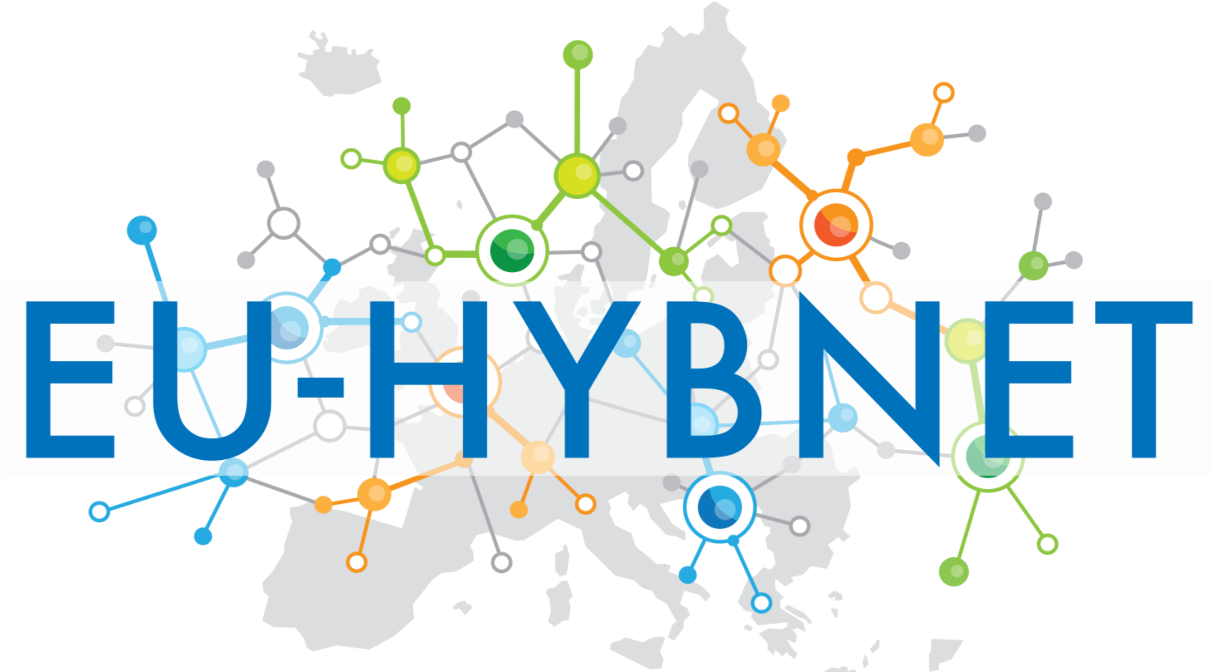
EUROPEAN POLICY BRIEF



Empowering a Pan-European Network to Counter Hybrid Threats

Reflections on the use of the DTAG Methodology for EU-HYBNET trainings (2020-2025)

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

Introduction

The EU-HYBNET project's principal objective is to bring together European practitioners and stakeholders to identify and define their common requirements for countering hybrid threats by undertaking an in-depth analysis and prioritisation of their organizational gaps and needs[1] in doing so. Over its tenure, the project has conducted research and highlighted innovation initiatives, arranging training and exercise events to test the most promising technical and non-technical innovations, which lead to recommendations for uptake, industrialisation, and standardisation. The training and exercise events undertaken in the project provided a unique way to enhance participants' understandings of hybrid threats and how best to counter them.

This policy brief is dedicated to policy makers formulating concepts and expectations for upcoming calls, as well as organizations implementing training activities which may involve the need to assess innovations. The brief summarizes the main aspects of the training design and methodology and focuses on the lessons identified in implementing training and exercise activities in the EU-HYBNET project. In addition, it provides insights and guidance to support the further development, or the uptake of the technologies and/or methodologies developed under different funding instruments. It does not support standardisation activities for trainings, as this may limit creativity of such actions, but it does provide some insights for standardisation.

Training design and methodology

The EU-HYBNET project was designed to have three full cycles (with a fourth cycle that is a wrap-up of all project components), each starting with the identification of European practitioners' gaps and needs in countering hybrid threats and ending with recommendations for innovation up-take and standardization[2]. One of the components of each cycle were the Training and Exercise activities, which were considered essential to increase participants' (such as industry, practitioners, academia, law enforcement agencies experts, etc.) knowledge about hybrid threats and how to counter them. Innovations were selected based on the project findings, and the most promising ones were then integrated into the training scenario. The goal, in addition to increasing participants' understanding of hybrid threats and testing the chosen innovations, was to present participants with the existing technological and non-technical solutions that can increase their knowledge of the potential of using innovations in countering hybrid threats. Further, the trainings were also beneficial in facilitating dialogue as well as the exchange of best practice and ideas among participants.

DTAG

A Disruptive Technology Assessment Game (DTAG)[3], adopted for the EU-HYBNET training and exercise needs and further developed by project partner TNO, was used to test identified innovative solutions and their impact on an operating environment. DTAG is a seminar type wargame that is used to assess different innovative solutions in the form of Ideas of Systems (IoS) and their impact on a given situation. IoS are not innovations, but concepts of potential end-results of an action. EU-HYBNET used the concept of IoS in order to explore the application of potential innovations identified throughout the project. This allowed for an understanding of how to operationalize the potential use of innovations and their vulnerabilities, as well as additional insights.

[1] In the EU-HYBNET project, one of the goals is to define European actors Gaps and Needs to counter hybrid threats. "Gaps" represent the space between the current and best practices and "needs" are the resources required to fill those gaps. More information about the project goals here: The Project – EU-HYBNET.

[2] More information about training and exercise in EU-HYBNET project: Empowering a Pan-European Network to Counter Hybrid Threats | EU-HYBNET | Project | Results | H2020 | CORDIS | European Commission

[3] The DTAG format was originally developed by an international team of researchers from NATO countries through NATO's Science and Technology Organisation in 2010. The overall method is described in the DTAG handbook: Disruptive Technology Assessment Game 'DTAG' Handbook V0.1 - DocsLib.

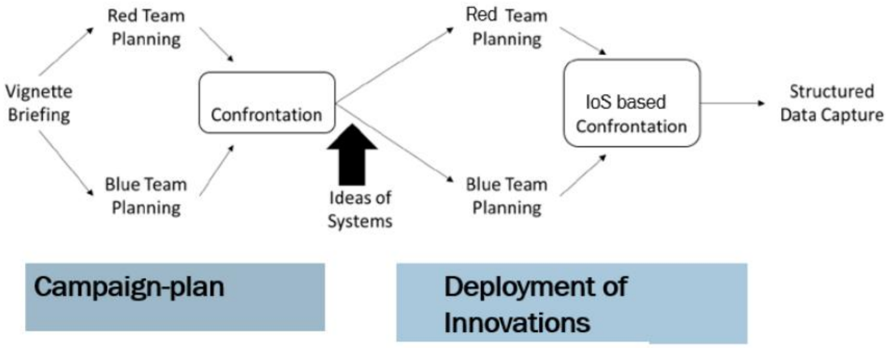


Figure 2. DTAG game concept[4]

Similarly to the original DTAG method, the project created a scenario for each project cycle. The scenarios were developed prior to training event to develop varied events in relation to hybrid threats within a realistic, near-future operational environment. The DTAG methodology has several benefits and limitations that should be considered during the planning phase. For example, it allows for a balance between plenary-style meetings with intense discussions on practicalities alongside the incorporation of innovations into the scenario play. On the other hand, it requires expertise and audience participation It also provides limited time to dive deeper into the preselected innovations.

In the EU-HYBNET project, the DTAG methodology was continuously refined based on lessons learnt from previous cycles. While DTAG is highly effective for introducing innovations and facilitating discussions on how they can enhance awareness of security threats, it has its limitations. The DTAG methodology helps organizations gain a better understanding of technological innovations and stay aware of developments in their respective fields. However, this methodology does not facilitate an in-depth understating of solutions or their functional capabilities (such as the detection of bots), unless the innovations are focused on solutions with limited functionalities and move practitioners directly to the up-take process. Therefore, to successfully utilize the DTAG methodology, it is crucial to manage expectations in the planning stage, before the implementation, and during the training itself.

Planning and implementation

Innovations were selected for training purposes with a goal of assessing their potential utility. The use of a training methodology provided a structured way to infuse the selected innovations into the context of a hybrid threat environment. Pre-reading materials to understand the methodological concept and selected innovations can be time consuming for participants and for this reason, the scenario was simplified after each cycle to avoid an overload of information.

The provision of ten innovative solutions divided into four groups (two to three per group) proved to be the optimal approach. Since the evaluation of these innovations and the assessment of their impact on hybrid threats was a key aspect of the trainings, the participants were given general descriptions of the innovations in order to effectively understand the innovation's potential and its future uptake possibilities. This especially

[4] To read more, please refer to *NATO CD&E Handbook: A Concept Developer's Toolbox (2021)* here: NATO-ACT-CDE-Handbook_A_Concept_Developers_Toolbox.pdf

applied to low TRL[5] or non-technological innovations. Possibility to have the scenario tailored as hand-on exercising using higher TRL level solutions could be the best way to get knowledge on how innovative solutions can add value and if they are of interest for further exploitation. Furthermore, the inclusion of red teams in security related trainings proved to be very valuable with more dynamic discussions. In the EU-HYBNET trainings, the red team members' role was to create and present cascading effects and to observe the reactions.

While the training events provided sufficient space for discussions and exchange of practices, they were planned with continuity in mind, with each training session incorporating modifications and improvements based on input from the previous session. This gave participants a better understanding of the training flow, as they spent less time on familiarizing themselves with the methodology. It also enabled moderators to observe the evolution of discussions in groups and pay further attention to details as the trainings progressed. Scenarios were tailored to represent a real-life situation for participants. Having participants with similar knowledge and understanding of the subject was important in order to have optimal training results. Participants could come from different fields, but a relative similarity of understanding and willingness to discuss is essential.

Experience from the training events have shown that the role of competent moderators is key to the success of the training. Having expert moderators who can handle different complex aspects of the innovation and work with the differing knowledge and experience levels of participants is key. Given the limited time available during trainings, the diversity of participants' knowledge on hybrid threats, the training methodology, and the complexity of hybrid threats as a phenomenon, moderators played a key role in ensuring the efficiency and take-aways of the training.

Lastly, the specific goals and training needs should be addressed during the planning phase. For instance, participant numbers are occasionally overestimated, which has a direct effect on the successful implementation of training plans. If the training is made to be more practical (such as in the case of EU-HYBNET, more focused more on understanding, assessing, and getting used to innovations), it may have a very limited capacity. In the case of DTAG application to a training, there can be a maximum of fifty participants, divided into four groups. Even with this number, the efficiency and outcomes of the training exercise could be limited due to size.

Recommendations and implications

The adopted DTAG method proved to be useful training method for experts working in the security field.
From the successive implementation of training events in the EU-HYBNET project, this policy brief recommends paying particular attention to the following:

- Managing and setting expectations in the planning stage and during the training.
- Using the same methodological approach with minor adjustments, enabling participants to understand the flow of the training sessions and understand the complexity of the topic.
- Ideas of Systems (IoS) need to be fit for the purpose of the event: training developers should carefully assess the need for the depth of description, complexity and applicability in the given situation. Dividing participants into smaller groups makes discussions more fruitful: a maximum of 50 participants is thus important as a cap for the entire exercise.

[5] Technology Readiness Levels refers to a scale to measure the progress or the maturity level of a technology.

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

- The role of moderators is key: it is easy for participants to feel a lack of direction during theoretical discussions. Therefore, it is especially important for moderators to keep track of the direction of discussions and direct it towards exploring solutions and IoSs.
- Leaving sufficient time for discussions is key to exchange views and to share and build knowledge.

The provided recommendations in this brief are not to be considered as fit for all training circumstances. They derive from specific areas, hybrid threats, and fit better to security-related trainings. They are also tailored for a high-level assessment of innovations. Despite their specifics, the DTAG or similar methodologies can be used in variety of fields, but in all cases, successfully facilitating such a training requires significant preparation efforts.

Research parameters

EU-HYBNET is a five-year (2020 - 2025) EU-funded project aiming to build a sustainable Pan-European network of security stakeholders to collaborate with each other to increase the capacity to counter hybrid threats on a European level. EU-HYBNET conducts research and highlights innovations and solutions that aim to close the identified gaps and fulfil practitioners' needs. The considered innovations and solutions, both technological and social, are assessed by practitioners, researchers, and in gamified training events. For innovations and solutions that are assessed to be promising, roadmaps for successful uptake, industrialisation, and standardisation are developed.

To achieve its goal, the project is organised in four Core Themes: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication. These Core Themes provide an opportunity to focus on all hybrid threat domains, especially interfaces between the domains, ensuring that the project delivers coherent results in relation to the European Commission's (EC) "The landscape of Hybrid Threats: A Conceptual Model"[6]. In this context, practitioners were invited to express their needs in countering hybrid threats, which were later analysed and prioritised.

Research outputs from the project will be presented in a series of policy briefs, position papers, and recommendations. The formulation of these outcomes will take place in close collaboration with pan-European security stakeholders, who are included in the project activities from its outset, thereby maximizing its intended impact.

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
Coordinator: Laurea University of Applied Sciences, Finland
Editors of this Policy Brief: Edmundas Piesarskas/L3CE

Consortium:

1. Arctic University in Norway (UiT), Norway
2. Bundeswehr University (COMTESSA), Germany
3. Central Office for Information Technology in the Security Sector (ZITiS), Germany
4. Espoo City and Region (Espoo), Finland
5. Estonian Information Systems Authority (RIA), Estonia

[6] JRC Publications Repository - The landscape of Hybrid Threats: A Conceptual Model (Public Version) (europa.eu)

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

6. The European Centre of Excellence for countering Hybrid Threats (Hybrid CoE), Finland
7. European Organization for Security (EOS), Belgium
8. France Ministry for an Ecological and Solidary Transition (MTES), France
9. International Centre for Defence and Security (ICDS), Estonia
10. Joint Research Centre EC (JRC), Italy
11. KEMEA, Greece
12. Laurea University of Applied Sciences (Laurea), Finland
13. Lithuanian Cyber Crime Centre of Excellence for Training, Research and Education (L3CE), Lithuania
14. Maldita, Spain
15. The Mihai Viteazul National Intelligence Academy (MVNIA), Romania
16. The Netherlands Ministry of Defence (MoD), Netherlands
17. Norwegian Directorate for Civil Protection (DSB), Norway
18. Polish Platform for Homeland Security (PPHS), Poland
19. Polish Internal Security Agency (ABW), Poland
20. Research Institutes in Sweden (RISE), Sweden
21. SATWAYS, Greece
22. TNO, Netherlands
23. Universita Cattolica Sacro Cuore (UCSC), Italy
24. University of Rey Juan Carlos (URJC), Spain
25. Valencia Local Police (PLV), Spain

Funding scheme: Horizon2020 Secure Societies Programme, General Matters-01-2029 call. GA No. 883054

Duration: May 2020 – April 2025

Budget: 3 496 837,50€

Website: https://euhybnet.eu/

For more information: Laurea/ Coordinator Isto Mattila isto.mattila@laurea.fi