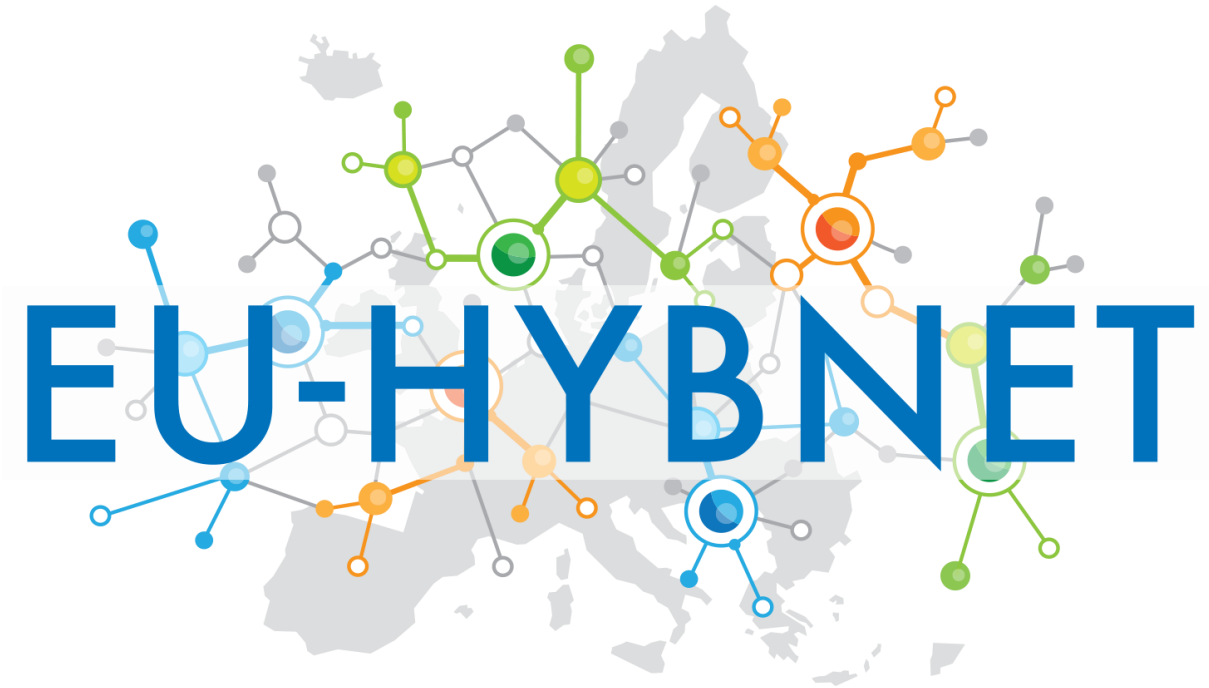

TRAINING AND EXERCICE, SCENARIO DELIVERY

DELIVERABLE 2.18

Lead Author: KEMEA

Contributors: HybridCoE, LAUREA, Satways, URJC
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

D2.18 TRAINING AND EXERCISE, SCENARIO DELIVERY

Deliverable number	**D2.18**	
Version:	**1.0**	
Delivery date:	**31/7/2022**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**First Version**	
Nature:	**Public Report**	
Main author:	**Athanasios Kosmopoulos, Vanessa Papakosta**	**KEMEA**
	Päivi Mattila, Jari Räsänen, Tiina Haapanen	**Laurea**
	Alex Koniaris	**KEMEA**
	Maxime Lebrun, Maria Soukkio	**Hybrid CoE**
	Edmundas Piersarskas, Evaldas Bruze	**L3CE**
	Rubén Arcos	**URJC**
	Souzanna Sofou	**Satways**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	29-05-2022	KEMEA/ Vanessa Papakosta	Table of Contents
0.2	30-05-2022	KEMEA/Athanasios Kosmopoulos	Scenario outline
0.3	04-07-2022	KEMEA/Athanasios Kosmopoulos, Vanessa Papakosta	Scenario updated
0.4	13-07-2022	KEMEA/ Vanessa Papakosta	Scenario updated
0.5	19-07-2022	Laurea/ Päivi Mattila	Text editing and describing how innovations link to the scenario and vignettes
0.6	20-07-2022	Laurea/ Päivi Mattila	Text editing and structure to describe innovations to be tested
0.7	21-07-2022	KEMEA/ Vanessa Papakosta	Describe innovations to be tested
0.71	22-07-2022	Laurea/ Jari Räsänen	Describe innovations to be tested
0.72	22-07-2022	Laurea/ Päivi Mattila	Describe innovations to be tested
0.73	23-07-2022	KEMEA/ Alexios Koniaris	Describe innovations to be tested
0.8	25-07-2022	Laurea/ Päivi Mattila	Text editing
0.9	26-07-2022	KEMEA/ Vanessa Papakosta	Text editing
0.91	28-07-2022	HCoE/ Maria Soukkio	Review/ Comments
0.92	28-07-2022	KEMEA/ Vanessa Papakosta, Athanasios Kosmopoulos	Text editing

0.93	29-07-2022	STWS/Souzanna Sofou	Review
0.94	29-07-2022	URJC/Rubén Arcos	Review
0.95	29-07-2022	KEMEA/ Vanessa Papakosta	Final text editing
1.0	31-07-2022	Päivi Mattila/ Laurea	Final review and document submission 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 European Commission (EC) Horizon2020 funded "Empowering a pan-European Network to Counter Hybrid Threats" (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 D3.4-*Second Report on Improvements and Innovation* and D3.8- *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 T2.4 – *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:

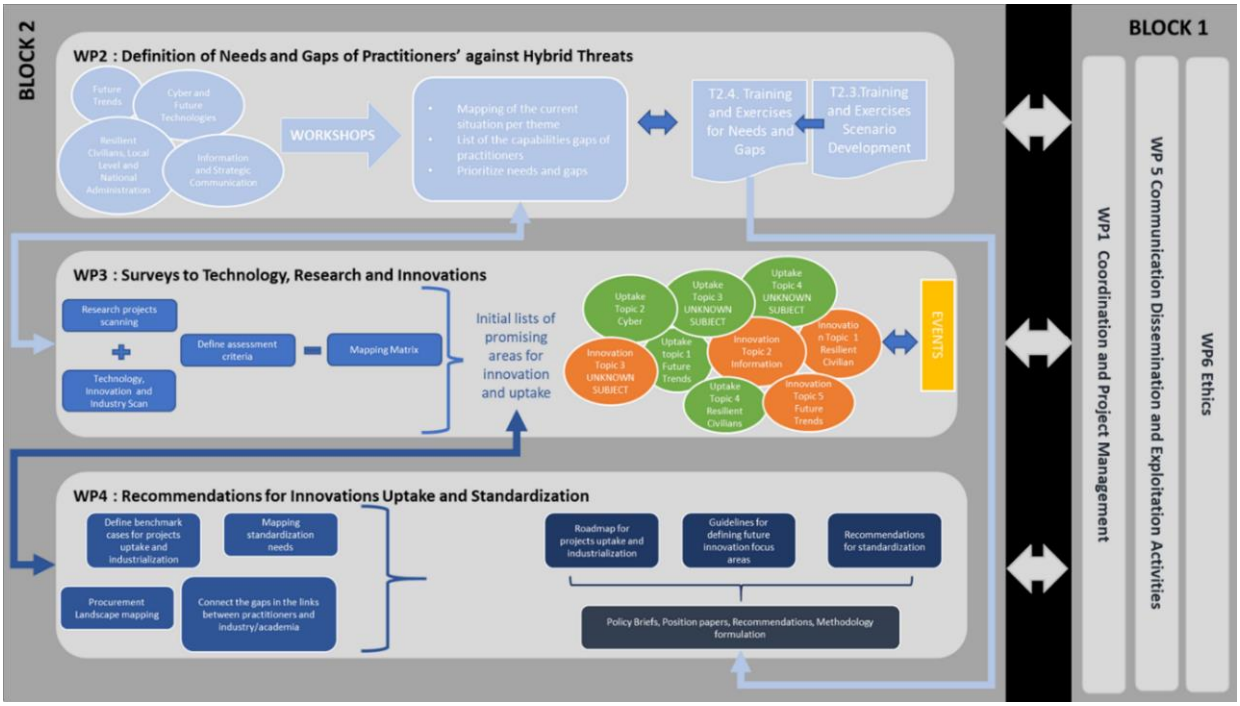

Figure1: EU-HYBNET structure of Work Packages and Main Activities

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, D2.18 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 D2.18 does not directly deliver results to certain EU-HYBNET project objectives (OB), still D2.18 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 andtake 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 table top 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 to give the reader a better overview of the rational of the training. The section also describes the training who will be the audience.

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 and represents the scenario vignettes as well as information regarding the actors and the situational setup.

Section 5 describes the connection between the vignettes and identified gaps and needs to counter Hybrid Threats under each of EU-HYBNET Four Core Themes. This will follow description of identified promising innovations to the gaps and needs under each of the Four Core Themes that will be tested during 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

Section 8 recommends the future work that needs to be done until the actual implementation of the training.

2. TRAINING METHODOLOGY

2.1 METHODOLOGY

In the context of EU-HYBNET training, the war gaming approach was chosen. A war game 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 and to test courses of action. Many war games 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 war games for naval and air combat as well.

War gaming 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 war gaming 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 'war gaming'. 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 war game players, not contained in the NATO definition, leads to the working definition of war gaming 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.

[5]https://nso.nato.int/natoterm/Web.mvc
[6]Development, Concepts and Doctrine Centre (DCDC), RedTeaming Guide, 2nd Edition, 2013, Lexicon.

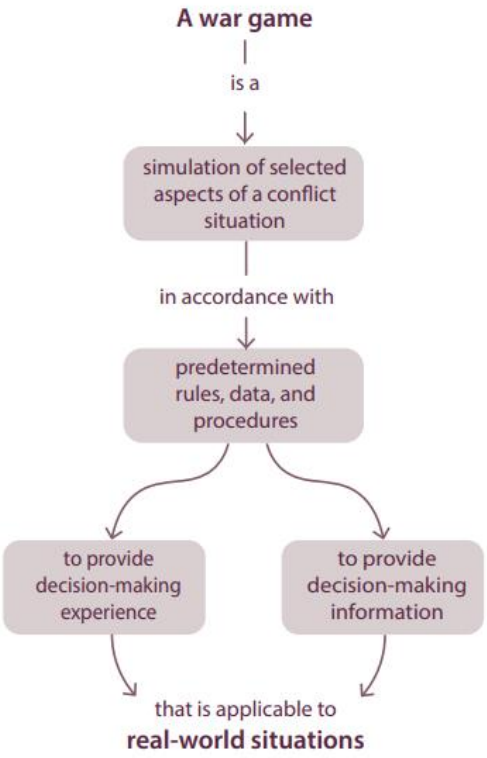

Figure 2The general purposes of war games[7]

In this context, a war game, 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. War games 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 war games 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') war games 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.

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

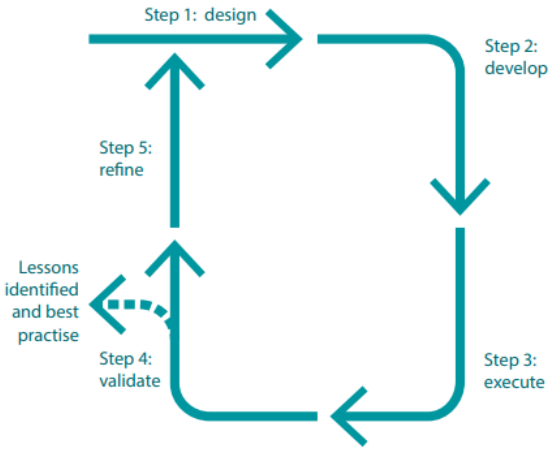

Figure 3Wargame training process[8]

The stepwise approach that needs to be followed for the implementation of the first step i.e. the design of the war game 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 different level of participants will be addressed and the proposed training approach that will be held. (section 5)

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

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.

2.2 TRAINING AUDIENCE

The EU-HYBNET training and exercise event is arranged by EU-HYBNET Task2.4 "Training and Exercises for Needs and Gaps" (L3CE) according to the training methodology and scenario created by T2.3 "Training and Exercises Scenario Development" (KEMEA). According to the EU-HYBNET Description of Action (DoA)/T2.3 the training audience will be the same as in T2.1 "Needs and Gaps Analysis in Knowledge and Performance" (Hybrid CoE) that means new EU-HYBNET network members who joined joined the T2.1 event alike EU-HYBNET consortium partners and stakeholder Group members. The

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

training participants represent mainly pan-European security practitioners next representatives coming from relevant NGOs, industry and SMEs and academia. Because the EU-HYBNET consortium includes 14 EU Members States (MS) and Norway and the EU-HYBNET Network includes also other EU MSs and Third Countries (e.g. Ukraine, Georgia), the training audience is to be pan-European wide.

3. EU-HYBNET EXERCISE OVERVIEW

3.1. AIM OF THE EXERCISE&OBJECTIVES

The aim of the EU-HYBNET training& exercise event 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 in WP2 "Gaps and Needs of European Actors against Hybrid Threats"/ T2.1 "Needs and Gaps Analysis in Knowledge and Performance" (D2.6. "Long list of defined gaps and needs") and T2.2 "Research to Support Increase of Knowledge and Performance" (D2.10 "Deeper analysis, delivery of short list of gaps and needs"). The EU-HYBNET training event is to test how identified innovations to EU-HYBNET gaps and needs would support pan-European security practitioners to counter Hybrid Threats, the identified gaps and needs. The scenario depicts various organisations that form a system in crisis confronted to a set of external actors. In this context, the participants will test a series of innovations 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"), whether technical and non-technical/social innovations and solutions are to support pan-European security practitioners and other relevant actors to counter hybrid threats to counter the challenge they face.

3.2. DTAG

The EU-HYBNET training and exercise event is arranged by EU-HYBNET Task2.4 "Training and Exercises for Needs and Gaps" (lead L3CE) and plan is to use a game called DTAG alike during the first EU-HYBNET training event. However, it has been under discussion, if Poseidon training platform from JRC could be used in the future.

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 WP3 T3.2/D3.4 "First mid-term report Improvement and innovations" and T3.3/D3.8 "First mid-term report Innovation and Research monitoring"), or so-called Ideas of Systems (IoSs) as described in WP3 (D3.4 and D3.8) 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.

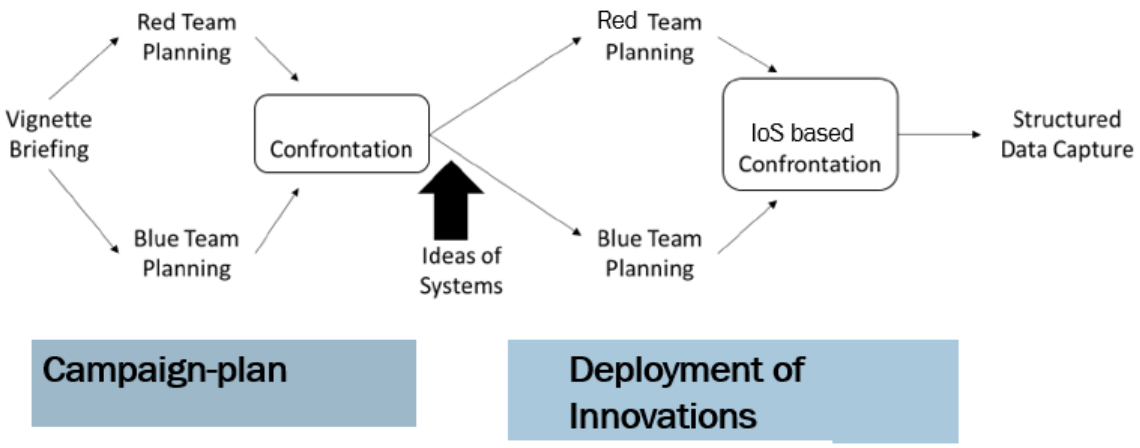

Figure4: DTAG concept

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.

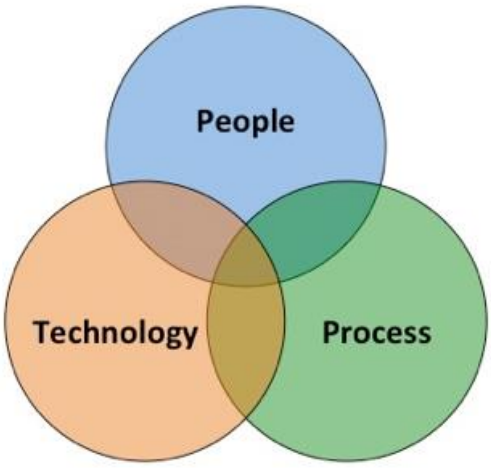

Figure 5Methodological Framework of people-processes- technology

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 scenario and its' vignettes should include the different views of the stakeholders, pan-European security practioners, 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 practioners' 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. The scenario and vignettes descriptions are 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) so that the innovations identified to counter the gaps and needs in under each of the Four Core Themes can be tested. This support EU-HYBNET to deliver recommendations of most promising innovations to counter Hybrid Threats as identified in EU-HYBNET gaps and needs analysis.

4.1. MAIN ACTORS

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".

4.2. SITUATIONAL SETUP

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.

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. 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.
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.
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.
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.
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.
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.
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.
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.

4.5. SCENARION 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 2nd EU-HYBNET training event (September 2022 in Vilnus, Lithuania). The goal of the training and exercises is to test identified promising innovations to EU-HYBNET 2nd project cycle (M18-M34/ Oct 2021 – Feb 2023) 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/D3.4 "First mid-term report Improvement and innovations" and T3.3/D3.8 "First 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 2nd project cycle specific gaps& needs to counter hybrid threats; the gaps and needs definition is deriving from EU-HYBNET deliverable D2.10. The Gaps and needs are mentioned as primary contexts.

Vignette 1. *Gas Flow to Bhic is paused after a Sharn Energy ministerial decision to shut down the gas pipeline was announced. Speculation that the Federation is behind this decision is strong.*

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

- Primary context/ G&N No 3.2 "Exploitation of critical infrastructure weaknesses and economic dependencies"
- Primary context/ G&N No 3.3 "Exploitation or investment in companies by foreign actors"

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.

Core theme 4: "Information and Strategic Communication"

- Primary context/ G&N No 4.1 "Information manipulation with the aim of destabilization"
- Primary context/ G&N No 4.2 "Foreign interference in key information institutions"

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.3. "Rise of populism"

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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"
- Primary context/ G&N No 2.3 "Disruptive innovation"

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

- Primary context/ G&N No 3.2 "Exploitation of critical infrastructure weaknesses and economic dependencies"

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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.1 "Space interference and counterspace weapons"

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.

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

Primary context/ G&N No 3.1 "Exploitation of existing political cleavages"

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.1. "Geopolitical heavyweight of domestic policy"

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.

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.2 "Digital escalation and AI-based exploitation"

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 “Offensive cyber capabilities”

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

- Primary context/ G&N No 3.1 “Exploitation of existing political cleavages”

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.

Core theme 4: “Information and Strategic Communication”

- Primary context/ G&N No 4.1 **“**Information manipulation with the aim of destabilization”
- Primary context/ G&N No 4.2 “Foreign interference in key information institutions”
- Primary context/ G&N No 4.3 “Promoted ideological extremism and violence

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

- Primary context/ G&N No 3.3 “Exploitation or investment in companies by foreign actors”

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.

Core theme 4: “Information and Strategic Communication”

- Primary context/ G&N No 4.1 **“**Information manipulation with the aim of destabilization”

Core theme 2: “Cyber and Future Technologies”

- Primary context/ G&N No 2.2 “Offensive cyber capabilities”

Core theme 1: “Future Trends of Hybrid Threats”

- Primary context/ G&N No 1.1. “Geopolitical heavyweight of domestic policy”

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

- Primary context/ G&N No 3.3 “Exploitation or investment in companies by foreign actors”

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/D3.4 and T3.3/D3.8 under the named Core Theme.

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.

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.3. "Rise of populism"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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")**[1] , duration : 1/8/2015-31/5/2021, GA No.638514 [1] https://cordis.europa.eu/article/id/434332-algorithms-are-reshaping-our-newsreading-habits-should-we-worry	No specific technologies were developed during this project but methodological approaches. EU-HYBNET training could focus PersoNews recommender models explained in a PersoNews' publication "On the Democratic Role of News Recommenders"[1]. 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 [1] https://www.tandfonline.com/doi/full/10.1080/21670811.2019.1623700

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.

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.1. "Geopolitical heavyweight of domestic policy"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

No. 1.1 Geopolitical heavyweight of domestic policy		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience**	How the innovation could improve the resilience in a situation where the country faces unexpectedly and unprepared a huge influx of refugees. **Practitioners in focus:** border and coast guards, authorities and ministries respsonsible for internal and external security and foreign affairs.
3.8	**Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)** EC funded H2020 project, duration : 3/2018-5/May 2021.[1] [1] https://cordis.europa.eu/project/id/769886/reporting	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.

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.2 "Digital escalation and AI-based exploitation"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

No. 1.2 Digital escalation and AI-based exploitation		
Deliverable	name of the innovation	Short description on the soundness to be tested
3.4	**N/A**	
3.8	**Concordia**, EC funded H2020 project.[1] [1] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-04-Reseach-and-Innovation.pdf	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.

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.

Core theme 1: "Future Trends of Hybrid Threats"

- Primary context/ G&N No 1.1. "Geopolitical heavyweight of domestic policy"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

No. 1.1 Geopolitical heavyweight of domestic policy		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**

3.4	**Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience**	How the innovation could improve the resilience in a situation where the country faces unexpectedly and unprepared a huge influx of refugees **Practitioners in focus:** border and coast guards, civil protection and first responders, authorities and ministries respsonsible for internal and external security and foreign affairs.
3.8	**Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)** EC funded H2020 project, duration : 3/2018-5/May 2021.[1] [1] https://cordis.europa.eu/project/id/769886/reporting	The project may be discussed under this vignette but the solution might not be able to deliver most sound solution to the challenge in question. 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 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.

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 "Cyber and Future Technologies" and the promising innovations to be tested as identified in WP3 T3.2/D3.4 and T3.3/D3.8 under the named Core Theme.

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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"
- Primary context/ G&N No 2.3 "Disruptive innovation"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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-defense products that use artificial

		intelligence to detect and even respond to emerging attacks are required. This type of solution is technical. **Practitioners 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)[1], which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021. [1] https://cordis.europa.eu/project/id/844129	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 to be tested in the training event according to D3.4 and D3.8 are following:

No. 2.3 Disruptive Innovations		
Deliverable	**name of the innovation**	**Short description on the soundness to be tested**
3.4	**The Development of a Deepfake 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 sollution is technical. **Practitioners in focus:** Cyber security authorities, intelligence, LEAs.
3.8	**INtelligent Security and Pervasive tRust for 5G and Beyond (INSPIRE-5Gplus)**[1] [1] https://cordis.europa.eu/project/id/871808	**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)[1] [1] https://cordis.europa.eu/project/id/101020788	**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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.1 “Space interference and counterspace weapons”

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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)[1]. This project was funded under FP7-Security in the period from 01.05.2014 to 31.10.2017. [1] https://cordis.europa.eu/project/id/607679	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[1].** This project was funded under H2020 in the period from 2020 to 2022. [1] https://www.7shield.eu/project/	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. The 7SHIELD project is also identified to deliver a promising solution to the named gaps & needs in EU-HYBNET Task 3.2 "Technology and Innovations Watch" deliverable 3.4 (submission DL M24/ April 2022), and hence more detailed description of the usability of the 7SHILED solutions in D3.4 **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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are the same as in vignette 6., see text in following sub-chapter below.

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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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 defense? 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)[1], which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021. [1] https://cordis.europa.eu/project/id/844129	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.

Core theme 2: "Cyber and Future Technologies"

- Primary context/ G&N No 2.2 "Offensive cyber capabilities"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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 defense? 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)[1], which is funded under EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions, from 01.07.2019 to 19.09.2021. [1] https://cordis.europa.eu/project/id/844129	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.

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

This sub-chapter presented how The EU-HYBNET training scenario vignettes are linked to EU-HYBNET Four Core Theme "Resilient Civilians, Local Level, National Administration" and the promising innovations to be tested as identified in WP3 T3.2/D3.4 and T3.3/D3.8 under the named Core Theme.

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.*

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

- Primary context/ G&N No 3.2 "Exploitation of critical infrastructure weaknesses and economic dependencies"
- Primary context/ G&N No 3.3 "Exploitation or investment in companies by foreign actors"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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**	This idea discusses a decision support approach for CI risk assessment with a holistic consideration of complexity, dual interdependency, vulnerability, and

	complex interdependent scenario	uncertainty. It is based on a paper by Weilan et al, 2019[9] and on the Critical Infrastructure Resilience Platform (CIRP) [10] 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 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

[9] 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).
[10] 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

		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)** [1] duration : 06/10/2021-30/10/2023, GA No. 101021668 [1] https://www.precinct.info/	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 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 to be tested in the training event according to D3.4 and D3.8 are following:

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.
3.8	Searches in the Cordis database concerning projects focusing on investments in general, and foreign direct investments (FDI) in particular, brought dozens of results (Collection: Projects, Domain of Application	A potential reason for such a shortage or lack of relevant research projects is most likely the EU's recently adopted investment screening mechanism. The mechanism has been in force only since October 2020 and experiences of its functioning are still preliminary. Yet, based on the initial conclusions from the EU's FDI screening[11], it is clear that EU should make further adjustments to extend the coverage of its screening mechanism to all Member States and to develop mechanisms for advanced cross border risk assessment. This might entail, for example, tools for tracking actions of foreign companies in different Member States or

[11] Ghiretti (2021), Screening foreign investment in the EU – the first year (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); First Annual Report on the screening of foreign direct investments into the Union. COM(2021) 714 final.

	Security/Society, Programme: H2020, Search term: investment), but none of them was relevant for EU-HYBNET purposes.	a platform for information sharing between the Member States. Recent research has included comparisons of different territorial or national FDI screening mechanisms.[12] These papers have shown the major similarities and differences between the regulatory systems. The findings would be beneficial for at least two different applications. First, they can be used for benchmarking. Alternatively, they provide food for thought for potential cross-border or even globalized risk assessment frameworks.

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.

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

- Primary context/ G&N No 3.2 "Exploitation of critical infrastructure weaknesses and economic dependencies"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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[13] and on the Critical Infrastructure Resilience Platform (CIRP) [14] developed by Satways Ltd.The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment. The essential elements for impact

[12] Chan, Z.T., Meunier, S. (2021). Behind the screen: Understanding national support for a foreign investment screening mechanism in the European Union. The Review of International Organizations.; Ghiretti, F. (2021). Screening foreign investment in the EU – the first year. (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); Jacobs, J. (2019). Tiptoeing the Line Between National Security and Protectionism: A Comparative Approach to Foreign Direct Investment Screening in the United States and European Union. International Journal of Legal Information, 47(2), 105-117; Rajavuori, M., & Huhta, K. (2020). Investment screening: Implications for the energy sector and energy security. Energy Policy, 144, 111646.

[13] 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).

[14] 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

		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 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 Cyberphysical Threats and effects with a focus on district or regional protection (PRECINCT)** [1][2] duration : 06/10/2021-30/10/2023, GA No. 101021668 [1] https://www.precinct.info/ [2] https://cordis.europa.eu/project/id/101021668	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 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.

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

Primary context/ G&N No 3.1 "Exploitation of existing political cleavages"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following :

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)** [1] [2] duration : 01/12/2018 – 30/11/2021 GA No. 825297 [1] https://weverify.eu/about/ [2] https://cordis.europa.eu/project/id/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.

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

- Primary context/ G&N No 3.1 "Exploitation of existing political cleavages"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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)** [1] [2] duration : 01/12/2018 – 30/11/2021 GA No. 825297 [1] https://weverify.eu/about/ [2] https://cordis.europa.eu/project/id/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.

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

- Primary context/ G&N No 3.3 "Exploitation or investment in companies by foreign actors"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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.
3.8	Searches in the Cordis database concerning projects focusing on investments in general, and foreign direct investments (FDI) in particular,	A potential reason for such a shortage or lack of relevant research projects is most likely the EU's recently adopted investment screening mechanism. The mechanism has been in force only since October 2020 and experiences of its functioning are still preliminary. Yet, based on the initial

	brought dozens of results (Collection: Projects, Domain of Application Security/Society, Programme: H2020, Search term: investment), but none of them was relevant for EU-HYBNET purposes.	conclusions from the EU's FDI screening[15], it is clear that EU should make further adjustments to extend the coverage of its screening mechanism to all Member States and to develop mechanisms for advanced cross border risk assessment. This might entail, for example, tools for tracking actions of foreign companies in different Member States or a platform for information sharing between the Member States. Recent research has included comparisons of different territorial or national FDI screening mechanisms.[16] These papers have shown the major similarities and differences between the regulatory systems. The findings would be beneficial for at least two different applications. First, they can be used for benchmarking. Alternatively, they provide food for thought for potential cross-border or even globalized risk assessment frameworks.

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.

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

- Primary context/ G&N No 3.3 "Exploitation or investment in companies by foreign actors"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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

[15] Ghiretti (2021), Screening foreign investment in the EU – the first year (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); First Annual Report on the screening of foreign direct investments into the Union. COM(2021) 714 final.

[16] Chan, Z.T., Meunier, S. (2021). Behind the screen: Understanding national support for a foreign investment screening mechanism in the European Union. The Review of International Organizations.; Ghiretti, F. (2021). Screening foreign investment in the EU – the first year. (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); Jacobs, J. (2019). Tiptoeing the Line Between National Security and Protectionism: A Comparative Approach to Foreign Direct Investment Screening in the United States and European Union. International Journal of Legal Information, 47(2), 105-117; Rajavuori, M., & Huhta, K. (2020). Investment screening: Implications for the energy sector and energy security. Energy Policy, 144, 111646.

		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.
3.8	Searches in the Cordis database concerning projects focusing on investments in general, and foreign direct investments (FDI) in particular, brought dozens of results (Collection: Projects, Domain of Application Security/Society, Programme: H2020, Search term: investment), but none of them was relevant for EU-HYBNET purposes.	A potential reason for such a shortage or lack of relevant research projects is most likely the EU's recently adopted investment screening mechanism. The mechanism has been in force only since October 2020 and experiences of its functioning are still preliminary. Yet, based on the initial conclusions from the EU's FDI screening[17], it is clear that EU should make further adjustments to extend the coverage of its screening mechanism to all Member States and to develop mechanisms for advanced cross border risk assessment. This might entail, for example, tools for tracking actions of foreign companies in different Member States or a platform for information sharing between the Member States. Recent research has included comparisons of different territorial or national FDI screening mechanisms.[18] These papers have shown the major similarities and differences between the regulatory systems. The findings would be beneficial for at least two different applications. First, they can be used for benchmarking. Alternatively, they provide food for thought for potential cross-border or even globalized risk assessment frameworks. **Practitioners in focus:** Intelligence, LEAs, Border Guard.

[17] Ghiretti (2021), Screening foreign investment in the EU – the first year (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); First Annual Report on the screening of foreign direct investments into the Union. COM(2021) 714 final.

[18] Chan, Z.T., Meunier, S. (2021). Behind the screen: Understanding national support for a foreign investment screening mechanism in the European Union. The Review of International Organizations.; Ghiretti, F. (2021). Screening foreign investment in the EU – the first year. (https://merics.org/en/short-analysis/screening-foreign-investment-eu-first-year); Jacobs, J. (2019). Tiptoeing the Line Between National Security and Protectionism: A Comparative Approach to Foreign Direct Investment Screening in the United States and European Union. International Journal of Legal Information, 47(2), 105-117; Rajavuori, M., & Huhta, K. (2020). Investment screening: Implications for the energy sector and energy security. Energy Policy, 144, 111646.

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 "Information and Strategic Communication" and the promising innovations to be tested as identified in WP3 T3.2/D3.4 and T3.3/D3.8 under the named Core Theme.

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.

Core theme 4: "Information and Strategic Communication"

- Primary context/ G&N No 4.1 "Information manipulation with the aim of destabilization"
- Primary context/ G&N No 4.2 "Foreign interference in key information institutions"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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.[1] [1] https://cordis.europa.eu/project/id/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 to be tested in the training event according to D3.4 and D3.8 are following:

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 : 11/2019 – 12/2024.[1] [1] https://cordis.europa.eu/project/id/819025	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.

Core theme 4: "Information and Strategic Communication"

- Primary context/ G&N No 4.1 "Information manipulation with the aim of destabilization"
- Primary context/ G&N No 4.2 "Foreign interference in key information institutions"
- Primary context/ G&N No 4.3 "Promoted ideological extremism and violence"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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.**[1]** [1] http://dlearn.eu/projects/online-and-offline-security/open-your-eyes/	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 to be tested in the training event according to D3.4 and D3.8 are following:

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.[1] [1] https://cordis.europa.eu/project/id/648311	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 to be tested in the training event according to D3.4 and D3.8 are following:

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. Duration: 10/2021 – 10/2024. GA No. 101020574.[1] [1] https://cordis.europa.eu/project/id/101020574	ALIGNER, is dedicated to broader set of technologies for law enforcement and policing. It aims to jointly identify and 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.

Core theme 4: "Information and Strategic Communication"

- Primary context/ G&N No 4.1 "Information manipulation with the aim of destabilization"

Proposed innovations to be tested in the training event according to D3.4 and D3.8 are following:

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.
3.8	n/a	n/a

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.

Participants should consider and discuss over *inter alia*:

- underlying implications at national, regional and local levels of each inject and their relations to each others:
- key policy challenges, response dilemmas, potential counterproductive reactions;
- Applicability and desirability of the various innovations summarily presented from WP3/ T3.2 and T3.2.

6.1. METHODOLOGY FOR MEASURING THE TRAINING IMPACT

Impact assessment of training can be a tool that gathers and organizes information so that firm inferences are drawn and decisions are made to reinforce the impact of the training on day-to-day work behaviour and attitudes of the personnel. The assessment process uses personal interviews and questionnaires to see whether training has produced a desired effect.

The proposed methodology is to conduct a Summative Evaluation. Some of the steps to conduct a summative evaluation are

- Testing trainees on how well they grasped the information provided
- Asking trainees for their opinion about the training program after it has been delivered
- Measuring changes in production and quality of work that has been accomplished post-training
- Conducting surveys or interviews with each trainer to gain a better understanding of what they learned

From the **quantitative point of view** questionnaires can be used after the completion of the exercise. Post-activity questionnaires generally consist of a limited number of questions that ask participants to rate the effectiveness of various aspects of the activity (eg. exercise). The focus of the questions should reflect the key evaluation questions and the related monitoring questions that we have identified in our plan.

Post-activity questionnaires tend to be short in order to reduce the amount of time respondents need to complete them, and therefore increase the response rate. Questions tend to be quantitative and generally consist of close-ended questions (tick the box, or scales). We can also include open-ended questions but it is best to limit these in order to make data analysis and reporting easier.

From the **qualitative point of view** Focus Group sessions may be applied. A focus group is where a group of people (from around 4 to 12) are asked questions about their experiences and opinions on particular topics. Focus groups use a facilitator and a semi-structured interview process to prompt discussion amongst a group of people. The group can be representative of the target group, or they may represent subsets of the target group if we are looking to identify how different groups have experienced a certain intervention. Focus groups can be used in a self-contained manner for the purposes of exploring new initiatives or for understanding participant's own perspectives on an exercise.

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 energy crisis, migration crisis, 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 eight 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.

8. FUTURE WORK

This deliverable plans the training scenarios and eventually the training activities where the most promising innovation to the identified gaps and needs will be tested. The work performed in D2.18 is of high importance in the project's proceeding and will feed information to T2.4 "Training and Exercises for Needs and Gaps". In particular, this training/knowledge exchange event is relevant to all in EU-HYBNET Network and will take place in M29 (Sept 2022), with its results reported in the relevant D2.21 "Training and exercises Delivery on up-to-date topics" (L3CE). It is important to highlight here that the final scenarios and vignettes can be refined in T2.4 in order to better serve the training needs that will occur in the future.

These changes will be introduced in D2.27 "*Training and Exercises Scenario and Training Material*" (KEMEA, M34/Feb 2023). More specifically, training material will be selected based on the vignettes mentioned in this deliverables.

Following the implementation of the EU-HYBNET training in T2.4 the project is to identify which innovations are important for the end users, especially pan-European security practitioners. This will be fed to EU-HYBNET Task 3.1 "Definition of Target Areas for Improvements and Innovations" (TNO) and WP4 "Recommendations for Innovations Uptake and Standardization" Tasks (KEMEA, RISE, PPHS, Hybrid CoE). With reference to this D2.24 "Training and Exercises Lessons Learned Report" (Hybrid CoE, M31/ Nov 2022) is important to T3.1 and WP4 also because it delivers evaluation results on training itself and the innovations that are seen most promising for innovation uptake.

Lastly, the importance of D2.18 to the future project's work is that the implementation of the training activities under the scenarios developed in T2.3 will provide input to the next cycle of the identification of new Gaps and Needs under the scope of T2.1. Moreover, and since several new needs may arise in the following cycles of the project, the scenarios will be developed with the overall goal to serve these needs against hybrid threats and taking into account the four core themes as well. In addition, these specific scenarios will include elements required to test innovative solutions related to T3.2 and T3.3 serve for the training and exercises arranged in the in the following cycles of EU-HYBNET respectively.

Annex I. References

[1] https://www.hybridcoe.fi/training-and-exercise/

[2] https://www.nato.int/cps/en/natohq/topics_156338.htm

[3] https://www.friendsofeurope.org/events/europe-in-2030-boosting-public-private-cooperation-in-hybrid-crises/

[4] https://euhybnet.eu/wp-content/uploads/2021/06/Conceptual-Framework-Hybrid-Threats-HCoE-JRC.pdf

[5] EUvsDisinfo, available here: https://euvsdisinfo.eu/about/

Annex II. Glossary and acronyms

Term	Definition / description
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
NL MoD	Ministry of Defence in Netherlands
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
PPHS	Polish Platform for Homeland Security
Laurea	Laurea University of Applied Sciences, EU-HYBNET coordinator
URJC	University of Rey Juan Carlos
UiT	Universitetet i Tromsoe, Artic University in Norway