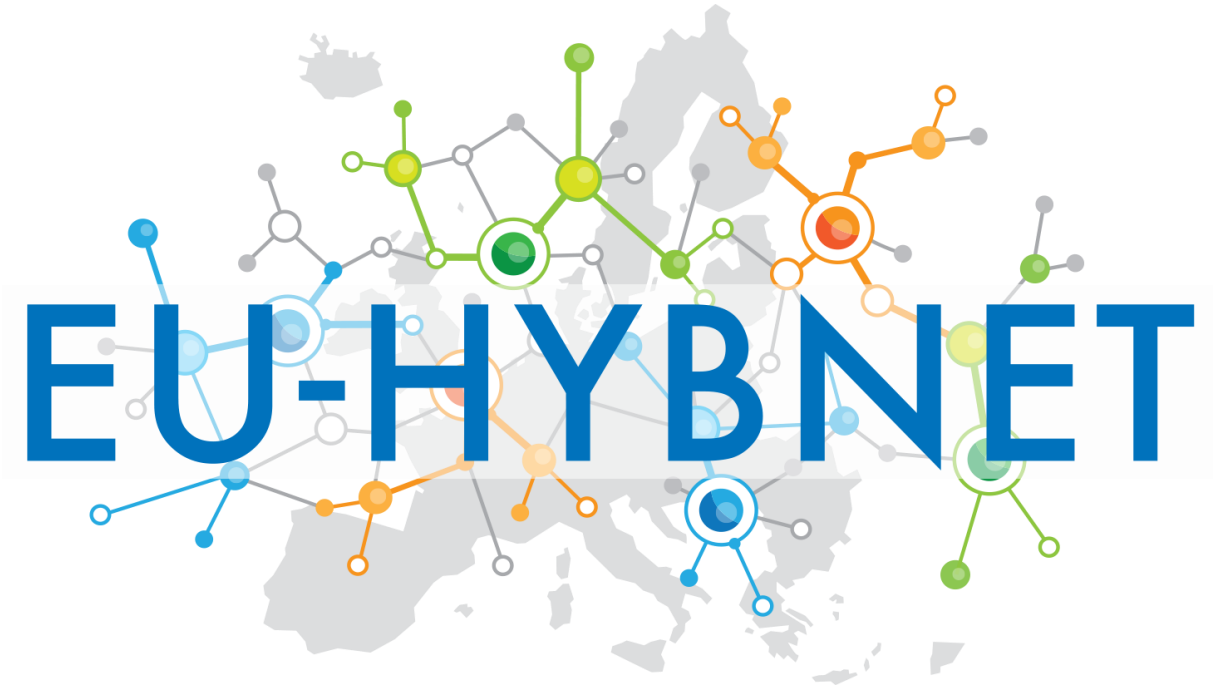


TRAINING AND EXERCISES DELIVERY ON UP-TO-DATE TOPICS

DELIVERABLE 2.21

Lead Author: L3CE
Contributors: UiT, URJC
Deliverable classification: Public (PU)

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

D2.21 TRAINING AND EXERCISES DELIVERY ON UP-TO-DATE TOPICS

Deliverable number	**2.21**	
Version:	**1.0**	
Delivery date:	**27/10/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Edmundas Piesarskas**	**L3CE**
Contributors:	**Marc Lanteigne** **Rubén Arcos Martín** **Evaldas Bruze** **Egidija Veršinskienė** **Valentin Stoian-Iordache** **Päivi Mattila**	**UiT** **URJC** **L3CE** **L3CE** **MVNIA** **Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	2022.10.03	Edmundas Piesarskas / L3CE	Structure provided
0.2	2022.10.07	Edmundas Piesarskas / L3CE	First draft
0.3	2022.10.14	Marc Lanteigne/ UiT	Inputs as Core Theme group moderators provided
0.4	2022.10.18	Edmundas Piesarskas / L3CE	Summery of evaluation survey included
0.5	2022.10.24	Rubén Arcos Martín / URJC Evaldas Bružė / L3CE	Inputs as Core Theme group moderators provided
0.6	2022.10.26	Edmundas Piesarskas / L3CE	Final version for review
0.7	2022.10.26	Päivi Mattila / Laurea	PM review and comments provided
0.8	2022.10.27	Valentin Stoian-Iordache /MVNIA	Review provided
0.9	2022.10.27	Edmundas Piesarskas / L3CE	Corrections after review. Document ready for submission.
1.0	2022.10.27	Päivi Mattila/ Laurea	Document submitted to the EC

DISCLAIMER

TABLE OF CONTENT

TABLES

FIGURES

EXECUTIVE SUMMARY

The purpose of this deliverables (D2.21) is to provide key insights regarding the main findings resulting from the "Empowering a Pan-European Network to Countering Hybrid Threats" (EU-HYBNET) project training effort, to provide a summary of training results and outcomes, as well as to identify improvements that could be incorporated into the next set of iterations of the Training and Exercises for the entire EU-HYBNET community. The EU-HYBNET training is the main activity in EU-HYBNET Project Task (T) 2.4 "*Training and Exercises for Needs and Gaps*".

The second EU-HYBNET training event was arranged in the Project month (M) 29 (29-30 September 2022, Vilnius). Event was organised as two days event of a hybrid format.

The report is structured to address two key aspects of the training initiative and aims to:

- Assess and evaluate the current training iteration.
- Serve as input to follow-on activities within Work Package 4.

At the same time, it summarises the reflections of participants, considering their feedback, insights, and provides a valuable overview of the overall EU-HYBNET training and exercise activity model.

Significantly, the EU-HYBNET Training concept is based on the reuse and adoption of existing training programs, resources, and knowledge within the different European Union Member States (EU MS) and the EU-HYBNET network. However, to avoid delivery of overlapping trainings, scenarios and materials, T2.4 executed a survey to identify relevant materials available among project partners and network members.

DTAG methodology developed by EU-HYBNET partner's, TNO's was adjusted to EU-HYBNET Core Themes approach and successfully implemented during the 1st Training and Exercise event. The decision to use DTAG game was done in EU-HYBNET T2.3 "Training and Exercises Scenario Development" that also delivered frames to the EU-HYBNET training methodology and training scenario and the Vignette descriptions. The 1st Training and Exercise event results demonstrated that DTAG was well accepted by participants, who rated the experience as either good or excellent. Some of the participants expressed a desire to participate in the next round of the training and were willing to recommend the training to their colleagues.

While designing the 2nd Training we analysed 1st post event evaluation results and recommendations provided by the training participants that helped us more precisely determine how to improve the DTAG methodology by making it more acceptable to the wider auditorium of stakeholders.

Several key recommendations made by participants of the 1st training event were:

- Desire to arrange the training on site instead of running it online.
- Limiting the complexity of both the Scenario and the Vignettes.
- Consider that innovation providers are invited to introduce their solutions and to demonstrate innovations value and role in the Hybrid Threats landscape in the next EU-HYBNET training event.
- Demonstrate an architecture that would define the place individual innovations held within a larger picture.
- Inclusion of competent Moderators into the training process should be continued.

All the above mentioned recommendations have been considered and implemented during the second cycle of Training event.

The registration process demonstrated the high and balanced interest in all Core Themes. In total 60 participants registered to the Training event among them.

22 participants physically attended the class others could follow the Training as it was streamed. All technical issues have been solved before the Training event therefore, all sessions have been synchronised ensuring that the break-out sessions, live innovations presentations and discussions ran without significant technical issues and same quality for participants in the class and online.

Besides the main objective of the Training to create and/or strengthen the capacities of European practitioners, industry, SME and academic actors to counter Hybrid Threats, Event should also provide inputs to innovation further innovations uptake process (WP4) and inputs to next cycle in a form of lessons learned.

Innovations that received highest priority ranking during the event are:

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

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

The evaluation results revealed that some organizational improvements still must be considered planning the final cycle. Relevance of current recommendations should be reconsidered as different methodological approach can be used during the 3rd cycle. Main recommendations from current Event include:

- Most of suggestions for improvement were related to Scenario. Balancing of the scenario presenting the complexity and making it simple to understand, interpret and apply should be considered for the up-coming cycle.
- Participants were lacking explicit descriptions of the innovations in order effectively understand the innovation's potential and its future uptake possibilities. This was improved by having 3 innovations presented live and having methodology of innovations in use presentation. But this still leaves too much space for very high level discussions.
- It is worth to consider that innovation providers are invited to introduce their solutions in more details or even providing the possibility to have hands-on training.
- It is recommended to the EU-HYBNET network to include more practitioners into future discussions and to make sure that a focus on creating added value to them is maintained

INTRODUCTION

This document aims to present results of the work carried out in the context of Work Package (WP) 2 "Gaps and Needs of European Actors against Hybrid Threats", Task 2.4 "Training and Exercises" arranged according to the cycles of the EU-HYBNET project. The EU-HYBNET has four project cycles to conduct its key activities, the first, second and third cycle last each 17 months and the last cycle will last 6 months.

The training development was based on the results of other EU-HYBNET Tasks and their respective inputs.

As a first step of the second cycle of EU-HYBNET project, the situational analysis was conducted in T2.1. "Needs and Gaps Analysis in Knowledge and Performance" in project M18 (September 2021) during the Gaps and Needs workshops with security practitioners and other relevant actors (industry, academics, NGOs) from the EU-HYBNET Consortium, network members and Stakeholder Group. The aim was to identify the most critical gaps and needs in the context of 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

A long and shortlist of gaps and needs was produced by T2.1 and T2.2 and new directions and further scanning activities were identified to address emerging research and innovation initiatives.

Following the work conducted with respect to identifying gaps and needs in countering hybrid threats, T3.2 "Technology and Innovations Watch" and T3.3 "Ongoing Research Projects Initiatives Watch" analysed and presented technologies, and technical/non-technical innovations for each of the EU-HYBNET project four Core Themes. Subsequently, a list of the most promising technologies and innovations was provided to T2.3 "Training and Exercises Scenario Development" for training and exercise purposes, and for development and delivery of appropriate Scenario and Vignettes.

The Training and Exercising results will be shared and elaborated on in WP4 "Recommendations for Innovations Uptake and Standardization" and T3.1 "Definition of Target Areas for Improvements and Innovations" to define the potential for standardisation and provide recommendations for uptake of the most suitable innovations (incl. industrialisation). In addition, D2.21 will provide inputs to the D2.24 "2nd Training and exercises Lessons Learned report" M31.

All aforementioned cycles are based on the activities depicted in the figure below:

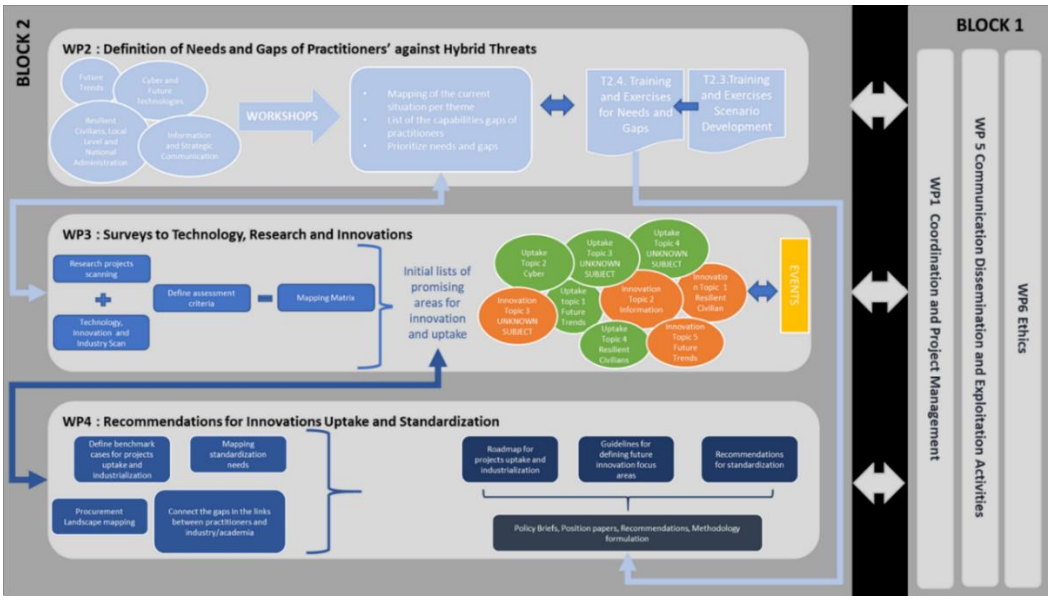


Figure 1 EU-HYBNET structure of Work Packages and Main Activities

More precisely, T2.4 has been dedicated to performing the following activities:

1. Survey of available training and exercise programmes at various EU MS and organisations
2. Planning and launching of training events for EU-HYBNET members and Associated partners
3. Employ an established Training Methodology
4. Design training evaluation forms
5. Provide Inputs to D2.24 Training and exercises Lessons Learned report
6. Produce a one-hour video for trainings in lecture format

Although D2.21 will not specifically deliver results to meet the majority of EU-HYBNET objectives (OB), nonetheless, this document strongly supports those EU-HYBNET Tasks that aim to deliver results focused on the following objectives:

- 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 4.1: To compile recommendations for uptake/industrialisation of innovation outputs (incl. social/non-technical); and provide opportunities for greater involvement from public procurement bodies upstream in the innovation cycle
- OB 4.4: To facilitate policy dialogues on future European research and innovation focus areas supporting innovation uptake
- OB2.1: To identify needs and gaps in areas of knowledge/performance (research, innovations, training) of practitioners (priority), industry, SMEs and academic actors
- 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

These Objectives closely follow related training activities, as well as innovation testing and selection processes.

STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1 introduces the methodology used in implementation of Training and Exercising Event.
- Section 2 provides a summary on collected training and other relevant materials, that can be used for training.
- Section 3 is dedicated to the participation, including main registration and participation indicators.
- Section 4 lists material shared with participant as pre-reading.
- Section 5 presents innovations prioritisation results and serves as an input to WP4.
- Section 6 presents results of the training evaluation, including comments provided.
- Section 7 is a closing section and is dedicated to main findings and lessons learned.

METHODOLOGY APPLIED

The overall objective of the EU-HYBNET Training and Exercising is to create and/or strengthen the capacities of European practitioners, industry, SME and academic actors to counter Hybrid Threats.

A Disruptive Technology Assessment Game (DTAG) was used to test the technical/social/human/organizational solutions and their impact on an operating environment during the 1st cycle Training and Exercising Event. For the 2nd cycle DTAG methodology was adjusted, reflecting experience, and Lessons Learned from the 1st cycle.

A DTAG is a seminar type wargame, used to assess potential innovations and their impact on the operating environment, in this instance a hybrid campaign. The DTAG essentially allows to employ the innovations, or so-called Ideas of Systems (IoSs) as described in WP3 "Surveys to Technology, Research and Innovations" (Deliverables D3.4 "First mid-term report on Improvement and innovations" and D3.8 "First mid-term report on Innovation and Research Project monitoring"), within a realistic operational context (Background Scenario) – that is, to understand the operationalization of the innovation, its impact on the operational environment, and the potential vulnerabilities adversaries might exploit. Thus, allowing for options in anticipating and countering the adversarial measures.

As such, the DTAG aims to:

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

The DTAG uses a Scenario and various Vignettes developed in EU-HYBNET T2.3 D2.18 "Training and Exercise, Scenario delivery" to sketch hybrid challenges within a realistic near-future operational environment. Scenario and Vignettes are described in the D2.18, the relevant sections of the deliverable are presented in the Annex I and were distributed to participants as pre-reading material.

During the Event participants are asked to freely assess the overall situation and to test the innovations presented for them as possible promising solutions. The aim is to hold a free discussion on the challenges and dilemmas that are underlying to the scenario Vignettes and to have discussion how the selected innovations could support the pan-European security practitioners to plan and conduct their counter measures to the challenges, Hybrid Threats.

It requires participant to exercise critical thinking and a creative approach, also to analyse and suggest new features to the selected and tested innovations. To "test the innovations", the training event provides the list of innovations, research monitoring results 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 to provide recommendations for most promising innovations uptake for pan-European security practitioners' needs.

The Training Agenda covered the introduction session with a brief overview of the training flow and introduction to Scenario helping the participants grasp and retain the information. This was followed by breakout sessions, focused on interactive discussions involved participants to share their experience and plan response campaigns. Hearing different voices also keeps the sessions varied and interesting. Agenda of the Event is presented in the Annex II.

During this Event some presentations of innovative solutions were made life. Three innovations were presented, all of them being high TRL level. In addition, example of operational level use of different solutions was presented by Lithuanian Armed Forces Strategic Communications department. Life presentations created a better understanding of the role of innovations.

Core Theme based teams have been elaborating how the solutions could improve response to different challenges described in Scenario and Vignettes. Teams have been asked to select most feasible innovative solution for selected vignette and after reaching group consensus to envision how it could be operationalized. It resulted in updated response campaigns, plans giving the basis to learn how innovations could be helpful in Hybrid Threat scenarios, similar to the ones provided in the exercise.

All of the above have been captured into solutions assessments by Core Theme leaders, moderators of the sessions. The outcomes of the innovations' validation and assessment are elaborated further in the report.

Finally, each participant has been provided with assessment form to give their structured feedback as well comments and other reflections. They also have been asked to provide relevant improvement points or additional expectations they would see relevant and important.

If to compare methodology used during the 1st and the 2nd cycles, there were some adjustments done. Following the experience, changes were made to simplify the description of circumstances (Scenario, Vignettes, etc.). Main changes applied:

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

REVIEW OF AVAILABLE TRAINING AND OTHER RELEVANT MATERIALS

Many EU-HYBNET consortium partners and network members are training providers, covering subject of Hybrid Threats. In order to avoid delivery of overlapping scenarios and training delivery EU-HYBNET T2.4 initiated a survey that aimed to identify and analyse other available trainings.

To accomplish this, T2.4 disseminated to the questionary between EU-HYBNET consortium partners and network members. Similar survey, using same questionnaire, was organised during the 1st cycle of the project implementation. Those who provided inputs during the 1st cycle, were asked not to repeat information. 2nd cycle survey was executed during July - August 2022.

Project partners and network members were invited to provide information on their training and education programs that can be relevant to Hybrid Threats domain. Requested information on sharable resources included trainings, research papers, scenarios and presentations relevant for the subject.

During the 2nd cycle survey relevant materials were provided by three partners:

Training programs:

- Horizon Global Academy - The course aims to increase knowledge and competences of institutional
- Pennasoft BVBA - Pennademy course for 'Cybersecurity Risk Management'

Articles:

- “Mihai Viteazul” National Intelligence Academy - Facts First: the European Approach to Fake History. Case study – EU vs. Disinfo and WWII Memories
- “Mihai Viteazul” National Intelligence Academy - Alternative scenarios in Security and Intelligence Studies: methods of identification and analysis of projection factors. Proposal of a class exercise.
- “Mihai Viteazul” National Intelligence Academy -Future Trends Exercise. Fractured Digital Futures: AI in Service or against Democracies? Solutions Ahead

Exercises**:**

- “Mihai Viteazul” National Intelligence Academy **-** Anticipating the level of involvement of the citizens in the security governance

In keeping with project goals and implementing the principle of non-overlapping components, the EU-HYBNET training was designed around the unique aspects of the Hybrid Threats domain and focused especially on innovative solutions mapped to gaps and needs identified in EU-HYBNET project T2.1 and T2.2.

Training materials collected from partners and network members were not prioritized for the 2nd training cycle. These will, however, be taken into account during the upcoming cycle.

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

TARGET AUDIENCE AND PARTICIPATION

The training was organized with a specific focus on EU-HYBNET consortium partners and network members. Participants represented a wide range of stakeholder groups (academia, RTO, industry, SMS, end-user organizations). The list of participants organizations can be found in the Annex III.

A total of 60 individuals registered for the Training and Exercising Event. 30 of them registered as participants on site and 28 registered to participate online (2 not indicated).

Initial selection of Core Themes, presented in the table below, was rather balanced.

Core Theme	September 29	September 30	Total
Future Trends of Hybrid Threats	21	10	31
Cyber & Future Technologies	14	12	26
Resilient Civilians, Local Level National Administration	11	12	23
Information and Strategic Communication	12	20	32

Table 1 Core Theme selection in registration.

The onboarding process for participants took almost two months. The registration process was started in middle of August. It proceeded slowly and was impacted by vacation period. The process was activated during September.

Actual participation in Training and Exercising Event was lower than registered participants. The same issue was observed during the 1st cycle. Reasons for such reduction are not clear, and most cases are very individual (changes in schedule, logistic issues, etc.). There were 44 participants present during the Event. 22 of them joint online and 22 were present on site.

The Event was organised in a hybrid format, encouraging participant to be present in person. As discussions and learning from each other are key elements in the methodology applied. It was challenging to productively involve online participants. While considering next Training and Exercising event, in-person participation should be requested. Online participation can be optional only for presentation or passive listening roles.

PRE-READING MATERIALS

Participants have been provided with a hand-out package of pre-reading materials 7 days before the Event. Participants pre-reading materials were reduced in complexity and included two documents:

- Scenario and Vignettes – including the detailed description of background scenario and all proposed vignettes, describing situation in more details.
- Innovations proposed for discussions – including description of innovative solutions and suggested aspects to be discussed during the Training. Document also provided linking of innovations to Vignettes and Core Themes.

Both documents originate from D2.18.

The Moderators have been provided with a template to present innovations, assigned to respective Vignette and Core Themes.

PRIORETISATION OF INNOVATIONS

The training was designed to assess innovations discussing which of these might be considered for formal uptake by practitioner organizations. During the 1st project cycle (M1-M17/ May 202- Sep 2022) prioritization and evaluation of innovations was made at the end of the Training Event. Survey, using specifically designed questionary was organized. Due to a very limited response rate, different approach was applied during the 2nd project cycle.

During the preparation phase different Vignettes were linked to Core Themes. Innovative solutions were linked to the Vignettes, assuming that they can provide additional value in the situation bound by it. In addition, 3 innovative solutions were presented during the Training. Those were also included in solutions list.

Each Core Theme group started their discussion with selection of the Vignette. After the first phase (situation assessment) participants were introduced to relevant innovations. List of innovations varied according to Vignette. Participants were asked to prioritize innovations presented and select the most appropriate (1 or 2) for further discussions.

Such prioritization does not provide a proper quantitative indication of their ranking but should be considered as qualitative indication of preference of a given group of participants.

Further in this section priorities prom different groups are presented.

CORE THEME: FUTURE TRENDS OF HYBRID THREATS

There were 4 Vignettes attributed to this Core theme.

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

During the first day of the Event (29th, September) Vignette No. 3 (Air bombing attack on one of the countries…) was selected. After the discussion, initial campaign plan was developed. Further discussion included prioritization of innovations. Respective innovations presented were:

- OSINT search (based on HENSOLD)
- Multi source integration (based on MALTEGO)
- DDS-Alpha (EEAS)
- Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience
- Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)

During the second round of discussions of the Event (30th, September) a different format was agreed to follow. All Vignettes were selected as one complex event within the period of 1 year, containing different threats of hybrid nature. All innovations, relevant to Core Theme were presented:

- OSINT capabilities (based on HENSOLD)
- Multi source integration (based on MALTEGO)
- DDS-Alpha (EEAS)
- Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience
- Europe's External Action and the Dual Challenges of Limited Statehood and Contested Orders (EU-LISTCO)
- Establishment and reinforcement of political education of democratic values
- Profiling and targeting news readers (PersoNews)

After innovations were presented, prioritization discussion was held. Priorities and essential comments are summarised in the table below.

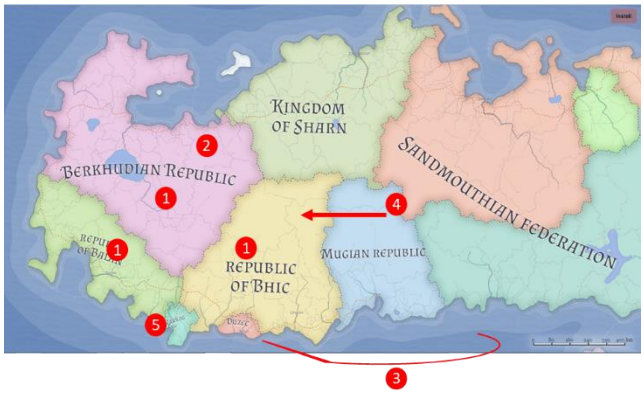
Discussion	Priority	Innovation	Comments
Day 1	1	OSINT	Mostly discussed. Some points for further considerations were identified: - Visual representation of key results of the request is very important. - Verification and traceability of information included is essential. - Some ML (AI) features can be added in the future for improved request execution.
	2-3	Digital Twins	Requires more information, but might be considered interesting solution for industry and critical supplies. Can be considered for the future as potential subject for regulation.
	2-3	DDS-alpha	Too early to evaluate at operational level. Considered interesting and valuable.
	4	Multi-source integr.	Needs significant preparation to be deployed.
	5	EU-LISTCO	
Day 2	General comment: the most valuable innovations were considered those, providing capabilities of collaborative response. OSINT, multi-source and DDS-alpha support such actions from the list provided. More attention was given for the innovations not discussed in previous round:		
		PersoNews	Ethical issues to be considered, as it can be interpreted as micro-targeting.
		Education	Rather long discussion emerged around the education issue. It was evaluated as rather low priority as if it is described at the moment, concluding that it should be changed, but providing no recommendations on “how”.

Table 2 Innovation evaluation results from Core Theme Future trends of Hybrid Threats

CORE THEME: CYBER & FUTURE TECHNOLOGIES

There were 5 Vignettes attributed to this Core theme.

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



During the first day of the Event (29th, September) Vignette No. 1 (Cyber-attacks causing major power outages, this causes serious problems on households as well as industrial control systems on a frequent basis...) was selected. After the discussion, initial campaign plan was developed. Further discussion included prioritization of innovations. Respective innovations presented were:

- OSINT capabilities (based on HENSOLD)
- Multi source integration (based on MALTEGO)
- DDS-Alpha (EEAS)
- 7 Shields innovation
- Integrated automated defense framework

During the second round of discussions of the Event (30th, September) a different format was agreed to follow as two Core Themes had a joint discussion under the subjects of Core Theme Future Trends of Hybrid Threats. All Vignettes were selected as one complex situation and discusssed from key considerable factors perspective. Same innovations, relevant to Core Theme were discussed:

After innovations were presented, prioritization discussion was held. Priorities and essential comments are summarised in the table below.

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	1	7 Shields	- It does not contribute to the prevention of crisis or attack but rather works for during and post crisis stages. - Works good for higher coordination and management capabilities involved in mid and high-level decision making processes. - Especially useful for information sharing cross institution and cross-borders among alliance partners. - Allows better to organize responsible capabilities for different actions. - Data correctness is key factor for platform to be trusted.

			- It should be developed further from security and high availability perspective as such a solution immediately becomes strategic target (decentralization should be a solution).
	2	Defence Framework	- How to ensure that it is correct? - In case on attack situation is changing too fast for system to learn and train on the data to address it correctly. - Typically, attacks are uniquely designed and there is high probability that it will miss the new major attacks. - Very dependent on data quality and there is not clear presentation how data quality will be addressed. - New technologies and software upgrades are released on daily basis that it is hardly imaginable how to maintain such a framework actuality.
	Key considerable factors for success: - it is important to address cascading effects therefore timely, precise communication with citizens in critical feature. All institutions having precise situational awareness information is a key. - In large scale crisis it is mandatory to enable local/regional autonomous handling of life critical functions, therefore localized situational awareness and coordination should be considered as improvement. - For cyber incidents quick analysis features can be considered additionally (who is behind analysis, attack scale assessment). - Integration of automated response protocols would be considered as one of features helping a lot to efficiently handle first stage after crisis incident report.		

Table 3 Innovation evaluation results from Core Theme Future trends of Hybrid Threats

CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL NATIONAL ADMINISTRATION

There were 5 Vignettes attributed to this Core theme.

1. Minority groups in one area activate discussions on independence during the national elections process.
2. Gas Flow shutdown after a gas pipeline explosion. Initial findings support the assumption that probably it is about a sabotage and not an accident.
3. A Fake news campaign on official media, that the electoral process is staged and premeditated is observed.
4. A new migrant area is created mainly by people from the adjacent majority region.
5. Telecoms are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations.

During the first day of the Event (29th, September) Vignette No. 2 (Gas Flow shutdown after a gas pipeline explosion…) was selected. During the second round of discussions (30th, September) Vignette No. 1 (Minority groups in one area activate discussions on independence…) was selected. All innovations, relevant to Core Theme were presented:

- OSINT search (based on HENSOLD)
- Multi source integration (based on MALTEGO)
- DDS-Alpha (EEAS)
- The Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-physical Threats, and effects with a focus on district or regional protection (PRECINCT)
- Development of Real-time Rapid Alert System on Disinformation
- A crawler for correlation of screened FDI with suspicious financial activity

After innovations were presented, prioritization discussion was held. Priorities and essential comments are summarised in the table below.

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	General comment: rationale for selecting these innovations when having the above-mentioned vignette in mind was their perceived level of readiness to be deployed in this case, as well as suitability to deal with such type of hybrid threats. One important downside of these innovations is their apparent focus on information exchange, but not on collection.		
	1	PRECINCT	- Assets used to support the national electoral process can be considered as CI and calls for independence from minority groups in this period may disrupt the established democratic procedures. - Innovation may be adapted for contingencies such as the one described in the respective vignette.
	2	Screened FDI	- Innovation could help with unveiling connections between organisations representing, (or claiming to be representing), minority groups and their financial backers, especially if the latter are operating covertly. - There are therefore specific concerns about the use and security of the data collected.

	3	Real-time Rapid Alert System	- Linking of information exchange systems on national level with those of the EU, (and potentially between both private and public entities). - Might produce 'false positives' and potentially lead to privacy issues, especially when it comes to the EU environment with its strict personal data exchange and processing policies.

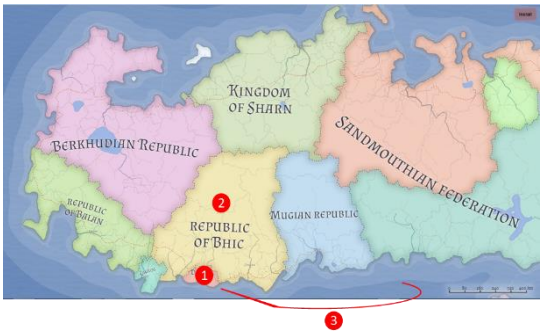
Table 4 Innovation evaluation results from Core Theme Resilient civilians, local level national administrations

The conclusion from discussions was that innovations proposed for discussion and review mostly focus on technology as a potential answer to hybrid threats. As good as such technological solutions may be, they may not be enough to deal with the whole spectrum of threats. Perhaps, such measures as strengthening democratic institutions could be used in combination with the proposed tools to combat minority jingoism and separatist tendencies in times of national elections.

CORE THEME: INFORMATION AND STRATEGIC COMMUNICATION

There were 3 Vignettes attributed to this Core theme.

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



During the first day of the Event (29th, September) Vignette No. 1 (Minority groups in one area activate discussions on independence during the national elections process) was selected. The same Vignette was discussed during the second round as well.

After the discussion, initial campaign plan was developed. Further discussion included prioritization of innovations. Respective innovations were presented:

- OSINT search (based on HENSOLD)
- Multi source integration (based on MALTEGO)
- DDS-Alpha (EEAS)
- Increasing capabilities to systematically assess information validity throughout the lifecycle
- Information and Misinformation Economics: Design, Manipulations and Countermeasures (IMEDMC)

During the second round additional innovations were presented:

- Integrated Monitoring System against cyber-enabled information operations
- Crowdsourced verification systems of fake news in encrypted messaging applications
- The Consequences of the Internet for Russia's Informational Influence Abroad (RUSINFORM)

After innovations were presented, prioritization discussion was held. Priorities and essential comments are summarised in the table below.

Discussion	Priority	Innovation	Comments
Day 1 / Day 2	1	DDS-Alpha (EEAS)	- Were considered helpful with regard to data collection and management but was also highlighted their limitations from the perspective of how to counter the threats.
	2	Systematically assess information validity	- Were considered helpful with regard to data collection and management but was also highlighted their limitations from the perspective of how to counter the threats.
	3	Integrated Monitoring System against cyber-enabled IO	- Making sense against deepfakes
		IMEDMC	- Raised doubts about its nature since this is a project at an early stage.
		RUSINFORM	- Was considered interesting from the perspective of understanding and methodology although having an external perspective and ignoring the hybrid dimension.

Table 5 Innovation evaluation results from Core Information and strategic communication

During the discussion there were some additional ideas on relevant innovations raised. One such example of non-technological innovation was enabling cross-government crisis management and organization cultural practices development.

Discussions resulted in a very different selection of innovations. Priorities can be grouped into several groups, that can be summarized as most relevant directions for innovation up-take:

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

The general comment from discussion was, that it is still very difficult to asses innovations, even at the prioritization stage. Early stage TRL innovation presented raised even more questions, most of them seem interesting, but estimation of their value in a given situation, described by Vignette, was very difficult.

EVALUATION OF TRAINING & EXERCISING EVENT

For the evaluation of the training questionnaire similar to 1st cycle was used. It contains 4 groups of questions:

Group 1: Evaluation of content of the training
Group 2: Evaluation of the guidance through the training
Group 3: Evaluation of the organization of the training
Group 4: Other (evaluation of individual experiences)

Example of the questionnaire is provided in Annex IV while the feedback is summarized in this section.

Overall, the response from participants was positive. The participants rated the experience as either good or excellent, 4 and 5 on a 5-point scale (where "5" indicates extremely valuable and "1" indicates not valuable). Written comments on the evaluations were also positive, indicating that the participants appreciated the learning opportunity.

8 responses were received. Those are presented in the Table below.

Assessment criteria	Number of responses	Cumulative score
The Content of the Training and Exercise event evaluation		
Relevance of the training	8	4.50 (4,38)[1]
Uniqueness of the training compared to other trainings on hybrid threats	8	3.75 (3,88)
Relevance of the scenario	8	4.00 (4,13)
Clarity of the scenario	8	3.88 (3,75)
Other relevant topics (if any) to be added for the upcoming trainings	3	• SocMINT and OSINT • The understanding of "hybridity" of the scenarios, as evident from the way they were constructed and what they contained, contains some elements of disinformation, some attacks on infrastructure / cyber, some migration. These are elements that we had over the past several years across several projects, and also in last year's Hybnet event. We should start looking at things that trump and/or weaponise our SOPs, laws, norms, emotions/values, etc. Could we have a session / training event where a behavioural sciences team leads on the outlining of the scenarios / injects? • True hybrid threat scenarios and not attention to single incident occurrences…
Comments	3	• I, unfortunately, could not attend in person, I connected to the event online and I missed the face-to-face contact when participating in the discussions. Still it was very interesting. • The scenario was great. It wasn't very clear but I think this is an added value in such event. • The training wasn't very relevant to my current position but I really enjoyed discussions and informal interactions with other participants. I would suggest a bit longer breaks. • Discussion sessions were excellent…

[1] Evaluation results from the 1st cycle presented in brackets.

Is there a need for any improvement of the content of the training and exercise? If yes, please, specify.	5	• Scenarios should be designed in a way that make the discussion of the solutions a direct exercise. Viewing / Reading of the documentation beforehand should be mandatory, as it saves time and creates, inherently, more time for discussion and the exercises. • The scenarios that were proposed were very well adjusted to the needs of the project (and also to current news) but perhaps they were too general. Including more details and creating more specific scenarios may lead to other relevant conclusions. • The content was perfect! Bravo! • We discussed a large number of very good points in each session, but for one of the sessions we were very lucky to have an exceptional summary done by the moderator, who also labelled each description per its meaning / impact - which was very useful; whereas in the second session the conversation did not flow as well and some elements escaped the group and the wider conversation after the session. • It would be ideal to standardise a way of taking notes and keeping track of everything discussed - sometimes we can review the notes or cross-share them after the events, and people could send in insights and ideas. Absent a proper and/or comprehensive outline and/or summary, we could be missing some insights. • Clear delineation of what we all mean by a hybrid threat…
Evaluation of support provided by Moderator through the training		
Completeness of information provided	8	4.38 (4,63)
Balance between theoretical and practical aspects on the subject	8	3.88 (4,38)
Support provided by moderator	8	4.38 (4,88)
The moderator was well prepared for the training	8	4.38 (4,88)
The moderator was an expert on the subject and provided all clarification needed	8	4.25 (4,75)
Comments	2	• Two moderators from UiT were excellent. Very clear and experienced. It was also a way to learn things. Thank you ! • Moderator did a great job…
Is there a need for any improvement of the moderation of the training and exercise? If yes, please, specify.	3	• Hybrid formats for these kind of exercises are not the best model. • Stay on course…moderation was well executed. • The moderator held quite long monologues...
Evaluation of Organization aspects of the training		
Prereading materials (sufficiency and clarity)	8	4.50 (3,5)
Training materials (sufficiency and clarity)	8	4.25 (3,88)
Was time sufficient to get into productive dialog and was time well structured	8	4.38 (3,75)

Possibility to interact, discuss, share with other participants	8	4.50 (4,63)
Suitability of Platform used	8	4.13 (4,38)
Comments	2	• Platform not assessed but I think there were some problems with people online. • Preparation materials should be sent out well in advance…
Is there a need for any improvement of the organization of the training and exercise? If yes, please, specify.	1	• Scenarios/vignettes should reflect true hybrid threat onslaughts…
Evaluation of your general impression of the training		
Evaluation of my (as a participant) involvement in the training	8	4.50 (4,13)
Evaluation of my knowledge on the training subject before the training	8	4.38 (2,88)
Evaluation of my knowledge on the training subject after the training	8	4.50 (3,63)
Would you recommend this training	8	4.63 (4,38)
Other general comments	1	• I learned a great deal… • It would have been great to have the possibility to get a proper meal at the venue (at own expense, if necessary).

Table 6 Training evaluation results.

Overall evaluation of the Training Event is positive. Most of components scored similar or close points. Some differences to be noted are related to scenario and knowledge level of participants. Pre-reading materials and Scenario scored better as they were considered more sufficient and clear compare to the 1st cycle. As it was mentioned in the previous sections, complexity of training content was reduced following evaluations received. Knowledge on the training subject have increased significantly. During the 1st cycle they scored 2.88 (out of 5), while during this cycle this parameter scored 4.57.

FINDINGS AND CONCLUSIONS

Participants reported on the important value of the training and the fact that they gained new knowledge and a broader understanding on the complexity of hybrid threats. Written comments on the evaluations were also positive, indicating that the participants appreciated the learning opportunity and would recommend the training to their colleagues.

More detailed findings and comments are provided below. These are based on evaluation results and observations reported by the training participants and organizers during the training planning, execution and post evaluation.

Finding 1:

Simplified pre-reading materials were evaluated positively. Significant time was also spent during the training to present the general scenario. Such modification reflects the findings from the 1st cycle.

Finding 2:

Most of suggestions for improvement were related to Scenario. Simplification made easier to understand and apply it during the event. But, on the other hand, in most Vignettes the complexity of hybrid threats was lost. Vignettes were more focussed on a standalone event. Balancing of the scenario presenting the complexity and making it simple to understand, interpret and apply should be considered for the up-coming cycle.

Finding 3

There were numerous registrants who were 'no-shows' without prior notice. Similar issue was observed during the 1st cycle as well. If similar methodology is to be applied for the next cycle, required participation on site and very limited possibilities to observe process online can be one of the ways to solve this problem.

Finding 4

Considering that evaluation of the innovations and assess their impact on hybrid threats was on of key aspects, the participants were lacking explicit descriptions of the innovations in order effectively understand the innovation's potential and its future uptake possibilities. This was improved by having 3 innovations presented live and having methodology of innovations in use presentation. But this still leaves too much space for very high level discussions.

Quote from participant:

« Nevertheless, our group had a hard time, assessing their importance/impact with regards to 'real' counter-hybrid operations. The reason for this lies in the vagueness of some innovations or in the early stage of their projects. »

It is worth to consider that innovation providers are invited to introduce their solutions in more details or even providing the possibility to have hands-on training. Such approach can provide different value for participants. At the same time it requires considerable changes in methodological approach. Keeping in mind very limited resources for implementation of Training and Exercising significant input should be provided by innovative solutions owners.

Quote from participant:

« Overall, our group had the impression that it would be good that as the EU-HYBNET project advances, we root the events, discussions, projects and products increasingly to the practitioners' realities and requirements. There are so many great ideas resting in the EU-HYBNET that it would be sad for any of it not to make it into the EU's or member states' practical counter-hybrid work. »

Finding 5

When pressed a bit harder on evaluating the innovations, we approached this by first asking what they should enable in a counter-hybrid operational or decision-making enablement context. This was very much an exploration of practitioners' requirements. While trying to find out how the proposed innovations could support practitioner requirements/deliverables it was observed that there was too much of a gap between innovative concepts and practical counter-hybrid operations/decision-making. Most innovations propose such complex setups or capabilities that they run the risk of becoming unusable in case of emergency, when crisis management is done by small circles under considerable time pressure, as is usually the case. In a crisis situation it would be unfortunate to miss out on the innovations' insights, though.

Quote from participant:

« The conclusion of our group was a recommendation to the EU-HYBNET network to include more practitioners into future discussions and to make sure that a focus on creating added value to them is maintained. That way, we could ensure that the maximum amount of delivered projects and recommendations would find their way into the practitioners' domain. We reckon that most innovations are in an early stage of development, but also had the impression that it seems to be the right time to start making them more concrete, where possible. »

Finding 6

The presence of a competent Moderator proved to be one of the key success factors of the training. Planning the set of next trainings of similar methodology, inclusion of competent experts into the training process should be continued.

Finding 7

Discussions in groups raised a number of questions that can be relevant to EU-HYBNET future activities. Those were:

- The question of vulnerability of information networks, not only to disinformation and abuse but also the misuse of data by governments or other bodies of authority.
- The matter of whether national laws regarding data protections reflect these rapid technological changes.
- Difficulties in building trust between state actors regarding information networks and the balance between liberty and security.
- Defining the openness of what information is being collected by governments.
- How do we increase dissemination capabilities – instead of just awareness and understanding.
- Timeframes: avoid analysis paralysis.
- Make innovations inter-operable with EU and NATO.

ANNEX I. SCENARIO AND VIGNETTES

DEFINITIONS

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. Within a training, a scenario builds on different assumptions 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.

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 practitioners, on possible alternative future developments that are hard to predict and the assumptions behind the scenario and vignettes must be made transparent. The scenario and vignettes need to represent different kind of challenges and alternatives to pan-European security practitioners' to deal with them.

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

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.

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".

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.

MAP

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

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. Mechanized infantry 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.

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.

CORE THEMES AND VIGNETTES

Core Theme #2: "Cyber and Future Technologies"	
Vignettes	• Cyber-attacks causing major power outages. This causes serious problems on households as well as industrial control systems on a frequent basis. (Vignette 3) • Telecoms are disrupted due to major problems on the satellite – land stations comms network, it seems that systems are compromised. The air traffic control system is temporarily down causing delays in airports operations. (Vignette 4) • The irregular migrant flows are facilitated, by allowing if not escorting with its coast guard forces. (Vignette 5) • Air bombing attack on one of the countries. Mechanized infantry units invade. Civilian refugees are fleeing. (Vignette 6) • A new migrant area is created mainly by people from the adjacent majority region. (Vignette 8)

Core Theme #3: "Resilient Civilians, Local Level National Administration"	
Vignettes	• Gas Flow shutdown after a gas pipeline explosion. Initial findings support the assumption that probably it is about a sabotage and not an accident. (Vignette 1) • Cyber-attacks causing major power outages. This causes serious problems on households as well as industrial control systems on a frequent basis. (Vignette 3) • The irregular migrant flows are facilitated, by allowing if not escorting with its coast guard forces.(Vignette 5) • Air bombing attack on one of the countries. Mechanized infantry units invade. Civilian refugees are fleeing. (Vignette 6) • A Fake news campaign on official media, that the electoral process is staged and premeditated is observed. (Vignette 7) • A new migrant area is created mainly by people from the adjacent majority region. (Vignette 8)

Core Theme #4: "Information and Strategic Communication"	
Vignettes	• Minority groups in one area activate discussions on independence during the national elections process. (Vignette 2) • A Fake news campaign on official media, that the electoral process is staged and premeditated is observed. (Vignette 7) • A new migrant area is created mainly by people from the adjacent majority region. (Vignette 8)

ANNEX II. AGENDA OF THE EVENT

EU-HYBNET 2nd Training and Exercise Event

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

Agenda

Day 1, September 29 (Thursday)

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

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

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

EU-HYBNET 2nd Training and Exercise Event

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

Agenda

Day 2, September 30 (Friday)

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

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

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

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

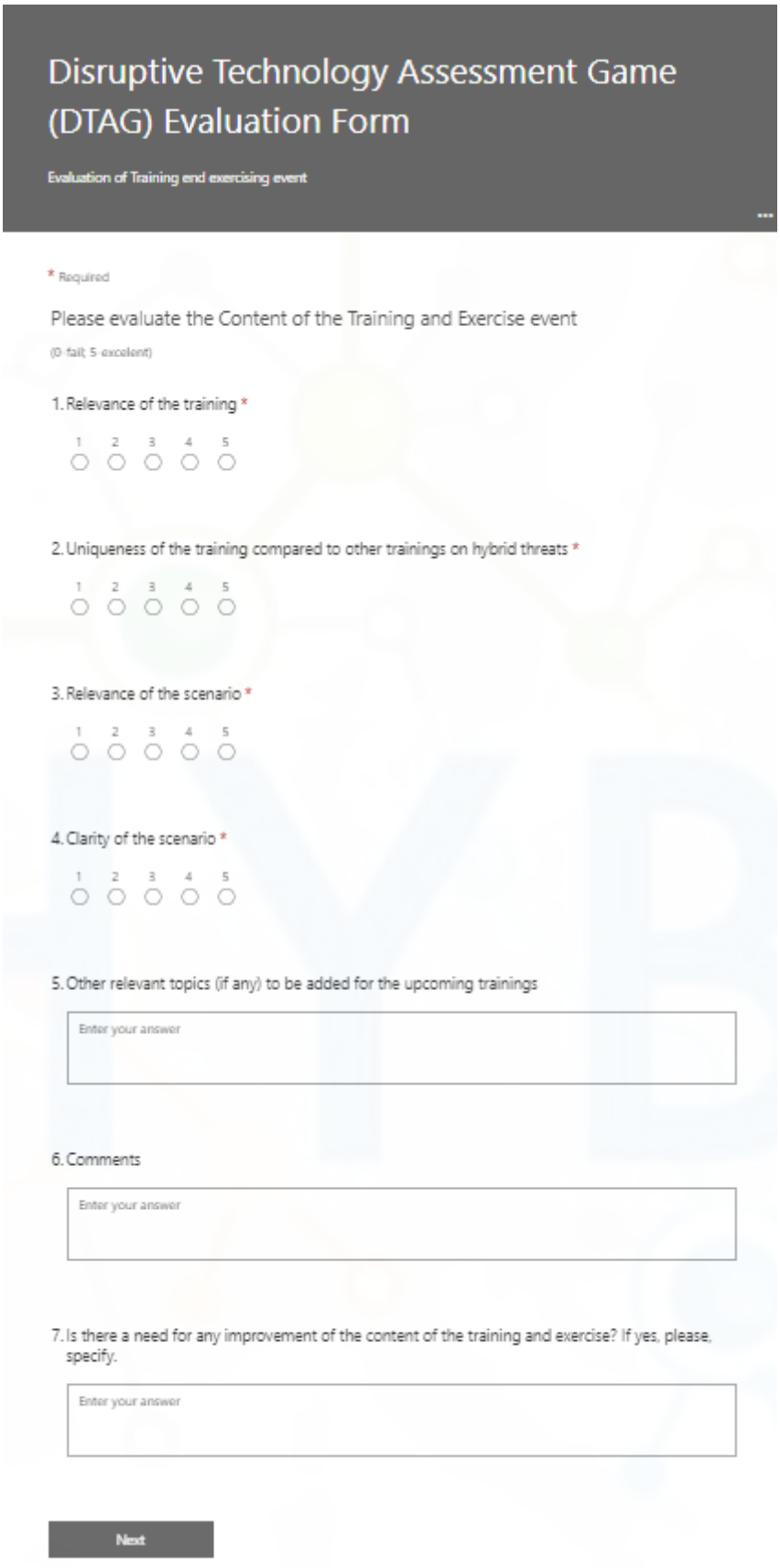
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 883054.

ANNEX III. THE LIST OF REGISTERED ORGANIZATIONS

No.	Organisation	No of participants
1	"Mihai Viteazul" National Intelligence Academy	3
2	Academic Centre for StratCom	1
3	Defence Institution Building School	1
4	EEAS	1
5	Estonian Information System Authority (RIA)	1
6	European Organisation for Security (EOS)	2
7	Friends of Europe	1
8	Hybrid CoE	1
9	Hybrid Warfare research Institute	1
10	Internal Security Agency	2
11	International Centre for Defence and Security (ICDS)	1
12	Istituto Affari Internazionali (IAI)	1
13	JRC	3
14	KEMEA	3
15	L3CE	4
16	Laurea	2
17	Maldita.es	1
18	Maltego	2
19	Ministère de la transition écologique	2
20	MTES	1
21	MVNIA	2
22	NORDLAB, Nord University	1
23	Policlinico Gemelli	1
24	Polish Platform for Homeland Security	3
25	RISE Research Institutes of Sweden	3
26	SSRI of MIA of Ukraine	1
27	State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"	1
28	The National Institute for Strategic Studies	1
29	TNO	1
30	UiT	1
31	Università Cattolica del Sacro Cuore	1
32	University of Georgia	1
33	University Rey Juan Carlos	1
34	Vilnius University/ Center for European Policy Analaysis	1
35	VOST Europe	1
36	Ministry of the Interior Finland	1
37	For an ecological transition ministry (transportation)	1

38	REA	1
39	University of Tromsø	1
40	Elsis Pro	1

ANNEX IV. TRAINING AND EXERCISING EVENTEVALUATION FORM



Disruptive Technology Assessment Game (DTAG) Evaluation Form

Evaluation of Training end exercising event

* Required

Please evaluate the Content of the Training and Exercise event

(0 fail; 5 excelent)

1. Relevance of the training *

1 2 3 4 5

2. Uniqueness of the training compared to other trainings on hybrid threats *

1 2 3 4 5

3. Relevance of the scenario *

1 2 3 4 5

4. Clarity of the scenario *

1 2 3 4 5

5. Other relevant topics (if any) to be added for the upcoming trainings

Enter your answer

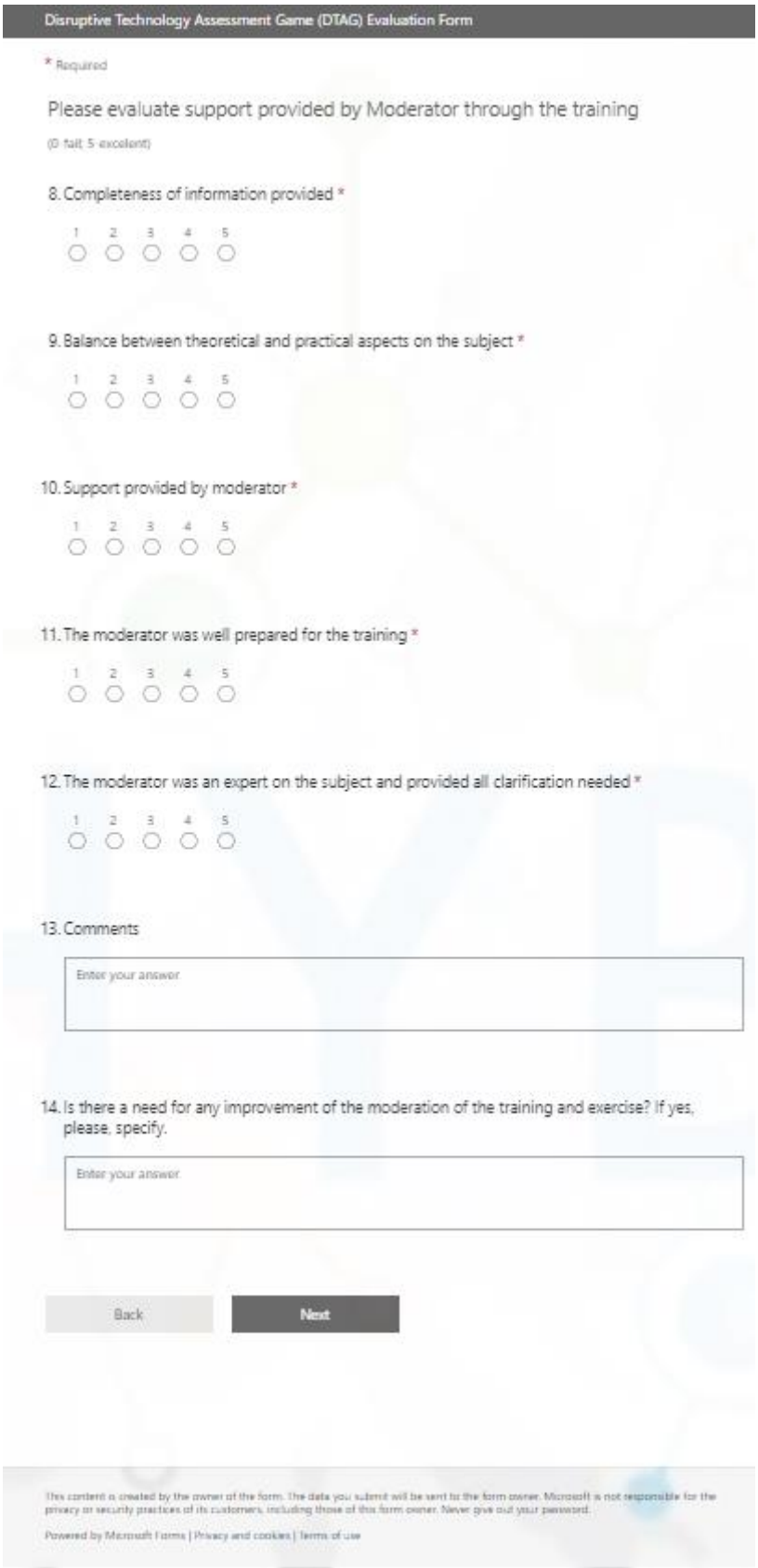
6. Comments

Enter your answer

7. Is there a need for any improvement of the content of the training and exercise? If yes, please, specify.

Enter your answer

Next



Disruptive Technology Assessment Game (DTAG) Evaluation Form

* Required

Please evaluate support provided by Moderator through the training

(0 fail, 5 excellent)

8. Completeness of information provided *

1 2 3 4 5

9. Balance between theoretical and practical aspects on the subject *

1 2 3 4 5

10. Support provided by moderator *

1 2 3 4 5

11. The moderator was well prepared for the training *

1 2 3 4 5

12. The moderator was an expert on the subject and provided all clarification needed *

1 2 3 4 5

13. Comments

Enter your answer

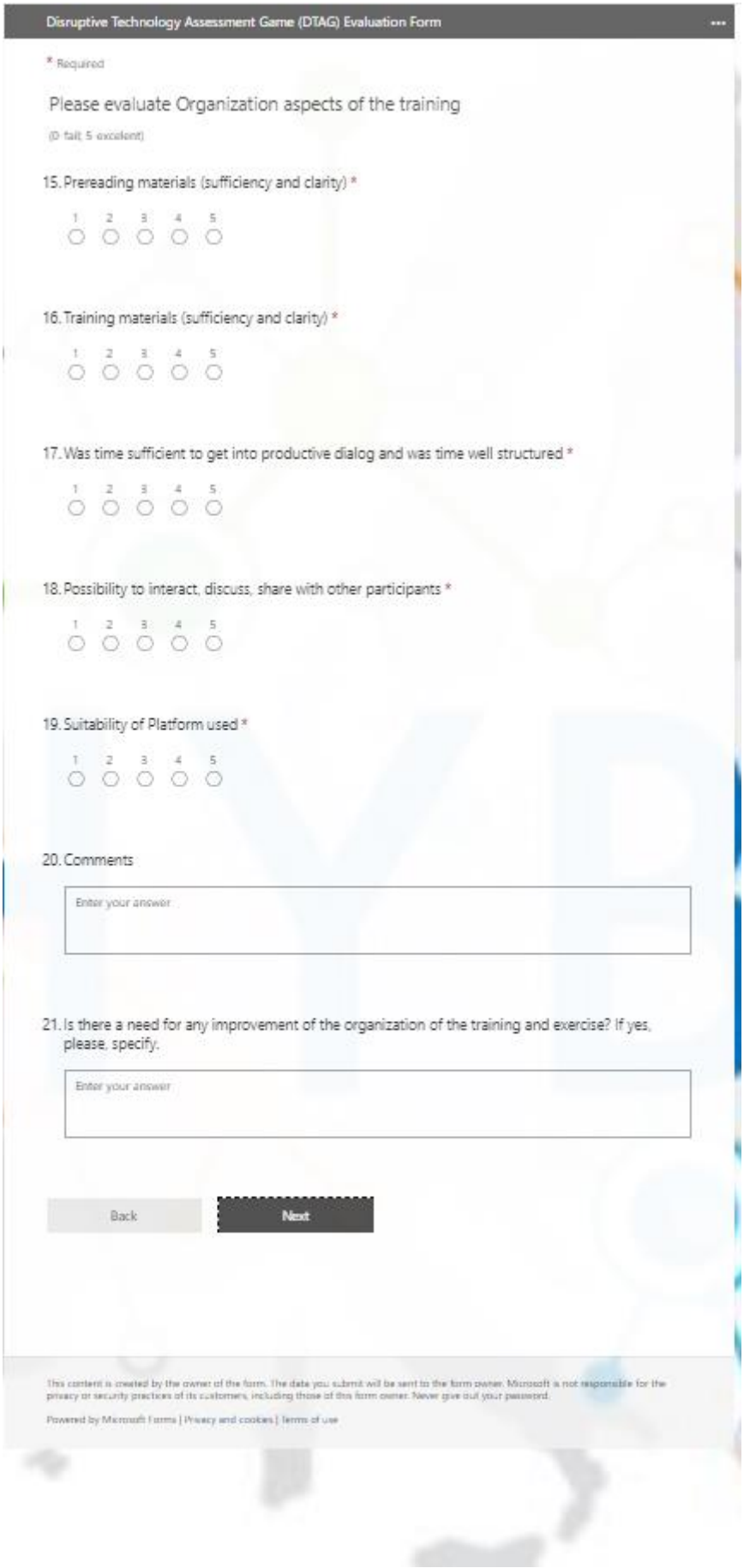
14. Is there a need for any improvement of the moderation of the training and exercise? If yes, please, specify.

Enter your answer

Back Next

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Powered by Microsoft Forms | Privacy and cookies | Terms of use



Disruptive Technology Assessment Game (DTAG) Evaluation Form

* Required

Please evaluate Organization aspects of the training

(0 fail, 5 excellent)

15. Prereading materials (sufficiency and clarity) *

1 2 3 4 5

16. Training materials (sufficiency and clarity) *

1 2 3 4 5

17. Was time sufficient to get into productive dialog and was time well structured *

1 2 3 4 5

18. Possibility to interact, discuss, share with other participants *

1 2 3 4 5

19. Suitability of Platform used *

1 2 3 4 5

20. Comments

Enter your answer

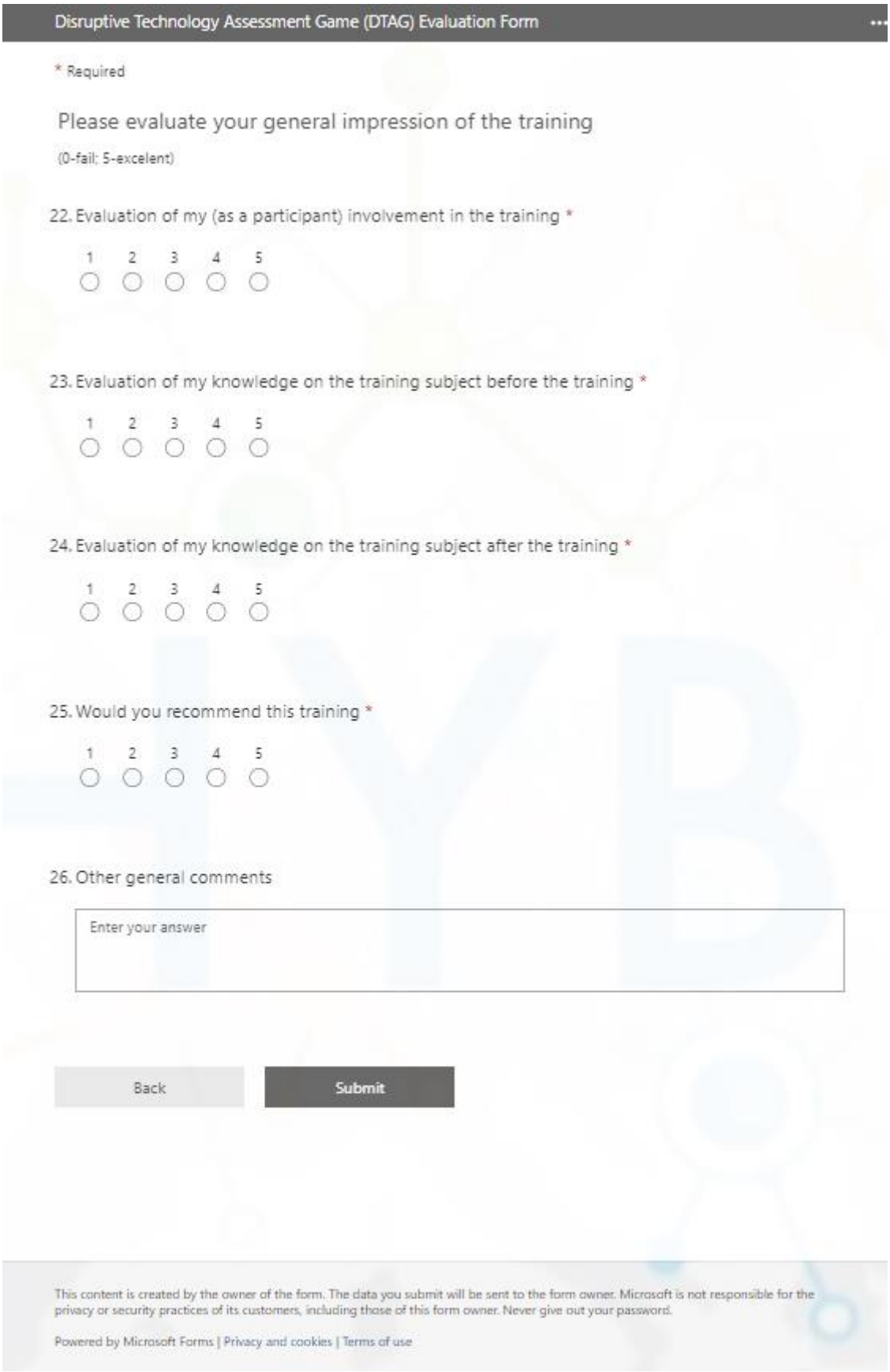
21. Is there a need for any improvement of the organization of the training and exercise? If yes, please, specify.

Enter your answer

Back Next

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Powered by Microsoft Forms | Privacy and cookies | Terms of use



Disruptive Technology Assessment Game (DTAG) Evaluation Form

* Required

Please evaluate your general impression of the training

(0-fail; 5-excelent)

22. Evaluation of my (as a participant) involvement in the training *

1 2 3 4 5

23. Evaluation of my knowledge on the training subject before the training *

1 2 3 4 5

24. Evaluation of my knowledge on the training subject after the training *

1 2 3 4 5

25. Would you recommend this training *

1 2 3 4 5

26. Other general comments

Enter your answer

Back Submit

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Powered by Microsoft Forms | Privacy and cookies | Terms of use

GLOSSARY AND ACRONIMS

Term	Definition / Description
EC	The European Commission
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats -project
WP	Work Package
T	Task
D	Deliverables
MS	Milestone
OB	Objectives
KPI	Key performance indicator
M	Project month
ML	Machine learning
MSs	Member States
IoS	Ideas of Systems
DTAG	Disruptive Technology Assessment Game