therefore, the sub-chapters below presents the innovations that were suggested for training participants analysis according to each of the Four Core Themes.

4.1.1 INNOVATIONS TO VIGNETTES – CORE THEME: FUTURE TRENDS OF HYBRID THREATS

The training team under the named Core Theme focused on have discussion and to analyse following pre-selected innovations that are originating from EU-HYBNET T3.2/D3.4 "*First mid-term report on Improvement and innovations*" and T3.3/D3.8 "*First mid-term report on Innovation and Research monitoring*". The documents and full description of the innovations can be found in CORDIS: https://cordis.europa.eu/project/id/883054/results The presented innovations were following.

Vignette 2. While preparations for the elections in Bhic are ongoing, the minority in Duzec declares the desire to call a referendum for independence, whereas social media in Bhic strongly support this issue.

Proposed innovations to be evaluated in the training event are linked to the Gaps and Needs (G&N) identified by security practitioners in the challenging area:

- "Rise of populism"

Proposed innovations-solutions in the field:

No. 1.3 Rise of Populism		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Establishment and reinforcement of political education of democratic values**	How the education system should be changed to mitigate the influence of populism. **Practitioners in focus:** ministries responsible for internal security, government and security practitioners, local political institutions responsible for education.
3.8	**Innovation coming from EC funded project PersoNews ("Profiling and targeting news readers – implications for the democratic role of the digital media, user rights and public information policy")**, duration: 1/8/2015-31/5/2021, GA No.638514	EU-HYBNET training could focus PersoNews recommender models explained in a PersoNews' publication "On the Democratic Role of News Recommenders". The article consolidates ideas around the ultimate question "how would news recommenders need to be designed to advance values and goals that we consider essential in a democratic society?". In addtion, EU-HYBNET could have discussion how to add hybrid threats dimension to the recommender model(s) alike alerts on information that seems to support populisitc ideas and foster polarization among citizens or between certain type of groups. **Practitioners in focus**: Intelligence, Stratocom LEA, Military.

Vignette 5. The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full of migrant on Duzec shores.

Vignette 8. A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions.

Proposed innovations to be evaluated in the training event are linked to the Gaps and Needs (G&N) identified by security practitioners in the challenging area and can be considered in the scenario of both Vignettes:

- "Geopolitical heavyweight of domestic policy"

Proposed innovation in the field:

No. 1.1 Geopolitical heavyweight of domestic policy		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.8	**Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)** EC funded H2020 project, duration : 1/3/2018-30/4/2021.	The project developed innovative quantitative and qualitative empirical methods for risk-scanning, foresight and forecasting. This included large-scale *statistical prediction of conflict* as well as development of in-depth qualitative *risk scenarios*. EU-LISTCO identified six risk clusters: (1) geopolitical rivalry and risks of major armed conflict; (2) unconventional security risks; (3) biological and environmental risks; (4) demography and uncontrolled migration; (5) global financial and other systemic economic risks, and; (6) technology-driven disruption. In EU-HYBNET training in could be tested if statistical prediction of conflicts and risk scenarios may support coherent response to migration flow especially in hybrid threats context. **Practitioners in focus**: border and coast guards, civil protection and first responders, authorities and ministries respsonsible for internal and external security and foreign affairs.

Vignette 6. Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanizedinfantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia.

Proposed innovations to be evaluated in the training event are linked to the Gaps and Needs (G&N) identified by security practitioners in the challenging area:

- "Digital escalation and AI-based exploitation"

Proposed innovations in the field:

No. 1.2 Digital escalation and AI-based exploitation		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.8	Concordia, EC funded H2020 project.	Artifical Intelligence (AI) is a key technology in the security and defense sectors. Often AI is used to strengthen cyber defense capabilities as well as enhance attack proficiency. In EU-HYBNET training CONCORDIA's key results on adversarial AI attacks and countermeasures can be shortly presented. This is to follow discussion on overarching and detailed view of the role AI in hybrid threat counter measures in defence context

		(e.g use of AI in cyber attacks against air forces). The discussion is also to highlight which features of AI solutions needs to be exhibit to make them trusted and secure. **Practitioners in focus:** Cyber security experts, defence authorities.

4.1.2 INNOVATIONS TO VIGNETTES – CORE THEME: CYBER AND FUTURE TECHNOLOGIES

The training team under the named Core Theme focused on have discussion and to analyse following pre-selected innovations that are originating from EU-HYBNET T3.2/D3.4 "*First mid-term report on Improvement and innovations*" and T3.3/D3.8 "*First mid-term report on Innovation and Research monitoring*". The documents and full description of the innovations can be found in CORDIS: https://cordis.europa.eu/project/id/883054/results The presented innovations were following.

Vignette 3. Cyber-attacks on Balan, Berkhudia and Bhic cause major power outages. This causes serious problems on households as well as industrial control systems on a frequent basis, having severe financial impact on trade exports.

Proposed innovations to be evaluated in the training event are linked to the gaps and needs (G&N) identified by security practitioners in the areas:

- "Offensive cyber capabilities"
- "Disruptive innovation"

Proposed innovations in the field:

No. 2.2 Offensive Cyber Capabilities		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**The Development of a Proactive Defensive Framework based on ML and cloud**	Offensive cyber capabilities run the gamut from sophisticated, long-term disruptions of physical infrastructure to malware used to target human rights journalists. As these capabilities continue to proliferate with increasing complexity and to new types of actors, the imperative to slow and counter their spread only strengthens. Innovation is critical to improving society and is key to the cyber domain. The rapid growth of the internet has meant that tools for operating in cyberspace have constantly evolved. Faced with a constant stream of threats from cybercriminals, hackers, and other malicious actors, it is almost impossible for anyone to keep up with any form of automation or artificial intelligence, so self-learning cyber-defence products that use artificial intelligence to detect and even respond to emerging attacks are required. This type of solution is technical.

		Partitionners in focus: Cyber security authorities, intelligence, LEAs.
3.4	**A fully automated incident response solution based on CT Intelligence**	This Automated Incident Response Solution maximizes an enterprise's ability to investigate all cyber-alerts, uncover hidden threats and remediate the full extent of a breach to increase the organization's productivity, reduce ongoing costs, and strengthen the organization's overall security. This type of solution is technical. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Strategic Cultures of Cyber Warfare** (CYBERCULT), which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01/07/2019 to 19/09/2021.	This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and cultural factors which motivates development of offensive cyber capabilities, and framework for achieving less destructive global cyberenvironment. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Proposed innovations in the field:

No. 2.3 Disruptive Innovations		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**The Development of a Deep fake Detection System**	Photo and video manipulation is crucial to the spreading of typically quite convincing disinformation on social media and cyberspace generally. Computer-generated photos of people's faces, conversely, have already become common hallmarks of subtle foreign interference campaigns, aiming to build faux accounts. In this respect deepfakes seem to be more authentic. One issue is of course very important, to find a lot of ways to identify media that has been manipulated or modified within the fight against on-line disinformation. The repercussions of such deepfakes are dangerous with compromised videos of public figures in circulation that threaten their name. Worse, it's anticipated that deepfakes might even play an outsized role in swaying elections of nations. Notably, Facebook, Twitter, and TikTok have already prohibited such deepfake content on their platform. This type of solution is technical. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

3.8	**INtelligent Security and Pervasive tRust for 5G and Beyond (INSPIRE-5Gplus)**	**INSPIRE-5Gplus** explores ways to improve control of systems and eliminate vulnerabilities for the infrastructure owners and tenants, employing machine learning, AI, and blockchain technologies. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Isogeny-based Toolbox for Post-quantum Cryptography (ISOCRYPT)**	**ISOCRYPT** is one of the projects exploring cryptography which would be usable in today's technological context, as well as remain secure when quantum computing capabilities are deployed. Project is exploiting mathematical maps called isogenies in new algorithms for security in a pioneering cryptographic paradigm. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Vignette 4. Telecoms in Berkhudia are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Space interference and counterspace weapons"

Proposed innovations in the field:

No. 2.1 Space interference and counterspace weapons		
Deliverable	**name of the innovation**	Short description on the soundness to be tested
3.4	**7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases**	The 7Shield framework is being developed to be able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely the pre-crisis, crisis and post-crises phases. The integrated framework is flexible and adaptable enabling the deployment of innovative services for cyber-physical protection of ground segments. The framework will integrate advanced technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection. *Pre-crisis* phase: An early warning mechanism is being used to estimate the level of risk before the occurrence of the attack. *Crisis* phase: During the attack, detection and response is effective and efficient, considering also budgetary constraints. A mitigation plan is

		designed and automatically updated to offer a quick recovery after an intentional attack or a system failure. Business continuity scenarios are also supporting the security and resilience of private installations. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Protection and Resilience Of Ground-based infRastructures for European Space Systems** (**PROGRESS**). This project was funded under FP7-Security in the period from 01/05/2014 to 31/10/2017.	PROGRESS focused on detecting and mitigating intrusions to GNSS from highly educated attackers whose numbers may increase soon. The goal of the project is to enable expanded intelligence in GNSS architectures to ensure the uninterrupted performance of services. The potential impact of attacks is to be reduced through protective solutions; attacks are to be detected and analyzed for impact, and where necessary, affected elements of the GNSS are to be reconfigured. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases.** This project was funded under H2020 in the period from 2020 to 2022.	The project focuses to enhance security concerns of ground segments that appear to be potential new targets for complex physical/cyber threats as they receive massive amounts of satellite data. In more detail, the ability to disrupt, inspect, modify or re-route traffic provides an opportunity to conduct cyber/physical attack. Such an attack could have a dramatic impact on the security of European citizens and can initiate cascading effects to other Critical Infrastructures. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Vignette 5. The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full with migrant on Duzec shores.

Vignette 6. Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanized infantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Offensive cyber capabilities"

Introduced innovations will be evaluated in both scenarios of Vignettes 5&6.

Proposed innovations in the field:

No. 2.2 Offensive Cyber Capabilities		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**

3.4	**A fully automated incident response solution based on CT Intelligence**	A fully automated incident response solution based on Cyber Threat Intelligence feed, that enables organizations to investigate every cyber-alert they receive and close out incidents in minutes, even seconds. This Automated Incident Response Solution maximizes an enterprise's ability to investigate all cyber-alerts, uncover hidden threats and remediate the full extent of a breach to increase the organization's productivity, reduce ongoing costs, and strengthen the organization's overall security. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.4	**The Development of a Proactive Defensive Framework based on ML and cloud**	Innovation is critical to improving society and is key to the cyber domain. The rapid growth of the internet has meant that tools for operating in cyberspace have constantly evolved. It has often been said, however, that the only innovation taking place in cyber warfare is in offensive operations. So where is the innovation for the defence? The development of a defensive framework for proactive situational awareness using Machine Learning technology and Cloud Computing, to better understand one's network and system can be a way to quickly identify and defend against cyberattacks and emerged types of offensive cyber capabilities. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Strategic Cultures of Cyber Warfare** (**CYBERCULT**), which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01/07/2019 to 19/09/2021.	This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and cultural factors which motivates development of offensive cyber capabilities, and framework for achieving less destructive global cyberenvironment. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

Vignette 8. A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Offensive cyber capabilities"

Proposed innovations in the field:

No. 2.2 Offensive Cyber Capabilities		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**A fully automated incident response solution based on CT Intelligence**	A fully automated incident response solution based on Cyber Threat Intelligence feed, that enables organizations to investigate every cyber-alert they receive and close out incidents in minutes, even seconds. This Automated Incident Response Solution maximizes an enterprise's ability to investigate all cyber-alerts, uncover hidden threats and remediate the full extent of a breach to increase the organization's productivity, reduce ongoing costs, and strengthen the organization's overall security. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.4	**The Development of a Proactive Defensive Framework based on ML and cloud**	Innovation is critical to improving society and is key to the cyber domain. The rapid growth of the internet has meant that tools for operating in cyberspace have constantly evolved. It has often been said, however, that the only innovation taking place in cyber warfare is in offensive operations. The development of a defensive framework for proactive situational awareness using Machine Learning technology and Cloud Computing, to better understand one's network and system can be a way to quickly identify and defend against cyberattacks and emerged types of offensive cyber capabilities. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**Strategic Cultures of Cyber Warfare** (CYBERCULT), which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01/07/2019 to 19/09/2021.	This project studied the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. It also reviewed the cultural, socio-political, historical, and ideological factors involved. CYBERCULT did not aim to create any technologies, but rather to deepen our understanding on strategic thinking and cultural factors which motivates development of offensive cyber capabilities, and framework

		for achieving less destructive global cyberenvironment. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.

4.1.3 INNOVATIONS TO VIGNETTES – CORE THEME: INFORMATION AND STRATEGIC COMMUNICATION

The training team under the named Core Theme focused on have discussion and to analyse following pre-selected innovations that are originating from EU-HYBNET T3.2/D3.4 "*First mid-term report on Improvement and innovations*" and T3.3/D3.8 "*First mid-term report on Innovation and Research monitoring*". The documents and full description of the innovations can be found in CORDIS: https://cordis.europa.eu/project/id/883054/results The presented innovations were following.

Vignette 2. While preparations for the elections in Bhic are ongoing, the minority in Duzec declares the desire to call a referendum for independence, whereas social media in Bhic strongly support this issue.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the areas:

- "Information manipulation with the aim of destabilization"
- "Foreign interference in key information institutions"

Proposed innovations in the field:

No. 4.1 Information manipulation with the aim of destabilization		
Deliverable	**Name of the innovation**	**Short description on the soundness to be tested**
3.4	**Increasing capabilities to systematically assess information validity throughout the lifecycle**	The parties who call a referendum for independence might use statements, which are not based official truth. Today the social media is perhaps the most powerful tool for sharing information and influences public opinion. This innovation focus on finding and tackle disinformation and manipulated information. **Practitioners in focus:** Intelligence, authorities responsible for internal security.
3.4	**DDS-alpha (EEAS)**	DDS alpha capabilities to collect evidences for Sandmouthian Federation campaign to support Duez call a referendum for independence. DDS-alpha is the Disinformation Data Space, a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan.

		Practitioners in focus: Intelligence, authorities responsible for internal security.
3.8	**Information and Misinformation Economics: Design, Manipulations and Coutermeasures** (IMEDMC) EC funded project. Duration: 1/5/2021 – 30/4/2026. GA No. 101001694.	IMEDMC will analyze the unexplored designer-agent-receiver class of games considering fake news production – state falsification, pure agency and state shifting, taking a systems approach. For simulations, IMEDMC will employ underutilized designer-agent-receiver class of games, in which the designer picks an information generation system, the agent takes an upstream decision affecting the states of the world, or manipulates the production of information, and receivers choose downstream actions based on realized signals. For EU-HYBNET training the IMEDMC approach, methods and games may render specific interest. It may be appropriate to observe successes and drawbacks of IMEDMC approaches and methods applied ,and to discuss their applicability to model and analysis of hybrid threats. In EU-HYBNET training the special focus would be means to influence general opinion via fake news. **Practitioners in focus:** Intelligence, authorities responsible for internal security.

Proposed innovations in the field:

No. 4.2 Foreign interference in key information institutions		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Integrated Monitoring System Against Cyber-enabled Information Operations**	The tool could be tested for detecting Deepfake operations and/or to find out cloned websites in order to influence common opinion. (Sandmouthian or Duez) **Practitioners in focus**: Intelligence, authorities responsible for internal security; LEAs.
3.4	**Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications**	Although this tool is under Information manipulation with the aim of destabilization, perhaps it could be tested how it could find and tackle the encrypted information shared by the Deuz for supporting their goal for call a referendum for independence. **Practitioners in focus**: Intelligence, authorities responsible for internal security; LEAs.
3.8	**The Consequences of the Internet for Russia's Informational Influence Abroad** (RUSINFORM) project - a closer look at Russia's digital disinformation. Funded by EC, H2020. Duration: 1/11/2019 – 31/10/2024.	RUSINFORM does not deliver any technical solution but introduces datamining techniques and automated text analysis in combination with traditional methods (surveys, in-depth interviews, grounded theory). The innovative combination of these techniques is to deepen understanding of the phenomena and build a better methodological basis for further analysis efforts. RUSINFORM results area

		important in advancing our knowledge of the mechanisms of foreign influence. In EU-HYBNET training RUSINFORM solution, namely combination of tools and techniques, and this approaches usability and benefits to security authorities analysis on malicious actors information interference and influence to SOME could be addressed. **Practitioners in focus**: Intelligence, authorities responsible for internal security; LEAs.

Vignette 7. A Fake news campaign on Bhic official media, that the electoral process is staged and premeditated is observed. Sandmouthian probes and outlets as for journalists and "independent" analysts are amplifying this narrative, provoking distrust sentiments to the citizens.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the areas:

- "Information manipulation with the aim of destabilization"
- "Foreign interference in key information institutions"
- "Promoted ideological extremism and violence"

Proposed innovations in the field:

No. 4.1 Information manipulation with the aim of destabilization		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4.	**DDS-alpha (EEAS)**	DDS alpha capabilities to collect evidences for Sandmouthian Federation campaign to interference and to reduce legality and legitimacy of the Bhic election **Practitioners in focus**: Intelligence.
3.8	Open Your Eyes: Fake News for Dummies Project. Funded by EC, Erasmus+ instrument.	The project is dedicated to improve the digital literacy of adult learners by providing them with tools to identify fake news and fight the spread of disinformation online. It is important to continue and extend of such project beyond "supply side" verification – how we recognize fakes, to understand more "demand side" of fakes. In EU-HYBNET training « Open Your Eyes » project's tools could be analysed in order to test their soundness to recognize hybrid threats fake news campaigns. **Practitioners in focus**: Intelligence.

Proposed innovations in the field:

No. 4.2 Foreign interference in key information institutions

Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**Integrated Monitoring System Against Cyber-enabled Information Operations**	In this case the tool could be used for finding and expressing the Sandmouthian deepfake operations for supporting the Duez ambitions. **Practitioners in focus:** Intelligence, LEAs.
3.8	**Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe (COMPROP).** Funded by EC, H2020. Duration 1/2016 – 12/2020.	COMPRPO researched specific aspects of "computational propaganda" involves the use of algorithms, automation, and big data analytics to purposefully disseminate manipulative and misleading messages over these social media networks. The project seeks to answer e.g. to a research questions: How are algorithms and automation used to manipulate public opinion during elections or political crises? What are the technological, social, and psychological mechanisms by which we can encourage political expression but discourage opinion herding or the unnatural spread of extremist, sensationalist, or conspiratorial news? What new scholarly research systems can deliver real time social science about political interference, algorithmic bias, or external threats to democracy? In EU-HYBNET training COMPROP's approach on needed solutions (e.g. big data analytics to LEAs) to real time reaction and analysis on information manipulation in SOME could be under discussion. **Practitioners in focus:** Intelligence, LEAs.

Proposed innovations in the field:

No. 4.3 Promoted ideological extremism and violence		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Collection and sentiment analysis of targeted communication**	The idea behind this is to find out whether this tool could help to identify impact of propaganda and disinformation against individual government ministers or ministers "Could the Duez propaganda against e.g. Bhich primeminister effect the elections and contribute to Duez goals" **Practitioners in focus:** Intelligence, LEAs.
3.8	**Artificial Intelligence Roadmap for Policing and Law Enforcement** (ALIGNER) EC funded projcet.	ALIGNER, is dedicated to broader set of technologies for law enforcement and policing. It aims to jointly identify and

	Duration: 1/10/2021 – 30/09/2024. GA No. 101020574.	discuss how to enhance Europe's security by employing AI and advanced technologies, it will pave the way for an AI research roadmap. Special focus is on Law Enforcement Authorities (LEAs). In EU-HYBNET training ALIGNER's identified needs of LEA's for most wanted AI technologies and solutions could be under discussion, especially focusing to the context of identifying information manipulation and interference by foreign actors. **Practitioners in focus:** Intelligence, LEAs.

Vignette 8. A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Information manipulation with the aim of destabilization"

Proposed innovations in the field:

No. 4.1 Information manipulation with the aim of destabilization		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging**	The tool could be tested how it could find and tackle the encrypted information shared by Sandmouthian and Duzec. **Practitioners in focus:** Intelligence, LEAs.
3.4	**DDS-alpha (EEAS)**	The tool could be used to prove as well as find out a disinformation aimed at influencing the decision of people to leave their homes and leave as a refugee to another country. **Practitioners in focus:** Intelligence, LEAs.

4.1.4 INNOVATIONS TO VIGNETTES – CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL AND NATIONAL ADMINISTRATION

The training team under the named Core Theme focused on have discussion and to analyse following pre-selected innovations that are originating from EU-HYBNET T3.2/D3.4 "*First mid-term report on Improvement and innovations*" and T3.3/D3.8 "*First mid-term report on Innovation and Research*

monitoring". The documents and full description of the innovations can be found in CORDIS: https://cordis.europa.eu/project/id/883054/results The presented innovations were following.

Vignette 1. *Gas Flow to Bhic from Sharn is paused after a gas pipeline explosion. Initial findings (IED) support the assumption that probably it is about a sabotage and not an accident. Speculation that the Federation is behind the incident is strong.*

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the areas:

- "Exploitation of critical infrastructure weaknesses and economic dependencies"
- "Exploitation or investment in companies by foreign actors"

Proposed innovations in the field:

No. 3.2 Exploitation of critical infrastructure weaknesses and economic dependencies		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Impact and Risk assessment of critical infrastructures in a complex interdependent scenario**	This idea discusses a decision support approach for CI risk assessment with a holistic consideration of complexity, dual interdependency, vulnerability, and uncertainty. It is based on a paper by Weilan et al, 2019[1] and on the Critical Infrastructure Resilience Platform (CIRP)[2] developed by Satways Ltd.The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment. The essential elements for impact assessment are hazards, assets and the assets' fragility. Hazard is considered as the descriptive parameter quantifying the possible phenomenon within a region of interest. The assets in a region exposed to hazards are defined by an inventory. Finally, fragility is the sensitivity of certain assets of an inventory when subjected to a given hazard. **Practitioners in focus:** Crisis Management experts in municipalities, ministries and critical infrastructures. What-if scenarios can be used for impact and risk assessment that will be used by the practitioners for preparedness, that is identifying measures to reduce the impact of the existing interdependencies. The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment that creates new capabilities for CI policy-makers, decision makers, and scientists by allowing them to use different and diverse modelling and risk assessment solutions, to develop risk reduction strategies and implement mitigation actions that help minimise the impact of climate change on CIs. The Ministry of Civil Protection could be informed for interdependencies and

[1] Weilan Suoa, Jin Zhangb, Xiaolei Suna, Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach, Safety Science, 120, 692-705 (2019).
[2] Kostaridis, A., et al, CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures, 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment

		their impact for strategic planning in cases of hybrid attack.
3.4	**ResilienceTool (incl. RiskRadar) Steinbeis EU-VRi (European Risk & Resilience Institute)**	The ResilienceTool is a web application for performing indicator-based resilience and functionality assessment for critical entities using a tested methodology based on composite indicators organized as a multi-level hierarchical checklist, known as dynamic checklists (DCLs). The key concept of the methodology involves the "resilience" of an infrastructure which describes its ability to cope with potential adverse scenarios or events that can lead to significant disruptions in its operation or functionality. The solution offered by the ResilienceTool is big data-oriented, customizable and dynamic in nature that can enable monitoring of operations and provide situational awareness, and adaptable to various threat-vulnerability combinations and anchored in national and international standards (ISO 31050, DIN SPEC 91461). The RiskRadar tool allows continuous and automated horizon scanning of "emerging risks" related to certain threats including hybrid threats that can potentially result in an "actual" risk in the medium to long term. The tool uses a natural language processing (NLP) algorithm to identify, locate and assess emerging risks by considering risks posed by threats based on factors including Environmental, Socio-political, Economic/Financial, Regulatory/Legal and Technological. It can extract textual data from a wide range of openly accessible documents from sources such as News media, Social media, Scientific publications, and Regulatory and Government agencies. It has been effectively used for the identification and location of different types of perceived and real emerging risks/threats. The RiskRadar tool can be used to identify and prioritize emerging risks related to a wide range of threats including hybrid threats assessed according to their criticality **Practitioners in focus:** From Infrastructure owners, First responders within Tactical (low level), to disaster management agencies, policymakers and governmental bodies at strategic (high level). For industry (to monitor resilience, understand and prepare for threat scenarios and identify gaps within current systems, plan and implement investment options to improve resilience), for policymakers (to have situational awareness, data-driven insights and take relevant and impactful policy decisions). It can identify gaps within current systems and help with plans to improve resilience
3.8	**The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading**	The project "aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures." PRECINCT will develop an ecosystem platform for

	Cyberphysical Threats and effects with a focus on district or regional protection (PRECINCT) duration: 06/10/2021-30/10/2023, GA No. 101021668	improving the security and resilience of interdependent critical infrastructures, specifically combining physical and cyber areas for wider situational awareness. It will develop tools and models for collaborative response action to identified threats. It will also develop a vulnerability assessment tool, based on serious games. It will aim to identify vulnerabilities to cascading effects and to assess measures for enhancing resilience. From EU-HYBNET's point of view, PRECINCT's approach is noteworthy because of its ambition to integrate private and public stakeholders under the same CI security framework. PRECINCT will bring together prior results from three EU-funded projects and capitalize on legacy structures. **Practitioners in focus:** Critical Infrastructure operators and those responsible for CI protection need to acquire technologies and skills to identify such complex attacks so that they may respond timely and adequately.

Proposed innovations in the field:

No. 3.3 Exploitation or investment in companies by foreign actors		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**A crawler for correlation of screened FDI with suspicious financial activity**	The main goal of this idea is to have strict procedures for the investigation of screened FDI, and at the same time exchange information with practitioners active in preventing criminal activity. The rational for this approach is based on the fact that such hybrid attacks would require some logistical infrastructure (such as illegal residencies) as well as anonymous bank accounts to fund relevant actions. Therefore, the ability to link screened FDI with various types of suspicious financial activity would provide evidence for rejecting such investments. The cooperation of the FDI screening practitioners with the practitioners active in preventing criminal activity could be enabled by a crawler that would automatically search for investors' information relative to suspicious financial activity and detect hidden connections with other investors, but also with entities that are engaged in illegal or criminal activities. Google and Bing search engines use web crawlers. **Practitioners in focus:** Ministry that is responsible for screening FDI, Police, Organised Crime Units. The Idea supports the Member States in applying Regulation (EU) 2019/452 of the European Parliament and of The Council. Therefore, it supports the protection of the Union from foreign actors trying to influence or take control of European firms.

Vignette 3. Cyber-attacks on Balan, Berkhudia and Bhic cause major power outages.This causes serious problems on households as well as industrial control systems on a frequent basis, having severe financial impact on trade exports.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Exploitation of critical infrastructure weaknesses and economic dependencies"

Proposed innovations in the field:

No. 3.2 Exploitation of critical infrastructure weaknesses and economic dependencies		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Impact and Risk assessment of critical infrastructures in a complex interdependent scenario**	This idea discusses a decision support approach for CI risk assessment with a holistic consideration of complexity, dual interdependency, vulnerability, and uncertainty. It is based on a paper by Weilan et al, 2019 [3] and on the Critical Infrastructure Resilience Platform (CIRP)[4] developed by Satways Ltd.The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment. The essential elements for impact assessment are hazards, assets and the assets' fragility. Hazard is considered as the descriptive parameter quantifying the possible phenomenon within a region of interest. The assets in a region exposed to hazards are defined by an inventory. Finally, fragility is the sensitivity of certain assets of an inventory when subjected to a given hazard. CIRP) creates new capabilities for CI policy-makers, decision makers, and scientists by allowing them to use different and diverse modelling and risk assessment solutions, to develop risk reduction strategies and implement mitigation actions that help minimise the impact of climate change on CIs. The Ministry of Civil Protection could be informed for interdependencies and their impact for strategic planning in cases of hybrid attack. **Practitioners in focus:** Crisis Management experts in municipalities, ministries and critical infrastructures.
3.4	**ResilienceTool (incl. RiskRadar) Steinbeis EU-VRi (European Risk & Resilience Institute)**	The ResilienceTool is a web application for performing indicator-based resilience and functionality assessment for critical entities using a tested methodology based on composite indicators organized as a multi-level hierarchical checklist, known as dynamic checklists (DCLs). The key concept of the

[3] Weilan Suoa, Jin Zhangb, Xiaolei Suna, Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach, Safety Science, 120, 692-705 (2019).
[4] Kostaridis, A., et al, CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures, 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment

		methodology involves the "resilience" of an infrastructure which describes its ability to cope with potential adverse scenarios or events that can lead to significant disruptions in its operation or functionality. The solution offered by the ResilienceTool is big data-oriented, customizable and dynamic in nature that can enable monitoring of operations and provide situational awareness, and adaptable to various threat-vulnerability combinations and anchored in national and international standards (ISO 31050, DIN SPEC 91461). The RiskRadar tool allows continuous and automated horizon scanning of "emerging risks" related to certain threats including hybrid threats that can potentially result in an "actual" risk in the medium to long term. The tool uses a natural language processing (NLP) algorithm to identify, locate and assess emerging risks by considering risks posed by threats based on factors including Environmental, Socio-political, Economic/Financial, Regulatory/Legal and Technological. It can extract textual data from a wide range of openly accessible documents from sources such as News media, Social media, Scientific publications, and Regulatory and Government agencies. It has been effectively used for the identification and location of different types of perceived and real emerging risks/threats. The RiskRadar tool can be used to identify and prioritize emerging risks related to a wide range of threats including hybrid threats assessed according to their criticality **Practitioners in focus:** From Infrastructure owners, First responders within Tactical (low level), to disaster management agencies, policymakers and governmental bodies at strategic (high level). For industry (to monitor resilience, understand and prepare for threat scenarios and identify gaps within current systems, plan and implement investment options to improve resilience), for policymakers (to have situational awareness, data-driven insights and take relevant and impactful policy decisions). It can identify gaps within current systems and help with plans to improve resilience
3.8	**The Preparedness and Resilience Enforcement for Critical INfrastructure Cascading Cyberphysical Threats and effects with a focus on district or regional protection (PRECINCT)** duration:	The project "aims to connect private and public CI stakeholders in a geographical area to a common cyber-physical security management approach which will yield a protected territory for citizens and infrastructures." PRECINCT will develop an ecosystem platform for improving the security and resilience of interdependent critical infrastructures, specifically combining physical and cyber areas for wider situational awareness. It will develop tools and models

	06/10/2021-30/10/2023, GA No. 101021668	for collaborative response action to identified threats. It will also develop a vulnerability assessment tool, based on serious games. It will aim to identify vulnerabilities to cascading effects and to assess measures for enhancing resilience. From EU-HYBNET's point of view, PRECINCT's approach is noteworthy because of its ambition to integrate private and public stakeholders under the same CI security framework. PRECINCT will bring together prior results from three EU-funded projects and capitalize on legacy structures. **Practitioners in focus:** Critical Infrastructure operators and those responsible for CI protection need to acquire technologies and skills to identify such complex attacks so that they may respond timely and adequately.

Vignette 5. The Sandmouthian Federation is facilitating irregular migrant flows to Duzec in Bhic, by allowing if not escorting with its coast guard forces, boats full with migrant on Duzec shores.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Exploitation of existing political cleavages"

Proposed innovations in the field:

No. 3.1 Exploitation of existing political cleavages		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**Development of Real-time Rapid Alert System on Disinformation**	The Rapid Alert System on Disinformation should link the national SITCEN-s with EU INTCEN via 24/7 operational information exchange platform in cause of time-criticality, especially in times of large-scale crises as pandemics, irregular immigration flows, etc. The platform should also be securely integrated with EU vs Disinfo database to enable hit-based and advanced searches for identifications of (original) sources and spread (possible impact) projections of disinformation. The main outcome of the innovation proposal could be better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups. **Practitioners in focus:** Member States' governments, municipalities, civil society.

3.4	**Detection of Disinformation Delivery Proxy Actors**	The EU vs Disinfo analytical capabilities should be further advanced and inter-connected with relevant media monitoring assets to detect and identify harmful disinformation delivery by proxy actors whose connections with their hostile 'employers' may be obscured or denied but could be better identified by integrating the most capable Media Monitoring Software assets with EU vs Disinfo database. The main outcome of the innovation proposal could be better situational awareness, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels. **Practitioners in focus:** NGO's, governmental institutions, private bodies, media outlets, academia. Different NGO's, governmental institutions, private bodies, media outlets and academia could use such integrated database to examine the background of particular (proxy) actor and its possible engagement of (previous) disinformation activities as an optional 'trust-measure' before accepting and delivering its messages, expertise, etc. information and publicity (re-)production.
3.8	**In the Wider and Enhanced Verification for You (WeVerify)** duration: 01/12/2018 – 30/11/2021, GA No. 825297	The aim of the project was to address the advanced content verification challenges through a participatory verification approach, open-source algorithms, low-overhead human-in-the-loop machine learning and intuitive visualizations. The project has developed the InVID-WeVerify browser plug-in that will help its user to verify online information. Furthermore, the WeVerify project assembled a companion to help citizens and fact-checking professionals to take advantage of the features of the plug-in. The companion also includes links for citizens to find online advice concerning disinformation threats. **Practitioners in focus:** NGO's, governmental institutions, private bodies, human rights activists, media outlets.

Vignette 6. Sandmouthian Federation land forces supported by air bombing attack Mugia. Mechanizedinfantry units invade. Civilian refugees are fleeing to Bhic and from there to Berkhudia.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area

- "Exploitation of existing political cleavages"

Proposed innovations in the field:

No. 3.1 Exploitation of existing political cleavages		
Deliverable	name of the innovation	Short description on the soundness to be tested

3.4	**Development of Real-time Rapid Alert System on Disinformation**	The Rapid Alert System on Disinformation should link the national SITCEN-s with EU INTCEN via 24/7 operational information exchange platform in cause of time-criticality, especially in times of large-scale crises as pandemics, irregular immigration flows, etc. The platform should also be securely integrated with EU vs Disinfo database to enable hit-based and advanced searches for identifications of (original) sources and spread (possible impact) projections of disinformation. The main outcome of the innovation proposal could be better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups. **Practitioners in focus:** Member States' governments, municipalities, civil society.
3.4	**Detection of Disinformation Delivery Proxy Actors**	The EU vs Disinfo analytical capabilities should be further advanced and inter-connected with relevant media monitoring assets to detect and identify harmful disinformation delivery by proxy actors whose connections with their hostile 'employers' may be obscured or denied but could be better identified by integrating the most capable Media Monitoring Software assets with EU vs Disinfo database. The main outcome of the innovation proposal could be better situational awareness, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels. **Practitioners in focus:** NGO's, governmental institutions, private bodies, media outlets, academia. Different NGO's, governmental institutions, private bodies, media outlets and academia could use such integrated database to examine the background of particular (proxy) actor and its possible engagement of (previous) disinformation activities as an optional 'trust-measure' before accepting and delivering its messages, expertise, etc. information and publicity (re-)production.
3.8	**In the Wider and Enhanced Verification for You (WeVerify)** duration: 01/12/2018 – 30/11/2021, GA No. 825297	The aim of the project was to address the advanced content verification challenges through a participatory verification approach, open-source algorithms, low-overhead human-in-the-loop machine learning and intuitive visualizations. The project has developed the InVID-WeVerify browser plug-in that will help its user to verify online information. Furthermore, the WeVerify project assembled a companion to help

		citizens and fact-checking professionals to take advantage of the features of the plug-in. The companion also includes links for citizens to find online advice concerning disinformation threats. **Practitioners in focus:** NGO's, governmental institutions, private bodies, human rights activists, media outlets.

Vignette 7. A Fake news campaign on Bhic official media, that the electoral process is staged and premeditated is observed. Sandmouthian probes and outlets as for journalists and "independent" analysts are amplifying this narrative, provoking distrust sentiments to the citizens.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Exploitation or investment in companies by foreign actors"

Proposed innovations in the field:

No. 3.3 Exploitation or investment in companies by foreign actors		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**A crawler for correlation of screened FDI with suspicious financial activity**	The main goal of this idea is to have strict procedures for the investigation of screened FDI, and at the same time exchange information with practitioners active in preventing criminal activity. The rational for this approach is based on the fact that such hybrid attacks would require some logistical infrastructure (such as illegal residencies) as well as anonymous bank accounts to fund relevant actions. Therefore, the ability to link screened FDI with various types of suspicious financial activity would provide evidence for rejecting such investments. The cooperation of the FDI screening practitioners with the practitioners active in preventing criminal activity could be enabled by a crawler that would automatically search for investors' information relative to suspicious financial activity and detect hidden connections with other investors, but also with entities that are engaged in illegal or criminal activities. Google and Bing search engines use web crawlers. **Practitioners in focus:** Ministry that is responsible for screening FDI, Police, Organised Crime Units. The Idea supports the Member States in applying Regulation (EU) 2019/452 of the European Parliament and of The Council. Therefore, it supports the protection of the Union from foreign actors trying to influence or take control of European firms.

Vignette 8. A new migrant area Zagrog in Balan is created mainly by people from the adjacent Duzec prefecture, where Sandmouthian cells are forcing people to move to Zagrog in order to find better living conditions.

Proposed innovations to be evaluated in the training event are linked to the (G&N) identified by security practitioners in the area:

- "Exploitation or investment in companies by foreign actors"

Proposed innovations in the field:

No. 3.3 Exploitation or investment in companies by foreign actors		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**A crawler for correlation of screened FDI with suspicious financial activity**	The main goal of this idea is to have strict procedures for the investigation of screened FDI, and at the same time exchange information with practitioners active in preventing criminal activity. The rational for this approach is based on the fact that such hybrid attacks would require some logistical infrastructure (such as illegal residencies) as well as anonymous bank accounts to fund relevant actions. Therefore, the ability to link screened FDI with various types of suspicious financial activity would provide evidence for rejecting such investments. The cooperation of the FDI screening practitioners with the practitioners active in preventing criminal activity could be enabled by a crawler that would automatically search for investors' information relative to suspicious financial activity and detect hidden connections with other investors, but also with entities that are engaged in illegal or criminal activities. Google and Bing search engines use web crawlers. **Practitioners in focus:** Ministry that is responsible for screening FDI, Police, Organised Crime Units. The Idea supports the Member States in applying Regulation (EU) 2019/452 of the European Parliament and of The Council. Therefore, it supports the protection of the Union from foreign actors trying to influence or take control of European firms.

4.1.5 INNOVATIONS TO VIGNETTES – THREE ADDITIONAL PRESENTATIONS

The three additional innovation presentations given during the training event were following.

EEAS, Strategic Communication Division/ DDS-Alpha tool for disinformation analysis and sharing

Focus in the presentation:

- Foreign Information Manipulation and Interference (FIMI) solution for information analysis. The presentation key elements highlighted the work done for the public report on EEAS work on FIMI – the report is published on February 2023, please see: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

HENSOLDT/ Open-source intelligence platform

Focus in the presentation:

- Open-source intelligence (OSINT) solution. More on Hensoldt's solution, please see: Home - HENSOLDT Analytics (hensoldt-analytics.com)
- Presentation described the OSINT search methods and capabilities including Hensold's own solution

Maltego/ Information analysis platform

Focus in the presentation:

- Solution of multi-source integration for information analysis, more on Maltego's solution, please see: https://www.maltego.com/

4.2 INNOVATION ANALYSIS GENERAL REMARKS

According to the discussions in the training teams following remarks of the innovations were done. In short, innovations that received highest priority ranking during the event were:

- Open source intelligence (OSINT) related tools (example: HENSOLD).
- Support of critical infrastructure in securing their services provision in case of direct attacks or supply chain breakdowns (example: Digital Twins, 7 Shield).
- Information about hybrid treats and relevant operations exchange and structurisation providing faster and more focused response (example: DDS-Alpha).
- Innovations, that provide possibilities for collective response to hybrid treats. Focusing on involvement at different levels, from crowd sourcing to international collective actions.
- Means for verification in different processes, starting from fact checking, debunking and going to decision making protection, ensuring ML credibility.

Innovations providing such capabilities are suggested to be considered for further analysis, uptake, and standardisation efforts.

All of the above have been captured into solutions assessments by Core Theme leaders who were the moderators of the sessions. The outcomes of the whole training event and the innovations' validation and assessment are elaborated further in this document chapters 5.-7.

5.TRAINING LESSONS LEARNED FOR FUTURE EVENTS

If to compare methodology used during the 1st and the 2nd EU-HYBNET project working cycles, there were some adjustments done in the training arrangements. Following the experience from the 1st cycle, changes were made to simplify the description of circumstances (Scenario, Vignettes, etc.). Main changes applied:

- Scenario was made simple and understandable. It also was tailored to realistic situation, where participants can associate events described with real situations across EU that have happened recently.
- Original DTAG methodology describes situation in three steps: Scenario, Vignette and Inject. In the 2nd cycle only Scenario and Vignettes were used to avoid the overload of information framing the situation.
- Preselected innovations were attached to Vignettes and those linked to Core Themes.
- As it was mentioned, some innovative solutions, that were not included in the primary deliverables, were presented life. The key aspects are that we lacked this is the 1st cycle, presenting live provides much better understanding of the innovation and it's functionalities.
- The Event was made in the hybrid format (on-line and on-site), making it more interactive and more technically challenging.

Furthermore according to the feedback given by the training participants, the training event evaluation results revealed that some organizational improvements still must be considered planning the 3rd EU-HYBNET project working cycle. On the whole, relevance of current recommendations should be reconsidered as different methodological approach can be used during the 3rd project working cycle. Main recommendations from the 2nd training event for future training event organizers include:

- Most of suggestions for improvement were related to Scenario. Balancing of the scenario presenting the complexity and making it simple to understand, interpret and apply should be considered for the up-coming cycle.
- Participants were lacking explicit descriptions of the innovations in order effectively understand the innovation's potential and its future uptake possibilities. This was improved by having three innovations (from EEAS, Maltego, HENSOLDT) presented live and having methodology of innovations in use presentation. But this still leaves too much space for very high level discussions.
- It is worth to consider that innovation providers are invited to introduce their solutions in more details or even providing the possibility to have hands-on training.
- It is recommended to the EU-HYBNET network to include more practitioners into future discussions and to make sure that a focus on creating added value to them is maintained

Finally, according to the training participants training assessment and structured feedback incl. relevant improvement points and additional expectations they would see relevant and important, following highly valuable insights were shared. These key points are:

- Simplified pre-reading materials were evaluated positively. Significant time was also spent during the training to present the general scenario. Such modification reflects the findings from the 1st cycle.
- Most of suggestions for improvement were related to Scenario. Simplification made easier to understand and apply it during the event. But, on the other hand, in most Vignettes the complexity of hybrid threats was lost. Vignettes were more focussed on a standalone event. Balancing of the scenario presenting the complexity and making it simple to understand, interpret and apply should be considered for the up-coming cycle.
- There were numerous registrants who were 'no-shows' without prior notice. Similar issue was observed during the 1st project working cycle as well. If similar methodology is to be applied for the next cycle, required participation on site and very limited possibilities to observe process online can be one of the ways to solve this problem.
- The presence of a competent Moderator proved to be one of the key success factors of the training. Planning the set of next trainings of similar methodology, inclusion of competent experts into the training process should be continued.

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 D2.21 «*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.

7.FUTURE WORK

This deliverable emphasizes on providing an overview of the training material developed and used during the EU-HYBNET training activities in September 2022. Overall, the documentation produced will serve as the basis for future training activities within and outside of the Consortium regarding the most up to date topics and innovations on the area of hybrid threats. In the third project working cycle, the task participants, based on the input provided by Task 2.3 and the training execution in T2.4, will produce the relevant report summarising the knowledge produced.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / description
DTAG	Disruptive Technology Assessment Game
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

ANNEX II. REFERENCES

[1] European Commission Decision C (2014)4995 of 22 July 2014.

[2] Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.

[3] EU-HYBENT Deliverable 2.18 Training and Exercise, Scenario delivery

[4] EU-HYBENT Deliverable 2.21 Training And Exercises Delivery On Up-To-Date Topics

[5] EU-HYBENT Deliverable 2.24 Training And Exercises Lessons Learned Report

ANNEX III. ADENDA OF THE EVENT

EU-HYBNET 2nd Training and Exercise Event

29-30 September, 2022, Vilnius Didlaukio g. 55, Lithuania

Agenda

Day 1, September 29 (Thursday)

Link for on-line participants in MS Teams platform: Click here to join the meeting
Meeting ID: 355 594 774 007
Passcode: PfkpnD

Time	Item	Room
12:00-12:10	Welcome and Introduction	102
12:10-12:30	Description of the training flow	
12:30-12:50	Introduction to Scenario	
12:50-13:00	Q & A	
13:00-13:15	**Break**	
	Breakout rooms: 1. "Future trends of Hybrid Threats" 2. "Cyber & Future Technologies" 3. "Information and Strategic Communication" 4. "Resilient Civilians, Local Level National Administration"	 104 102 101 407
13:15-14:30	Breakout rooms: • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
14:30-15:00	**Break**	
15:00-15:30	Presentation of results of Core Themes	
15:30-17:00	Live innovation presentations: • LT Armed Forces StratCom (innovative tools and methodology application) • HENSOLDT (open-source intelligence) • MALTEGO (solution) • European External Action Service (EEAS) (tool for strategic communication)	102
17:00-17:15	Closing remarks	102

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

EU-HYBNET 2nd Training and Exercise Event

29-30 September, 2022, Vilnius Didlaukio g. 55, Lithuania

Agenda

Day 2, September 30 (Friday)

Link for on-line participants in MS Teams platform: Click here to join the meeting
Meeting ID: 355 594 774 007
Passcode: PfkpnD

Time	Item	Room
10:00-10:15	Welcome and Introduction	102
	Breakout rooms: 1. "Future trends of Hybrid Threats" 2. "Cyber & Future Technologies" 3. "Information and Strategic Communication" 4. "Resilient Civilians, Local Level National Administration"	 104 102 101 407
10:15-11:45	Breakout rooms: • Introduction to innovations • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
11:45-12:15	**Break**	

Link for on-line participants in MS Teams platform: Click here to join the meeting
Meeting ID: 355 361 106 128
Passcode: jtvEi9

Time	Item	Room
12:15-14:00	Breakout rooms: • Introduction to innovations • Campaign planning • Presentation of the campaign plan	101, 102, 104, 407
14:00-14:15	**Break**	102
14:15-14:45	Presentation of results of Core Themes	102
14:45-15:00	Closing remarks	

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