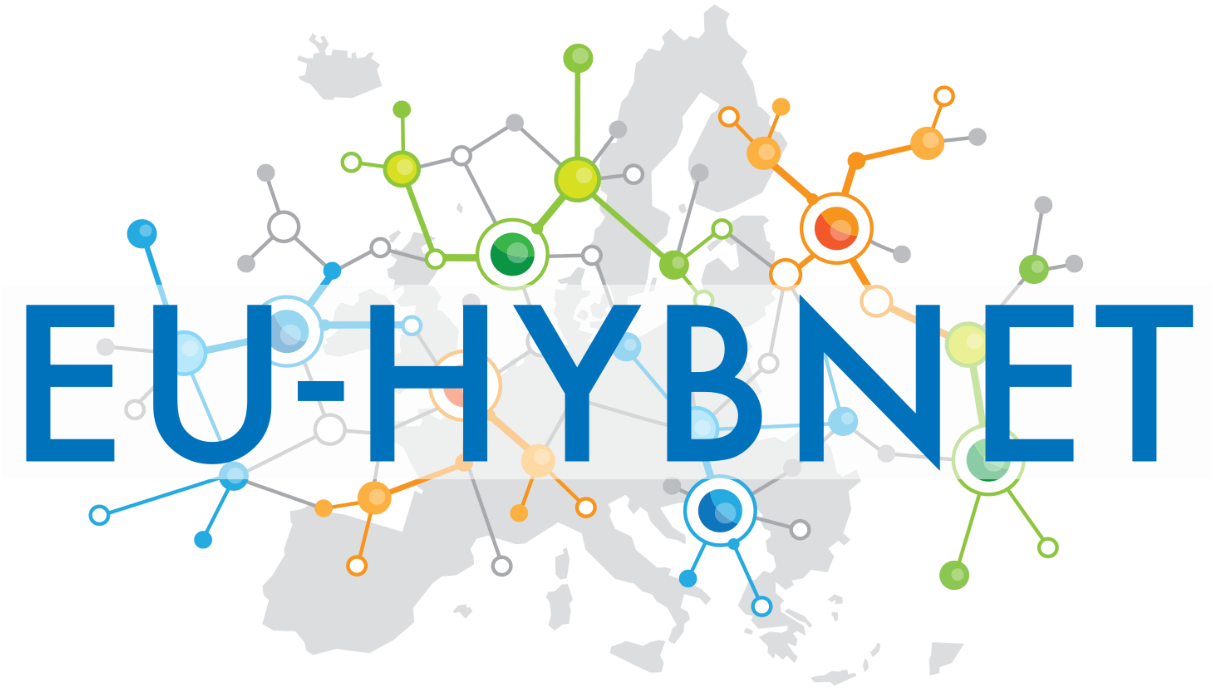


TRAINING AND EXERCISES DELIVERY ON UP-TO-DATE TOPICS

DELIVERABLE 2.20

Lead Author: L3CE

Contributors: TNO, KEMEA, Hybrid CoE, UiT, Laurea

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

D2.20 TRAINING AND EXERCISES DELIVERY ON UP-TO-DATE TOPICS

Deliverable number	**2.20**	
Version:	**3.0**	
Delivery date:	**25/5/2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Egidija Versinskiene**	**L3CE**
Contributors:	**Anja van der Hulst** **Päivi Mattila** **Dominykas Versinskas** **Evaldas Bruze** **Edmundas Piesarskas** **Willem Verdaasdonk**	**TNO** **Laurea** **L3CE** **L3CE** **L3CE** **TNO**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	2021.04.21	Dominykas Versinskas/L3CE	First draft.
0.2	2021.05.16	Maxime Lebrun/ Hybrid CoE	Review.
0.3	2021.05.16	Anja van der Hulst/ TNO	Updated the chapters 3 and 4 to reflect the final version of the moderator guide. Review.
0.4	2021.05.17	Päivi Mattila/ Laurea	Text editing, review.
0.5	2021.05.18	Egidija Versinskiene/ L3CE	Updated the document based on provided comments.
1.0	2021.05.20	Dominykas Versinskas/ L3CE	Updated document based on provided comments, prepared final version.
1.1	2021.05.25	Päivi Mattila/ Laurea	Review and final comments.
2.0	2021.05.25	Dominykas Versinskas /L3CE	Updated document based on provided comments.
3.0	2021.05.25	Päivi Mattila/ Laurea	Final review. Document ready for submission.

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.
This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

1 TABLE OF CONTENT

D2.20 TRAINING AND EXERCISES DELIVERY ON UP-TO-DATE TOPICS 1

DOCUMENT CONTROL 1

DISCLAIMER 1

1 TABLE OF CONTENT 2

2 TABLES 3

3 FIGURES 3

4 Executive Summary 4

5 Introduction 6

5.1 Overview 6

5.2 Structure of the deliverable 7

5.3 Background 8

5.4 Objective 8

5.5 Review of available training and other relevant materials 9

6 DTAG Training methodology 12

6.1 Gameplay summary 12

6.2 Definitions and terms 12

6.3 Teams 13

6.4 Moderator 13

6.5 Observer 14

6.6 Team roles description 14

6.7 Devil’s advocate 15

6.8 Virtual environment 15

7 Gameplay - Gameplan DTAG 16

7.1 Introduction – 30 minutes 16

7.2 Phase 1: Campaign planning – 40 +15 mins 17

7.3 Phase 2: IoS operationalization – 10 + 50 +15 mins 17

7.4 Questionnaire, Reflection and closing words 18

8 Target audience and attendance 19

8.1 Registration results 19

9 List of materials distributed 20

10 Evaluation 21

11 Evaluation results 22

12 Findings and conclusions 34

13 Annex I. Disruptive technology assessment game (DTAG) evaluation form 36

14 Annex II. invitation letter 45

15 ANNEX III. The list of participants organizations 46
16 ANNEX IV. GLOSSARY AND ACRONYMS 47

2 TABLES

Table 2 shows the general flow of the DTAG game- all times shown are based off CET on the game day itself . 16
Table 3 DTAG EVALUATION RESULTS 25
Table 4 VIGNETTE 1 INJECT 1 EVALUATION RESULTS 26
Table 5 VIGNETTE 2 INJECT 1 EVALUATION RESULTS 27
Table 6 VIGNETTE 2 INJECT 2 EVALUATION RESULTS 27
Table 7 VIGNETTE 3 INJECT 1 EVALUATION RESULTS 28
Table 8 VIGNETTE 3 INJECT 2 EVALUATION RESULTS 29
Table 9 VIGNETTE 4 INJECT 1 EVALUATION RESULTS 30
Table 10 VIGNETTE 4 INJECT 2 EVALUATION RESULTS 30
Table 11 VIGNETTE 2 INJECT 1 EVALUATION RESULTS 31
Table 12 VIGNETTE 2 INJECT 2 EVALUATION RESULTS 32
Table 13 Glossary and Acronyms 47

3 FIGURES

Figure 1 EU-HYBNET structure of Work Packages and Main Activities 7
Figure 2 Shows a brief outline of the entire DTAG gameplay (more info in section 4) 12
Figure 3 Shows Central room with two breakout room teams 13
Figure 4 THE DTAG EVALUATION QUESTIONARIES 39
Figure 5 THE IoS EVALUATION FORM 43
Figure 6 QUESTIONEER: SOURCES TO BE SCANNED ON RESEARCH AND PROJECTS IN HYBRID THREATS 44

4 EXECUTIVE SUMMARY

The purpose of this deliverables (D) 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*" and the first EU-HYBNET training event was arranged in the Project month (M) 12/ April 2021.

The report is structured so as 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, taking into account their feedback, insights, and other considerations, 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 determine the level of experience of network partners and the training exercises were adjusted accordingly in order to meet the goals and objectives of the EU-HYBNET project.

As a format for the training it was decided to develop EU-HYBNET partner's, TNO's, so called Disruptive Technology Assessment game (DTAG) for four different vignettes that each targeted one of the core themes of EU-HYBNET. The EU-HYBNET project four core themes are following: *Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; and Information and Strategic Communication.* 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 DTAG evaluation results demonstrated that training 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 are willing to recommend the training to their colleagues.

In addition, participants reported that the training gave them a valuable and broader understanding of the complexity associated with hybrid threats, hybrid attacks and cascading effects; and how the innovations presented can support their organization in addressing various crisis situations.

The registration process revealed that interest in the topics presented in the four Vignettes under each of core theme differed significantly among registrants. The most popular choice was "STRATCOM and state-citizen-Media trust" vignette which received much more attention than the other three.

The biggest challenge was to organise the DTAG online because the resolution of technical issues took time away from direct training activities. Thus, it was concluded that a one hour introductory session, one week before the training commenced, would help participants to get a better understanding of the innovations involved, evaluation methodology and of the basic training concept.

In addition, the evaluation results revealed that some organizational improvements have to be considered planning the second cycle of training such as preparation, registration, on-boarding of participants and pre-reading materials.

The following is a summary of key recommendations for future actions:

- Considering that the training participants and in particular practitioners expressed a huge need for trainings in Hybrid Threats domain, the training could include dedicated training groups for practitioners only.
- The complexity of limited to the level necessary to provide a meaningful context for the implementation of innovations.
- Support for the preparation and training of participants should be provided. Introductory sessions one week prior to commencement of training could be organized for this purpose.
- Descriptions of innovations should be very detailed and include variety of key features in order to know their applicability in the various crises situations. Innovation providers could be involved in the organisation of training sessions.

5 INTRODUCTION

5.1 OVERVIEW

This deliverable 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, the situational analysis was conducted in EU-HYBNT T2.1. “Needs and Gaps Analysis in Knowledge and Performance” in project M1 (May 2020) during the Gaps and Needs workshops with security practitioners and other relevant actors (industry, academics, NGOs) from the EU-HYBNET Consortium 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 “Research to Support Increase of Knowledge and Performance” 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. Materials produced by T2.3 served as a basis for enabling successful training execution. The trainings were preselected during the design phase of the project and served as a major input in identifing gaps and associated innovations that might be feasible for adoption and possible alignment to meet defined objectives and priorities.

The DTAG 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” in order to define the potential for standardisation and provide recommendations for uptake of the most suitable innovations (incl. industrialisation). In addition, D2.20 will provide inputs to the D2.23 “1st Training and exercises Lessons Learned report” M14 (June 2021).

All aforementioned aspects were based on the activities depicted in the figure below:

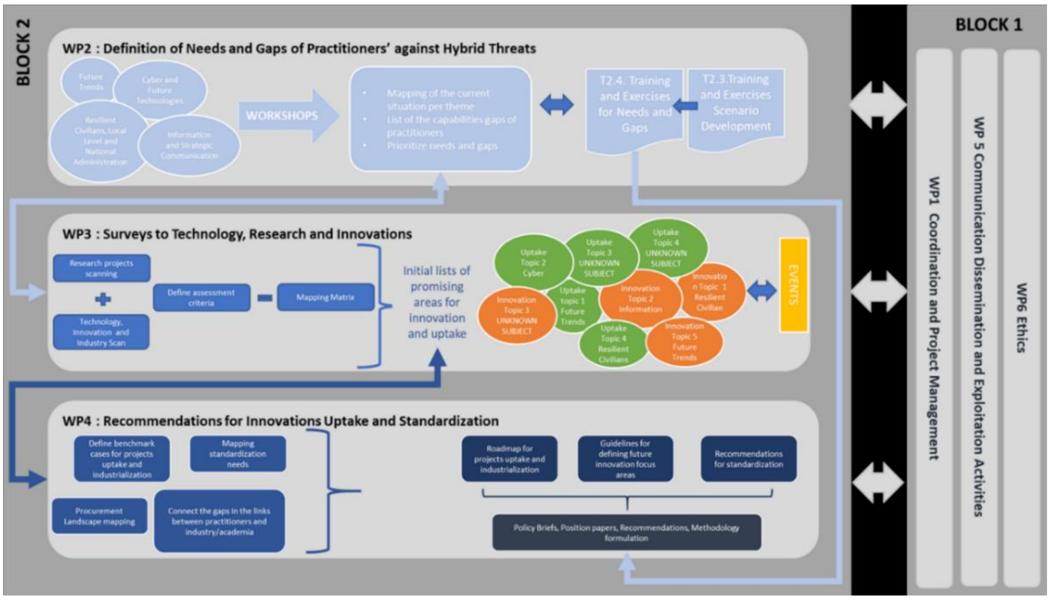

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

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

More precisely, T2.4 has been dedicated to perform 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. Deliver a Training Report
6. Produce a one-hour video for trainings in lecture format

Although D2.20 will not specifically deliver results to meet the majority of EU-HYBNET objectives (OB), nonetheless, this deliverable 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.

5.2 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1 introduces the objectives of this report and describes the deliverable
- Section 2 provides an executive summary that highlights the main results and recommendations
- Section 3 provides objectives and the background information i.e. training preparation, launching and training schedule
- Section 4 outlines the proposed training methodology, audience and registration issues
- Section 5 presents a training evaluation process and evaluation results
- Section 6 provides the training results, conclusions and recommendations for continuing the work in the next training cycle.

5.3 BACKGROUND

A Disruptive Technology Assessment Game (DTAG) was used to test the technical/social/human/organizational solutions and their impact on an operating environment. The DTAG format was originally developed by an international team of researchers from NATO countries through NATO's Science and Technology Organization in 2010. For the purposes of using the DTAG for EU-HYBNET, the gaming format was tailored to better fit the aims and objectives of the EU-HYBNET project.

5.4 OBJECTIVE

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

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 D3.3 "First report on Improvement and innovations" and D3.7 "First 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 innovations and solutions to counter hybrid threats through the analysis of the IoS cards.
- Explore the potential impact of the IoS in an operational hybrid setting.
- Identify the potential vulnerabilities in the (use of) the IoS that adversaries might exploit, thereby mitigating the intended effects of the IoS.
- 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 D2.17 "Training and Exercise, Scenario delivery" to sketch hybrid challenges within a realistic near-future operational environment. The scenario and Vignettes portray a crisis situation, giving opportunities to hybrid threat actors to leverage 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.

Four Vignettes were explored during the training:

- Future Trends of Hybrid Threats: Strategic inter-agency coordination-need for damage assessment and contingency management at a strategic level;
- Cyber and Future Technologies: Attacks on financial sector, vaccine chain and individual data – need for response;
- Resilient Civilians: Local Level and National Administration: Sanitary restrictions and regionalized protest and movement – need for integration;
- Information and Strategic Communication: STRATCOM and state-citizen – media trust.

Each Vignette was supplemented by a selection of Injects – additions to the vignette, which add new challenges, tensions and difficulty to the crisis situation.

Selected training participants collected the data using pre-designed PowerPoint slides. These were filled in during the execution of the DTAG. As well, the Menti-Meter tool coupled with structured discussion during the reflection phase provided the insights into the relative merits of IoSs and hybrid campaign plans.

DTAG have been designed with specific focus to assess innovations and innovative solutions identified during the first cycle of Hybrid Threats gaps-solutions analysis and research. It was presented during the exercise in the form of IoS relevant for each Vignette and specific challenges (Injects). Each Vignette have been provided with 5-7 possible solutions.

During the exercise each Vignette team have been split into two competing groups in order to gamify the process and to provide structure allowing second opinion on each case.

In the, first place, teams have been working on scenario provided including Injects based on their current knowledge and using the solutions available on the market. Afterwards teams have been introduced with new relevant developments and innovative solutions planned to be available in near future. It was introduced by moderating teams with solutions presentations and explanation on overall solutions idea, objectives as well core design. Teams have been elaborating how the solutions could improve response to different challenges as well to overall scenario. The teams have been asked to select most feasible innovative solution for each individual challenge 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 (organized anonymously using assessment tool). Finally, each participant have been provided with assessment forms to give their structured feedback as well comments and other reflections per each scenario, per each selected innovation. They also have been asked to provide relevant improvement points or additional expectations they would see relevant and important for each innovation.

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

NB! In short, all innovations introduced have been named as really necessary and important for future Hybrid Threats domain evolution.

5.5 REVIEW OF AVAILABLE TRAINING AND OTHER RELEVANT MATERIALS

Many EU-HYBNET consortium partners and stakeholder group members have background of training provider on Hybrid Threats and the exciting programs and materials is well know. However. In order to avoid delivery of overlapping scenarios and training and delivery of overlapping training materials EU-HYBNET T2.4 initiated a survey that aimed to identify and analyse other available trainings.

To accomplish this, T2.4 created a Questionnaire that was disseminated to EU-HYBNET consortium partners and Stakeholder Group members. Survey was executed during September, 2020.

27 organizations participated in the survey and provided information on their training and education programs in the Hybrid Threats domain.

Overview of the training programs and materials received during the survey

Training programs:

- Hybrid CoE – two training programs reviewed:
    - Countering Electoral Influence training.
    - Hybrid Deterrence training
- MVNIA - "Strategic Communication to Counter Security Threats in the Disinformation Era"
    - The course aims to increase knowledge and competences of institutional spokespersons and journalists (including young professionals in journalism and related areas) in the field of security and defense.
- ESDC – Few training programs were reviewed:
    - Cyber Security Basics for non Technical Experts
    - Training in Information Security Management
    - Cybersecurity Organizational and Defensive Capabilities
    - Critical Infrastructures in the Context Of Digitization
    - The Role of the EU Cyber Ecosystem in the Global Cyber Security Stability
    - Challenges EU Cyber Security
- MALDITA - raining program
    - Complete curricula of training and courses on fact checking, hoax debunking, media literacy and critical thinking.
- L3CE - Societal Impact Assessment Training (designed and given within the scope of the Driver+ project)
    - Raise awareness of the concept of Societal Impact of solutions used during a crisis, i.e. regarding the possible detrimental impacts of the unexpected and unintentional negative use of solutions.
- URJC – Training on intelligence gathering and analysis.

Research papers, scenarios and presentations relevant for the subject were also collected. They could serve as an input for scenarios, Vignettes or other forms of inputs also as other components that can be included to the trainings.

Research papers:

- MTES - "Hybrid Threats and Ecological Transition"
    - Focuses on prospective issues related to Hybrid Threats, analyses how the ecological transition, relying on digital and interconnected technologies, might be a hybrid vector.
- MTES - Outputs of "SANCTUM" project (Strategic decision-making tool)
    - Provides a description of SANCTUM concepts and initial results. SANCTUM is being developed by a consortium of French engineering "Grandes écoles", Freie Universität and Institute Fraunhofer of Berlin and Bundeswehr University of Munich. It aims to develop a decision support tool dedicated to crisis management by combining social sciences and computational sciences, and to develop anticipatory skills and good habits in dealing with hybrid threat issues.
- PLV – research about the main security aspects and threats of the country.

Exercises**:**

- Hybrid CoE – two report on exercises were presented
    - COVID mapping exercise
    - Deterrence exercise
- MVNIA - Security Gaming Scenario: "The new power kit"
    - Deals with policies of attraction, subversion and projection in the Black Sea Region; was designed to serve as an interactive training tool for the participants in the "Security in the Black Sea Region: Shared Challenges, Sustainable Future" Program. The exercise embraces the need to bring together practitioners, policymakers and stakeholders from a variety of

national backgrounds, and incorporates multicultural formats and multi-purpose teams. The learning model employed integrates specific conceptual and practical elements.

Experimental initiatives:

- MVNIA - Experimental laboratories designed in the ARMOUR project
  - This project aims to address societal polarization caused by the adoption and spread of extremist ideologies by creating an interdisciplinary model of learning that will be used to educate individuals and mainstream communities.

Presentations (online, based on volume):

- MVNIA - Countering Hybrid Threats: Lessons Learned from Ukraine
- MVNIA deliverables from the CARISMAND project – Culture And RISK management in Man-made And Natural Disasters, Risk communication and the role of the media in risk communication, and Report on the Role of the Media in Disaster Risk Communication
- UniBW/COMTESSA - How to improve security using artificial intelligence/machine learning tools and how they can be applied to improve security in many domains such as cybersecurity, open-source intelligence, etc.

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.

The training programs assessed focused more on the methodological, topical approaches and less on the innovations applicability to prioritized hybrid threats those have been named by practitioners as gaps. As most suitable approach NATO DTAG framework was chosen for the first training cycle as a training format.

Several of the training materials proposed were not prioritized for the first training cycle. These will, however, be taken into account during the next set of cycles.

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

Questionnaires are presented in Annex I. Survey results can be found in Section 8 - Evaluation results.

6 DTAG TRAINING METHODOLOGY

The DTAG is meant to stimulate a creative discussion between practitioners on the impact of new technologies on hybrid threats. It is intended to be fun, flexible and thought-provoking. There is no predetermined “right answer.” At the same time, the results of the DTAG are meant to be aggregated in order to provide insights that could be leveraged by the project and allow for the identification of promising areas of research, synergies and gaps to be addressed further, and most importantly to test the selected innovations to the gaps and needs.

6.1 GAMEPLAY SUMMARY

The

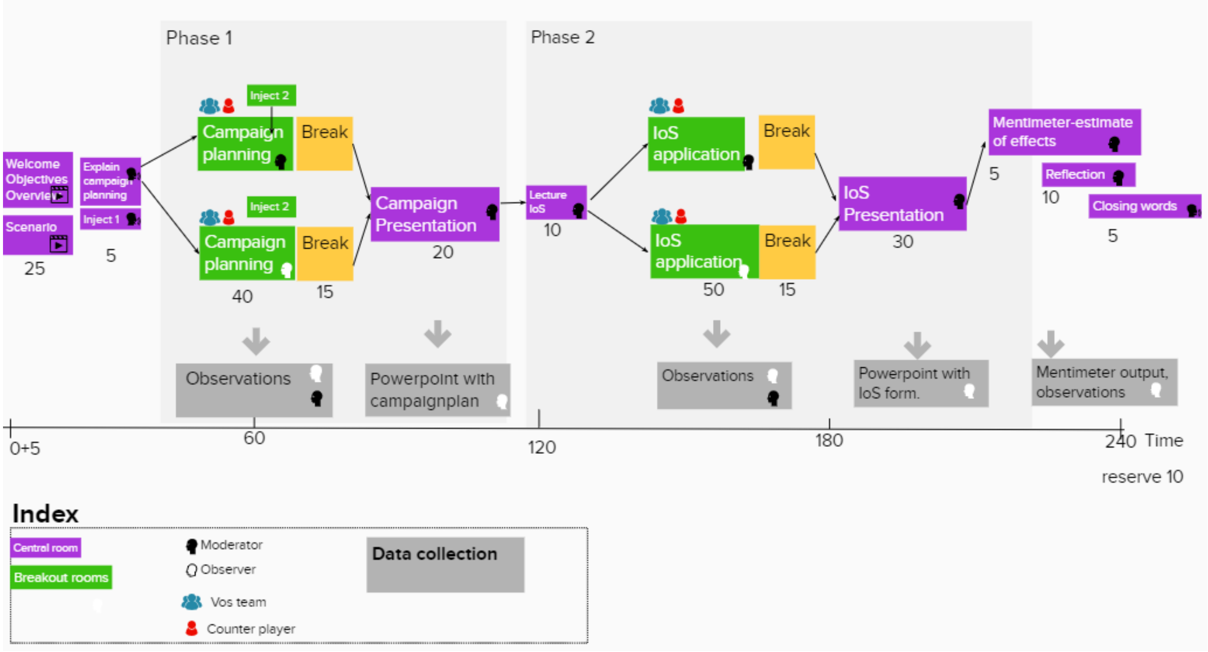


Figure 2 Shows a brief outline of the entire DTAG gameplay (more info in section 4)

The image above shows a brief overview of the entire gameplay which is expanded upon in section 4. The DTAG begins with a welcome, informing the players of the schedule and objectives of the game, an introduction to the scenario and the objectives of the vignette and the first inject in the central room. This is followed by a campaign planning phase where players are split into two teams and will have to tackle the different hybrid threats within the vignette as well as the second inject. After this players are brought back into the central room where they will present their campaign plan to tackle the threats.
After this the IoS cards that are relevant to the vignette are introduced and the players select the IoSs they want to use in their campaign and describe how they will apply those IoSs in their campaign. The players come back to the central room again and both teams present their operationalization of their IoSs. Finally, all players make a judgement of the effectivity of each IoS, followed by a brief reflection on the game and closing words.
For further reference and detailed explanation of the game phases, please see section 4.

6.2 DEFINITIONS AND TERMS

- Scenario – the overall campaign setting
- Vignette – the specific events which occurs within the scenario
- Injects(s) – additions to the vignette which add new challenges, tensions and difficulty.
- Campaign planning - Players enter a breakout room whereby they must develop a campaign plan to tackle the injects and vignette
- Campaign presentation- players present their teams campaign plan in the central room.
- Lecture IoS – Ideas of Systems innovations which are presented
- IoS Application - Players describe how they will apply the IoSs they selected in their campaign.

IoS Presentation - players present their teams operationalization of the IoSs selected in the central room.

6.3 TEAMS

Players will be placed into their respective central room, corresponding with their assigned vignette. Each DTAG will have 6-8 players, an observer, and a moderator (see section 3.4-3.8 for further descriptions). Each DTAG shall play a single vignette building on the overall scenario.

Furthermore, later in the DTAG, players will be placed into breakout rooms. 4 players will be chosen to play team 1 while 4 other players will be chosen to play team 2.

We encourage all members to turn on their cameras throughout the session. This is an essential element of gameplay as it encourages team discussion and active participation. Similarly, the chat function should be enabled for those who wish to comment during a discussion or write out their comments/inputs for the moderator.

In the image below you will find the room structure.

Syndicate room

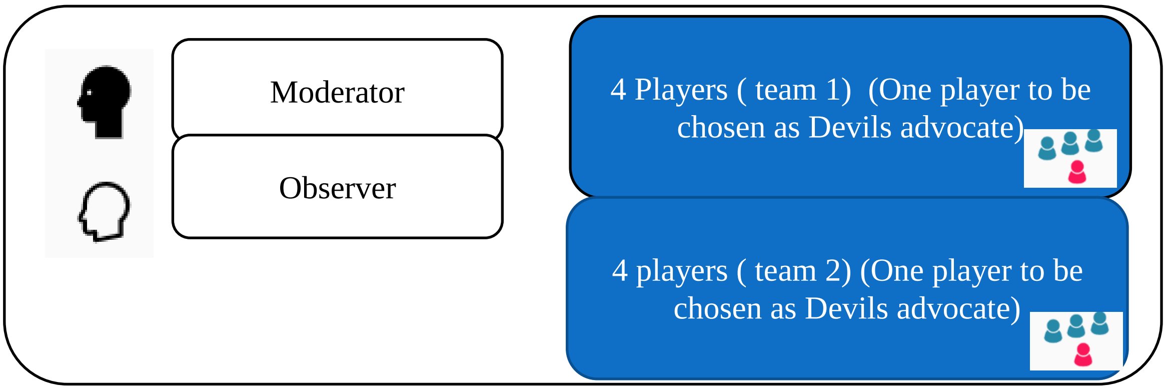

Moderator
Observer
4 Players (team 1) (One player to be chosen as Devils advocate)
4 players (team 2) (One player to be chosen as Devils advocate)

Figure 3 Shows Central room with two breakout room teams

6.4 MODERATOR

As a moderator you have a number of responsibilities both in the Central room as well as in the breakout room of Team 1.

Central room

The moderator is responsible for making sure the DTAG runs smoothly, on time and without issue. You will be in charge of making sure that during the campaign presentation phase(s) of the DTAG the two discussions and presentations between the two teams run seamlessly and that all points have been discussed within the central room when players return from their breakout rooms.

In the central room you the moderator needs to ensure that players discuss how they would operationalize their IoSs in the context of their campaign plan, how they would utilize it within the context of the vignette as well as why they would choose these specific IoSs.

Further tasks include introducing the scenario and the vignette to the players before they begin with their campaign planning.

Breakout room

While the teams are in their separate breakout rooms you will also be responsible for facilitating the discussion in teams 1 room. Additionally, make sure that a single player is chosen to be the so called “devils advocate” (see 3.7) Furthermore, in the first phase of the DTAG you will also need to introduce the predefined inject 2 for the players. These injects are small additions to the vignette which increase both the tension within and difficulty of the vignette, **inject 2 will need to be introduced after 20 minutes, in the first phase of the DTAG.**

Data collection on IoS application
Players will be provided with 2 PowerPoints (available on EU-HYBNET intranet platform “Eduuni” and players have access to these within their player guide).

1. For the campaign planning and
2. For the IoS operationalization phase in which they will be asked how they would use a particular IoS .

In addition, all supplementing materials have been provided to the training participants via email.

6.5 OBSERVER

As an observer you have a number of responsibility both in the central room as well as in the breakout room of Team 2.

Video capture of the whole session: elements of the DTAG are used for the training package and hence the full session needed to be captured. Participants were notified of this and asked whether they had reservations about their face being visible on the video. If they had objections, they could switch teams (the moderator does not capture anything on video) and switch of their camera during the central sessions.

Central room
The main tasks of the observer is to make observations during the discussions and to collect the written results of the discussion held by the teams.
There are three moments when data is needed to collect:

1. After the Campaign presentations (phase 1);
2. After the IoS presentations (phase 2), and
3. When players have filled out the Menti-meter towards the end of the DTAG. (see section 4)

Also, if something of interest is discussed by the teams during the campaign presentation phases then these remarks should be noted down by the observer.

Menti-meter- Assessment of effectivity
When players present their IoS operationalization, the observer will set up a Menti-meter in which the players will be asked whether they believe the chosen IoS would be effective in the hybrid scenario with which they have been presented.

Breakout room
While the teams are in their separate breakout rooms, the observer will also be responsible for facilitating discussion in the team 2 room. Additionally, to make sure that a single player is chosen to be the so called “devil’s advocate” (see 3.7). Furthermore, in the first phase of the DTAG observer also needed to introduce inject 2 for the players. This inject is a small addition to the vignette which increase both the tension and difficult of the vignette, **inject 2 will need to be introduced after 20 minutes to the players in the first phase of the DTAG.**

Data collection on IoS application
Players will be provided with 2 PowerPoints (players have access to these within their player guide):

1. For the campaign planning and
2. For the IoS operationalization phase in which they were asked how they would use a particular IoS .

6.6 TEAM ROLES DESCRIPTION

The purpose of the DTAG is to discover how participants face disruptions and hybrid threats.
First phase: They do so by developing a campaign plan in which they highlight how they aim to tackle the various different Hybrid Threats using present day ways and means. They will be provided a pre-made PowerPoint slide in which they can describe their campaign plan and will present these in the campaign presentation phase.
Second phase: In the second phase of the DTAG, players will be introduced to various different IoS cards linked to their particular vignette. The players will need to develop a IoS plan in which they will discuss which IoS they would find suitable for a given vignette/inject and how they would apply it within the context of their campaign plan. **They may only choose a total of 2 IoSs.** They will be provided a pre-made PowerPoint slide in which they

can fill in their information and will present these in the second campaign presentation phase (IoS campaign presentation).

6.7 DEVIL'S ADVOCATE

At the beginning of phase 1, every team shall designate a single player to be the devil's advocate of the team. Essentially this player represent the *adversary* and by that, this player shall take on the responsibility of indicating how he/she would counter the actions taken by the team. This should make the team think about how to anticipate such countering.
In the first phase of the game, this player indicates how the campaign created by the team could be countered.
In the second phase of the DTAG, the devils advocate player takes on a similar role; Arguing against the chosen IoS and possibly also providing insights into how the IoS may be exploited by adversaries.

6.8 VIRTUAL ENVIRONMENT

The DTAG uses Zoom as the communications medium. Participants receive an e-mailed invitation to the game which takes them straight to the central room based on their assigned vignette. An example of the invitation letter can be found in Annex II. All breakout rooms together with the central room will have been set up in advance by the moderators. However, if moderators prefer a different virtual environment, they are free to use that instead.

7 GAMEPLAY - GAMEPLAN DTAG

The DTAG was organized in the following way:

- Four parallel sessions delivered on April 22nd, 2021 (12:30CET-16:30 CET)
- Four parallel sessions delivered on April 29th, 2021 (12:30 CET-16:30 CET)

All sessions were to be executed simultaneously. Participants were encouraged to participate in one training session out of the four offered training sessions:

- Strategic inter-agency coordination-need for damage assessment and contingency management at strategic level;
- Attacks on financial sector, vaccine chained individual data – need for response;
- Sanitary restrictions and regionalized protest and movement-need for integration;
- STRATCOM and state-citizen-Media trust.

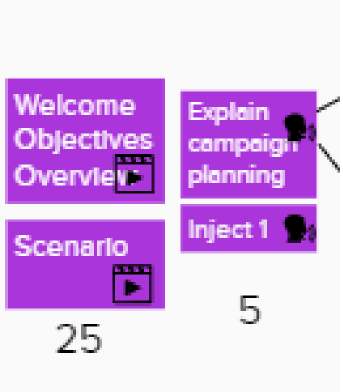
The table contains the general flow of the game.

Time	Item	Purpose
12:30-13:00 (30 min)	Introduction (Welcome and introduction to campaign)	General introduction
13:00- 13:45 (45 min)	Breakout rooms blue teams- Campaign planning	Have players become acquainted with the vignette, injects, and campaign plan of the DTAG
13:45-14:00 (15 min)	Break	Break
14:00-14:20 (20 min)	Presentation of campaign plan	Have players become acquainted with how interaction works
14:20-14:30 (10 min)	Introduction to IoS cards	Introduce players to IoS in Vignette
14:30-15:20 (50 min)	Breakout rooms blue teams - IoS campaign planning	Have players develop a campaign plan with the introduced IoS cards.
15:20-15:35 (15 min)	Break	
15:35- 16:05 (30 min)	Presentation of campaign plan	Have players discuss with one another how the IoS cards will be utilized
16:05-16:10 (5 min)	Questionnaire – round off	
16:10-16:20 (10 min)	Quick reflection	
16:20-16:25 (5 min)	Closing words	

Table 1 shows the general flow of the DTAG game- all times shown are based off CET on the game day itself

7.1 INTRODUCTION – 30 MINUTES

Overall there was 4 simultaneous DTAGs training session taking place during both 22nd and 29th of April (8 in total). This document describes the course of a single DTAG because the frames were the same to all training sessions.



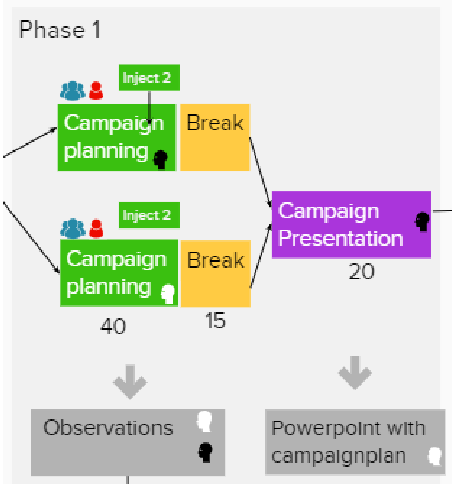
In the first part of the DTAG, all players are placed in their own central room together with a game moderator, and an observer (see section 3 for role description). After a brief welcome they will be introduced to the scenario and vignette.

The moderator will give instructions about the roles and tasks of the players. Once this has been done players will be split in two teams and put into separate breakout rooms. Each team shall consist of 4 players, one of which will be facilitated by the moderator, while the other by the observer.

When players enter their breakout rooms two things need to be agreed upon:

- one of the 4 players must be chosen/volunteered to *play the devil's advocate role*. (see section 3.7).
- one of the 4 players must be chosen/volunteered to *present the campaign-plan* later on in the central room, he/she also needs to take notes in the PowerPoint template which they can found in the player handbook.

7.2 PHASE 1: CAMPAIGN PLANNING – 40 +15 MINS



In the first phase of the DTAG both teams are tasked to develope a campaign plan on how they would deal with the events happening within the Vignette as well as the increasing tension and difficulty brought on by the injects. Players must look at current day tools, technology and social innovations which they might utilize in order to combat the evolving situation. In the meantime, the devil's advocate must provide counter-arguments against the ideas being developed within their blue team, that is, indicate how an adversary would counter the activities the campaign plan.

Campaign planning – 40 minutes

The total time for this campaign plan is 40 minutes and the facilitators will provide an inject after 20 minutes. (see section 3) An inject will provide an extra challenge for players and it is the task of both blue teams to think of ways in which they can counter these threats. In this phase, both teams can only use current day tools, technology and social innovations. During the first phase the IoS cards are not yet shared with nor used by the players. If players do use an innovation which is currently already present that is completely fine.

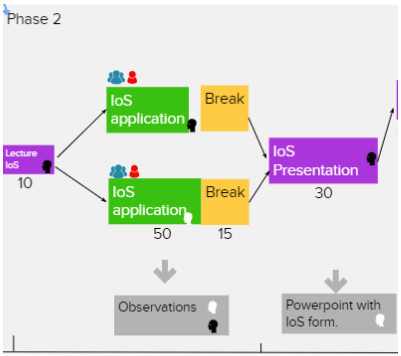
Break – 15 minutes

After players have decided on their campaign plan, a brief break will follow.

Campaign plan presentation(s) phase 1 – 20 minutes

After the break, the players return to the main central room and a presentation of their campaign plan phase will take place between the two teams (5 minutes each). Both teams present their campaign plan and the intended effects and the other team can ask questions or challenge elements of the campaign plan.

7.3 PHASE 2: IOS OPERATIONALIZATION – 10 + 50 +15 MINS



Lecture IoSs– 10 minutes

Once the first campaign presentation phase is over, the moderator gives a short 10 minutes lecture about the IoS cards associated with their vignette. A PowerPoint is provided (in Eduuni) but moderators can change this presentation if that better suit their needs. After this presentation and questions, the team goes back to the break out rooms.

IoS operationalization –50 minutes

In their breakout rooms, the teams have 50 minutes to choose which IoS cards they would use within their earlier developed campaign plan and discuss how they would operationalize and utilize their chosen IoSs. Players need to select a maximum of 2 IoS total. Players may not come up with their own IoS ideas as this goes against the aims of the EU-HYBNET Project. Both teams need to operationalize their chosen IoS cards and explain how they'd implement this innovation in the context of the Vignette. In the meantime the devil's advocate to provide counter advice tries to come up with ways to counter the implementation of the IoSses. Both teams are provided PowerPoint templates to fill out their actions.

Please note: Selection of IoSs: Short- versus long term

In the dry run T2.4 noticed that the selection of IoSs triggered a discussion on whether to select IoSs that would take years to develop. In the middle of a major crisis, generally players would only select measures that can be implemented right away and not select innovations that would still be years away from implementation. We really want to avoid that players only select IoSs that offer short term solutions. So this requires the following explanation to the players:

The crisis in the scenario takes place in **2025**. However, we assume that our players could have decided in **2021** which innovations to develop in anticipation on evolving hybrid threats. So, this would have given 4 years to develop the IoSs and thus have them available in this crisis, hybrid attack.

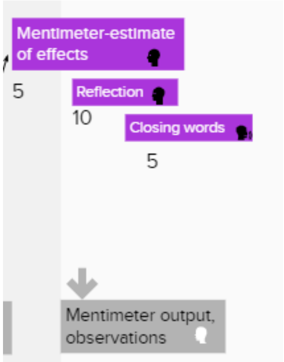
Break – 15 minutes

After players have filled out the PowerPoint slides on the operationalization of the IoSses, a 15 minute break follows.

IoS campaign plan presentation phase 2 -30 minutes

Central room: After the players return from their break, the IoS presentations take place (7 minutes for each team) using the PowerPoint template for the IoSs. After both teams have presented their campaign plan for the inject and discussed which IoS they may use.

7.4 QUESTIONNAIRE, REFLECTION AND CLOSING WORDS


Mentimeter-estimate of effects
5
Reflection
10
Closing words
5
Mentimeter output, observations

After ending the discussion on the IoSs, both teams were asked via the use of a Menti-meter vote on how effective they believe the IoS(s) of both teams would be within the context of the vignette, given the presentation of both teams. For this they will have to act as a objective observer and this set aside their team perspective.

Finally, the moderator runs a short reflection on the game and ends the game with some closing words. With that the DTAG is run and observers collect the PowerPoints, and Menti-meter results.

8 TARGET AUDIENCE AND ATTENDANCE

The DTAG training was organized with a specific focus on EU-HYBNET consortium partners and Stakeholder Group members. Registrants 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.

8.1 REGISTRATION RESULTS

A total of 64 individuals registered for the DTAG.
The Vignette : "STRATCOM and state-citizen-media trust" was the most popular choice among the participants and their registration was completed in a couple of days. Less popular Vignettes required extra work and time to confirm the planned number of participants.

The onboarding process for participants took over two months. The registration process proceeded slowly and was impacted by different commitments and engagements on the part of various organizations, whether parallel EU events, projects or initiatives. Due to the limited availability of experts in the field, some organizations sent participants that were less familiar with the hybrid threats domain though they had the interest to increase their knowledge on hybrid threats.

As Vignettes are designed to address the highly complex nature of hybrid threats and attacks, it is critical to have sufficient expertise around the table. Unfortunately, that was not the case in all instances. In future, it may be necessary to introduce a screening process of participants or a clear definition of minimum expertise requirements for successful participation, as well minimum critical value maintenance for all process execution. In addition, it is important to have a lecture in the beginning of the training focused of hybrid threats topicality. This will ensure that all training participants are familiar with the EC Conceptual Model of Hybrid Threats. Still a goal of EU-HYBNET project is to increase knowledge of hybrid threats and how to counter hybrid attacks. Therefore, participants who aim to increase their knowledge on the field, can be seen very valuable for the EU-HYBNET project training and project impact in general.

9 LIST OF MATERIALS DISTRIBUTED

Participants have been provided with a Hand-out package of pre-reading materials 4 days before the DTAG including:

- IoS form
- IoS cards that describe the innovations for entire DTAG
- IoS cards for Vignettes
- Player guide – EU-HYBNET Vignette
- Scenario and Vignette overview: Vignette

The Moderators have been provided with a Moderator care package which includes:

- Master slide deck –It included;
    - Introduction slide
    - Video with scenario explanation
    - Vignette and Injects
    - IoS presentation
    - Menti-meter reminder slide
    - Reflection slide
- Scenario and vignette overview
- IoS cards DTAG – a PDF that includes all the IoS innovations
- IoS cards Vignette 1 –a PDF which contains the IoS innovations which will be used for particular vignette.
- Moderator guide.
- The powerpoint fill in forms for the players to use.

10 EVALUATION

The DTAG training was designed to test innovations in order to assess which of these might be considered for formal uptake by practitioner organizations. In this context the EU-HYBNET training evaluation component focused on both, the skill levels of practitioners and the importance of specific innovations to the participants involved.

Two types of questionnaires were used as a means of evaluation:

- The participating organization and the current state of the trainee, regarding their knowledge and skill level.
- IoS feasibility in solving the challenges posed by different Vignettes, as well as its potential to be effectively operationalized. IoS included both technical and non-technical/ human science based innovations

The DTAG training evaluation was based on 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)

The innovations evaluation was based on the EU-HYBNET innovation assessment methodology developed by WP3 T3.1 and covers three main aspects:

- Excellence
- Impact
- Implementation

Scoring of innovation effectiveness employed a scale of 0-5 and addressed various issues, adopting relevant interpretations.

Questionnaires were administered electronically using measurement forms, which allowed for the collection of a large dataset of information with relatively little effort.

Copies of the questionnaires are included in Annex I while the feedback from each tool is summarized in Section 11 – “EVALUATION RESULTS”.

11 EVALUATION RESULTS

Overall, the response from participants was positive. The DTAG format was accepted well. 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.

DTAG EVALUATION:

Assessment criteria	Number of responses	Cumulative score	Key Comments
The Content of the Training and Exercise event evaluation			
Relevance of the training	8	4,375	
Uniqueness of the training compared to other trainings on hybrid threats	8	3,875	
Relevance of the scenario	8	4,125	
Clarity of the scenario	8	3,75	
Other relevant topics (if any) to be added for the upcoming trainings	3	• Some of the participants have found the scenarios useful however to challenging to play • Some comments from participants having less technical knowledge especially cyber related therefore identified the need to have well balanced team • Some comments related to innovations deeper analysis expressed the willingness to invite technology providers and industry partners • Most of participants have identified and expressed the need for much more explicit preparation before the event • Some of the participants have questioned necessity of the scenario and suggested to have more emphasis on IoS's • A lot of participants have commented (verbally during the feedback time of the event but not in formal assessments) that they are lacking of knowledge, skills and experience to participate in such kind of exercise in full capacity • Also it was commented that scenario have been too much repeating the current pandemic situation and could be redesigned more for the future	
Comments	5	• Some comments provided great recognition of the event and all the aspects related to it and in addition would prefer more explicit information on IoS	

		• Some of participants have identified lack of in-depth description and interconnectedness between provided IoS's • Some of the participant identified the need of experts participation or experts opinions provided upfront, some kind of the hints • Some participants expressed the need to organise the training onsite instead of online.	
Is there a need for any improvement of the content of the training and exercise? If yes, please, specify.	5	• Few participants have identified provided injects too surprising and challenging • A lot of participants have identified the need for balanced teams • The devil's advocate position could be played by an expert • Some requested to have possibility to play on-site.	
Evaluation of support provided by Moderator through the training			
Completeness of information provided	8	4,625	
Balance between theoretical and practical aspects on the subject	8	4,375	
Support provided by moderator	8	4,875	
The moderator was well prepared for the training	8	4,875	
The moderator was an expert on the subject and provided all clarification needed	8	4,75	
Comments	4	• Lots of comments recognising the great training exercise	
Is there a need for any improvement of the moderation of the training and exercise? If yes, please, specify.	1	• Have been suggested to reconsider timing of different agenda sections	
Evaluation of Organization aspects of the training			
Prereading materials (sufficiency and clarity)	8	3,5	
Training materials (sufficiency and clarity)	8	3,875	

Was time sufficient to get into productive dialog and was time well structured	8	3,75	
Possibility to interact, discuss, share with other participants	8	4,625	
Suitability of Platform used	8	4,375	
Comments	4	• Some participants have found scenario too complicated for them • Some participants expressed the need for longer exercise organization and more space for group activities and considerations as they felt time pressure and rush • Suggested to organise it on site	
Is there a need for any improvement of the organization of the training and exercise? If yes, please, specify.		• Organise the event on site • Suggested to reconsider scenario while simplifying it. • Requested general lecture on Hybrid Threats. • Increase the number of participants in individual groups • Provide the space for self introduction of individual participants in order to learn individual backgrounds. • Engage innovation providers	
Evaluation of your general impression of the training			
Evaluation of my (as a participant) involvement in the training	8	4,125	
Evaluation of my knowledge on the training subject before the training	8	2,875	
Evaluation of my knowledge on the training subject after the training	8	3,625	
Would you recommend this training	8	4,375	
Other general comments	2	• High recognition for the training • Identified the problem particular with participants of this group as some of participants have been not open and talkative. Also lacking base knowledge • Suggested also to include expert feedback on participants solutions and response plan to address the challenges	

		provided in the scenario in order to learn how professional and valid it is in comparison to reality.	

Table 2 DTAG EVALUATION RESULTS

EVALUATION RESULTS OF MENTI-METER

The question was: How effective would you judge each of team innovations per inject

No. of vignette	Inject	Selected IoS on the 22nd of April	Selected IoS on the 29th April	The 22nd of April Score	The 29th of April Score
1	Inject 1	Cyber Information sharing system	Resilient democracy infrastructure platform	-	-
	Inject 2	Resilient democracy infrastructure platform	Resilient democracy infrastructure platform	-	-
2	Inject 1	OPENQD	Blockchain	7,6	8
	Inject 2	Public-Private information sharing groups developing collaborative investigations and collective action	Hyper connectivity	8,2	8,2
3	Inject 1	Public-Private information sharing groups developing collaborative investigations and collective action	Resilient democracy infrastructure platform	5,3	6,3
	Inject 2	Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination	Resilient democracy infrastructure platform	7	6,3
4	Inject 1	Debunking fake news	Non-partisan native-language news channels and debunk fake news platform	-	7
	Inject 2	A guide to identifying fakes	Automated fact checker	-	7,3

THE 22ND OF APRIL TRAINING IOS EVALUATION FORMS (EACH IOS HAS ITS OWN EVALUATION FORM)

Vignette 1 Inject 1. Name of the IoS - Cyber Information sharing system

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	1	Pains	
Please evaluate the level of relevance of the innovation for your organization	1	4	
Please evaluate the Excellence of the innovation			

Overall score	1	4	
Clear definition of intended scope / applicability	1	4	
Clarity and pertinence of the solution description	1	4	
Credibility and soundness of the concept	1	4	
Please evaluate potential Impact of the innovation			
Overall score	1	4	
The coverage.	1	4	
The scope	1	4	
Acceptance	1	4	
Effectiveness and robustness	1	4	
Please evaluate expected up-take/implementation difficulty level			
Overall score	1	3	
Precondition	1	4	
Implementation effort	1	4	
Implementation resources	1	4	
Life-cycle maintenance	1	4	
Time aspects	1	4	
Please provide any additional comments on innovation or up-take	0		

Table 3 VIGNETTE 1 INJECT 1 EVALUATION RESULTS

Vignette 1 Inject 2. Name of the IoS - RDIP - Resilient democracy infrastructure platform.

No evaluation was submitted.

Vignette 2 Inject 1. Name of the IoS - OPENQD

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	1	DESIRES	
Please evaluate the level of relevance of the innovation for your organization	1	1	
Please evaluate the Excellence of the innovation			
Overall score	1	3	
Clear definition of intended scope / applicability	1	2	
Clarity and pertinence of the solution description	1	2	
Credibility and soundness of the concept	1	2	
Please evaluate potential Impact of the innovation			
Overall score	1	4	
The coverage.	1	3	
The scope	1	3	
Acceptance	1	3	
Effectiveness and robustness	1	3	
Please evaluate expected up-take/implementation difficulty level			
Overall score	1	3	
Precondition	1	3	
Implementation effort	1	4	
Implementation resources	1	3	

Life-cycle maintenance	1	3	
Time aspects	1	2	
Please provide any additional comments on innovation or up-take	1	More explicit information on the innovation would help to make deeper assessment	

Table 4 VIGNETTE 2 INJECT 1 EVALUATION RESULTS

Vignette 2 Inject 2. Name of the IoS - Public-Private information sharing groups developing collaborative investigations and collective action

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	1	DESIRES	
Please evaluate the level of relevance of the innovation for your organization	1	2	
Please evaluate the Excellence of the innovation			
Overall score	1	2	
Clear definition of intended scope / applicability	1	3	
Clarity and pertinence of the solution description	1	2	
Credibility and soundness of the concept	1	2	
Please evaluate potential Impact of the innovation			
Overall score	1	4	
The coverage.	1	3	
The scope	1	3	
Acceptance	1	4	
Effectiveness and robustness	1	3	
Please evaluate expected up-take/implementation difficulty level			
Overall score	1	2	
Precondition	1	2	
Implementation effort	1	2	
Implementation resources	1	2	
Life-cycle maintenance	1	2	
Time aspects	1	2	
Please provide any additional comments on innovation or up-take	1	Difficult to assess the innovation on the information available.	

Table 5 VIGNETTE 2 INJECT 2 EVALUATION RESULTS

Vignette 3 Inject 1. Name of the IoS - Public-Private information sharing groups developing collaborative investigations and collective action

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	1	DESIRES	
Please evaluate the level of relevance of the innovation for your organization	1	2	
Please evaluate the Excellence of the innovation			
Overall score	1	2	
Clear definition of intended scope / applicability	1	2	
Clarity and pertinence of the solution description	1	3	
Credibility and soundness of the concept	1	2	
Please evaluate potential Impact of the innovation			
Overall score	1	2	
The coverage.	1	2	
The scope	1	3	
Acceptance	1	2	
Effectiveness and robustness	1	2	
Please evaluate expected up-take/implementation difficulty level			
Overall score	1	4	
Precondition	1	3	
Implementation effort	1	2	
Implementation resources	1	2	
Life-cycle maintenance	1	2	
Time aspects	1	2	
Please provide any additional comments on innovation or up-take	1	Innovations integrity aspects are not covered	

Table 6 VIGNETTE 3 INJECT 1 EVALUATION RESULTS

Vignette 3 Inject 2. Name of the IoS - Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	1	DESIRES	
Please evaluate the level of relevance of the innovation for your organization	1	2	

Please evaluate the Excellence of the innovation			
Overall score	1	2	
Clear definition of intended scope / applicability	1	2	
Clarity and pertinence of the solution description	1	2	
Credibility and soundness of the concept	1	2	
Please evaluate potential Impact of the innovation			
Overall score	1	2	
The coverage.	1	2	
The scope	1	3	
Acceptance	1	2	
Effectiveness and robustness	1	2	
Please evaluate expected up-take/implementation difficulty level			
Overall score	1	1	
Precondition	1	3	
Implementation effort	1	2	
Implementation resources	1	2	
Life-cycle maintenance	1	4	
Time aspects	1	1	
Please provide any additional comments on innovation or up-take	1	encompassing ARCHITECTURE and integrity aspects not individual innovations are not covered	

Table 7 VIGNETTE 3 INJECT 2 EVALUATION RESULTS

Vignette 4 Inject 1. Name of the IoS - Debunking fake news

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	2	DESIRES 1 PAINS 1	
Please evaluate the level of relevance of the innovation for your organization	2	3,5	
Please evaluate the Excellence of the innovation			
Overall score	2	4	
Clear definition of intended scope / applicability	2	4	
Clarity and pertinence of the solution description	2	4	
Credibility and soundness of the concept	2	4	
Please evaluate potential Impact of the innovation			
Overall score	2	4	
The coverage.	2	4,5	
The scope	2	4	
Acceptance	2	4	
Effectiveness and robustness	2	3,5	
Please evaluate expected up-take/implementation difficulty level			
Overall score	2	3,5	

Precondition	2	3,5	
Implementation effort	2	3,5	
Implementation resources	2	4	
Life-cycle maintenance	2	3,5	
Time aspects	2	3,5	
Please provide any additional comments on innovation or up-take	0		

Table 8 VIGNETTE 4 INJECT 1 EVALUATION RESULTS

Vignette 4 Inject 2. Name of the IoS - A guide to identifying fakes

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	2	PAINS 1 NEEDS 1	
Please evaluate the level of relevance of the innovation for your organization	2	3,5	
Please evaluate the Excellence of the innovation			
Overall score	2	3,5	
Clear definition of intended scope / applicability	2	3	
Clarity and pertinence of the solution description	2	3,5	
Credibility and soundness of the concept	2	3,5	
Please evaluate potential Impact of the innovation			
Overall score	2	3,5	
The coverage.	2	3,5	
The scope	2	3,5	
Acceptance	2	3,5	
Effectiveness and robustness	2	3,5	
Please evaluate expected up-take/implementation difficulty level			
Overall score	2	3,5	
Precondition	2	3	
Implementation effort	2	3,5	
Implementation resources	2	3,5	
Life-cycle maintenance	2	3,5	
Time aspects	2	4	
Please provide any additional comments on innovation or up-take	0		

Table 9 VIGNETTE 4 INJECT 2 EVALUATION RESULTS

THE 29TH OF APRIL TRAINING IOS EVALUATION FORMS (EACH IOS HAS ITS OWN EVALUATION FORM)

Vignette 1 Inject 1. Name of the IoS - Resilient democracy infrastructure platform, Hyper-personalized advertising
No evaluation received

Vignette 1 Inject 2. Name of the IoS - Resilient democracy infrastructure platform, Early damage assessment system
No evaluation received

Vignette 2 Inject 1. Name of the IoS - Blockchain

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	3	DESIRES	
Please evaluate the level of relevance of the innovation for your organization	3	3	
Please evaluate the Excellence of the innovation			
Overall score	3	2,67	
Clear definition of intended scope / applicability	3	3	
Clarity and pertinence of the solution description	3	2,67	
Credibility and soundness of the concept	3	3	
Please evaluate potential Impact of the innovation			
Overall score	3	3.33	
The coverage.	3	3.67	
The scope	3	3.67	
Acceptance	3	3.33	
Effectiveness and robustness	3	3.67	
Please evaluate expected up-take/implementation difficulty level			
Overall score	3	3.33	
Precondition	3	3.67	
Implementation effort	3	3.33	
Implementation resources	3	4	
Life-cycle maintenance	3	3.33	
Time aspects	3	3	
Please provide any additional comments on innovation or up-take	2	• To consider the innovation up take potential participants identified the need for more detailed innovation description provided by innovation developers. • Demonstration of integrity level of innovations	

Table 10 VIGNETTE 2 INJECT 1 EVALUATION RESULTS

Vignette 2 Inject 2. Name of the IoS - Hyper connectivity

Assessment criteria	Number of responses	Cumulative score	Key Comments
How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your: PAINS – would make operations more effective and innovation is very relevant. NEEDS – would expand our daily operations and/or widen scope of our current activities. DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.	2	PAINS NEEDS	
Please evaluate the level of relevance of the innovation for your organization	2	4	
Please evaluate the Excellence of the innovation			
Overall score	2	4,5	
Clear definition of intended scope / applicability	2	4ies.	
Clarity and pertinence of the solution description	2	2,5	
Credibility and soundness of the concept	2	3	
Please evaluate potential Impact of the innovation			
Overall score	2	4	
The coverage.	2	4,5	
The scope	2	4,5	
Acceptance	2	4	
Effectiveness and robustness	2	4	
Please evaluate expected up-take/implementation difficulty level			
Overall score	2	4	
Precondition	2	4	
Implementation effort	2	4,5	
Implementation resources	2	4,5	
Life-cycle maintenance	2	3,5	
Time aspects	2	3,5	
Please provide any additional comments on innovation or up-take	2	• More information is needed for deeper understanding of the innovation potential and uptake possibilities. • Participation of Innovations providers in the Trainings • Lack of information properly to assess the merits of the innovation.	

Table 11 VIGNETTE 2 INJECT 2 EVALUATION RESULTS

Vignette 3 Inject 1 and Inject 2. Name of the IoS - Resilient democracy infrastructure platform
No evaluation received.

Vignette 4 Inject 1 Name of the IoS - Non-partisan native-language news channels and debunk fake news platform
No evaluation received.

Vignette 4 Inject 2. Name of the IoS - Automated fact checker and debunking disinformation as well as Strategic personalized advertising
No evaluation received.

12 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, especially the impact of cascading effects and the role of innovations in the different security domains. In addition, they expressed a desire to arrange this type of training on site instead of running it online. 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 and should be taken into account in developing the next cycle of training.

Finding 1:

Despite the fact that the preparatory materials had been disseminated 4 days before the DTAG, due to their size and complexity, not all participants were able to get acquainted with the documents on time and prepare properly for the event. We conclude that the following would be beneficial:

- Presentation of a one hour introductory session a week prior to the commencement of training.
- Condensing the amount of pre-reading materials.
- Limiting the complexity of both the scenario and the Vignettes.

Finding 2:

Scenario and Vignettes are designed to address the complexity of the hybrid threats and attacks environment. It is critical to have a high level of expertise at the table. Including a screening process of participants or definition of minimum expertise requirements would be beneficial for successful execution of the DTAG , as well secure critical value for all process execution. However, it is important for EU-HYBNET trainings that the knowledge of hybrid threats and counter measures will increase among pan-European practitioners and other relevant actors (industry, academia, NGOs) and hence participants with good knowledge of hybrid threats and interest to learn on counter measures are seen important for training participants as well. The increase of knowledge of hybrid threats and counter measure to hybrid attacks is a key goal of EU-HYBNET trainings.

Finding 3

To maintain a proper structure for the DTAG it is critical to ensure that the relevant number of participants are included i. As a consequence, registering for the event should imply a solid commitment on the part of those intending to participate. In our case, there were numerous registrants who were 'no-shows' without prior notice. This impacted our efforts in two ways: i) there was no possibility for timely replacement of participants; and ii) this complicated the overall process, its organization and effectiveness.

The impacts varied:

- There was no possibility to split the actual attendees into two competitive groups.
- For some Vignettes, It narrowed the number of different perspectives which could have contributed to a unified hybrid campaign position.
- Small participant numbers lowered the potential impact of game results and outcomes.

The original plan was to have participants comprised of multidisciplinary groups dominated by practitioners, including RTO, industry, academics and individual discipline experts. For that to be achieved, it would be critical to structure the groups well in advance and with confirmed attendees.

Finding 4.

Four Vignettes were explored during development of the training, and two of them, "Strategic inter-agency coordination-need for damage assessment and contingency management'' and ''Strategic level and STRATCOM and state-citizen-Media trust,'' gave rise to considerable interest at the time of registration. In developing the training content for the next prject cycle, it might be worth evaluating the broader range of needs that require the most urgent attention.

At the same time, the DTAG was oriented in such a way so as to address future scenario development and the most plausible anticipated threat phenomena. For individuals who are not practitioners working in the domains of research and innovation development, this would be “Unknown” territory and therefore harder for them to understand or appreciate their respective roles. As a result, there will always be a tendency to play it safe and stick with known phenomena when challenged by the Vignettes, rather than face the “Unknown” and risk stepping outside of a comfort zone. It requires a high level of expertise and confidence, as well as a genuine interest in the context of the situation, to work in these new areas. Therefore, it is critical that we have a high level of expertise at the table in future training efforts while the project also wishes to widen the amount of hybrid threats experts.

Finding 5:

Considering that the most important aspect of the training was to evaluate the innovations and assess their impact on hybrid threats, the participants were lacking in more explicit descriptions of the innovations in order to more effectively understand the innovation’s potential and its future uptake possibilities; In general soft and social innovations were easier to understand and work with, while more complex, high tech enabled innovations lacked sufficient detail to be useful.
It is worth to 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.

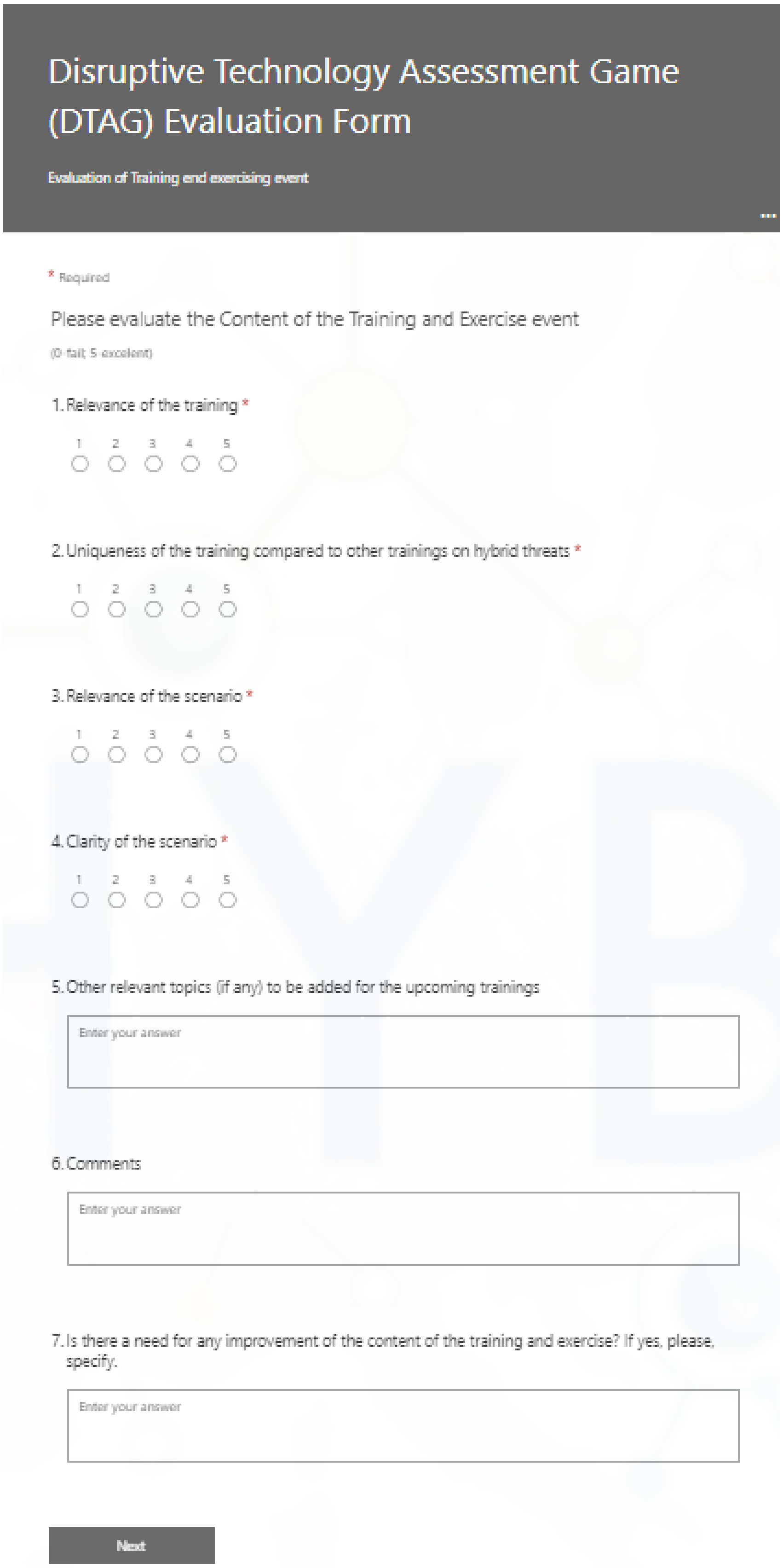
Finding 6

Even though part of the assignment was to brainstorm and come up with different ways of how IoSs can be adopted for future scenarios or new ideas as to how these might be operationalized, a few participants considered some of the IoSs to be presently available and not as innovations. There were requests as well for a comprehensive architecture that would define the place individual innovations held within a larger picture. In our subjective view, for some Vignettes, this has led to the hypothesis that we are severely lacking in the creative adoption of novel ways of thinking “out of the box” and taking advantage of skills among the practitioners and other different stakeholder group representatives who are not directly associated with research and innovation initiatives.

Finding 7

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

13 ANNEX I. DISRUPTIVE TECHNOLOGY ASSESSMENT GAME (DTAG) EVALUATION 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

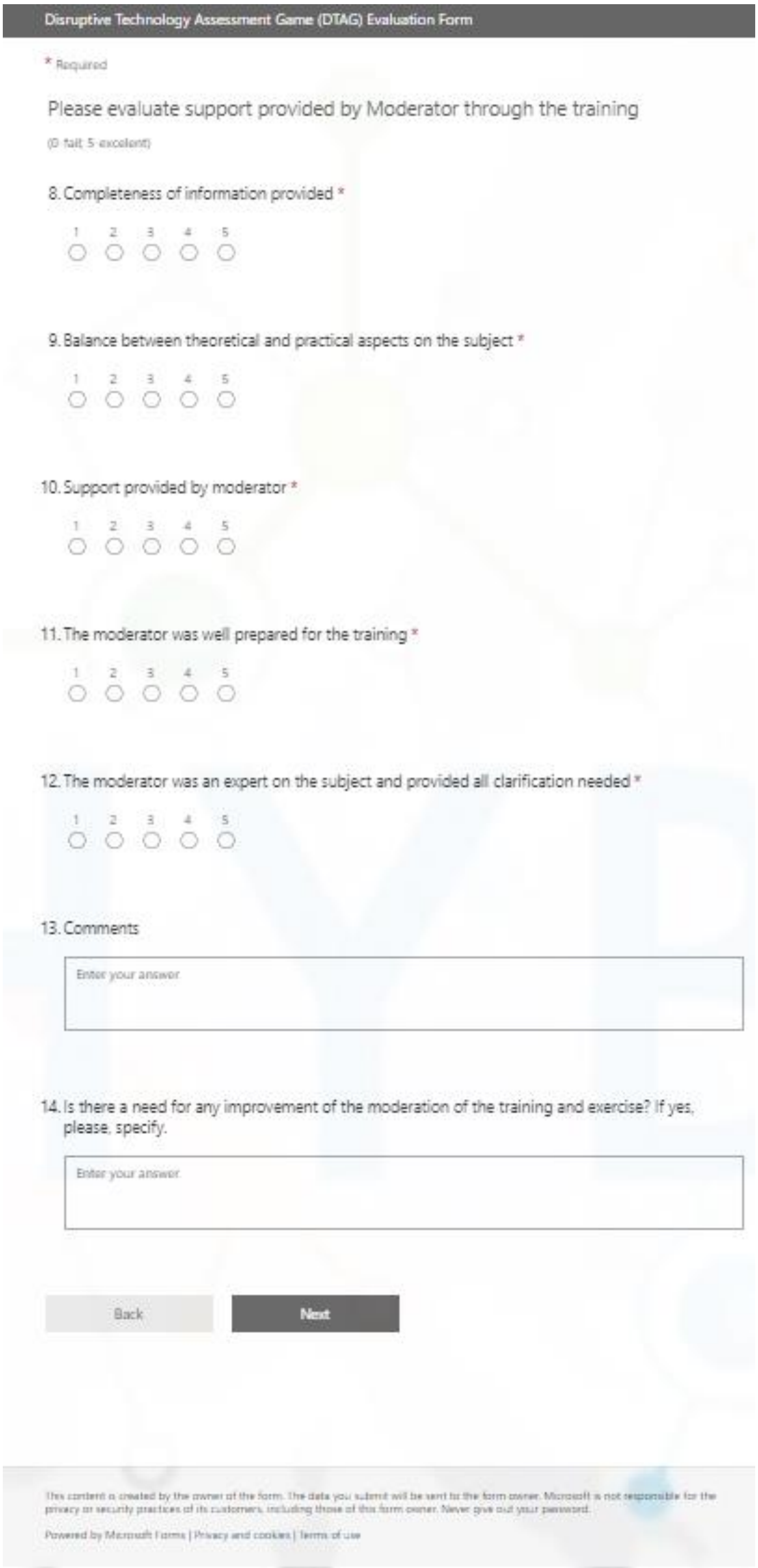
Enter your answer

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



Disruptive Technology Assessment Game (DTAG) Evaluation Form

* Required

Please evaluate support provided by Moderator through the training

(0 fail; 5 excelent)

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

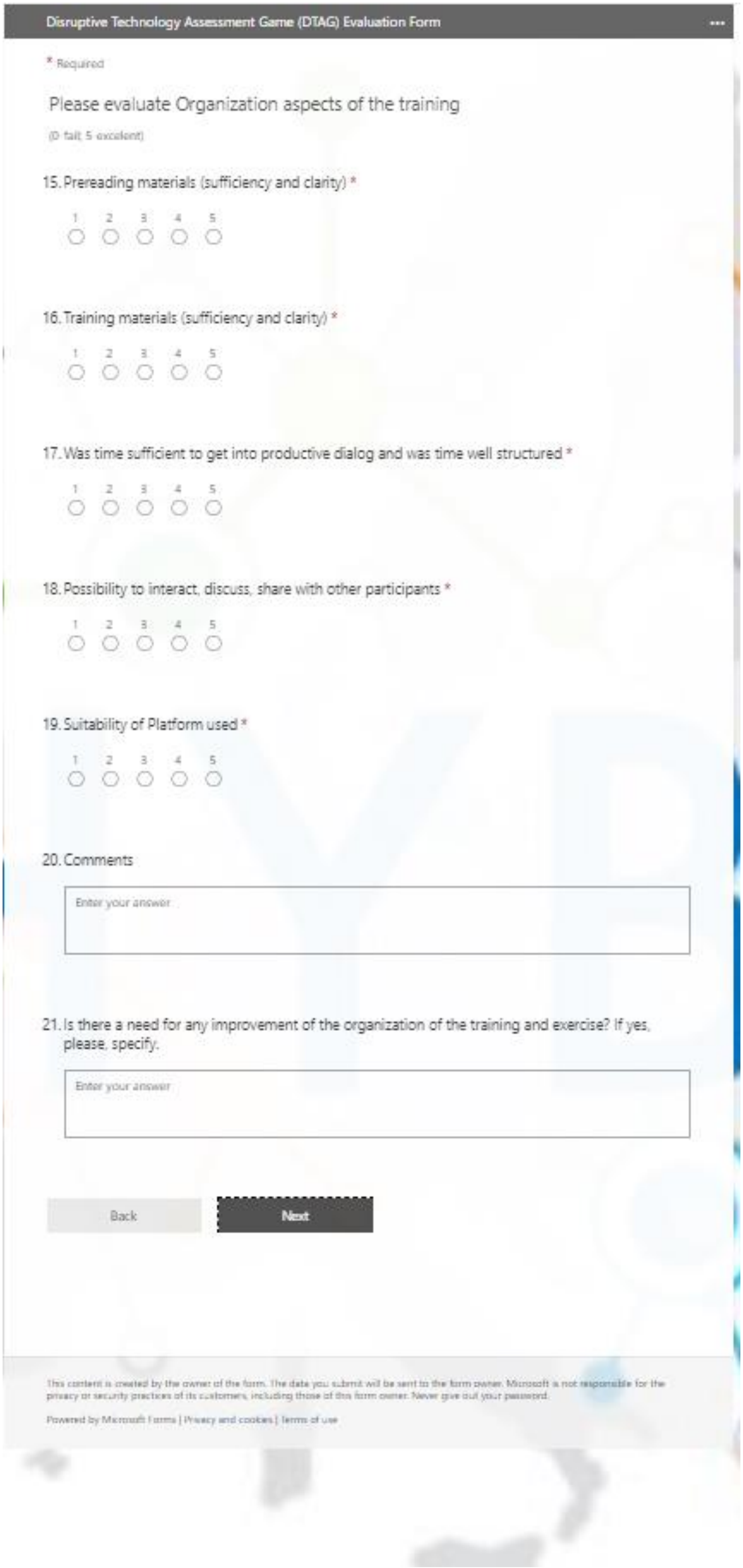
Enter your answer

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

Enter your answer

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 excelent)

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

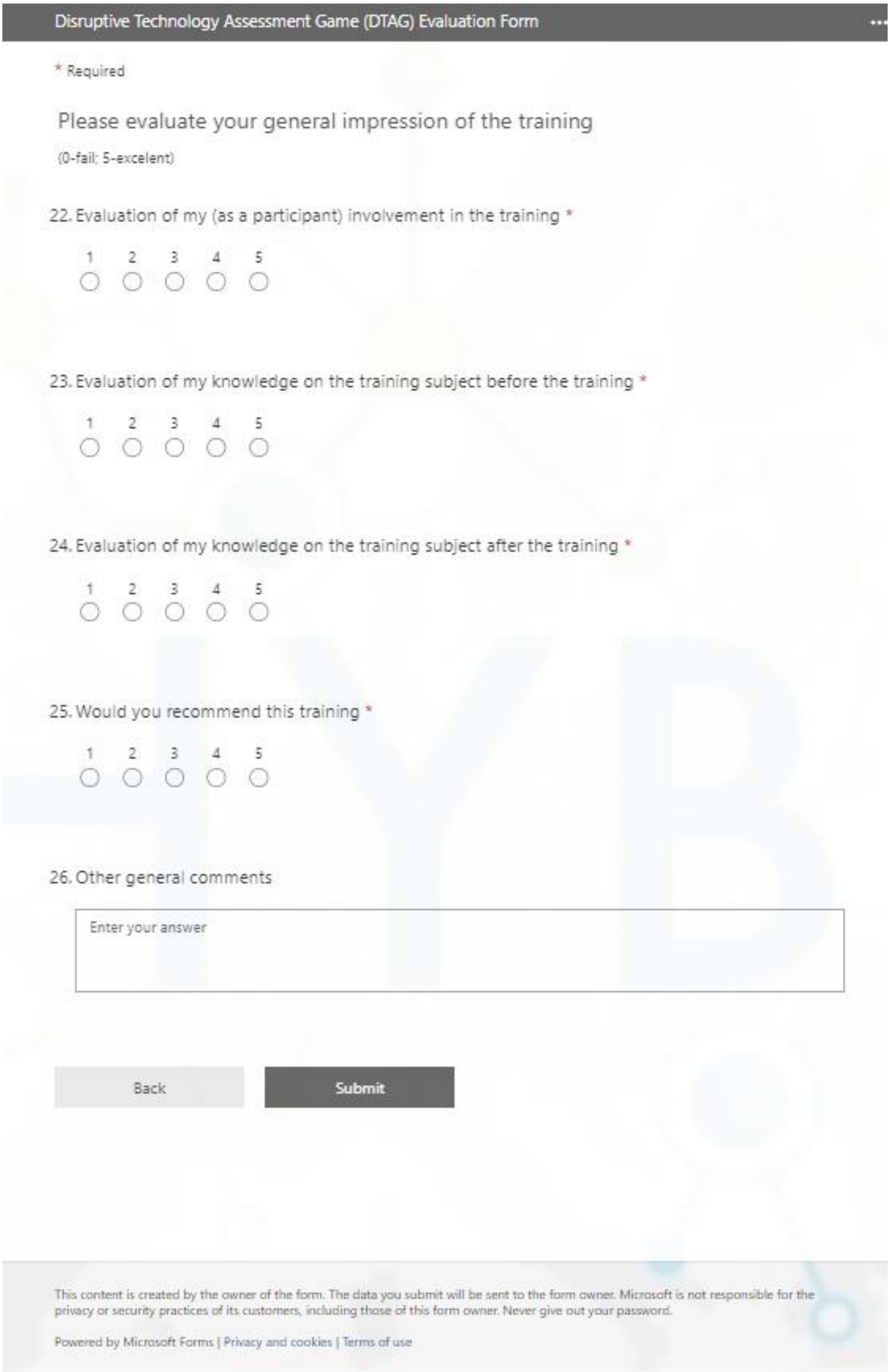
Enter your answer

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

Enter your answer

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
○	○	○	○	○

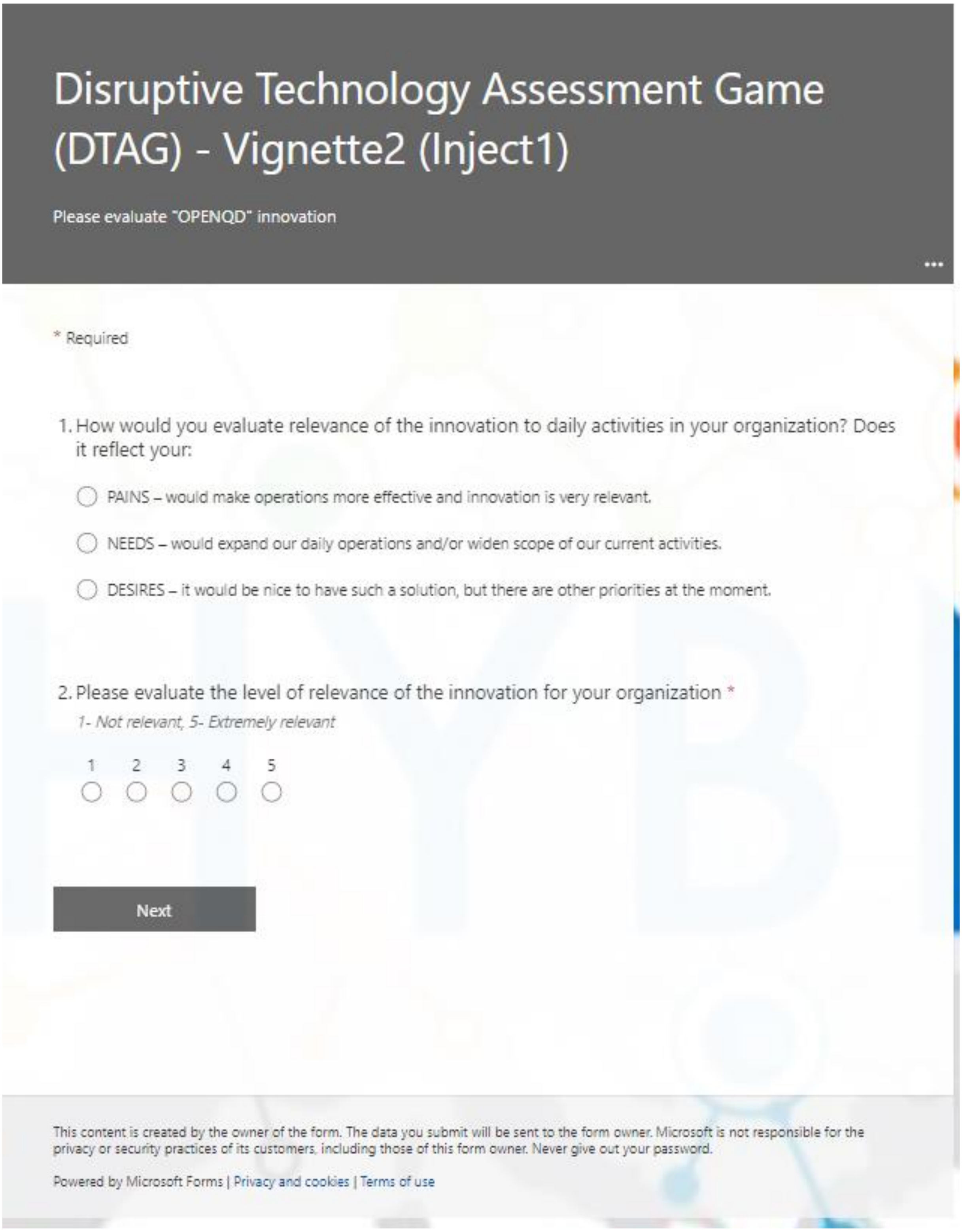
26. Other general comments

Enter your answer

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

Figure 4 THE DTAG EVALUATION QUESTIONARIES



Disruptive Technology Assessment Game (DTAG) - Vignette2 (Inject1)

Please evaluate "OPENQD" innovation

* Required

1. How would you evaluate relevance of the innovation to daily activities in your organization? Does it reflect your:

○ PAINS – would make operations more effective and innovation is very relevant.

○ NEEDS – would expand our daily operations and/or widen scope of our current activities.

○ DESIRES – it would be nice to have such a solution, but there are other priorities at the moment.

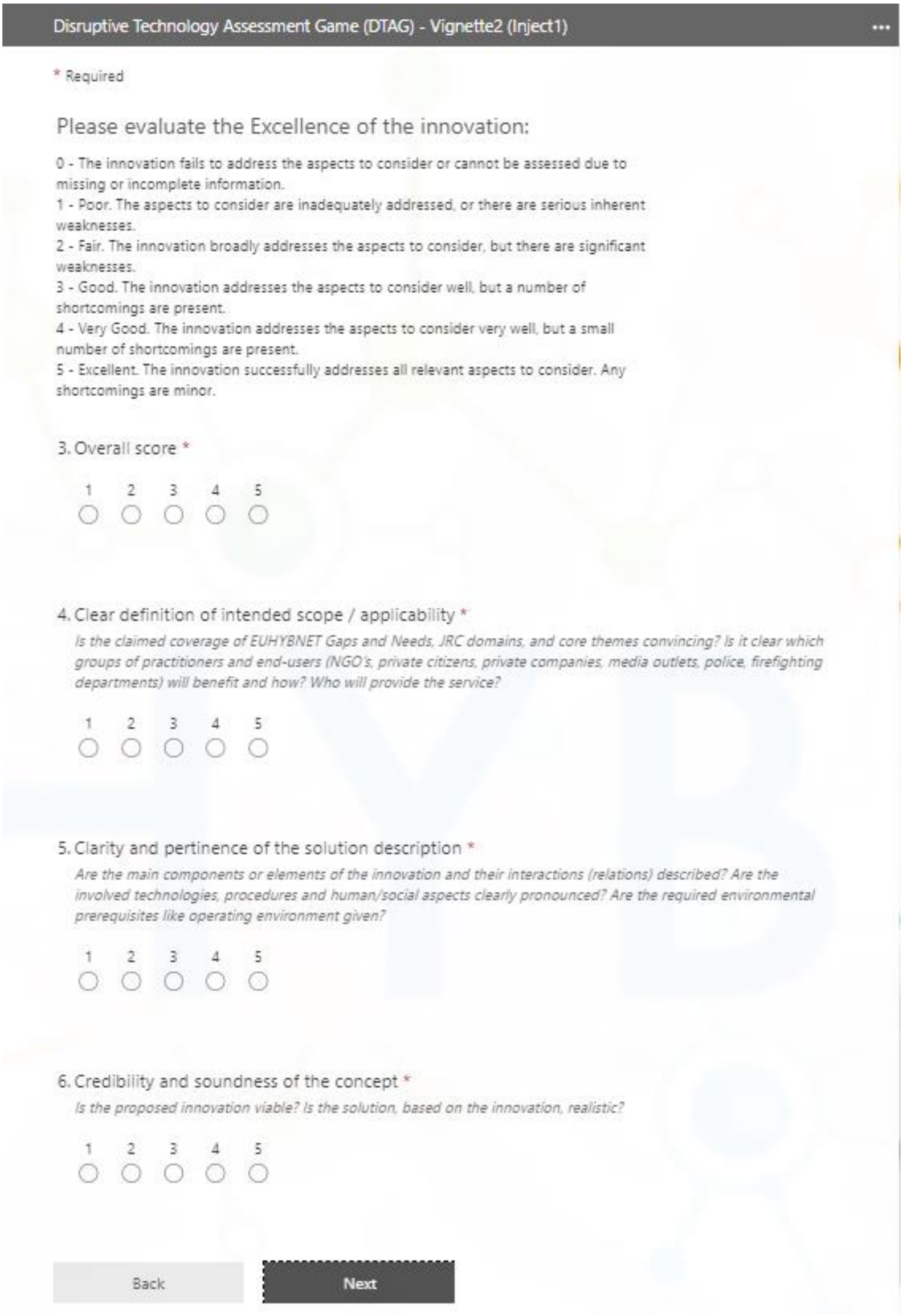
2. Please evaluate the level of relevance of the innovation for your organization *

1- Not relevant, 5- Extremely relevant

1	2	3	4	5
○	○	○	○	○

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) - Vignette2 (Inject1)

* Required

Please evaluate the Excellence of the innovation:

0 - The innovation fails to address the aspects to consider or cannot be assessed due to missing or incomplete information.
1 - Poor. The aspects to consider are inadequately addressed, or there are serious inherent weaknesses.
2 - Fair. The innovation broadly addresses the aspects to consider, but there are significant weaknesses.
3 - Good. The innovation addresses the aspects to consider well, but a number of shortcomings are present.
4 - Very Good. The innovation addresses the aspects to consider very well, but a small number of shortcomings are present.
5 - Excellent. The innovation successfully addresses all relevant aspects to consider. Any shortcomings are minor.

3. Overall score *

1	2	3	4	5
○	○	○	○	○

4. Clear definition of intended scope / applicability *

Is the claimed coverage of EUHYBNET Gaps and Needs, JRC domains, and core themes convincing? Is it clear which groups of practitioners and end-users (NGO's, private citizens, private companies, media outlets, police, firefighting departments) will benefit and how? Who will provide the service?

1	2	3	4	5
○	○	○	○	○

5. Clarity and pertinence of the solution description *

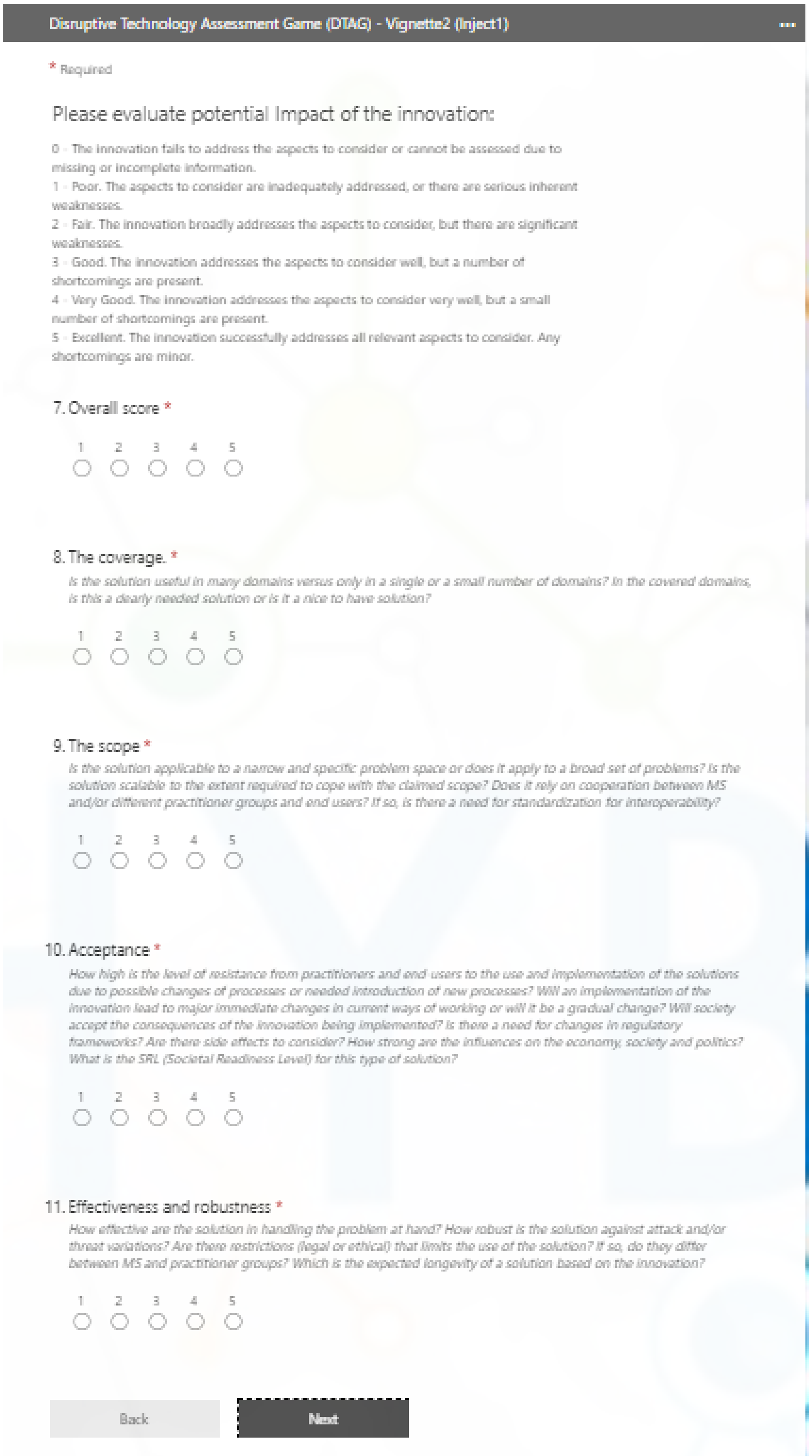
Are the main components or elements of the innovation and their interactions (relations) described? Are the involved technologies, procedures and human/social aspects clearly pronounced? Are the required environmental prerequisites like operating environment given?

1	2	3	4	5
○	○	○	○	○

6. Credibility and soundness of the concept *

Is the proposed innovation viable? Is the solution, based on the innovation, realistic?

1	2	3	4	5
○	○	○	○	○



Disruptive Technology Assessment Game (DTAG) - Vignette2 (Inject1)

* Required

Please evaluate potential Impact of the innovation:

0 - The innovation fails to address the aspects to consider or cannot be assessed due to missing or incomplete information.
1 - Poor. The aspects to consider are inadequately addressed, or there are serious inherent weaknesses.
2 - Fair. The innovation broadly addresses the aspects to consider, but there are significant weaknesses.
3 - Good. The innovation addresses the aspects to consider well, but a number of shortcomings are present.
4 - Very Good. The innovation addresses the aspects to consider very well, but a small number of shortcomings are present.
5 - Excellent. The innovation successfully addresses all relevant aspects to consider. Any shortcomings are minor.

7. Overall score *

1 2 3 4 5
○ ○ ○ ○ ○

8. The coverage. *

Is the solution useful in many domains versus only in a single or a small number of domains? In the covered domains, is this a clearly needed solution or is it a nice to have solution?

1 2 3 4 5
○ ○ ○ ○ ○

9. The scope *

Is the solution applicable to a narrow and specific problem space or does it apply to a broad set of problems? Is the solution scalable to the extent required to cope with the claimed scope? Does it rely on cooperation between MS and/or different practitioner groups and end users? If so, is there a need for standardization for interoperability?

1 2 3 4 5
○ ○ ○ ○ ○

10. Acceptance *

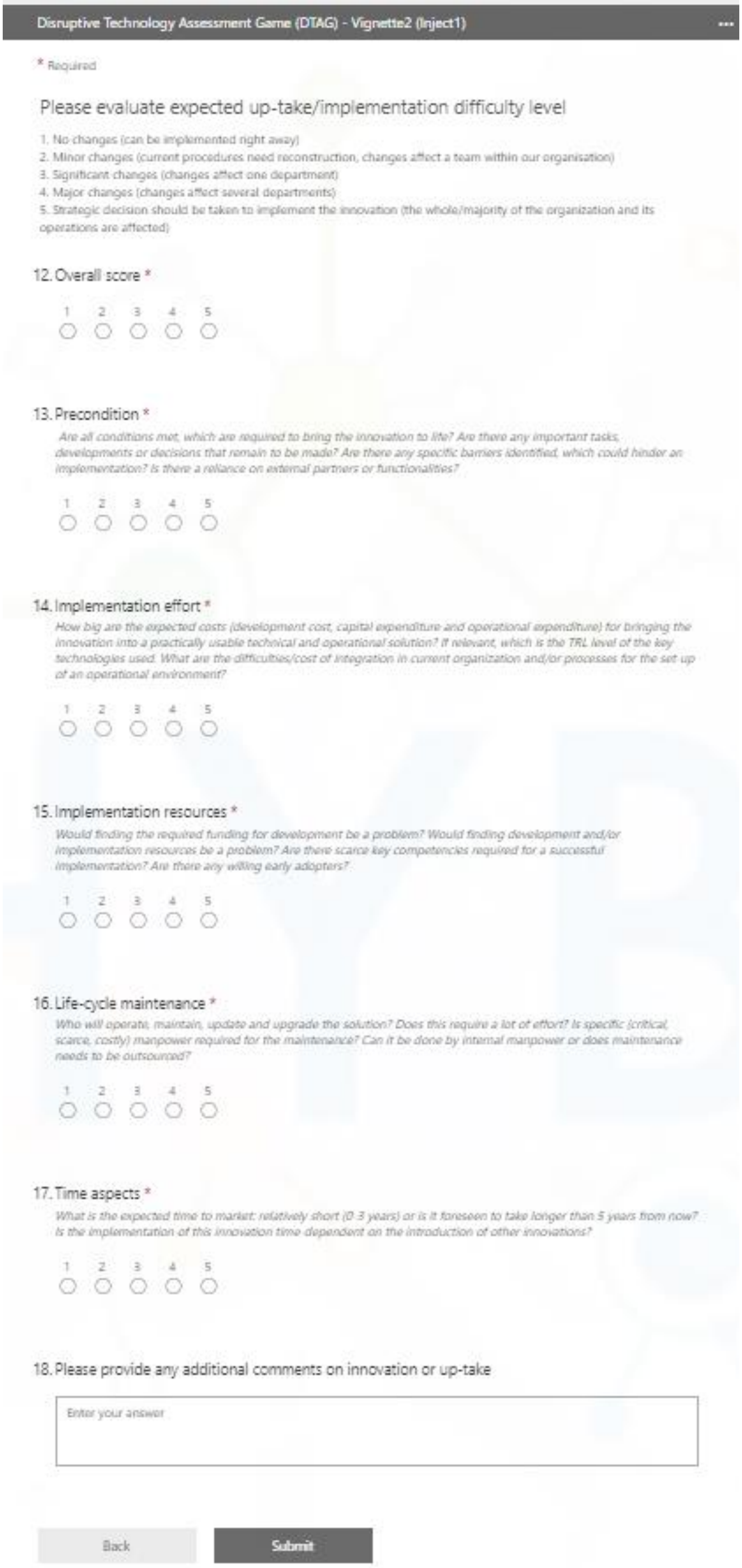
How high is the level of resistance from practitioners and end-users to the use and implementation of the solutions due to possible changes of processes or needed introduction of new processes? Will an implementation of the innovation lead to major immediate changes in current ways of working or will it be a gradual change? Will society accept the consequences of the innovation being implemented? Is there a need for changes in regulatory frameworks? Are there side effects to consider? How strong are the influences on the economy, society and politics? What is the SRL (Societal Readiness Level) for this type of solution?

1 2 3 4 5
○ ○ ○ ○ ○

11. Effectiveness and robustness *

How effective are the solution in handling the problem at hand? How robust is the solution against attack and/or threat variations? Are there restrictions (legal or ethical) that limits the use of the solution? If so, do they differ between MS and practitioner groups? Which is the expected longevity of a solution based on the innovation?

1 2 3 4 5
○ ○ ○ ○ ○



Disruptive Technology Assessment Game (DTAG) - Vignette2 (Inject1)

* Required

Please evaluate expected up-take/implementation difficulty level

1. No changes (can be implemented right away)
2. Minor changes (current procedures need reconstruction, changes affect a team within our organisation)
3. Significant changes (changes affect one department)
4. Major changes (changes affect several departments)
5. Strategic decision should be taken to implement the innovation (the whole/majority of the organization and its operations are affected)

12. Overall score *

1	2	3	4	5
○	○	○	○	○

13. Precondition *

Are all conditions met, which are required to bring the innovation to life? Are there any important tasks, developments or decisions that remain to be made? Are there any specific barriers identified, which could hinder an implementation? Is there a reliance on external partners or functionalities?

1	2	3	4	5
○	○	○	○	○

14. Implementation effort *

How big are the expected costs (development cost, capital expenditure and operational expenditure) for bringing the innovation into a practically usable technical and operational solution? If relevant, which is the TRL level of the key technologies used. What are the difficulties/cost of integration in current organization and/or processes for the set up of an operational environment?

1	2	3	4	5
○	○	○	○	○

15. Implementation resources *

Would finding the required funding for development be a problem? Would finding development and/or implementation resources be a problem? Are there scarce key competencies required for a successful implementation? Are there any willing early adopters?

1	2	3	4	5
○	○	○	○	○

16. Life-cycle maintenance *

Who will operate, maintain, update and upgrade the solution? Does this require a lot of effort? Is specific (critical, scarce, costly) manpower required for the maintenance? Can it be done by internal manpower or does maintenance needs to be outsourced?

1	2	3	4	5
○	○	○	○	○

17. Time aspects *

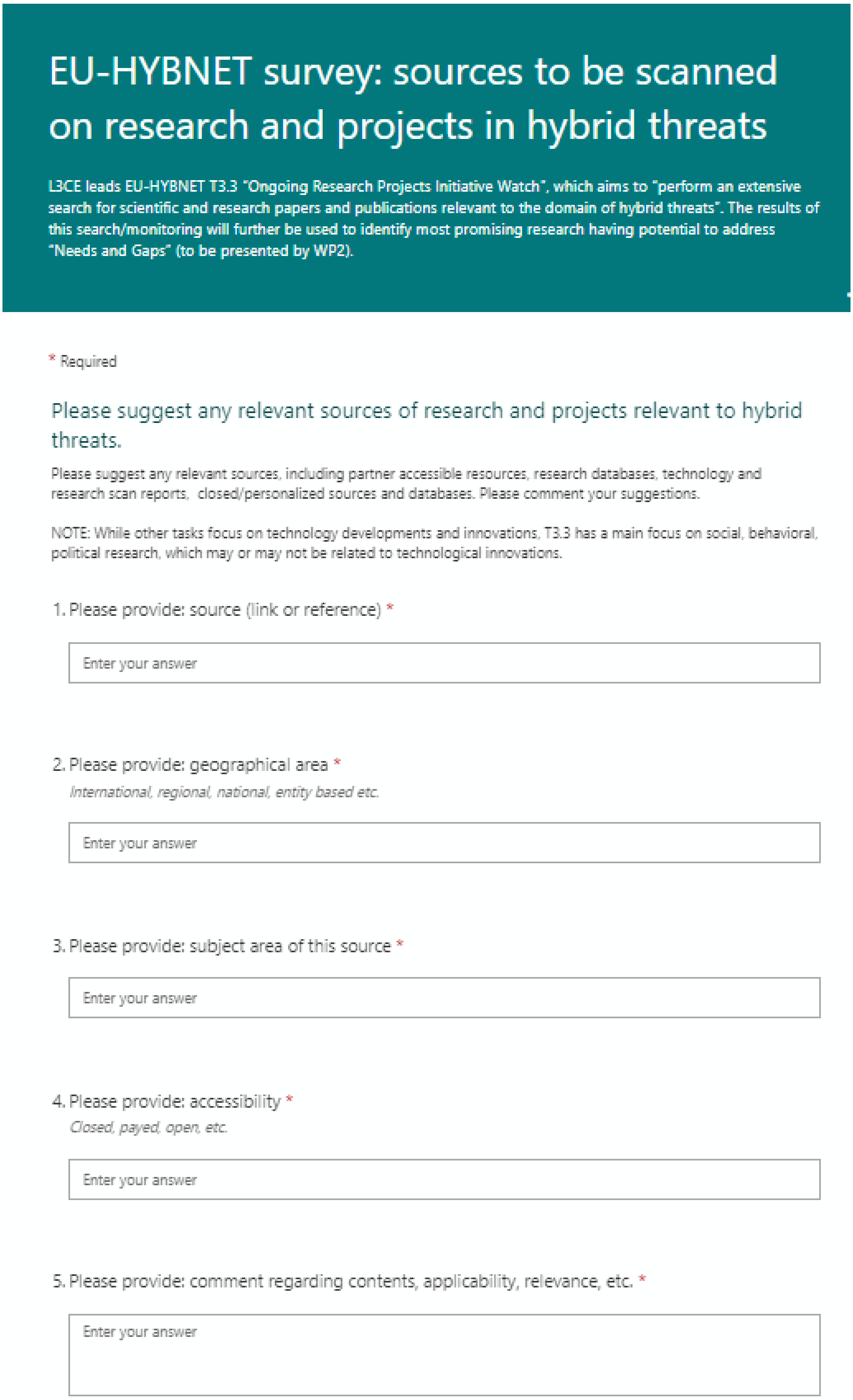
What is the expected time to market: relatively short (0-3 years) or is it foreseen to take longer than 5 years from now? Is the implementation of this innovation time dependent on the introduction of other innovations?

1	2	3	4	5
○	○	○	○	○

18. Please provide any additional comments on innovation or up-take

Enter your answer

Figure 5 THE IoS EVALUATION FORM



EU-HYBNET survey: sources to be scanned on research and projects in hybrid threats

L3CE leads EU-HYBNET T3.3 "Ongoing Research Projects Initiative Watch", which aims to "perform an extensive search for scientific and research papers and publications relevant to the domain of hybrid threats". The results of this search/monitoring will further be used to identify most promising research having potential to address "Needs and Gaps" (to be presented by WP2).

* Required

Please suggest any relevant sources of research and projects relevant to hybrid threats.

Please suggest any relevant sources, including partner accessible resources, research databases, technology and research scan reports, closed/personalized sources and databases. Please comment your suggestions.

NOTE: While other tasks focus on technology developments and innovations, T3.3 has a main focus on social, behavioral, political research, which may or may not be related to technological innovations.

1. Please provide: source (link or reference) *

Enter your answer

2. Please provide: geographical area *

International, regional, national, entity based etc.

Enter your answer

3. Please provide: subject area of this source *

Enter your answer

4. Please provide: accessibility *

Closed, payed, open, etc.

Enter your answer

5. Please provide: comment regarding contents, applicability, relevance, etc. *

Enter your answer

Figure 6 QUESTIONEER: SOURCES TO BE SCANNED ON RESEARCH AND PROJECTS IN HYBRID THREATS

14 ANNEX II. INVITATION LETTER

Dear Sir/Madam,

EU-HYBNET
1st Training Event
22nd & 29th April 2021
SAVE THE DATE
4 hours on both days
www.euhybnet.eu
@EuHybnet
EU-HYBNET

L3CE team would like to encourage your organization to participate in the 1st **EU-HYBNET Training and Exercise Event #TEE.** Please find the **link** to register for the event. A registration link is also provided in the booklet. *Registrations will be open until 4th April 2021 COB*.

Should you need any other information or support, please contact us: dominykas@l3ce.eu and edmundas@l3ce.eu

Don't forget to follow EU-HYBNET on Twitter, LinkedIn and to check the website for the latest news and events.

15 ANNEX III. THE LIST OF PARTICIPANTS ORGANIZATIONS

Organization name	Organization short name
Laurea-ammattikorkeakouu Oy	LAUREA
Polish Platform for Homeland Security	PPHS
The Arctic University of Norway	UiT
RISE Research Institutes of Sweden Ab	RISE
Kentro Meleton Asfaleias	KEMEA
Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras	L3CE
Universidad Rey Juan Carlos	URJC
Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria	MTES
European Organisation for Security Scrl	EOS
Universita Cattolica del Sacro Cuore	UCSC
JRC - Joint Research Centre - European Commission	JRC
Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy	MVNIA
Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats	Hybrid CoE
"International Centre for Defence and Security, Estonia"	ICDS
Ayuntamiento de Valencia / Valencia Local Police	PLV
Polish Internal Security Agency	ABW
MALDITA.ES (Asociación Maldita)	MALDITA
Zentrale Stelle für Informationstechnik im Sicherheisbereich	ZITIS
Universität der Bundeswehr München	COMTESSA

16 ANNEX IV. GLOSSARY AND ACRONYMS

Table 12 Glossary and Acronyms

Term	Definition / Description
EC	The European Commission
EU-HYBNET	Empoewring 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
ACT	Allied Command Transformation
MSs	Member States
IoS	Ideas of Systems
DTAG	Disruptive Technology Assessment Game
LAUREA	Laurea-ammattikorkeakoulu Oy
PPHS	Polish Platform for Homeland Security
UiT	Universitetet i Tromsoe
RISE	RISE Research Institutes of Sweden Ab
KEMEA	Kentro Meleton Asfaleias
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
URJC	Universidad Rey Juan Carlos
MTES	Mistere de la Transition Ecologique et Solidaire / Ministry for an Ecological and Solidary Transition; Ministry of Territory Cohesion; General Secreteria
EOS	European Organisation for Security Scrl
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
SATWAYS	SATWAYS
ESPOO	Espoon Kaupunki / Region and city of Espoo, Finland
UCSC	Universita Cattolica del Sacro Cuore
JRC	JRC - Joint Research Centre - European Commission
MVNIA	Academia Nationala de Informatii Mihai Vieazul / The Romanian National Intelligence Agademy
Hybrid CoE	Euroopan hybridiuhkien torjunnan osaamiskeskus / European Center of Excellence for Countering Hybrid Threats
NLD MoD	Ministry of Defence/NL
ICDS	International Centre for Defence and Security, Estonia
PLV	Ayuntamiento de Valencia / Valencia Local Police
ABW	Polish Internal Security Agency
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (DBS) / Norway, DSB/ Norwegian Directorate for Civil Protection
RIA	Riigi Infosusteemi Amet / Estonian Information System Authority
MALDITA	MALDITA
ZITIS	Zentrale Stelle für Informationstechnik im Sicherheisbereich
UniBW/ COMTESSA	Universitaet der Bundeswehr München