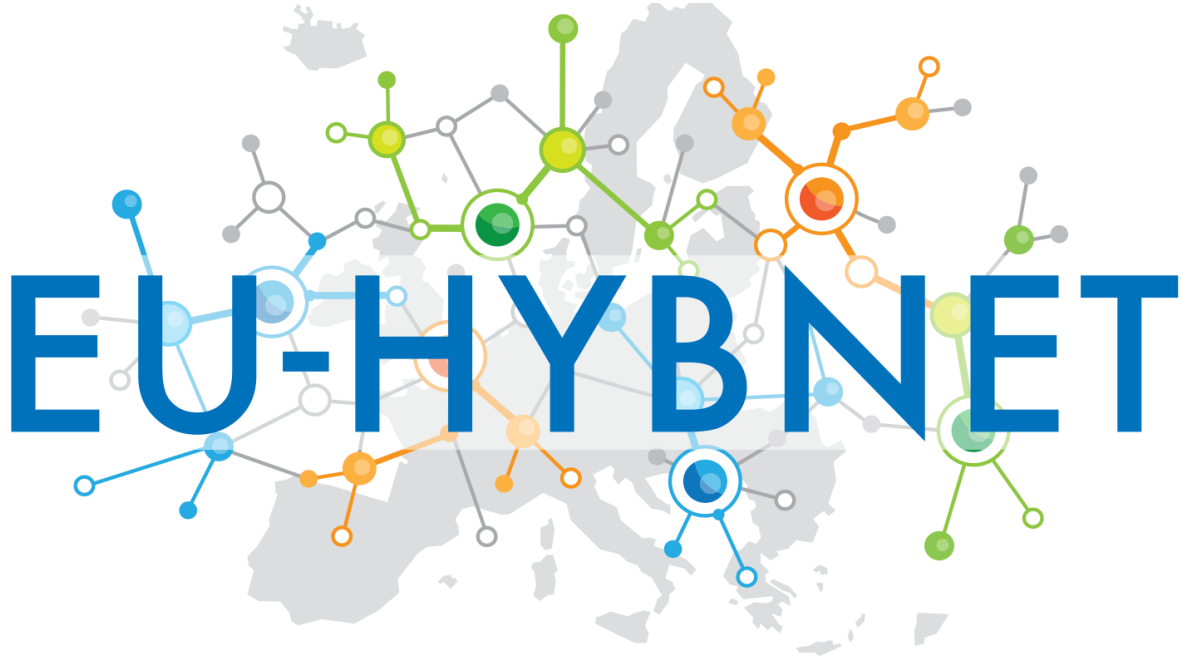


TRAINING AND EXERCICE, SCENARIO DELIVERY

DELIVERABLE 2.19

Lead Author: KEMEA

Contributors: HybridCoE, LAUREA, L3CE, 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

D2.19 TRAINING AND EXERCISE, SCENARIO DELIVERY

Deliverable number	**D2.19**	
Version:	**1.0**	
Delivery date:	**21/12/2023**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Final Version**	
Nature:	**Public Report**	
Main authors:	**Vanessa Papakosta, Athanasios Kosmopoulos**	**KEMEA**
Contributors:	**Vanessa Papakosta**	**KEMEA**
	Päivi Mattila	**LAUREA**
	Alex Koniaris	**KEMEA**
	Julien Theron	**JRC**
	Hanne Dumur-Laanila	**HybridCoE**
	Edmundas Piesarkas	**L3CE**
	Petri Häkkinen, Satu Laukkanen	**Espoo**
	Dimitri Teperik, Ivo Juurvee	**ICDS**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	26-10-2023	KEMEA	Table of Contents
0.2	06-11-2023	KEMEA	Scenario outline
0.21	15-11-2023	KEMEA	Update to Section 5
0.3	20-11-2023	Laurea	Update to Section 5
0.4	22-11-2023	KEMEA	Update to Section 6
0.5	23-12-2023	JRC	Edit to text
0.5	27-11-2023	Hybrid CoE	Update to Section 5
0.6	01-12-2023	KEMEA	Edit to text
0.7	06-12-2023	KEMEA	Text conceptualization
0.8	11-12-2023	L3C3	Edit Text
0.9	11-12-2023	KEMEA	Finalize the text
0.91	13-12-2023	Laurea	Review and text editing
0.92	13-12-2023	Espoo	Review
0.93	13-12-2023	ICDS	Review
0.94	21-12-2023	KEMEA	Final review
1.0	21-12-2023	Laurea	Final review and submission of the document to the EC

DISCLAIMER

TABLE OF CONTENTS

FIGURES

1. INTRODUCTION

1.1 DELIVERABLE OVERVIEW

This deliverable aims to present the work carried out in the frame of the preparation of the training activities of the H2020 EU-HYBNET project.

The aim of the current document is to prepare the exercise/training material that will be used to test the most promising innovations (technical and non-technical) to identified gaps and needs under each one of four core themes. The D3.5-*Second Report on Improvements and Innovation* and D3.9- *Second Report on Innovation and Research Project Monitoring* deliverables have provided the innovations that address the short list of the gaps and needs for the EU-HYBNET practitioners, available from D2.10– *Deeper Analysis, delivery of short list of Gaps and Needs*, and in this regard should be tested. The scenario preparation and the training structure are two important aspects that will be fed to T2.14 – *Training and Exercises for Needs and Solutions for Gaps* so as to arrange the actual training and to start planning the evaluation of the innovations and the training itself. The evaluation of the innovations will serve as the basis for WP4 in order to know what will be stated as innovation uptake recommendations. All the aforementioned aspects are depicted in the image below:

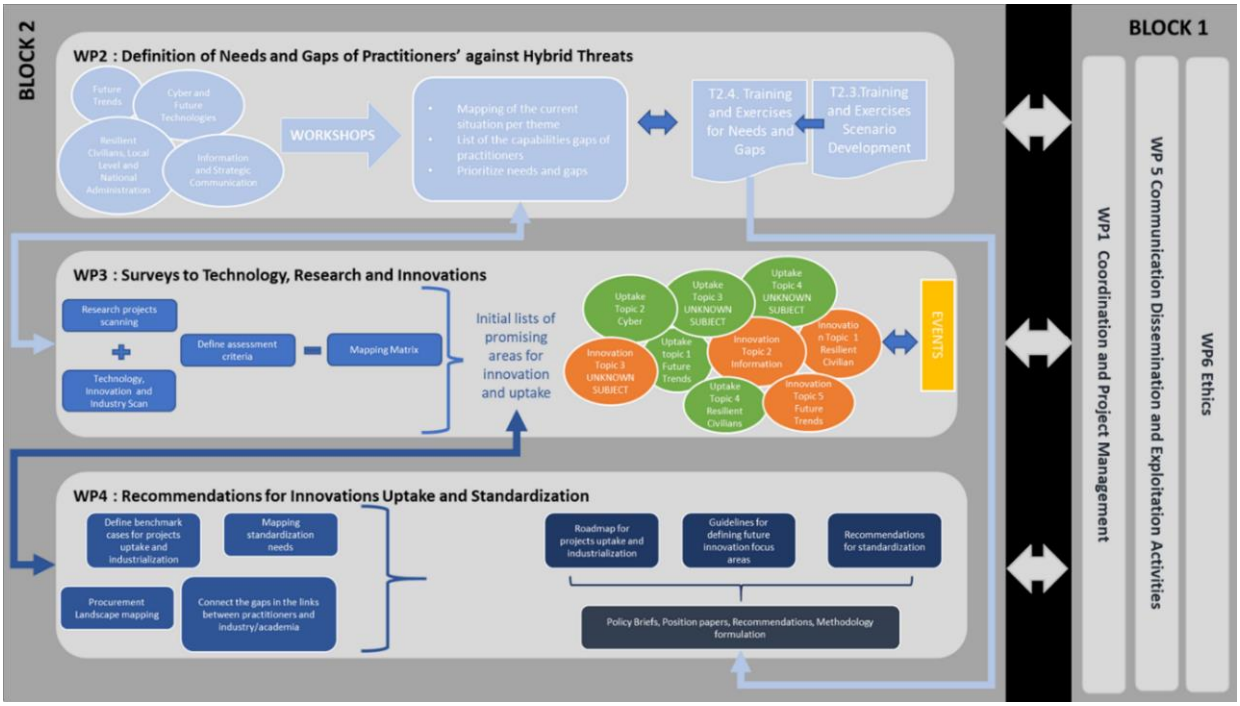


Figure1: EU-HYBNET structure of Work Packages and Main Activities

In more detail, following the relevant work in identifying the short list of the gaps and needs in countering hybrid threats, as well the analysis of the available technological and non-technological solutions under T2.2 and WP3 respectively, D2.19 will serve as the basis in order to:

1. build the objectives of learning and training that will be performed under Task 2.4;
2. develop the scenarios that will be used for the training and exercise delivery taking into account all four Core Themes: [1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication and select the innovations to be tested during the training.

3. set the tools to be used to achieve the objectives as well as the evaluation methodology framework.

Nonetheless D2.19 does not directly deliver results to certain EU-HYBNET project objectives (OB), still D2.19 strongly supports other EU-HYBNET Task to deliver results especially to:

- OB 6.4 : To empower European practitioners, industry, SME and academic actors' capacity to counter hybrid threats by offering relevant trainings and materials
- OB 7.1 : To share information on EU-HYBNET activities and training possibilities among European stakeholders
- OB 2.2 : To define innovations that can overcome the identified gaps and needs in certain focus areas in order to enhance practitioners (priority),industry, SME and academic actors capabilities
- OB 2.4 : To develop a roadmap of the requirements for on-going research and innovation necessary to build the preferred system of the future for confronting hybrid threats

The named Objectives are following and closely related to training arrangements and innovation testing and selection.

1.2 DEFINITIONS

Hybrid threats: Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties."[1]Hybrid threats can be characterised as coordinated and synchronised actions that deliberately target democratic vulnerabilities of states and institutions through a wide range of means. The aim is to influence different forms of decision making at institutional, local, regional and state levels to favour and/or achieve strategic goals while undermining and/or hurting the target. To effectively respond to hybrid threats, improvements in information exchange, along with breakthroughs in relevant research, and promotion of intelligence-sharing across sectors, and between the EU and its MSand partners, are crucial[2].

According to the joint framework on countering hybrid threats[1], while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept of the framework aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. Diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Practitioners at different levels: The EU-HYBNET H2020 project follows the European Commission definition of practitioners which states that "a practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection." In addition, practitioners in the hybrid threat context are expected to have a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats[3].

Therefore, EU-HYBNET practitioners are categorized as follows: i) ministry level (administration), ii) local level (cities and regions), iii)support functions to ministry and local levels (incl. Europe's third sector). EU-HYBNET includes practitioner partners from all these levels and its primary focus is on civilian security issues.

Training: is teaching, or developing in oneself or others, any skills and knowledge or fitness that relate to specific useful competencies. Training has specific goals of improving one's capability, capacity, productivity, and performance.

Table-top Exercise: A tabletop exercise is an activity in which key personnel assigned emergency management roles and responsibilities are gathered to discuss, in a non-threatening environment, various simulated emergency situations.

Scenario: a coherent, internally consistent, and plausible description of a potential future trajectory of a system to assess current practice, screen new opportunities, and improve the design and implementation of policy responses[4]. Within a training, a scenario builds on different assumptions

[1] Joint Framework on CounteringHybridThreats, Join (2016) 18 Final, European Commission
[2]EU-Hybnet Description of Action, Coordination and Support Action, Grant Agreement No 883054
[3]https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156
[4]Gómez et al. 2017

about future developments and the effects of measures. The purpose of a scenario creation is to understand the future trajectories' impact on the system, when no action is taken or when alternative options are considered, and uncertainties associated with complex dynamic systems. One scenario can serve different purposes and it can be constructed from multiple sources, even multiple other scenarios (e.g., external inputs, narratives, or model simulations).

Vignettes are brief stories or scenarios that describe hypothetical characters or situations. Stories must be believable and appear as realistic as possible to participants. This means that the vignette needs to be relatable for the participant. Vignettes need to contain sufficient context for respondents to have an understanding about the situation being described but be vague enough to for participants to provide additional factors which influence their decisions. It is important that the stories presented in the vignettes are easily understood, internally consistent and not too complex.

1.3 STRUCTURE OF THE DELIVERABLE

This document includes the following chapters:

Section 1 includes the objectives of this report, some important definitions and the deliverable structure description.

Section 2 introduces the aim of the exercise and the exercise methodology in order to give the reader a better overview of the rational of the training.

Section 3 presents the EU-HYBNET exercise details, i.e. the aim, the tool to be used and the necessary concepts.

Section 4 provides the background scenario as well as information regarding the actors and organisations that are involved.

Section 5 presents the four vignettes that will be used for the training event.

Section 6 outlines the proposed methodology for measuring the impact of the EU-HYBNET training and how this will be achieved.

Section 7 provides the conclusion of the current document

2. TRAINING METHODOLOGY

In the context of EU-HYBNET training, the war gaming approach was chosen. A wargame is a type of strategy game that realistically simulates warfare, as opposed to abstract strategy games such as chess. War gaming may be played for recreation, to train military officers in the art of strategic thinking, or to study the nature of potential conflicts. Many wargames recreate specific historic battles, and can cover either whole wars, or any campaigns, battles, or lower-level engagements within them. Many simulate land combat, but there are wargames for naval and air combat as well.

Wargaming in its modern form originated in Germany in the 1820's. Over the next two centuries, the armed forces of most nations employed various forms of wargaming for training and planning purposes, and war gaming was generally accepted across the military by the mid-twentieth century.

However, up to now there is no single, commonly accepted, definition of 'wargaming'. NATO defines a war game as: a simulation of a military operation, by whatever means, using specific rules, data, methods and procedures[5]. The importance placed on the decisions of the wargame players, not contained in the NATO definition, leads to the working definition of wargaming contained in the Red Teaming Guide[6]: A scenario-based warfare model in which the outcome and sequence of events affect, and are affected by, the decisions made by the players.

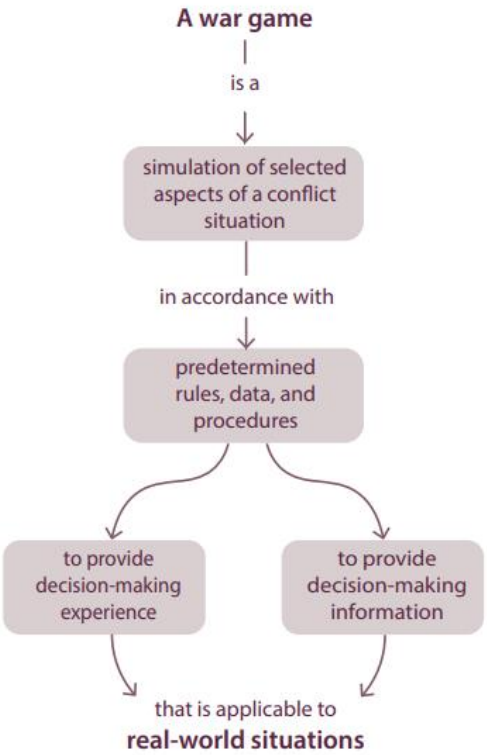


Figure 2The general purposes of wargames[7]

[5]https://nso.nato.int/natoterm/Web.mvc
[6]Development, Concepts and Doctrine Centre (DCDC), RedTeaming Guide, 2nd Edition, 2013, Lexicon.
[7]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

In this context, a wargame, which is a recognized red teaming tool, serves as a process of adversarial challenge and creativity, delivered in a structured format and usually umpired or adjudicated. Wargames are dynamic events driven by player decision making. As well as hostile actors, they should include all 'oppositional' factors that resist a plan. At the core of wargames are:

- the players;
- the decisions they take;
- the narrative they create;
- their shared experiences; and
- the lessons they take away.

In this regard, training ('learning') wargames are a 'fitness programme for thinking', enabling practice in the conceptual elements of command and control. In common with all training methods, a war game is best considered in terms of a holistic life cycle, as shown in Figure 3.

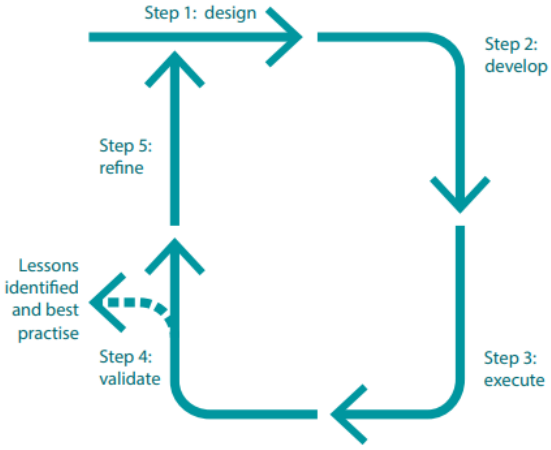


Figure 3Wargame training process[8]

The stepwise approach that needs to be followed for the implementation of the first step i.e. the design of the wargame training, which is the purpose of the current document, is described below:

1. Specify the aim and training objectives. (section 3)

2. Identify how the outputs will be used and integrated. (section 3)

3. Identify the people to be trained, their roles and the decisions they will be expected to make. (see section 5)

4. Determine the desired effects on the players, and the exercise activities required to create these. (section 3)

5. Determine the scenario, and any specific vignettes, required to enable the training execution. (section 4,5)

[8]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/641040/doctrine_uk_wargaming_handbook.pdf

6. Identify the tool needed to enable these structures and processes. (section3)

8. Create an evaluation methodology of the training(section 6)

All the aforementioned are analysed in the context of the EU-HYBNET training in the upcoming sections.

3. EU-HYBNET EXERCISE OVERVIEW

3.1.AIM OF THE EXERCISE & OBJECTIVES

The aim of the exercise is to face participants, acting at various levels of responsibility and decision making in a given state / multinational context with a series of disruptions (accidents and threats) in order to make apparent the different policy, strategic, operational and tactical dilemmas that arise for the organisation or system in crisis. In this content war gaming was considered the appropriate training approach. **The exercise depicts a system whose essential means are affected by the threats to such a degree that the resilience of the system does not suffice to manage the system in crisis.**

This setting utilizes and operationalizes the main **gaps and needs** in countering hybrid threats that were identified throughout WP2, and the EU-HYBNET training event is expected to discover new gaps and needs through practice. The scenario depicts various organisations that form a system in crisis confronted to a set of external actors. In this context, the participants will be requested to test a series of innovation solution possibilities (identified under WP3), whether technical, social, material and immaterial, in order to assess their opportunity, fitness, utility and readiness to help organisations manage the crisis and solve the dilemma they face.

3.2. DTAG

A DTAG is a seminar type wargame, used to assess potential innovations and their impact on hybrid campaigns and the operating environment. A Disruptive Technology Assessment Game (DTAG) will be used to test the innovations identified in WP3 in a realistic setting. The DTAG essentially allows the deployment of innovations (available in D3.3 and D3.7), or so-called Ideas of Systems (IoSs) as described in WP3 (Deliverables D3.3 and D3.7) within a realistic operational context. That is, to understand the operationalization of the innovation, its impact on the operational environment, the potential vulnerabilities adversaries might exploit and thus allow countering of the innovative measure and finally, how to anticipate such countering. The DTAG format was originally developed by an international team of researchers from NATO countries through NATO's Science and Technology Organisation in 2010. The overall method is described in the DTAG handbook [5] as supplied by NATO's Allied Command Transformation.

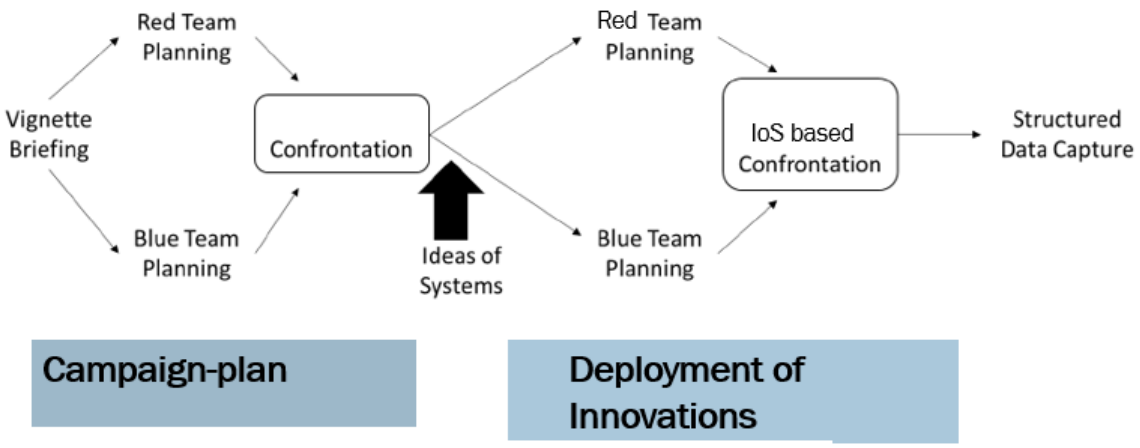


Figure4: DTAG concept

A DTAG uses a scenario and one or more vignettes (see section 4,5) to sketch hybrid challenges within a realistic future operational environment.

With reference to Figure 4, a DTAG assumes a BLUE (friendly or allied forces) and a RED (adversarial) team that both are asked to create a campaign plan a series of challenges. A confrontation follows which helps to inform the teams on the BLUE Course of Action (CoA) and the possible countering by RED. This process aims to help participants understand the vignette, its challenges, the teams' objectives and the potential CoAs, it creates a baseline from which to work. Then cards with the Ideas of Systems (the Innovations) are being introduced. Now the BLUE teams select the relevant Innovations and aims to implement the Innovations in their campaign plan. They describe 1) how they implement those IoSs, 2) why, 3) what the implications are for their campaign plan and finally 4) the possible counter measures by RED they would anticipate. The RED team attempts to undermine the BLUE campaign by countering it, if possible, by exploiting possible vulnerabilities within the IoSs applied.

There will be structured data capture by analysts taking notes during the discussion, by means of forms that participants will fill out during the operationalization of the IoS and by means of a structure's discussion during the validation phase.

3.3.CONCEPTS

Organisations in crisis - organisations in crisis are defined by their mission and values that they are founded upon. The main objective of organisations is to defend these respective values. The objectives of organisations are allocated per their fields of competence: the objectives aim at fulfilling these values. In other words, **organisations in crisis defend their values by pursuing objectives that are responding to the dilemma they face**. *The implementation of those objectives is hampered by sources of risk that lie in accidents or threats.* Organisations to this end, make use of tangible and intangible means.

Objectives of organisations - participants following the scenario and each of the vignettes must respond to a series of objectives, related to the organisation / system in crisis that they represent. The **main objective is to maintain and safeguard the organisation / system's core values and interests while facing dilemmas caused by the unanticipated nature of events.** Participants have at their disposal the IoSs cards of the DTAG that present innovation solution possibilities (tangible and intangible means) in order to achieve their objectives while balancing their values and interests within the specific crisis management needs. DTAG cards are perceived as those means that enable organisations to preserve their objectives.

Risk mitigation as means to pursue the following objectives:

- impact reduction
- occurrence probability reduction
- reduction of destructive / lethal force
- reduction of attractiveness and feasibility.

In this context, each organisation / system that its participants use the vignettes has the objective to assess the specific needs of the situation and has specific requirements for situational awareness. The cards at their disposal are given to balance their objectives**.**

Translating the methodological framework of people-processes –technology into the EU-HYBNET exercise we can define the following:

People = participants; processes = objectives / values / interests assessed; technology = technical and non-technical innovation solution possibilities.

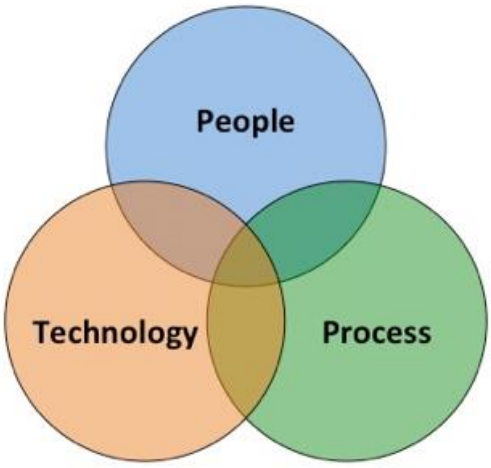


Figure 5Methodological Framework of people-processes- technology

4.EU-HYBNET SCENARIO

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

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

The scenario is about six different entities that are interacting in the same geopolitical context, while different attack surfaces are developed suitable to deploy hybrid ops vectors on all four Core Themes :

- FUTURE TRENDS OF HYBRID THREATS
- CYBER AND FUTURE TECHNOLOGIES.
- RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION
- INFORMATION AND STRATEGIC COMMUNICATIONS

4.1. MAIN ACTORS

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

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

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

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

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

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

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

4.2. SITUATIONAL SETUP

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

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

- Disinformation in LATARUM includes fake news and fake videos

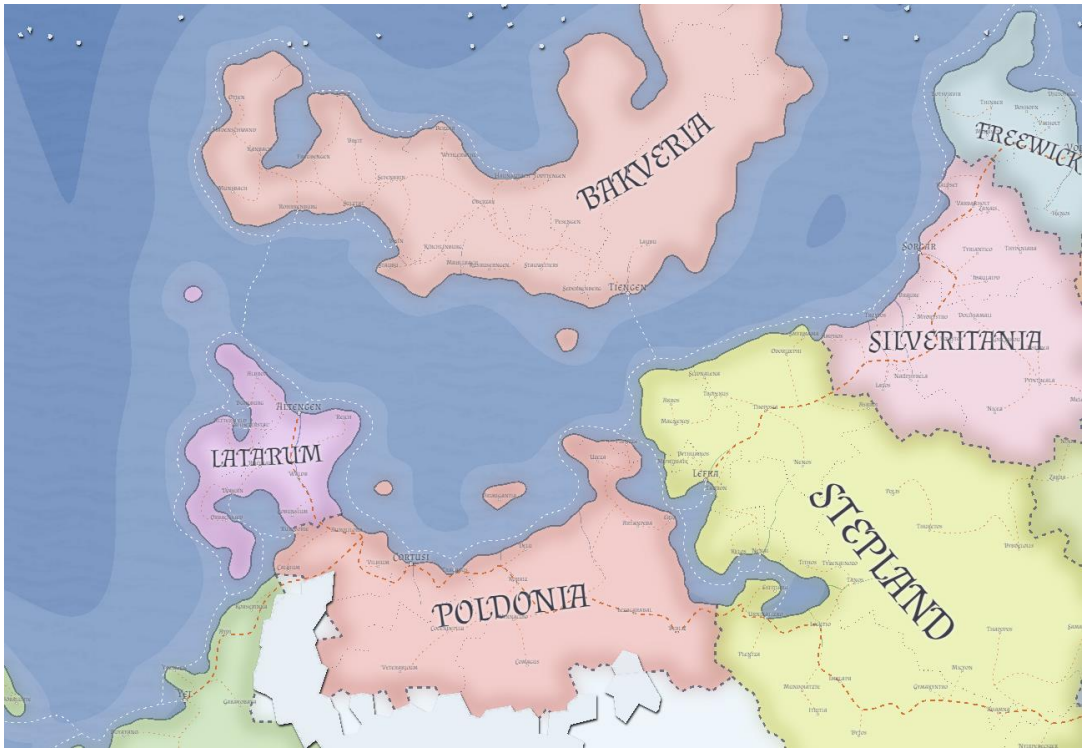
- Critical infrastructure in BAKVERIA is attacked, public safety is also at risk with bombing attacks. Physical attacks on important infrastructure lead to social unrest and fear. Compromising access to basic needs such as emergency and health services can increase population insecurity and hardship.

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

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

4.3. MAP

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



4.4. VIGNETTES

The EU-HYBNET training and exercise scenario vignettes are following:

1. Wide spread of online harassment and acts of violence in LATARUM against POLDONIAN ethnic groups related to STEPLAND escalates to riots. Police and rescue agencies are trying to control and use their resources more efficiently while managing the situation.
2. The President of LATARUM has allegedly declare in videos that a referendum will be called regarding the self-determination and autonomy of Poldovian residents in the North area of the country. These videos are considered fake.
3. Hospitals and emergency services are targeted, physical attacks with IED on their premises affect their ability to provide rapid and efficient assistance in the event of an emergency in BAKVERIA.
4. Telecoms operators in Silveritanian Hospitals are facing a chaos. During the Mega fire crisis the number of emergency calls has proven to be exponential, from 1 per minute to over 100 per minute, becoming impossible to sort out by emergency dispatchers, especially with the average emergency call lasting from 3 to 15 minutes dealt by just a few emergency dispatchers. Creating a massive telephonic congestion, the population is no longer capable to reach by phone the emergency services, report their positions and the evolution of their situation. This lack of communication increases the workload of Search & Rescue, which in the aftermath have to go place by place instead of focusing on population's reported positions.
5. The internal integrity of the Silveritanian Hospitals is under attack by hostile messaging, and disinformation, via Viber and Telegram messaging to the staff, that the higher management is unreliable and incompetent to handle the situation. Not only the employees of the Hospitals but also outside stake holders are targets of hostile messaging and this put additional pressure to the organization and creates serious problems for the organization that causes its integral structure disintegrating.
6. The impact of increasing levels of visual misinformation by STEPLAND regarding the illegal actions of its Airforce and Navy changes the social and political climate. It undermines democratic processes, distorts the public and fuels social unrest. False or manipulated images can incite violence, trigger outrage and provoke conflict by exploiting people's emotions. The spread of visual misinformation also poses challenges for media companies and technology platforms responsible for moderating content.
7. News media industry in FREEWICK has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. This has led to a merger and acquisitions policy that ended into almost all media outlets in the country belonging to a very powerful financially individual. Evidently questions are raised on the objectivity of these media and the control exercised over them.
8. No specific regulatory framework exists in FREEWICK regarding Disinformation by major online platforms. Social media giants present a manipulative danger combined with the media ownership status, at the same time the situation remains hardly reachable from regulatory perspective.

4.5. SCENARIO CONCLUSION

The EU-HYBNET training and exercise event participants are asked to freely assess the overall situation and to test the innovations presented for them as possible promising solutions.

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

5. INNOVATIONS TO BE TESTED DURING THE TRAINING & EXERCISE

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

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

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

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.1 "Political Deficiency"

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

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.3 "Substitutive Reality"

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

Core theme 2. "Cyber and Future Technologies"

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

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

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

- Threat No 3.2. "Attack on Social Structures"

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

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

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

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

Core theme 4. "Information and Strategic Communication"

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

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

Core theme 4. "Information and Strategic Communication"

- Threat No 4.1. "Media Conundrum"

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

Core theme 2. "Cyber and Future Technologies"

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

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

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

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

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.1 "Political Deficiency"

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Mobile application to pinpoint acts of harassment/violence on the street and online**	Countering online harassment and acts of violence requires to link the victims or witnesses of these actions and the dedicated law enforcement agencies. This requires the solution to cover a larger surveillance area, to be fast and avoid the situation to enter into a spiral of kinetic violence such as riots. Such a detrimental situation would indeed require more police and rescue resources, with a reduced ability to control the situation. It also promotes a whole-of-society approach. The proposed solution has a dual interest for the violence occurring in LATARUM against POLDONIAN ethnic

		groups related to STEPLAND: not only it can detect and regulated online situations, but also physical violence if the online behaviours spill over the streets. This solutions should therefore have a double impact to restore the rule of law.
3.9	**SMIDGE**	Online extremism can result being extremely destabilizing, even if a short amount of activists are propelled into action. Attempts to overthrow democratic government regularly occur from reduced and clandestine cells praising extremist ideologies. The solution proposes to provide a dual effect. The first one concerns the promotion of a sane information through counter-narrative and reliable resources for professionals dealing with information. The second one deals with policy- and decision-makers through guidelines and recommendation.

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

Core theme 1. "Future Trends of Hybrid Threats"

- Threat No 1.3 "Substitutive Reality"

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

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

		critical thinking is also accompany through this solution with a more long-term education to responsible behaviour regarding information and online communication.

5.2. INNOVATIONS TO CORE THEME: CYBER AND FUTURE TECHNOLOGIES

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

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

Core theme 2. "Cyber and Future Technologies"

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

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Advanced Surveillance Systems with Perimeter security**	Attacks on the critical infrastructure such as health care deprive people from urgent needs of care, endanger staff working conditions and undermine the whole infrastructure system. The Advanced Surveillance Systems (ASS) and Perimeter security is built to protect the critical infrastructure from physical threats. The ASS and Perimeter security tools could be used to mitigate physical threats to the critical infrastructure reinforcing the protection. A central monitoring station with trained personnel continuously monitors the real-time camera images transmitted via redundant channels and enables and ensures an immediate response to suspicious activities. This innovation relates especially to physical threat No. 2.1. "Stealing Data, attacking individuals" and to the scenario case where the critical infrastructure in BAKVERIA is attacked and public safety is at risk.
3.5	**Code of Practice on Disinformation**	Disinformation is widespread across different social media channels making it difficult to mitigate. The Code of Practice on Disinformation, which is a self-regulatory tool aims to counter disinformation worldwide in

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

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

Core theme 2. "Cyber and Future Technologies"

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

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Starlight Disinformation-Misinformation Toolset**	STARLIGHT project (https://www.starlight-h2020.eu/) is one of the flagship projects dedicated to deliver easy deployable toolset to address various need of LEA and other security practitioners driven by constantly changing tech driven crimes modus operandi. In particular, STARLIGHT has one direction dedicated for disinformation and misinformation related threats. This direction is composed of several organisations developing different tooling enabling deep access of information in social platforms and tools to detect different misleading aspects of the information. There are tools dedicated to access information on general internet, communication platforms such as Telegram or X (Twitter) platforms, but majority are focused on detection of fault or forbidden content. Majority of them can work on different languages. All of Starlight tools listed are planned to be integrated in one interface, making them easier to use. At this point of time Starlight project is developing solutions for LEA, but it can be developed further for different target groups and serves as a good example of what is needed to handle artificial amplification complexity. In the context of the vignette Starlight could provide support for LEAs to discover manipulation in information and also have material to prove the manipulation. This could ease the citizens to gain trusted informaiton from LEAs that the citizens are under influencing. Furthermore, this could support the regime to develop new legistlation that will ask media giants to check the possible false information and to prevent spreading the information.
3.9	**Innovative Cluster for Radiological and Nuclear Emergencies,** INCLUDING https://cordis.europa.eu/project/id/833573	The EU-funded INCLUDING project will build a dynamic cluster of 15 partners from 10 EU Member States acting in the INCLUDING Federation. An advanced web platform will shape a map of cooperation between governmental, security and medical institutions, industrial services and others. Partners will provide multidisciplinary knowledge, research, new technologies and infrastructure. Procedures will be formed for joint actions: field exercises, training and

		simulations. The project will be a base for a modern flexible network for better security in the RN field in Europe. In the context of the vignette, INCLUDING could be an example how information sharing from authorities side will remain crucial in society even though Media Outlets would be bought by malicious actors.

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

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

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

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

- Threat No 3.2. "Attack on Social Structures"

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**AI-enhanced disaster emergency communications -innovation**	The starting point for the selected innovation is that the technology can be applied to enhance the resilience of social structures in the face of hybrid threats. The company HighWind has developed and patented the first Artificial Intelligence that can assess a patient's emergency priority level in less 100

		millisecond thanks to Computer Vision and Deep learning using a crossed analysis on traumatology (nature of the wounds), emotions (pain, fears, etc.) and contextual elements (fire, smoke, etc.). Applied to major disasters, and encompassed within an smartphone "Disaster Mode" app for the population (downloaded or emulated by text-message link), it gives the emergency responders the ability to immediately visualize who are the persons most at risks on a map, prioritize search & rescue efforts to the most vulnerable persons, avoid the emergency calls congestion and facilitate patient referrals to hospitals based on the severity of their injures, thereby mitigating the potential influx of patients in hospitals. Instead of taking one by one, lengthy emergency calls due to stressed persons, the emergency dispatch centre can perform several actions at once: send a "Disaster Mode" notification to the population, receive an accurate view on the emergency requests critical levels and positions on a map in few seconds, to better coordinate SAR efforts. Leveraging on basic smartphone features, the AI is capable to immediately sort out victims, saving hours for the SAR teams and significantly increasing chances of survival. The "Disaster Mode" is also capable to take decisions to optimize communication based on available networks quality (no data, 2G to 5G). On the whole, the solution can be used to protect the social infrastructure to potential attacks and increase resilience of health sector during the crisis situations. The solution is specifically designed to enable an early assessment of the crisis. Initial triage at the crisis scene serves the purpose of enabling hospitals and all involved stakeholders better understand the severity of crisis and prepare appropriately. N.B. The innovation primary pertains to technical aspects. However, to make the solution operational ready there is a need to develop a framework of utilization of the "Disaster Mode"

		solution and its AI-enhanced Safety Check ensuring compliance to EU General Data Protection Rules (GDPR), considering level of risks of a given disaster for the safety and health of the persons and ensure compliance of the prototype toward EU main guidelines: AI Act, Data Act and GDPR.
3.9	**The Countering Foreign Interference (CFI) project** https://www.iss.europa.eu/content/euiss-launches-eu-funded-project-countering-foreign-interference	The FCI project focuses on improving understanding of potential threats in the information space. It will utilize accumulating knowledge for developing improved tools and methods to identify, monitor and counter those threats. Often adversaries aim to amplify the present crises by increasing disinformation in the information flow. Therefore, in a case of crises, it is important for the authorities that their guidance and information can be well reached so that the crises will not escalate further on the basis of false information. Therefore, it is important for the authorities to have the improved tools and methods to identify, monitor and counter disinformation in early phase.

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

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

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

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**'Antidote' to hostile messaging delivered by private messaging apps**	The starting point and goal of the solution is very straight forward: to improve people's resilience to hostile messaging and hence fostering the integrity of organizations. The starting point in the suggested solution is that information is to be shared in order to

		raise awareness and standard of critical thinking. I.e. messages like "this is not true" may not be the most efficient, but rather the games attracting attention to the problem may be used. Technically most simple solutions are sharing the link to freely available and already existing games but games takes time and 'Antidote' can be shared in other ways too. For an example the simplest, but also much more expensive way, is to buy "antidote" as advertisement. The more complex, but much cheaper and more efficient way, would be to collaborate with the owners of the private messaging apps in order to sort out the target groups to be immunized and share the content for free. Although the best 'antidote' could be chosen by the organization which integrity needs protection, the communication and dealing with private messaging app owners should be handled centrally. This asks time but is still seen as a sound and well recommended solution. Furthermore, the technical solution – private messaging apps – is already there. There is only a need to start using them more efficiently in the fight countering disinformation and getting the owners of the app on board.
3.9	**EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective** https://cordis.europa.eu/project/id/608385	It is expected that information sharing platforms for strategic security institutions would provide not only needed tools for information sharing inside the organization but also between the institutions. The platforms are also to increase cooperation between actors and to increase traceability and trust alike motivation for the cooperation due to enhanced results. The gained trust in cooperation builds resilience to adversaries possible attempts to harm the trust and to paralyze joint proceeding in critical cases and in crises. A successful project to increase cooperation in information sharing and cooperation has been EUCISE2020 project in European maritime domain. The project has lead to development of Common Information Sharing Environment (CISE) to pan-European and national maritime authorities. On the whole, CISE is not only to support various pan-European security authorities to increase their cooperation, but it also empowers the cooperation in national level due to the development of national nodes. In short, without the cooperation

		between the national security institutions and authorities in the specific security domain (e.g. in maritime domain/ border guards, navy, police, customs) development of the solution/CISE national node would not have been possible. In short, the pan-European CISE has pushed national security authorities and institutions to find and definite new ways of cooperation and information sharing reducing partly also the culture of secrecy between institutions and inside the institutions. An example of increased cooperation between national *strategic security institutions* is a FINCISE project from Finland **FINCISE 2.0 Project** CISE | The Finnish Border Guard (raja.fi) (Duration: 2022 -2024) where all Finnish Maritime Cooperation (FIMAC) authorities joined to CISE development and finding new ways for future cooperation. On the whole, the takeaway from the above mentioned CISE projects' is that the approach seems to work in various security domains and hence also hybrid threats related security authorities could consider to develop CISE for their purposes. Furthermore, CISE seems to support cooperation between strategic security institutions and diminish culture of secrecy between institutions, also in the institution.
3.9	**STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats** https://cordis.europa.eu/project/id/740610	Also solutions that have trained actors in organizations, or between organizations, to work together during crises (e.g. during malicious influencing campaigns to cooperation) are much needed in order to ensure critical institutions solid work flow. With reference to this, STOP-IT project has developed a solution that ensures training for organization to face future severe cases in a manner that trust and knowledge how to proceed without severe challenges will be maintained. STOP-IT has delivered an integrated, modular platform that supports strategic/tactical planning, real time operational decision making and post-action assessment for the key parts of the water infrastructure. The focus in the platform can be in any other infrastructure too. The STOP-IT platform is scalable (scaling from small utilities to large ones); adaptable (including various modules addressing different needs, with expandability for future modules); and flexible (the utility managers can decide how to use it and it will

		be usable by experts, novices, and even non-technical staff). The categories in the platform are: Decision Makers; Risk Officers and Modellers; Real Time Operators and Maintenance Managers. Even though the platform has been developed to three different user categories in organizations, it can also host multi-agency/ institutions discussion and planning. On the whole, the STOP-IT platform supports to enhance cooperation skills and trust between the users because its use provides exercise(s) that may then ease the cooperation in the future in real cases.

5.4. INNOVATIONS TO CORE THEME: INFORMATION AND STRATEGIC COMMUNICATION

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

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

Core theme 4. "Information and Strategic Communication"

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

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

Core theme 4. "Information and Strategic Communication"

- Threat No 4.3. "Attack on information"

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**Blockchain -based verification -innovation**	Blockchain technology can play a crucial role in the fight against the increasing use of visual misinformation. By leveraging the inherent security and transparency of blockchain, a robust system can be established to verify the authenticity of images and videos. Blockchain allows us to timestamp visual content at the time of creation. Each medium is linked to a unique cryptographic hash and recorded on the blockchain, creating an immutable record of its provenance. This timestamp ensures that the authenticity of the content can be easily verified, thus helping to identify real footage and distinguish it from manipulated images. Fact-checking organizations are integrating this blockchain technology into their processes by recording their findings and conclusions on the blockchain. This creates an immutable record of verified information, increasing confidence in their reviews. Collaborating with content creators is essential. Encouraging professionals and journalists represents a sign of trustworthiness to certify the authenticity of their work on the blockchain. This also increases trustworthiness in a time plagued by misinformation. Public blockchain visual content verification databases managed by a consortium of organizations can further improve transparency and accountability. Furthermore recognizing blockchain as evidence in court cases related to misinformation is an incentive to use this technology to verify content.
3.5	**Media Pluralism Monitor (MPM)** https://cmpf.eui.eu/media-pluralism-monitor/	Media Pluralism Monitor (MPM) is a tool developed by the Centre for Media Pluralism and Media Freedom (CMPF) of the European University Institute (EUI) to assess the potential weaknesses in national media systems that may hinder media pluralism. Based on 20 indicators, summarizing 200 variables, it covers four areas:

		1. Fundamental protection 2. Market plurality 3. Political independence 4. Social inclusiveness. The news media industry has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. Although the shock was largely foreseeable due to the extraordinary circumstances, its depth and the diverging effect between different countries has to be investigated.
3.9	**ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE (Grant agreement ID: 101094742)** **Website:** https://resilientmedia.eu/ **Cordis:** https://cordis.europa.eu/project/id/101094742	Resilient Media for Democracy in the Digital Age (ReMeD) responds to the European Commission's call HORIZON-CL2-2022-DEMOCRACY-01-06: "Media for democracy – democratic media" and will tackle existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. ReMeD could contribute to the identification and sharing of best

		practices for economic sustainability of journalistic media, in the same way project MeDeMAP can. By gathering, analysing, comparing and contrasting data regarding professional journalists, alternative media content producers and citizens which operate in technologically mediated configurations, as well as the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape, ReMeD could, as a biproduct identify trends and qualitative indicators which could help better understand the demand of and thus the sustainability of quality journalistic media.

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

Core theme 4. "Information and Strategic Communication"

- Threat No 4.1. "Media Conundrum"

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

Deliverable	name of the innovation	Short description on the soundness to be tested
3.5	**The Media Pluralism Monitor (MPM) tool**	The Media Pluralism Monitor (MPM) is a tool developed by the Centre for Media Pluralism and Media Freedom (CMPF) of the European University Institute (EUI) to assess the potential weaknesses in national media systems that may hinder media pluralism. Based on 20 indicators, summarizing 200 variables, it covers four areas: 1.Fundamental protection, 2.Market plurality, 3.Political independence, 4.Social inclusiveness. The solution can be used to prevent the deprivation of market shares from quality journalistic media by ensuring that sufficient investment in investigative journalism is not sacrificed in the face of journalistic competitiveness, by identifying and sharing

		best practices for journalistic media economic sustainability. In the context of the vignette, Media outlets, journalists, publishers, broadcasters, editors and other related stakeholders are the end-users of the idea. Media Pluralism Monitor (MPM) assesses the potential weaknesses in national media systems that may hinder media pluralism and covers the areas of fundamental protection, market plurality, political independence and social inclusiveness.
3.9	**Resilient Media for Democracy in the Digital Age (ReMeD) project** https://resilientmedia.eu/	Resilient Media for Democracy in the Digital Age (ReMeD) tackles existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act. In the context of the vignette ReMeD could contribute to the identification and sharing of best practices for economic sustainability of journalistic media.
D3.9	**INJECT Innovative Journalism: Enhanced Creativity Tools -project** https://cordis.europa.eu/project/id/732278	INJECT's objective was to transfer new digital technologies to news organisations to improve the creativity and the productivity of journalists, to increase the competitiveness of European news and media organisations. To achieve this objective, INJECT extended and aggregated new digital services and tools already developed by consortium members to support journalist creativity and efficiency, and integrated the services and tools with

		current CMSs and journalist work tools in order to facilitate their uptake and use in newsrooms. The services undertook new forms of automated creative search on behalf of journalists, using public sources (e.g. social media) and private digital resources (e.g. digital libraries of political cartoons) to generate sources of inspiration for journalists who were seeking new angles on stories. The tools provide new interactive support for journalists to think creatively about new stories and reuse news content in new ways to increase productivity. To transfer the new services and tools to Europe's news and media organisations, INJECT established a new INJECT spin-off business, built up and expanded multiple vibrant ecosystems of providers and users of new digital technologies, and exploited its position at the heart of Europe's journalism industry to raise market awareness and take-up on the services and tools. With respect to Call ICT21, INJECT increased the competitiveness of one of Europe's most important creative industries – journalism - by stimulating ICT innovation in SMEs, by effectively building up and expanding vibrant EU technological ecosystems that met the emerging needs of Europe's new and existing news and media organisations. In the context of the vignette, INJECT could deliver new ideas on ways how small scale media outlets may compete against giant Media outlets and have their news feed also heard by the citizens.

.

6. PROPOSED TRAINING APPROACH

The training under EU-HYBNET project is composed of in-person training and is addressed to different levels of pan-European security practitioners, and keeps an inclusive set up to researchers, academics, civil society and the business community in articulating dilemmas, innovations and responses in relation the scenario and innovations in its entirety. The training approach is about making sure and enticing that participants conserve a comprehensive approach of the problems at hand and consider the insertion of the innovations and research ideas in the overall scheme of the situation.

6.1. METHODOLOGY FOR MEASURING THE TRAINING IMPACT

Experience of training events during 2 previous cycles provide some insights for impact assessment methodology selection:

- Audience attending trainings is very different in their background, knowledge, interest and scope of hybrid threats they are interested or face. It makes it complicated to use traditional assessment tools, that are measuring participants knowledge / skills before the training and after completion of trainings.
- Due to the difference of audience, the expected take-aways are also very different. In some cases this is only about expending knowledge, in some cases generating and gathering new ideas or improvement aspects. For some particular innovations and technicalities are of interest, while others are more keen to asses innovations on a higher level and get to know that such capabilities exists. In addition take-aways are more of long term impact and thus making it difficult to assess directly after the training.
- Experience show that response rate to the evaluation questionnaires send out after the trainings is very low.

Considering all mentioned, the proposed evaluation of the training in general and possible impact can be done in two phases:

- Short feedback during the training using interactive tools (e.g.: Mentimeter) gathering feedback from separate sessions and overall event.
- Post event questionnaire, to ensure continuity and possibilities to compare results, even though response rate can remain low.

Both methods should contain quantitative evaluations (e.g.: scales, marks, etc.) and qualitative questions, reflecting more individualised evaluations. Those can be made using open ended questions, word clouds and other similar methods.

7. CONCLUSIONS

In this document we have described the important aspects for the execution of the exercise and training on the most promising innovations (technical and non-technical) to identified gaps and needs under each one of four core themes of EU HYBNET.

The relevant scenario and eight (8) vignettes that will be used as the backbone of the training have been described. The exercise methodology that is selected is briefly introduced as well as the DTAG tool that will be used for the implementation of the training itself.

In more detail, the current deliverable has presented one background scenario depicting a situation similar to a combination of physical attacks, minorities upset, elections and disinformation / misinformation activities. In order to support the training implementation, the different actors and the relevant organisations that participate in the scenario are also described in order to give a clear picture to the training participants of the general context that the vignettes will be played. Following the above, in section 4.4 six vignettes are introduced, addressing accordingly the four core themes of the EU-HYBNET project (i.e. 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication). Finally, in section 5 the proposed training outline and the methodology for measuring the training impact are briefly introduced.

Overall, the scenario and vignettes design address important challenges in the hybrid threats sphere tackling the identified practitioners needs. Based on these needs the training objectives have been set and the most suitable training format has been chosen. Moreover, the innovations, technical and non -technical ones, have been presented as playing cards in order to identify their importance to the end users in the context of a real-life situation. The innovations testing is in the central of the training in order to learn what are the innovations that may work as solutions to practitioners gaps and needs to counter hybrid threats. The deliverable serves as the first step for the implementation of the training, setting up the training principles and content.

Annex I. References

[1] Andrew N. Liaropoulos (2023), Victory and Virality: War in the Age of Social Media, Georgetown Journal of International Affairs, Volume 24, Number 2, Fall 2023, pp. 198-203 (Article), Published by Johns Hopkins University Press, DOI: https://doi.org/10.1353/gia.2023.a913646

[2] Thomas Zeitzoff, "How Social Media is Changing Conflict," Journal of Conflict Resolution, 61, no. 9 (2017): 1979, https://doi.org /10.1177/0022002717721392.

[3] ENISA THREAT LANDSCAPE 2023, October 2023, ISBN: 978-92-9204-645-3, DOI: 10.2824/782573

[4] Dr. Patrick J. Cullen, Erik Reichborn-Kjennerud, A Multinational Capability Development Campaign project, Understanding Hybrid Warfare, MCDC January 2017

[5] Mikael Wigell (2021) Democratic Deterrence: How to Dissuade Hybrid Interference, The Washington Quarterly, 44:1, 49-67, DOI: 10.1080/0163660X.2021.1893027

Annex II. Glossary and acronyms

Term	Definition / description
EC	European Commission
WP	Work Package
T	Task
AI	Artificial Intelligence
CDA	Cyber Defense Alliance
CDC	Center For Disease Control
CI	Critical Infrastructure
DCU	Digital Crime Unit
DTAG	Disruptive Technology Assessment Game
EU	European Union
ISAC	Information Sharing And Analysis Centers
IT	Information Technology
IoS	Ideas Of Systems
MRI	Magnetic Resonance Imaging
MS	Member States
NGO	Non-Governmental Organisations
PC	Personal Computer
PR	Personal Relation
QR	Quick Response
SOME	Social Media
TPM	Techniques- Processes- Methodologies
TRL	Technology Readiness Level

WHO	World Health Organisation
KEMEA	Kentro Meleton Asfaleias
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
HybridCoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
L3CE	Lithuanian Cyber Crime Center of Excellence for Training, Research and Education
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
JRC	Joint Research Centre - European Commission
ICDS	The International Center for Defence and Security
Espoo	Espoo City and Region in Finland