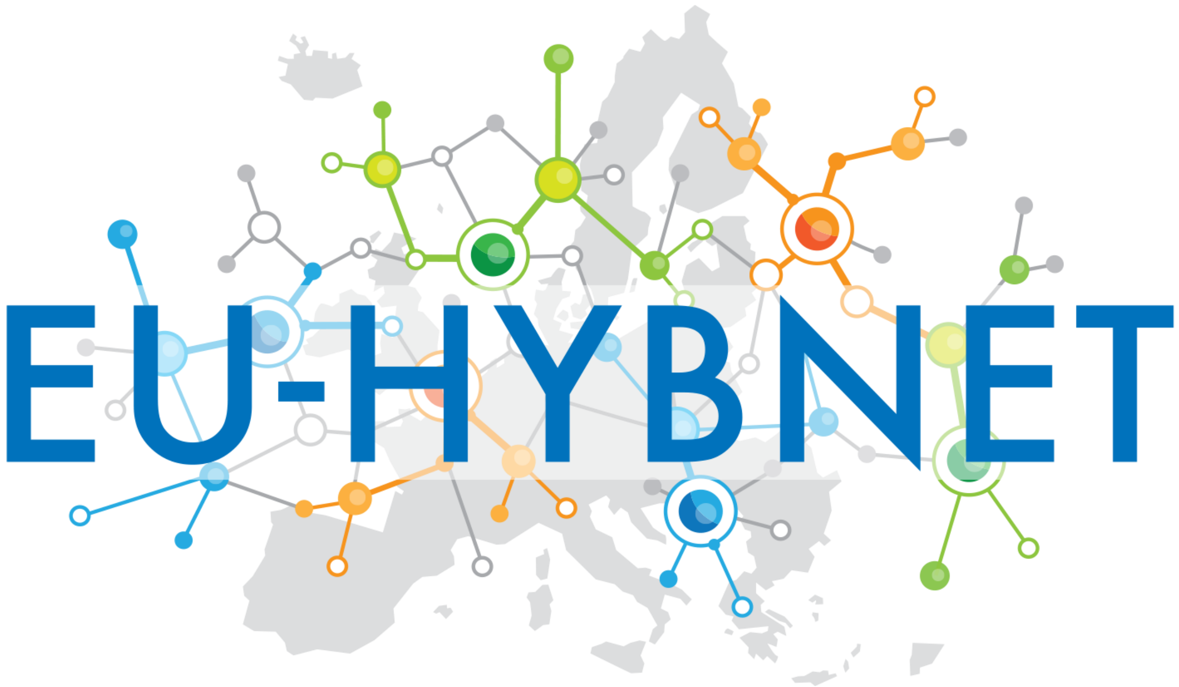


Annual Workshop Report 4

DELIVERABLE 5.13

Lead Author: PLV

Contributors: Laurea, EOS, PPHS

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

D5.13 ANNUAL WORKSHOP REPORT 4

Deliverable number	**5.13**	
Version:	**V1.0**	
Delivery date:	**27/06/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public (PU)**	
Status	**Ready report**	
Nature:	**Report**	
Main authors:	**Susana Sola, Iván Luis Martínez**	**PLV**
Contributors:	**Tiina Haapanen, Päivi Mattila, Jari Räsänen**	**LAUREA**
	Vincent Perez de Leon-Huet, Kristian Reeson	**EOS**
	Magda Okuniewska, Rashel Talukder, Malgorzata Wolbach	**PPHS**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	30/05/2024	Susana Sola, Iván Martínez/ PLV	First draft, text to all chapters
0.2	31/05/2024	Susana Sola, Iván Martínez/ PLV	Text editing
0.3	03/06/2024	Susana Sola, Iván Martínez/ PLV	Content delivery, text editing
0.4	18/06/2024	Tiina Haapanen/ Laurea	Content delivery, text editing
0.5	18/06/2024	Vincent Perez de Leon-Huet, Kristian Reeson/ EOS	Content, material delivery
0.6	20/6/2024	Susana Sola, Iván Martínez/ PLV	Draft for review
0.7	27/06/2024	Päivi Mattila/ Laurea	Review and comments for the text
0.8	27/06/2024	Magda Okuniewska, Rashel Talukder, Malgorzata Wolbach/ PPHS	Review
0.9	27/06/2024	Susana Sola, Iván Martínez/ PLV	Final editing and ready document for submission
1.0	27/6/2024	Päivi Mattila/ Laurea	Final review and submission of the document to the EC

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.

CONTENTS

TABLES

FIGURES

1. INTRODUCTION

1.1 OVERVIEW

The purpose of this report is to summarize EU-HYBNET (Pan-European Network to Counter Hybrid Threats) project's third Annual Workshop's objectives and outcomes.

Annual Workshops are designed to disseminate project findings for a large audience of stakeholders and to ensure vivid interaction with industry, academia, policy makers, security practitioners, SMEs, NGOs, and other providers of innovative solutions outside of the project consortium. Its purpose is to assess the feasibility of the project findings and possible recommendations to innovations uptake (incl. industrialisation) and standardisation.

Annual Workshops are part of Work Package number 5, *Communication, Dissemination and Exploitation Activities*. The 4th Annual Workshop presented the project's 4th year findings and focused on new innovations and networking. The event was addressed to the EU-HYBNET network members and pan-European stakeholders; it hosted lectures from policy makers, security practitioners, industry, SMEs, academia, and NGOs. Additionally, the workshop hosts a handful of presenters and European projects, introducing their unique innovation ideas to counter hybrid threats.

The PLV, EOS and LAUREA organized the fourth EU-HYBNET Annual Workshop that took place on April 24th 2024, in Valencia Local Police premises (Spain). The event was attended by 82 participants from 45 organizations in 16 countries, out of a total of 108 registered people. The event was live-streamed, and 27 registered representatives attended online.

Participant organisations in the AW included 18 of the 25 project partners, 5 European institutions or EU agencies (European Commission, European Parliament, EUROPOL, EEAS and FRONTEX), 2 stakeholders of the 17 stakeholder group organizations, 0 External Advisory Board (EAB) member of the 5 EU HYBNET EAB member organizations, and 11 members out of 140 network member organizations (at that time). 16 participating organisations came from outside EU-HYBNET networks. Full list of organisations that were present and participant statistics can be found in Annex III.

1.2 STRUCTURE OF THE DELIVERABLE

The Annual Workshops report is divided into five sections:

Chapter 1: Provides introduction and describes the importance and content of this deliverable.

Chapter 2: Focuses on Annual Workshop objectives which explains the goals and objectives of the workshop, and how they are related to the project objectives.

Chapter 3: Describes the Annual Workshop's agenda and summarizes the main discussion points. The chapter also highlights the key take-aways gained in the Annual Workshop.

Chapter 4: Introduces and summarizes feedback from the workshop participants collected during and after the event.

Chapter 5: Provides summary of the importance of findings for the future work of the project.

2. WORKSHOP OBJECTIVES

Objectives of Work Package 5, of which the Annual Workshops are part of, are 1) to disseminate results and interact with other related networks; 2) to create conditions for better interaction with industry, research and academia; 3) to enrich the existing network against hybrid threats with academics, practitioners, stakeholders and industry actors across Europe.

Annual Workshops work towards these Work Package objectives, which are grounded in the whole of the project's objectives. The key project objectives for the Annual Workshop are the following:

Table 1 the key project objectives for the Annual Workshop

Project Objective 1: *To enrich the existing network countering hybrid threats and ensure long term sustainability*	Aiming to further extend the existing EU-HYBNET network, the project partners disseminated among their networks the opportunity to participate and to learn about joining the EU-HYBNET network. The event was also advertised on social media channels and on platforms used by relevant stakeholders and other EU funded projects.
Project Objective 3: *To monitor developments in research and innovation activities as applied to hybrid threats*	The event aimed also at identifying organizations and projects working with security-related innovative solutions which may contribute to preventing/ countering hybrid threats. As such, a call for pitches was publicly disseminated on platforms, social media channels and among the partners' networks. Innovations were assessed by a committee formed of the innovation manager, LAUREA, EOS, SATWAYS and PLV. Out of 7 proposals received, 4 were accepted. The presented innovations were further assessed by the audience in a questionnaire.

The first of the project's objectives – ***to enrich the existing network countering hybrid threats and ensure long term sustainability.*** The annual Workshop does this by identifying potential new members to the network, as the events are public and enable all participants to interact with the network members. To ensure a wide range of participants, the event was advertised on EU-HYBNET website (www.euhybnet.eu), project's social media channels (Twitter and LinkedIn) and via e-mail to EU-HYBNET consortium partners, stakeholders group, network members, External Advisory Board members, innovation providers, industry, small and medium-sized enterprises, and non-governmental organizations. Also, the project partners disseminated the event among their networks.

The 3rd project's objective - ***to monitor developments in research and innovation activities as applied to hybrid threats.*** As part of the 4th Annual Workshop, EU-HYBNET also invited providers of innovative solutions on security-related topics to present research and/or innovations which could contribute to countering hybrid threats in the following areas:

Future trends in hybrid threats: detection of the weak signals and vulnerabilities to improve foresight capability in the areas of:

- Political deficiency (Political volatility – structural threat/ Lack of policy foresight)

- New agit-prop (Disinformation spread through encrypted and multiple private messaging apps/Anti –system movements)
- Substitutive reality (Conspiracy theories spread to European realities / Alternativisation of reality)

Cyber and Future Technologies: monitor and analyse attempts to manipulate civil societies in digital environment (combat information manipulation) such as:

- Stealing data attacking individuals (Theft of work or employee data in politically exposed institution / Doxing civil society organization (CSO) activist / Leak of hospital patient data / Social engineering (impersonation, taming with billing systems and obligations))
- Online manipulation attacking democracy (AI generated content – structural threat / Content moderation weaponization / Artificial amplification (CIB)
- Attack on services (Denial-of-service/DDOS/ Physical attack on infrastructures critical to population livelihood (cyber-physical))

Resilient civilians, local level and national administration: increase trust among government and people:

- Spreading violence (Increasing tolerance for violence as a mode of political dissent-structural threat / Online political harassment and “SLAPP”
- Attack on social structures (Vulnerability of higher education institutions to interference /Collapse of the hospital system under massive patient afflux)
- Undermining institutions’ internal organisation (Personnel tensions in critical areas – structural threat / Obsolete hierarchies in national security agency)

Information and strategic communication:

- Media conundrum (Difficult sustainability of quality journalistic media)
- Victimization narratives in the informational space (Generalization of narratives based on victimized identities)
- Attack on information (Pressures onto independent fact checkers / increased use of visual misinformation)

In order to disseminate the call for pitches, there were used channels such as online platforms, social media channels, or the partners’ networks.

Innovations were assessed by a committee formed of the innovation manager, LAUREA, EOS, PLV and representatives from L3CE, TNO, Satways as WP3 task leaders.

Out of 7 proposals received, 4 were accepted. The presented innovations were further assessed by the audience through a questionnaire sent after the presentation of pitches.

With the organisation of the fourth Annual Workshop in Valencia, the following EU-HYBNET project milestone was achieved: MS 37 “Fourth Annual Workshop”.

Figure 1 highlights the role of EU-HYBNET WP5 and of the Annual Workshop to promote the project’s results and to support the project’s key activities:

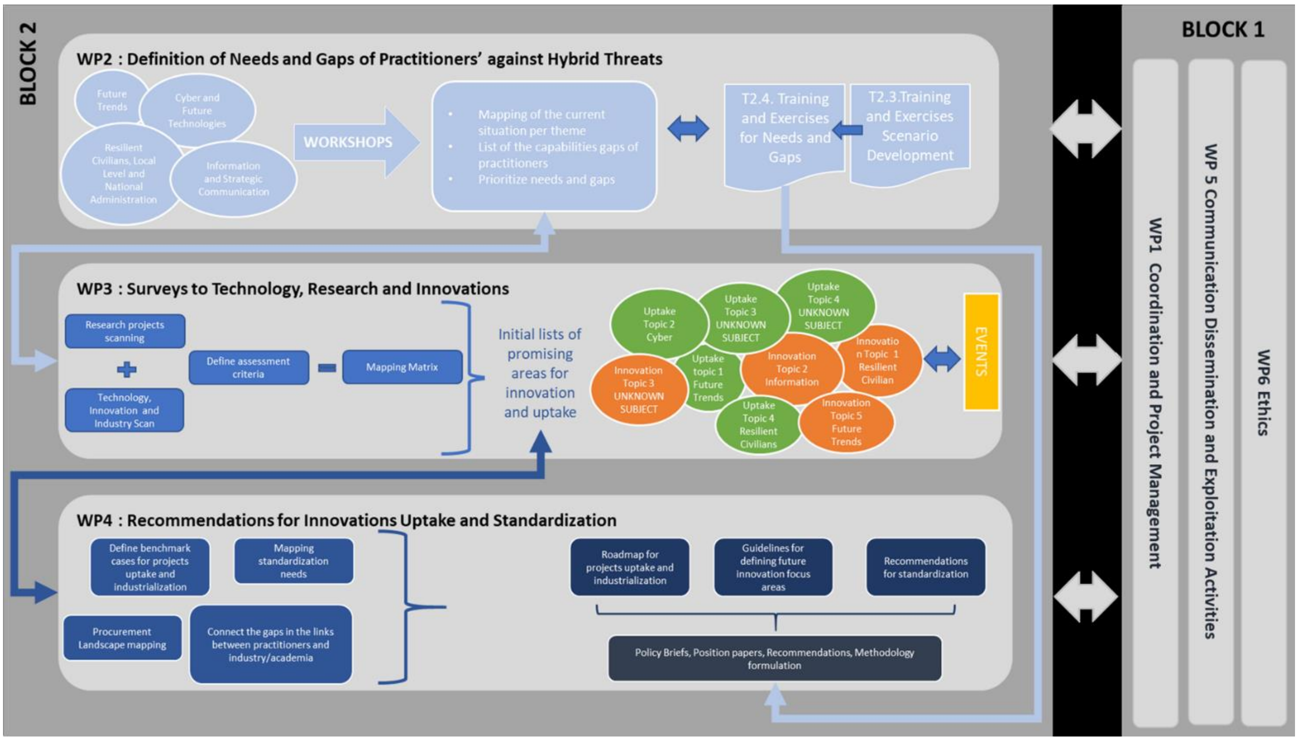

BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities 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

3. WORKSHOP AGENDA

The workshop consisted of three parts:

1. three high-level keynote speeches;
2. discussions in the format of a round table, with the aim to have dialogue on the hybrid threat landscape and on the project results, and to bring new insights to EU-HYBNET's future work, so that it would benefit the EU-HYBNET network, stakeholders and the invited organizations;
3. Pitches and European projects introducing innovations and ideas to counter hybrid threats;

3.1 KEYNOTE SPEECHES

The three keynote speeches were provided by high-level speakers from recognized institutions: **Ms Chiara Pacenti**, *Information Systems Officer SG.STRAT.2, European External Action Service (EEAS),* **Mr. Torben Fell**, *Policy Officer SECDEFPOL.2, European External Action Service (EEAS)* and **Mr. Manuel Rodríguez Vico,** *Director for Technologies and Information, DG SAFE, European Parliament*.

"***From analysis to (re)action – a framework for networked defence***": Our first keynote speaker, Ms. Chiara Pacenti from the European External Action Service (EEAS)/Strategic Communication, delivered an insightful speech outlining a framework for networked counter measures to Foreign Information Manipulation and Interference (FIMI) alongside other hybrid threats. Ms. Pacenti emphasized that actions against FIMI should be approached as a network effort, requiring coordination and collaboration across the community. Each member of this community must assess their role and potential contributions to activating effective responses against FIMI and related threats.

"***The EU approach to countering hybrid threats***": Mr Torben Fell from the EEAS/Security Defence Policy ilustrated The EU approach to countering hybrid threats. The keynote speech highlighted elements like a whole-of-society approach and the shared means that the EEAS has with Member States. Cooperation with various actors was also highlighted as key to enhancing situational awareness, boosting resilience in various domains, and providing support for joint measures.

"**European elections 2024 and hybrid threats**": The 3rd keynote was given by representative of European Parliament, Mr. Manuel Rodríguez from DG SAFE on European elections 2024 and hybrid threats, discussing the case of cyber attacks and disinformation in the elections and the actions carried out in safeguarding the MEPs from cyber attacks. Mr Rodriguez outlined Russia and China's efforts in influencing the upcoming European elections through FIMI. The speech concluded that cooperation is key in safeguarding our open and free elections and contrasting FIMI and other hybrid threats.

3.2 ROUND TABLE – PROJECTS RESULTS AND LATEST FINDINGS IN COUNTERING HYBRID THREATS

Round Table Discussion: EU-HYBNET 4th year findings and results to countering hybrid threats

In the second part of the morning, EU-HYBNET partners presented their latest findings and results from the past 12 months through a round table discussion. The **topics** discussed in the round table were:

- "Finding on present pan-European security practitioners' gaps & needs / threats to counter hybrid threats"
- "Identified promising innovations to counter hybrid threats"
- "Innovation uptake recommendations"
- "EU-HYBNET Network activities and sustainability

Roundtable experts Julien Theron / JRC and Souzanna Sofou / Satways discussed innovations mapped to EU-HYBNET's core themes, such as "WeVerify" – a video plugin to debunk fake videos on social media in order to contrast future trends in Hybrid threats and the EC funded project's Starlight Disinformation-misinformation toolset to contrast online manipulation and attacks to democracy within the context of cyber and future technologies. The Roundtable also discussed the importance of contrasting emerging threats and finding solutions to them such as doxing, SLAPP lawsuits.

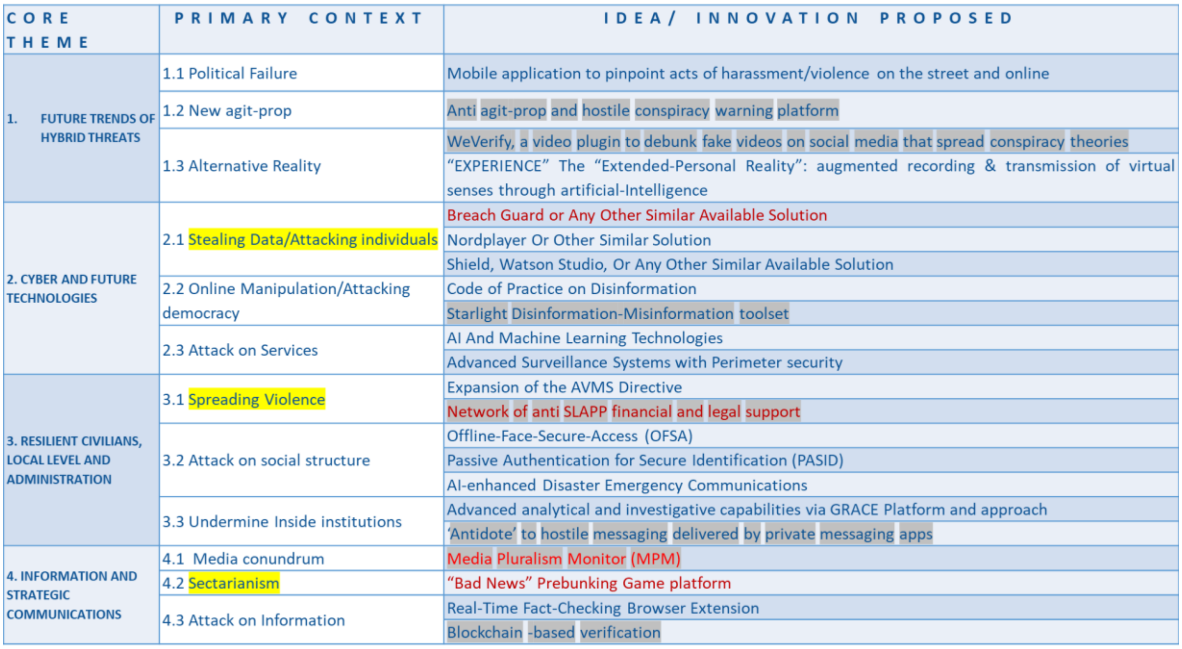
EU-HYBNET 3rd cycle scenario and training activities were presented by L3CE/ Evaldas Bruze. Adapted version of DTAG was used as a training method and this time the Red team in the form of "devils advocate" was used more actively and this was seen very beneficial. Main finding of the training was that we do know the situation we live in and the gaps and needs we are experiencing, but as red team participation showed, we are only prepared for yesterday problems. The challenge for next cycle is how to be prepared in research, policy, technology development and capability development levels for challenges of tomorrow and the day after.

In the context of Innovation uptake and standardisation the most promising innovations from 2nd and 3rd cycle were presented on behalf of KEMEA and RISE and PPHS by Laurea/ EU-HYBNET coordinator Päivi Mattila. Procurement landscape for 2nd cycle is ready and analyses for 3rd cycle was still ongoing.

In the final presentation of the round table current status of the network was given by Hybrid CoE/ Hybrid CoE Project Coordinator Hanne Dumur-Laanila. It was highlighted how EU-HYBNET network has a key role in providing information and discussions that lead to results of EU-HYBNET. It was also pointed that during past project year network has been very active and there had been various collaboration with consortium and network, such as co-authored articles and webinars. EU-HYBNET network is a growing and active network with c. 140 members and Hybrid CoE is currently preparing for the transfer of the network after project end in April 2025.

EU-HYBNET Work Package (WP) Presentation

- **Hanne Dumur –Laanila,** Analyst, Research & Analyses, European Center of Excellence for Countering Hybrid Threats
- **Evaldas Bruze,** L3CE
- **Souzanna Sofou, Senior Research and Innovation Manager, Satways**
- **Julien Theron,** Researcher in Hybrid Threats, Joint Research Centre (JRC)
- **Päivi Mattila,** EU-HYBNET coordinator, LAUREA



CORE THEME	PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED
1. FUTURE TRENDS OF HYBRID THREATS	1.1 Political Failure	Mobile application to pinpoint acts of harassment/violence on the street and online
	1.2 New agit-prop	Anti agit-prop and hostile conspiracy warning platform
	1.3 Alternative Reality	WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories
		"EXPERIENCE" The "Extended-Personal Reality": augmented recording & transmission of virtual senses through artificial-Intelligence
2. CYBER AND FUTURE TECHNOLOGIES	2.1 Stealing Data/Attacking individuals	Breach Guard or Any Other Similar Available Solution
		Nordplayer Or Other Similar Solution
		Shield, Watson Studio, Or Any Other Similar Available Solution
	2.2 Online Manipulation/Attacking democracy	Code of Practice on Disinformation
		Starlight Disinformation-Misinformation toolset
	2.3 Attack on Services	AI And Machine Learning Technologies
		Advanced Surveillance Systems with Perimeter security
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1 Spreading Violence	Expansion of the AVMS Directive
		Network of anti SLAPP financial and legal support
	3.2 Attack on social structure	Offline-Face-Secure-Access (OFSA)
		Passive Authentication for Secure Identification (PASID)
		AI-enhanced Disaster Emergency Communications
	3.3 Undermine Inside institutions	Advanced analytical and investigative capabilities via GRACE Platform and approach
		'Antidote' to hostile messaging delivered by private messaging apps
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1 Media conundrum	Media Pluralism Monitor (MPM)
	4.2 Sectarianism	"Bad News" Prebunking Game platform
	4.3 Attack on Information	Real-Time Fact-Checking Browser Extension
		Blockchain -based verification

Figure 2 the technological and non-technological solutions EU-HYBNET had identified as most promising

3.3 INNOVATION PRESENTATIONS

Pitches - Innovation and ideas to counter hybrid threats by organizations and projects. The workshop included the introduction of innovation ideas to counter hybrid threats by four organisations:

1. "**Denial-of-service/DDOS/attack on infrastructures critical to population livelihood**", by Mr. Marios Thoma, CyberEcoCul Global Services;

2. "**Smart City**", by Mrs. Marina Galiano Botella, from CSIRT-CV. This second pitch examined smart cities and the use of technologies to improve the life of citizens by checking the threats against these systems & how their vulnerabilities can be exploited and solutions e.g. specialised training;

3. "**Resilience Assessment Tool (R/VAT)**", by Mr. Vazha Sopromadze, University of Georgia, Security, Policy and Nationalism Center. This pitch focused on a Resilience Assessment Tool (R/VAT) to assess real threats coming from hybrid activities, in particular to counter Russian disruptive acts;

4. "**Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats**", by David Arroyo, Spanish National Research Council (CSIC). Mr Arroyo focused on the importance of tracking clickbait and marketing techniques as well as comparing request maps to compare social media platforms to detect disinformation.

The workshop also included the presentation of four European funded projects whose results can contribute to countering hybrid threats:

1. **EU-CIP** – Horizon Europe GA 101073878: "**European knowledge Hub and Policy –testbed for Critical Infrastructure Protection**", by Ms. Emilia Gugliandolo, EU-CIP coordinator, Senior Researcher, EINGINEERING. The main goal of EU-CIP is to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs). In this direction, the partners have already established the European Cluster for Securing Critical infrastructures (ECSCI), which brings together more than 30 projects that collaborate in CI Resilience. EU-CIP will leverage the capacity, organization, community, and achievements of the ECSCI cluster towards establishing an EU-wide knowledge network with advanced analytical and innovation support capabilities.

   More on EU-CIP: https://www.eucip.eu/

2. **AHEAD** – Horizon Europe GA 101121338: "**Toward Sustainable Foresight Capabilities for Increased Civil Security**", by Ms. Laure Brévignon-Dodin, Head of office, Directorate for International Security Cooperation, Ministry of the Interior in France. AHEAD, a 30-month HE2022 project, led by Law Enforcement Agencies (LEAs) will take a comprehensive approach when designing and implementing a sustainable framework and foresight means for anticipating future civil security needs. This approach will consider both major future trends and specific local contexts in order to provide outputs such as actionable foresight in 5 security topics.

   More on AHEAD: https://he-ahead-project.eu/

3. **GEMS** – Horizon Europe GA 101121345: "**Gaming Ecosystem as a Multi-Layered Security Threat**", by Bledar Feta, Hellenic Foundation for European and Foreign Policy. The project aims to combat radicalization in game spaces, a community currently forgotten by research. The social aspects are profoundly addressed in the project in order to deliver tangible project results answering to the complex challenges in radicalization means in gaming environment.

The GEMS project is coordinated by Trinity College Dublin/ Maja Halilovic-Pastuovic. More on GEMS: https://www.projectgems.eu

4. **PAVED** – H2020 GA 883054 "**Protecting our strategic Assets, Values and Economy against harmful Disinformation**", by Frederic Tatout, ANATASE, and Anne-Marie Duval, Ministry of Ecological Transition in France. This project and working group composed of experts in different disciplines (law, social sciences, cybernetics AI, etc.) focuses on acute risks posed by information disorders to infrastructure and economic key operators.

The innovation and solutions to counter hybrid threats by organizations and projects were received with great interest. All pitches and projects were assessed by the audience through a questionnaire. According to the evaluation, ATENEA and AHEAD obtained the highest score in excellence (clarity, pertinence and soundness). In relation to the potential impact (coverage, scope and effectiveness), EU-CIP was the highest rated followed by ATENEA. Finally, R/VAT and ATENEA were outstanding in regards to suggested implementation, considering required resources and maintenance.

Identifying ideas and innovations in countering hybrid threats contributes to the task T3.1. *Definition of Target Areas and for improvement of innovation*, as it encourages the collaboration with the private sector. The presentation of pitches can lead to monitoring developments in innovative tools and methods applied to preventing/ countering hybrid threats.

4. FEEDBACK

As with each EU-HYBNET event, participants were given a feedback form (see Annex) to be filled out at the end of the event or after its conclusion.

The format used was a Microsoft Form, and the link was shared via QR code towards the end of the event and printed on a piece of paper placed in the main entrance as well as sent to registered participants after the conclusion of the event. The event conductor encouraged participants to fill in the evaluation forms.

The results will be the average of the answers given by participants, with graphs showing the distribution available in the annex V. Overall, the event received quite favourable feedback, as the results for overall satisfaction of the event and assessment of the general content were 4.80 out of 5. The questions regarding the more specific content echoed the same sentiment, with the panel session and keynotes receiving a score of 4.60 and 4.80, respectively, as well as the pitches which received the same score. The pitches were well evaluated because they provided insights on a variety of solutions to counter hybrid threat.

In regard to the organization and hosting, EU-HYBNET events have once again received very positive feedback. All of the respondents were quite satisfied with the organization that they found very helpful, and the arrangements were well done, both scored 5 out of 5.

In terms of general comments and feedback, there were a few comments applauding the event and the organisation, and one final comment that say: “it would be god to have more concrete projects, for instance the project on radicalisation”.

All pitches and projects were also assessed by the audience in a questionnaire shared via QR. According to the evaluation, ATENEA and AHEAD obtained the highest score in excellence (clarity, pertinence and soundness) since both scored 4.29 out of 5. With regards to their potential impact (coverage, scope and effectiveness), EU-CIP was the highest rated, 4.43 out of 5, followed by ATENEA which rated 4.29 out of 5. Finally, R/VAT and ATENEA obtained both 4.14 out of 5 in suggested implementation (considering required resources and maintenance). Overall, ATENEA has been the most valued innovation.

All of this feedback will be used to improve the next EU-HYBNET event to ensure a high quality and relevancy for project partners and stakeholders.

5. CONCLUSION AND FUTURE WORK

The last year has been very active in EU-HYBNET regarding the 3rd iteration of identifying pan-European security practitioners' gaps and needs to counter hybrid threats followed by the mapping of promising innovations, both technological and non-technological, to the identified threats. This has been supported by various project events where innovative solutions have been presented and their possibilities for uptake under discussion.

The 4th Annual Workshop has achieved its goals to disseminate the project's 4th year findings, to discuss ideas and innovations to counter hybrid threats, together with a large audience of pan-European stakeholders, representatives from industry, academia, SMEs, NGOs, policy makers and security practitioners, and other providers of innovative solutions outside of the project consortium.

Furthermore, it has been EU-HYBNET's pleasure to count also with the cooperation of 5 European institutions or EU agencies: European Commission, European Parliament, EUROPOL, EEAS and FRONTEX. Of course, also cooperation with other relevant EC funded project stays in the core of establishing synergies in countering pan-European security concerns and building on joint results.

The 4th Annual Workshop has been successful based on the evaluations feedback. In fact, the overall event has been rated with an average satisfaction rate of 4.80 out of 5. This is an indicator that proves the high quality of EU-HYBNET events, with interesting discussion topics and the presentation of the latest innovations and trends. One of the favourite parts of the event was the discussions between sessions, according to the evaluations. The pitches were also well evaluated because they provide insights on a variety of solutions to counter hybrid threats.

The 5th, final Annual Workshop will be arranged by Joint Research Centre (JRC) in February 2025 (M58).The objective will be to present EU-HYBNET's 5th year results to counter hybrid threats, and innovative solutions to counter hybrid threats as well as to form an arena for security practitioners, industry, SMEs and academia to present & future policy discussions and network building.

ANNEX I. GLOSSARY AND ACRONYMS

Table 2 Glossary and Acronyms

Term	Definition / Description
AW	Annual Workshop
EOS	European Organization for Security
EU-HYBNET	Pan-European Network to Counter Hybrid Threats
LAUREA	LAUREA University of Applied Sciences
JRC	Joint Research Centre
NGO	Non-governmental organization
FIMI	Foreign Information Manipulation and Interference
EEAS	European Union External Action
CTI	Open Cyber Threat Intelligence Platform
EAB	External Advisory Board
SMEs	Small and medium-sized enterprises
SATWAYS	State of art Incident Management & Computer Aided Dispatch
TNO	Netherlands Organisation for Applied Scientific Research
L3CE	Lithuanian Cybercrime Center of Excellence for Training, Research and Education
PLV	Valencia Local Police
WP	Work Package
OB	Objective
D	Deliverable
PU	Public
KPI	Key performance indicators
MS	Milestone
EMSA	European Maritime Safety Agency
AI	Artificial Intelligence
GDPR	General Data Protection Regulation
FTW	Future Trends Workshop
EU	European Union
MEP	Member of the European Parliament
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
EUROPOL	European Union Agency for Law Enforcement Cooperation
FRONTEX	European Border and Coast Guard Agency
DG SAFE	European Parliament Directorate-General for Security and Safety
EU-CIP	European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection
AHEAD	Towards Sustainable Foresight Capabilities for Increased Civil Security

ANNEX II. WORKSHOP AGENDA

Time CET	Topic	Speakers
Welcome and registration		
8:30-9:00	Registration	
9:00-9:10	Welcome & Practical information	José L. Diego, Inspector, Head of Innovation & Project Management Division, PLV Päivi Mattila, EU-HYBNET Coordinator, Laurea
9:10-9:20	Keynote Speech "From analysis to (re)action – a framework for networked defence"	Chiara Pacenti Information Systems Officer European External Action Service (EEAS)/ Strategic Communications and Information Analysis
9:20-9:30	Keynote Speech "The EU approach to countering hybrid threats"	Torben Fell, Policy Officer EEAS/SECDEFPOL.2, Hybrid Threats and Cyber, Hybrid Threats Sector
9:30-9:40	Keynote Speech "European elections 2024 and hybrid threats"	Manuel Rodríguez Vico Director for Technologies and Information, DG SAFE – European Parliament
9:40-10:10	Audience Q&A	**Host**: José L. Diego, PLV
EU-HYBNET's latest findings and results		
10:10-11:10	Round Table Discussion on "EU-HYBNET 4th year findings and results to counter hybrid threats" – topics:	**EU-HYBNET Consortium:** - Hanne Dumur-Laanila, Analyst, Reseach & Analyses, European Center of Excellence for Countering Hybrid Threats

	• “Findings on present pan-European security practitioners’ gaps&needs/ threats to counter hybrid threats” • “Identified promising innovations to counter hybrid threats” • “Innovation uptake recommendations” • “EU-HYBNET Network activities and sustainability”	- Evaldas Bruze, L3CE - Souzanna Sofou, Senior Research and Innovation Manager, Satways - Julien Theron, Researcher in Hybrid Threats, Joint Research Centre (JRC) - Päivi Mattila, EU-HYBNET Coordinator, Laurea
11.10-11:20	Audience Q&A	**Hosts:** Tiina Haapanen, EU-HYBNET Project Manager, Laurea Iván Luis Martínez Villanueva, Project Manager at the Innovation & Project Management Division, PLV
11:20-11:50	Coffee break	
Pitches Innovations and solutions to counter hybrid threats by organizations and projects		
11:50-12:00	Denial-of-service/DDOS / attack on infrastructures critical to population livelihood - Pitch	Marios Thoma, Director, CyberEcoCul Global Services
12:00-12:10	Smart City -Pitch	Marina Galiano Botella, CSIRT-CV
12:10-12:20	Resilience Assessment Tool (R/VAT) -Pitch	Vazha Sopromadze, The University of Georgia Security, Policy and Nationalism Center
12:20-12:30	Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats - Pitch	David Arroyo, The Spanish National Research Council
12:30-12:40	“European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection“ (EU-CIP), Horizon project	EU-CIP coordinator Emilia Gugliandolo, Senior Researcher, ENGINEERING
12:40-12:50	“Toward Sustainable Foresight Capabilities for Increased Civil Security” (AHEAD), Horizon project	Laure Brévignon-Dodin, Head of Office, Directorate for International Security Cooperation, Ministry of the Interior in France

12:50-13:00	“Gaming Ecosystem as a Multi-Layered Security Threat” (GEMS), Horizon project	Bledar Feta, Hellenic Foundation for European and Foreign Policy
13:00-13:10	“Protecting our strategic Assets, Values and Economy against harmful Disinformation” (PAVED) project, initiative of France	Frederic Tatout, Anatase; Anne-Marie Duval, Ministry of Ecological Transition in France
13:10-13:40	Audience Q&A	**Host:** Isto Mattila, EU-HYBNET Innovation Manager, Laurea
13:40-13.50	Closing remarks	José L. Diego, PLV
13:50-15.00	Lunch	
15.00-16.30	EU-HYBNET General Assembly *EU-HYBNET Consortium partners only*	

Table 3 AW agenda

Biography

Anne-Marie Duval

Anne-Marie Duval worked for 20 years as geophysicist in the field of seismic risk. Then, as deputy director for the activities of research, she helped build an institution with national expertise in all areas of the ecological transition. Today, she is part of a ministerial department that prepares and manages crises in technical sectors such as energy, transport, water or natural and technological hazards.

Bledar Feta

Bledar Feta, IR Specialist & P/CVE Researcher, GEMS Research Team, ELIAMEP Bledar Feta is a PhD candidate in International Relations at the University of Macedonia in Thessaloniki, Greece and a P/CVE Researcher on the South-East Europe Programme of the Hellenic Foundation for European and Foreign Policy (ELIAMEP), a think tank based in Athens. He is a member of ELIAMEP's Horizon 2020 PAVE and Horizon Europe GEMS projects' research teams. A significant part of his research portfolio is dedicated to violent extremism and radicalisation, and the role that online spaces play in (de)radicalisation processes. He has extensive experience in identifying and analysing online extremist contents/narratives and a deep understanding of the online and offline recruitment methods used by extremist groups. Bledar is also skilled in the design and implementation of counter-messaging campaigns that seek to fight extremist propaganda. He also provides consultancy services as a subject matter expert in the field of radicalisation for different organisations, global analysis and advisory firms, governments, international organisations and private companies, such as the Moonshot CVE and the Radicalisation Awareness Network (RAN). Bledar Feta holds a Master of Arts (M.A) in Political Science from the National and Kapodistrian University of Athens, and a Bachelor of Arts (B.A) in International and European Studies from the University of Piraeus where he graduated with a first-class honors degree as the first departments' graduate in 2009. Twitter: @see-eliamep

Chiara Pacenti

Chiara Pacenti is a Data Analyst in the Information Analysis, Open Source, and Data Strategy Team at the European External Action Service's Strategic Communications Division. She is currently working on analytical projects aimed at improving a common framework and methodology to collect evidence on foreign information manipulation and interference (FIMI). Previously she worked for the spokesperson's service of the European Parliament on data-driven projects related to the fight against disinformation, awareness raising and media literacy.

David Arroyo

Dr. David Arroyo is Tenured Scientist in the Institute of Physical and Information Technologies (ITEFI) of the Spanish National Research Council (CSIC). He has a MSc in Telecommunication Engineering from the University of Seville (Spain) and a PhD in Physics of Complex Systems from the Polytechnic University of Madrid. His research focuses on cryptography, information security and privacy, disinformation. David is member of the Forum against Disinformation Campaigns in the field of National Security of the Spanish Department of Homeland Security. Dr. Arroyo's research on "Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats" is conducted with a team. Team members are:

- Dr Sara Degli-Esposti is Research Scientist in Ethics and AI in the Institute of Philosophy of the Spanish National Research Council (CSIC).

- Dr Carlos Galán Cordero is Adjunct Professor in the Double Degree in International Relations & Security of Carlos III University of Madrid.

- Javier Valencia Martínez de Antoñana is the CEO of LYRA engineering & consulting and Adjunct Professor at Nebrija University in Madrid.

Emilia Gugliandolo

Mrs. Emilia Gugliandolo (female) graduated as Doctor with Laude in Management Engineering from the University of Salento (Lecce, Italy). Currently she is working as Project Manager in the Data & Analytics R&I Lab at Engineering Ingegneria Informatica S.p.A. as part of Decision Support Systems unit. She deals with Security, Intelligent Systems & Internet of Things, Big Data Analytics & Business Intelligence, and Social Business.

Since 2015, she has focused her expertise in the Disaster Resilience and Critical Infrastructure Protection domains, being involved in numerous H2020 and HEU projects dealing with Security, Critical Infrastructure Protection and Disaster Resilience: STORM (H2020-DRS-2015), DEFENDER (H2020-CIP-01-2016-2017), FASTER (H2020 - DRS02-2018), 7SHIELD (H2020-SU-INFRA-2019), ENSURESEC (H2020-SU-INFRA-2019), PRECINCT (H2020-SU-INFRA-2020), RESCUER (H2020-SU-SEC-2020), ATLANTIS (Horizon Europe HORIZON-CL3- 2021-INFRA-01), EU-CIP (Horizon Europe HORIZON-CL3-2021-SSRI-01). She is the EU-CIP Project Coordinator. She is also specialised in the roles of Innovation and Exploitation Manager.

Frederic Tatout

Dr. Eng. Frederic Tatout, two decades at the service of the ministries in charge of defense and industry, as scientist, technical architect and project manager, emerging technologies evangelist (e.g information security, data protection, IoT) and senior (complex) project manager. Founder of ANATASE, a company active in startup development and digital transformation, with a focus on security and governance

Hanne Dumur-Laanila

Mrs. Hanne Dumur-Laanila works as an analyst at the Hybrid CoE Research and Analysis team. As a part of the Hybrid CoE EU-HYBNET team, she is responsible for coordinating the EU-HYBNET project. Prior to joining Hybrid CoE in October 2022, she worked at the Hanken School of Economics, located in Helsinki, where she supported the planning and coordination of large national and international research projects. She has also worked for the Finnish Defence Forces in various positions. Hanne holds a master's degree in world politics from the University of Helsinki. In addition, she has studied management at Aalto University and military strategy at the Finnish National Defence University.

Isto Mattila

R&D Director of Laurea University of Applied Sciences, Isto Mattila, has wide working experience covering diverse assignments in different organisations national and international level. He is a Captain Navy, Finnish Border Guard. As from 2008 to 2014 he has worked for the European Commission, DG MARE. He was a second penholder for Maritime Security Strategy and designed new information sharing mechanism (CISE) between maritime authorities in EU, which is now hosted by EMSA. Today he is responsible for R&D activities, mainly in international scale at Laurea. He is also a project coordinator of the AI-ARC Horizon 2020 project, which aims to build information sharing and anomaly detection to Arctic stakeholders.

Iván L. Martínez Villanueva

Mr Iván L. Martínez is a Project Manager at the Innovation & Project Management Division of PLV: Police officer in Valencia Local Police (Spain) since 2002, he studied Agricultural Engineering and Social Work; currently he is studying network systems administration and cybersecurity. In the professional field, he has worked in community policing, patrolling, police headquarters - police data analysis -, Security councillor consultancy and finally in the management of researching projects in the security field, being currently project manager in the R+D division of this LEA. He has managed PLV's participation in 7 H2020 projects over the last 7 years, currently managing 3 projects linked to Domestic Violence, AI, AR, Smart Cities and Hybrid Threats. As a teacher, he has given several training courses in various municipalities in the Valencian Community, especially in subjects related to school bullying, cyberbullying, cybersecurity, new technologies applied to LEAs, social media, etc. In addition, he is teacher at the Valencian police academy (IVASPE) in the Hate Crimes subject.

José L. Diego

José L. Diego is Head of the Innovation and Project Management Division of Valencia Local Police and an expert-evaluator for the European Commission within different initiatives:

- Horizon Europe - Security
- EUROPOL Platform for experts
- DG JUSTICE Research Programmes
- DG HOME Research Programmes
- Radicalisation Awareness Network

He began his career as a consultant at Deloitte, and nowadays is a Police Inspector, Head of Innovation & Project Management in the Valencia Local Police, as well as International Lecturer, OSCE Hate crimes trainer & Liaison officer and also Professor for a Master on Human Resources, for two Masters in Criminology and for the Chiefs´ Police Academy as well. He has managed +30 EU projects (including 15 Horizon-Security projects) in matters like R&D, domestic violence, police mediation and training, community policing, forensics, youth offending, crime fighting, road traffic, police management, diversity, emergencies, environmental police, cybercrime, Police ICTs, hybrid threats, AI, AR, smart cities & security, etc. He holds Degrees in Law and in Criminology and a Master in Human Resources Management as well.

Julien Théron

Dr Julien Théron taught at the universities of Budapest (BME), Beirut (USJ, USEK), Paris (Nanterre, Panthéon-Assas). He also collaborated with the French Institute of International Relations (IFRI) and the International Institute for Strategic Studies (IISS). He is a former Senior Fellow in European Security of the Norwegian Institute for Defence Studies (IFS). In policy, he worked for the French government (MFA, MoD, INSP) as well as for the European Union (EU) and the United Nations (UN). He is a lecturer in War Studies at Sciences Po's Paris School of International Affairs and a researcher in Hybrid Threats for the European Commission Joint Research Centre (JRC).

Laure Brévignon-Dodin

Laure Brévignon-Dodin is the head of the research & innovation office at the Directorate for International Security Cooperation of the French Ministry of Interior where her work is mainly concerned with fostering police cooperation in innovation. She is part of the coordination team of AHEAD, a HE2022 project concerned with developing a foresight approach to help civil security actors anticipate their capability needs. Prior to joining the French Ministry of Interior in May 2021, Laure worked for 3 years in a consultancy and EU project management company, where she specialised in security and crisis management and for 13 years as a researcher in innovation systems for the Department of Engineering of the University of Cambridge, UK.

Manuel Rodríguez

Manuel Rodríguez Vico initiated his professional career as Lieutenant in the Guardia Civil after graduating from the military college of Zaragoza in 1992. He is an official of the European Institutions since 2003 where he has been working in different managerial positions in the areas of Justice and Interior and Security. Currently, he is Director for Technologies in Directorate General for Security in the European Parliament, in charge of preventing and combating hybrid threats and providing information and technology solutions in the field of security for Members, parliamentary bodies and services. He holds a degree in Philosophy, a Master in Security and Defence and Ph Doctorate.

Marina Galiano Botella

Biomedical Engineer; Industrial cybersecurity responsible in CSIRT-CV; Experienced in the development of projects and operation of services in the industrial and healthcare fields.

Marios Thoma

Dr. Thoma is a retired military officer, having achieved the rank of Colonel in Signals. He commenced his military career after graduating from the Hellenic Military Academy and joining the National Guard of Cyprus in 1997. He holds a Master of Science degree in communications and computer science from the University of Athens, Greece, and is a graduate of the Hellenic Military School of Signals Officers, specializing in Telecommunications and Electronics. In 2018, he obtained his PhD degree from the Department of Electrical and Computer Engineering at the University of Cyprus. His doctoral research focuses on cyberspace defence, particularly on modelling and early detection techniques for cyber-attacks, with a specific emphasis on Advanced Persistent Threats (APTs). Throughout his career, Dr. Thoma has amassed significant expertise across various domains such as Information Assurance, Development Security Operations, Cyber Security Engineering, Data Governance and Information Security Management. He has been involved in a multitude of projects, ranging from accrediting Communication Information Systems to crafting Business Continuity and Recovery Plans. Furthermore, his knowledge extends to Hybrid Threats and Space, particularly in conjunction with Cybersecurity. Dr. Thoma has actively participated in strategic, operational, and technical endeavours within both national and EU contexts.

Currently, he holds the position of Director at Cyberecocul Global Services, a newly established startup, committed to delivering cybersecurity services spanning research, development and innovation domains.

Päivi Mattila

Dr. Päivi Mattila holds a position of Director of Security Research Program at Laurea University of Applied Sciences (Finland), and she is responsible for quality and growth and strategic goals of security RD activities. Dr. Mattila is the coordinator of EU H2020 funded EU-HYBNET project. She is a Doctor of Philosophy (General History). Formerly she has worked as the head of the Project and Development Unit at the Crisis Management Centre Finland (CMC Finland) and in the Embassy of Finland in Tel Aviv and in the Finnish Institute in the Middle East alike in the Ministry for Foreign Affairs in Finland.

Souzanna Sofou

Dr. Souzanna Sofou, Senior Research and Innovation Manager, is a Dipl. Mining and Metallurgical Engineer and a holder of an MBA in Engineering -Economic Systems. With respect to basic research, her Doctoral Thesis and most of her published research work fall in the fields of computational rheology, rheometry and polymer processing. She has worked in applied research FP7 & Horizon 2020 projects in various fields, including security, new product development, metallurgy, polymer processing, RET modelling, software development and value management. She also has background and experience in Intellectual Property, as she has received relevant training and has worked in this field as a Product Design Engineer for a multinational company. Dr. Sofou has served as the innovation, exploitation and dissemination manager in 3 H2020 projects (PROCETS, z-fact0r, OACTIVE) and as the Innovation Manager in InDeal H2020 project. For the last years, she has been working in security H2020 projects: as the dissemination & communication manager for the ANDROMEDA project, as the innovation manager for the INGENIOUS & the STRATEGY projects, leading the exploitation of the InfraStress project and the IP Management of the EFFECTOR project. She was also actively involved in the SATIE project and serves as the EU-HYBNET WP3 Leader: Surveys to Technology, Research and Innovations. Dr. Sofou is responsible for the Innovation Management of SATWAYS products.

Tiina Haapanen

Tiina Haapanen is Project Specialist at Laurea University of Applied Sciences and the Project Manager of EU-HYBNET project. She has over 10 years expertise in EC funded research project (H2020, Horizon Europe, Erasmus+) administration and management.

Torben Fell

Torben Fell is a Policy Officer in the Hybrid Threats & Cyber division (SECDEFPOL.2) of the European External Action Service (EEAS), working in the hybrid threats sector. SECDEFPOL.2 leads on and coordinates the EU's efforts to address external security threats in the fields of hybrid and cyber, in particular through the development and operationalisation of policies, operational tools and international engagement, fulfilling the EU level of ambition, as expressed in the Strategic Compass. Prior to joining the EEAS in 2020, Mr Fell worked on counter terrorism in DG Migration & Home Affairs of the European Commission, covering issues such as critical infrastructure protection and countering terrorist financing, and has also previously worked in both the private and public sectors.

Vazha Sopromadze

The University of Georgia Security, Policy and Nationalism research center (UGSPN) research fellow. In 2016, he was awarded a bachelor's degree in political science from the University of Georgia. In 2020, he received a master's degree in international relations from the University of Georgia, specializing in Russian foreign policy research. From 2022, Vazha has been working on a doctoral research project in political science, focusing on the process of transformation of Georgian political elites. Along with his academic activities, Vazha has extensive experience working in the public service in the areas of Euro-Atlantic integration and foreign policy analysis.

Project descriptions

AHEAD

AHEAD is a 30-month HE2022 project concerned with providing a tested prospective methodology tailored to the civil security domain. Taking into account long-term driving forces and contextual elements, it aims to generate foresight-informed roadmaps that anticipate the capability needs of civil security forces when potentially facing threats posed by new technologies. Concretely, iterative foresight exercises covering the 5 operational destinations of Horizon Europe Cluster 3 (crime and terrorism, border management, resilient infrastructures, cyber security and disaster resilient society) and involving a combination of workshops and interviews with multidisciplinary experts and civil protection representatives are to be conducted throughout the project. AHEAD's ultimate aim is to strengthen a forward-looking civil protection culture and embed in a more systematic way strategic foresight into decision-making.

The AHEAD is coordinated by Ministry of the Interior in France/ Thierry Hartmann. More on AHEAD: https://he-ahead-project.eu/

EU-CIP: European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection

The main goal of EU-CIP is to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs). In this direction, the partners have already established the European Cluster for Securing Critical infrastructures (ECSCI), which brings together more than 30 projects that collaborate in CI Resilience. EU-CIP will leverage the capacity, organization, community, and achievements of the ECSCI cluster towards establishing an EU-wide knowledge network with advanced analytical and innovation support capabilities.

To facilitate information collection and analysis, the project established a FAIR data observatory of research projects, research outcomes, technologies, standards, and policies. Along with analytical capabilities for evidence-based policies, the project organizes and offers a rich set of innovation support services to EU projects and other innovators in CI security and resilience. These services include training, support in business planning and access to finance, as well as support in the validation, standardization, and certification of novel solutions. The projects outcomes are integrated and made available through a Knowledge Hub, which provides a singly entry point to the EU-CIP results. EU-CIP will build a vibrant ecosystem of over 1000 stakeholders around this Knowledge Hub. To animate and grow the project's community, EU-CIP will execute an ambitious set of dissemination activities, including the establishment and organization of an annual conference on Critical Infrastructures Resilience, which will become a flagship event for critical infrastructures.

The EU-CIP is coordinated by Engineering/ Emilia Gugliandolo. More on EU-CIP: https://www.eucip.eu/

GEMS - "Gaming Ecosystem as a Multi-layered Security Threat" Project

The HORIZON EUROPE research project GEMS aims to contribute to the fight against the rapid spread of extremism across the gaming ecosystem. The GEMS´ aims are: To contribute to a scientific advancement of the field of radicalisation and violent extremism by developing a new academic field of Sociology of Gaming and Radicalisation; To provide European Police Authorities (EPAs) with a novel Training Curriculum and an innovative tool, the Watchtower (a future-proof AI platform trained to recognise and prevent the spread of extremist content and recruitment in the online gaming space); To create a new cross-sectoral collaborative network dedicated to countering extremist presence in the gaming ecosystem - European Networks Against Gaming-

Related Extremism (ENgaGE); To develop an effective Citizens Awareness Campaign and evidence-based Policy Solutions which will greatly improve high level decision making, empower citizens and enhance youth/gamers protection. In order to achieve these aims GEMS will coalesce the knowledge, expertise and experiences of the security community, the European police authorities, technical innovators, academics from a host of disciplines, policy makers and influencers, all led by a profound dedication to the protection and security of EU citizens.

GEMS is a project which answers a particular security challenge, i.e., the presence of extremism in the gaming ecosystem. Consequently, it is envisioned as a product-oriented, practical project, with major contributions from EPAs and the technical sector, especially the AI developers. The overarching aim of the project is to minimize if not outright remove the threat of extremist recruitment in the gaming ecosystem in its earliest stages. GEMS will be in the position to reach this aim by focusing on arguably the only area where meaningful and effective intervention during the radicalization process is in fact possible, i.e., the in-game communication platforms.

The GEMS is coordinated by Trinity College Dublin/ Maja Halilovic-Pastuovic. More on GEMS: https://www.projectgems.eu

PAVED

Over the past few years, the development of public capabilities to combat the risks posed by information disorders focused on hybrid acts targeting security, defence and public order. PAVED is both a project, and a Working Group composed of experts in different disciplines (law, social sciences, cybernetics and AI, cognition, social sciences and crisis management), focusing on acute risks posed by information disorders to infrastructure and economic key operators. In a first step, PAVED produced a broad (horizontal) analysis of the phenomena and the risks, and carried out a more in-depth analysis in two concrete cases, the individual vehicle and strategic minerals. The groupe explored FIMI as well as ideological and activist mobilizations likely to be violently translated on the ground. Current work (second step) aims at integrating several dimension of “complex" threats / crisis (Hybrid operations, natural, industrial, etc.), in the perspective of resilience.

ANNEX III. LIST OF PARTICIPANT ORGANISATIONS AND COUNTRIES

Nr.	Organisation	Country	Type of Organisation
1.	ANATASE	France	Industry - SME
2.	ABW	Poland	Practitioner
3.	Belgian General Intelligence and Security Service, Belgian Armed Forces (BEL DOD)	Belgium	Public Sector
4.	CEA	France	Resarch/Academia
5.	City of Vilnius	Lithuania	Public sector
6.	City of Espoo	Finland	Public sector
7.	Correcta Digital, SL	Spain	Industry - SME
8.	CSIRT-CV, IT Security Center (Valencian Regional Government)	Spain	Public Sector
9.	Cyberecocul Global Services	Cyprus	Industry/SME
10.	DSB - Norwegian Directorate for Civil Protection	Norway	Public Sector
11.	District Prosecution Office	Albania	Other (Law enforcement government institution)
12.	Engineering Ingegneria Informatica S.p.A.	Italy	Industry/SME
13.	European Commission, Joint Research Centre	EU	Research/Academia
14.	European External Action Service (EEAS)	EU	Public Sector
15.	European Organization for Security - EOS	Belgium	Industry - SME
16.	European Parliament	EU	Public Sector
17.	Europol Innovation Lab	EU	Public Sector

18.	Finnish Ministry of Interior	Finland	Public Sector
19.	GLOBSEC	Slovakia	Civil Society
20.	Hellenic Foundation for European and Foreign Policy (ELIAMEP)	Greece	Research/Academia
21.	Hybrid CoE	Finland	Other (An international, autonomous network-based organization promoting a whole-of-government and whole-of-society approach to countering hybrid threats)
22.	International Security Agency	Poland	Public sector
23.	International Centre for Defence and Security - ICDS	Estonia	Research/Academia
24.	L3CE	Lithuania	Research/Academia
25.	LAUREA University of Applied Sciences	Finland	Academic/RTO
26.	MALDITA	Spain	Civil Society/ NGO
27.	"Mihai Viteazul" National Intelligence Academy - MVNIA	Romania	Research/Academia
28.	Ministry of Defense	Spain	Public Sector
29.	Ministry of Ecological Transition in France	France	Public Sector
30.	Ministry of the Interior	Spain	Public Sector
31.	Ministry of the Interior	France	Public Sector
32.	Polish Financial Supervision Authority	Poland	Public Sector
33.	Prosegur Research	Spain	Industry (International)
34.	Satways Ltd	Greece	Industry - SME
35.	Spanish National Research Council (CSIC)	Spain	Public sector
36.	TNO- Netherlands Organisation for Applied Scientific Research	Netherland	Academic/RTO

37.	University of Georgia	Georgia	Research/Academia
38.	Universidad CEU Cardenal Herrera	Spain	Research/Academia
39.	Universidad Internacional de Valencia (VIU)	Spain	Research/Academia
40.	Universidad Isabel 1	Spain	Research/Academia
41.	Università Cattolica del Sacro Cuore - UCSC	Italy	Research/Academia
42.	University of the Bundeswehr Munich	Germany	Research/Academia
43.	Valencia Local Police (Valencia City Council)	Spain	Public Sector (LEA)
44.	VOST Europe	EU	Civil Society
45.	FRONTEX	EU	Public Sector

Table 4 List of participants organisations and countries

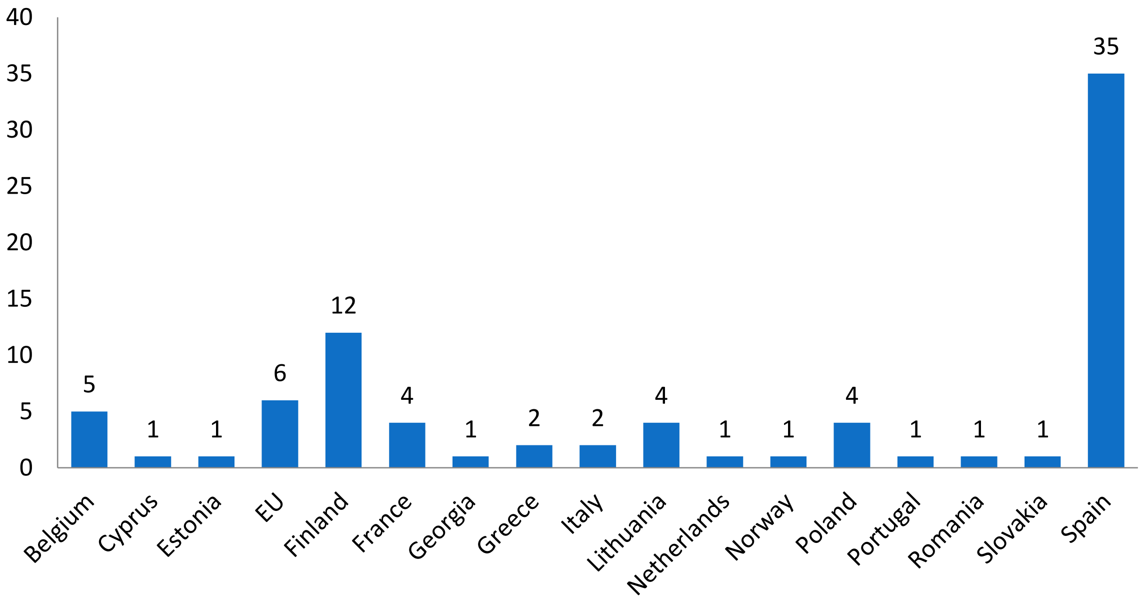


Figure 3 Distribution per countries

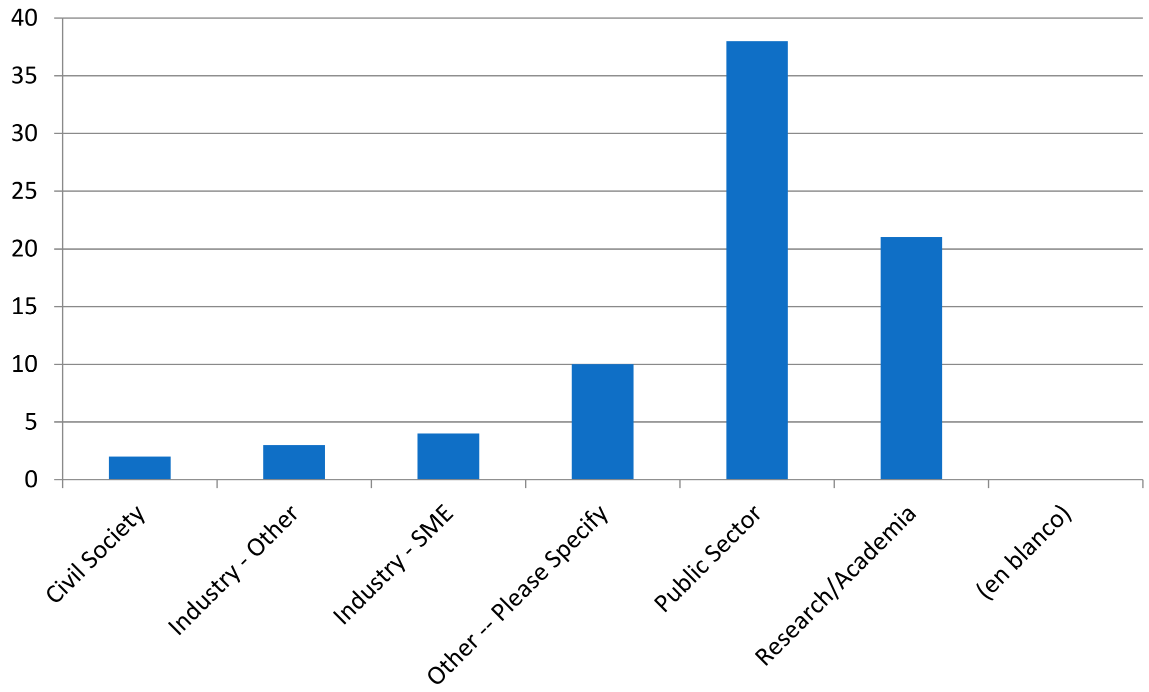


Figure 4 Distribution of number of participant organizations per type of organization

Country	Civil Society/ NGO	Industry – SME and other	Public Sector	Resarch/Academia	Other	Grand Total
Belgium		4	1			5
Cyprus		1				1
Estonia				1		1
Finland			3	6	3	12
France			2	1		3
Georgia				1		1
Greece				1	1	2
Italy		1		1		2
Lithuania				1	3	4
Netherlands				1		1
Norway			1			1
Poland			4			4
Portugal					1	1
Romania			1			1
Slovakia	1					1
Spain	1	1	22	7	2	33
EU			4	1		5
Total	**2**	**7**	**38**	**21**	**10**	**78**

Table 5 Distribution of number of participant organizations per type of organization and country

ANNEX IV. INNOVATION ASSESSMENT RESULTS

The pitches were firstly assessed by a project committee formed of the innovation manager, LAUREA, EOS and PLV and representatives from L3CE, TNO, Satways as core theme leaders. Out of 7 proposals received, 4 were accepted:

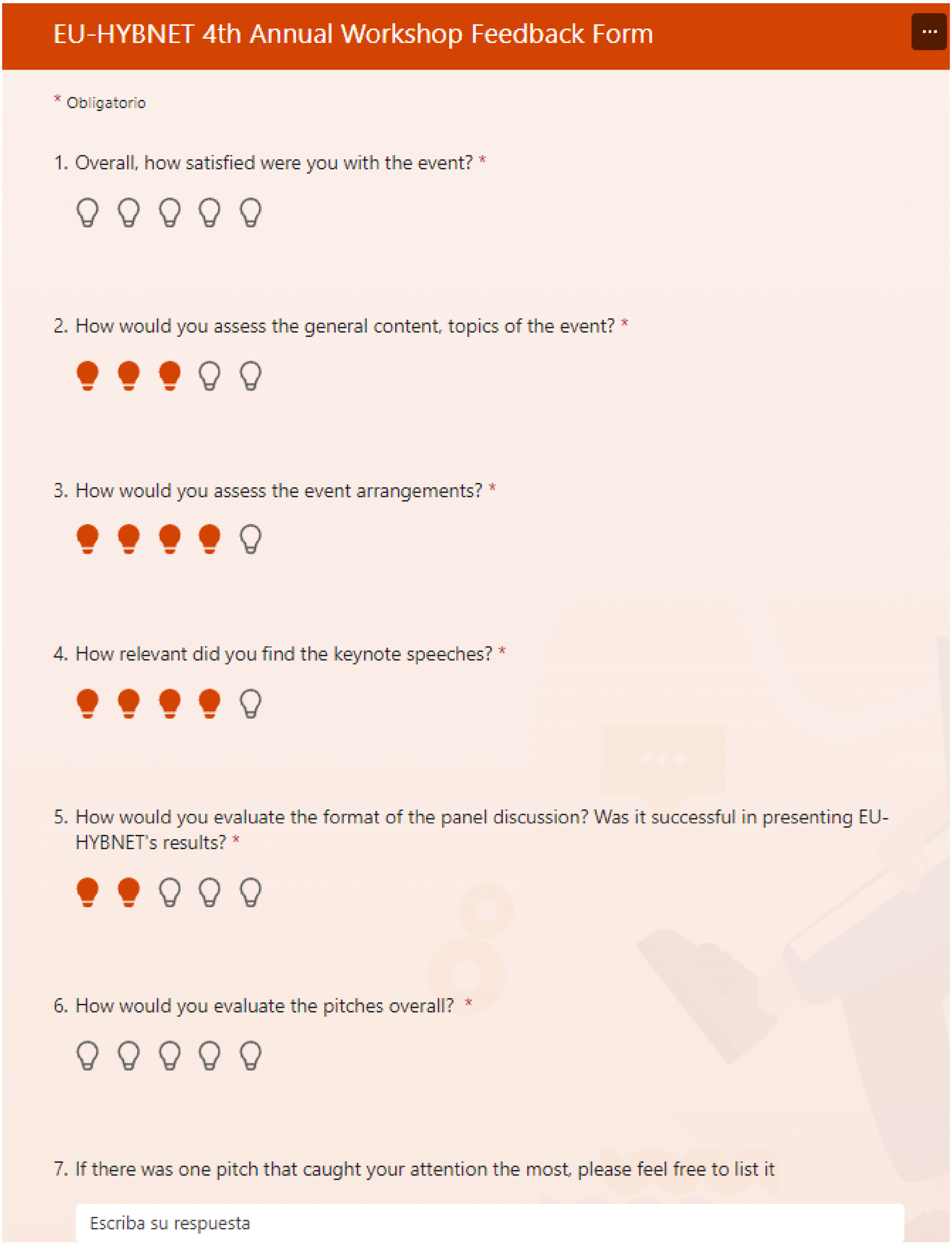
Innovation	Short description of the innovation	Result
Denial-of-service/DDOS / attack on infrastructures critical to population livelihood	The idea is based on the methodology developed in the article ‘’ Detection of collaborative misbehaviour in distributed cyber-attacks’’ and the goal is to identify early enough DDoS attacks targeting Large Critical Information Infrastructures. (https://www.sciencedirect.com/science/article/abs/pii/S0140366421001493) . This innovation is based on time observation which means that works for advance persistent threats, giving the possibility to defender to identify early enough cyber attacks that could be the first stage of hybrid threats, affecting large critical infrastructures vital for the states.	Accepted
Smart City’s Testbed as Cybersecurity Lab	The Smart City's digital twin is a demonstrator that is composed of several devices that can be found in the city. These devices that help us to improve the connectivity of the city can also be susceptible to cyber-attacks. The objective of the Smart City's digital twin is to study the weaknesses that these devices integrated in a city may have, as well as to simulate cyberattacks that can then be used for cybersecurity training. On the other hand, it also helps us in the research to protect us from these threats.	Accepted
Resilience Assessment Tool (R/VAT)	Countries like Georgia are especially susceptible to hybrid threats, these threats exploit vulnerabilities within a nation's political, economic, and social structures. To address this complex challenge team of researchers at the UGSPN come up with the idea of the Resilience/Vulnerability assessment Tool. R/VAT is a comprehensive framework designed to evaluate a nation's preparedness across multiple domains relevant to its overall resilience. It meticulously examines existing policies, available resources, and their implementation readiness within various sectors. By breaking down these sectors into sub-components, the tool provides granular assessments. It utilizes index-based scoring to quantify resilience levels, allowing for both horizontal (within sectors) and vertical (across policy, resources, and implementation) analysis. This multifaceted approach aims to identify systemic strengths and weaknesses, highlight areas for improvement, and provide data-driven insights. The R/VAT's adaptability allows it to be customized for specific resilience areas such as cybersecurity, critical infrastructure protection, public health preparedness, economic stability, and social cohesion, making it a valuable tool for strategic planning and resource allocation.	Accepted

Understanding the financing of disinformation campaigns: ATENEA and other tools for tracking hybrid threats	As is known, there are many elements that make up the panorama of actors involved in the socalled hybrid threats and, specifically, orchestrated disinformation campaigns. These human elements, generally paid proxies of the real agents of the threats - state or state-sponsored actors -, immersed in a global scenario of increasingly strict control of the movement of funds, have been recurrently using specific patronage platforms - such as Patreon, YouTube, etc. -, to receive opaque external financing, as compensation for disseminating or exhibiting content supposedly supported by specialized studies or scientific or academic behaviors. Knowing these financing channels is essential to counteract the risk of the dissemination of the aforementioned disinformation campaigns, of which the aforementioned actors are an essential part.	Accepted

Table 6 Description of innovations, pitches

The accepted and presented innovations were further assessed by the audience through a questionnaire.

ANNEX V. EVALUATION FORMS AND ANSWERS



EU-HYBNET 4th Annual Workshop Feedback Form

* Obligatorio

1. Overall, how satisfied were you with the event? *

○ ○ ○ ○ ○

2. How would you assess the general content, topics of the event? *

● ● ● ○ ○

3. How would you assess the event arrangements? *

● ● ● ● ○

4. How relevant did you find the keynote speeches? *

● ● ● ● ○

5. How would you evaluate the format of the panel discussion? Was it successful in presenting EU-HYBNET's results? *

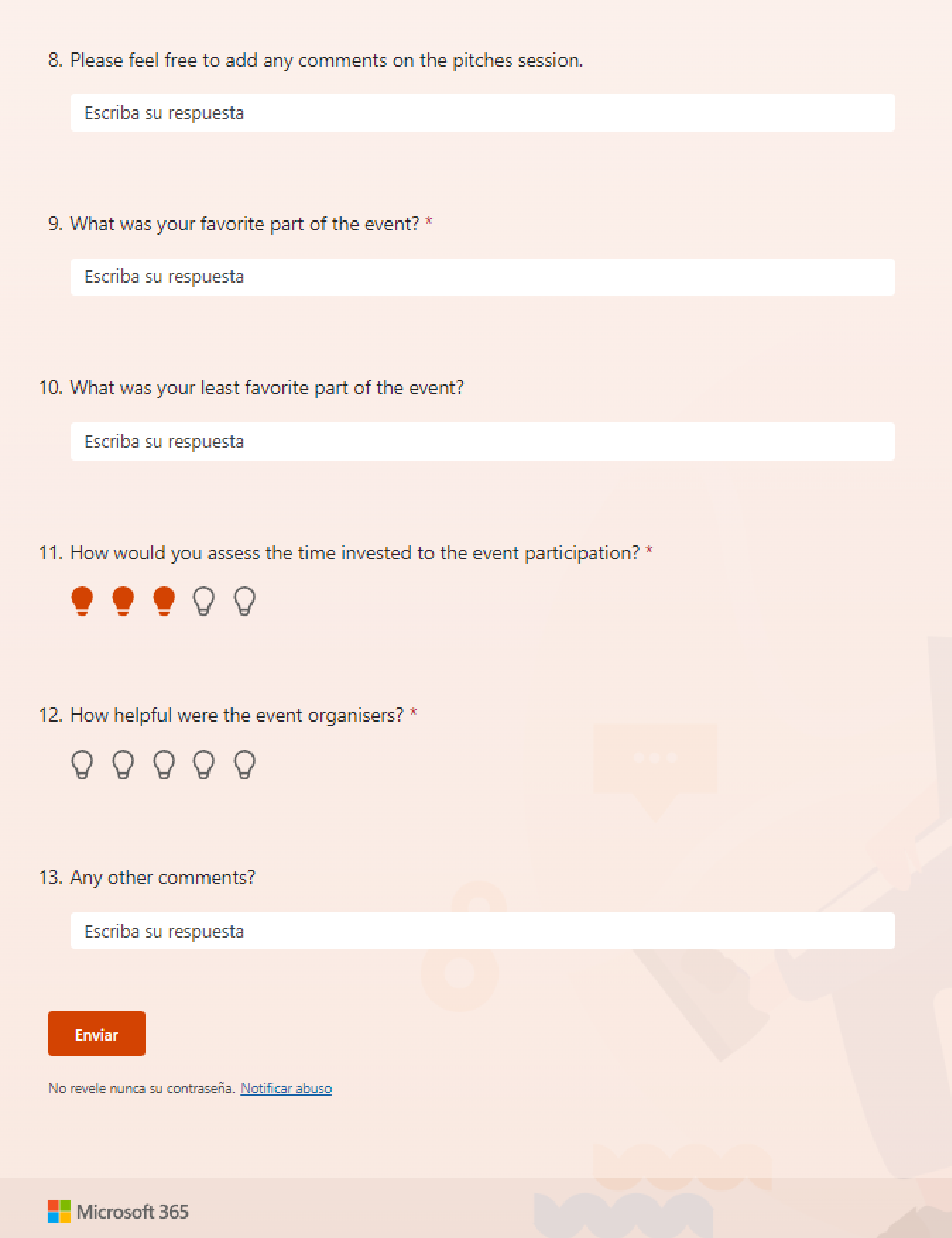
● ● ○ ○ ○

6. How would you evaluate the pitches overall? *

○ ○ ○ ○ ○

7. If there was one pitch that caught your attention the most, please feel free to list it

Escriba su respuesta



8. Please feel free to add any comments on the pitches session.

Escriba su respuesta

9. What was your favorite part of the event? *

Escriba su respuesta

10. What was your least favorite part of the event?

Escriba su respuesta

11. How would you assess the time invested to the event participation? *

● ● ● ○ ○

12. How helpful were the event organisers? *

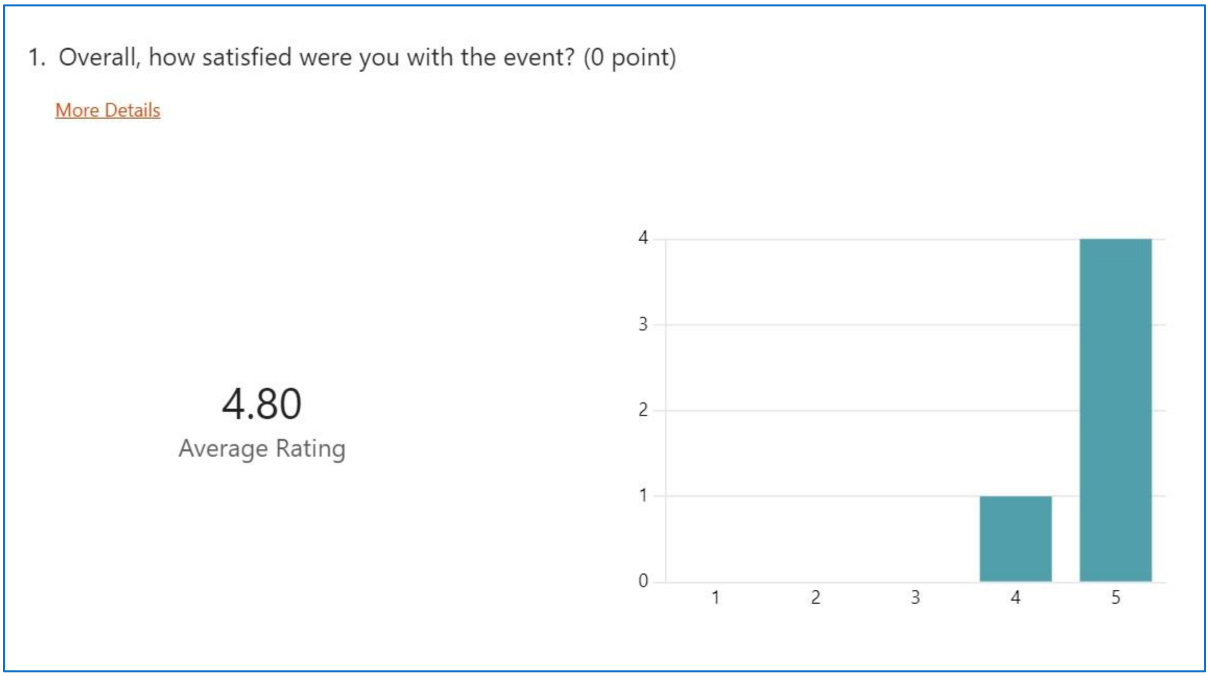
○ ○ ○ ○ ○

13. Any other comments?

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso

Figure 5 EU-HYBNET 4th AW Feedback Form

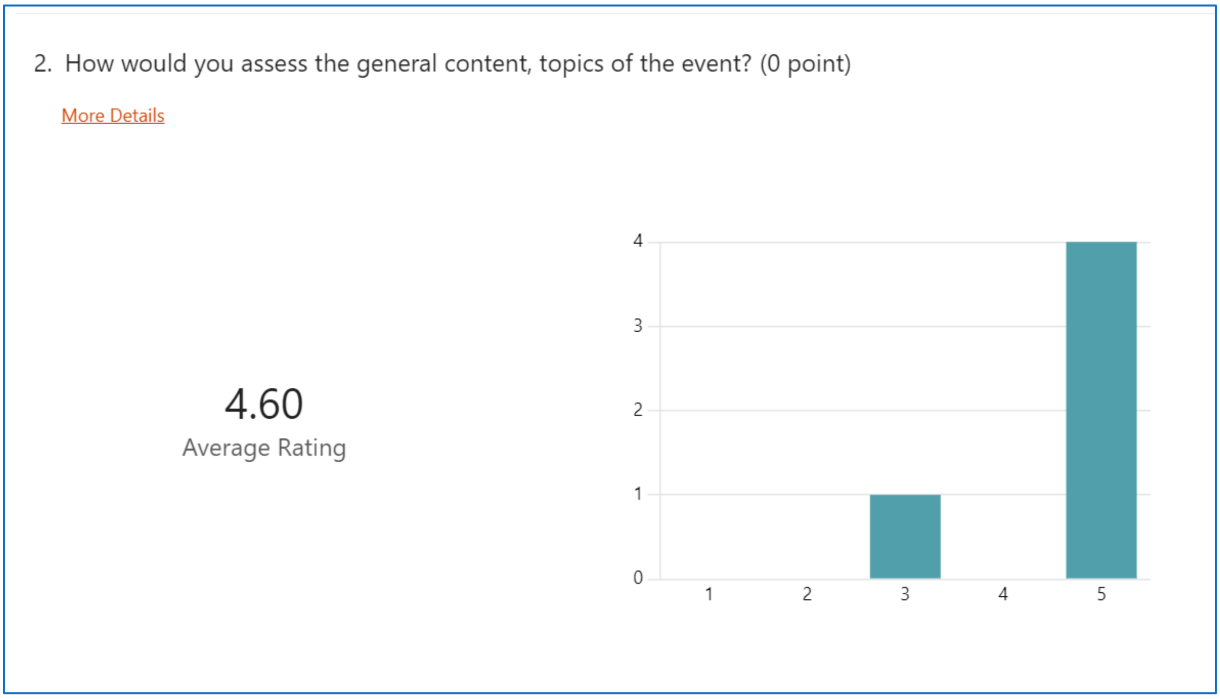


1. Overall, how satisfied were you with the event? (0 point)

More Details

4.80
Average Rating

Figure 6 Evaluation form: event overall satisfaction

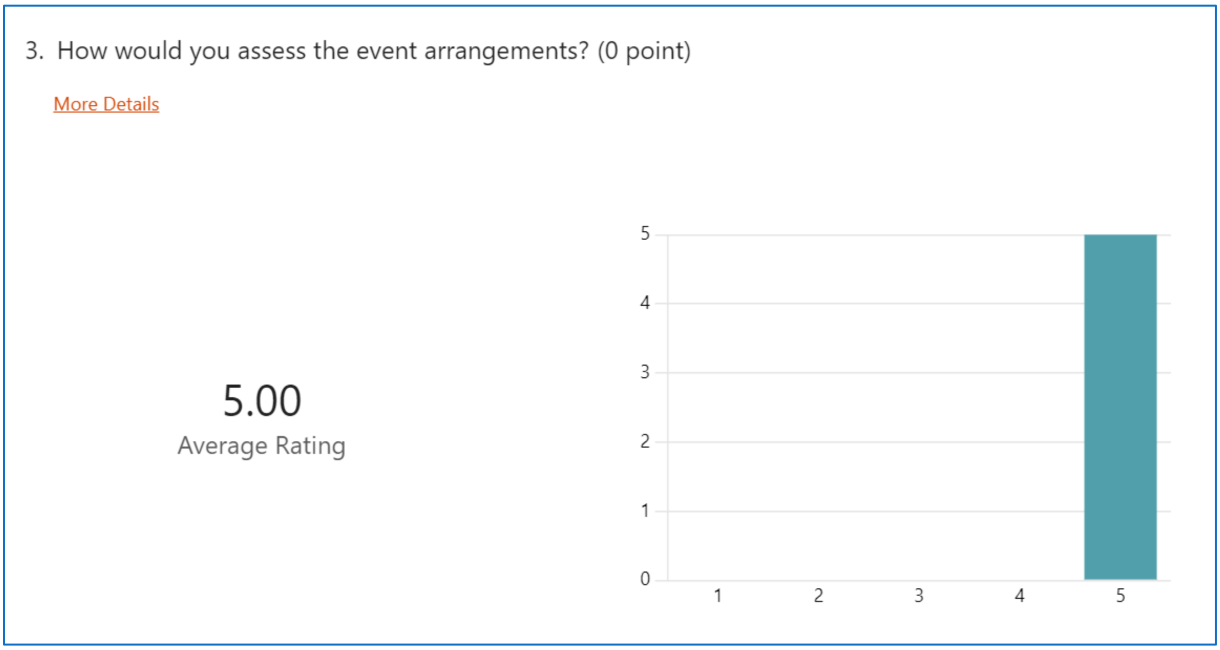


2. How would you assess the general content, topics of the event? (0 point)

More Details

4.60
Average Rating

Figure 7 Evaluation form: general contents' assessment



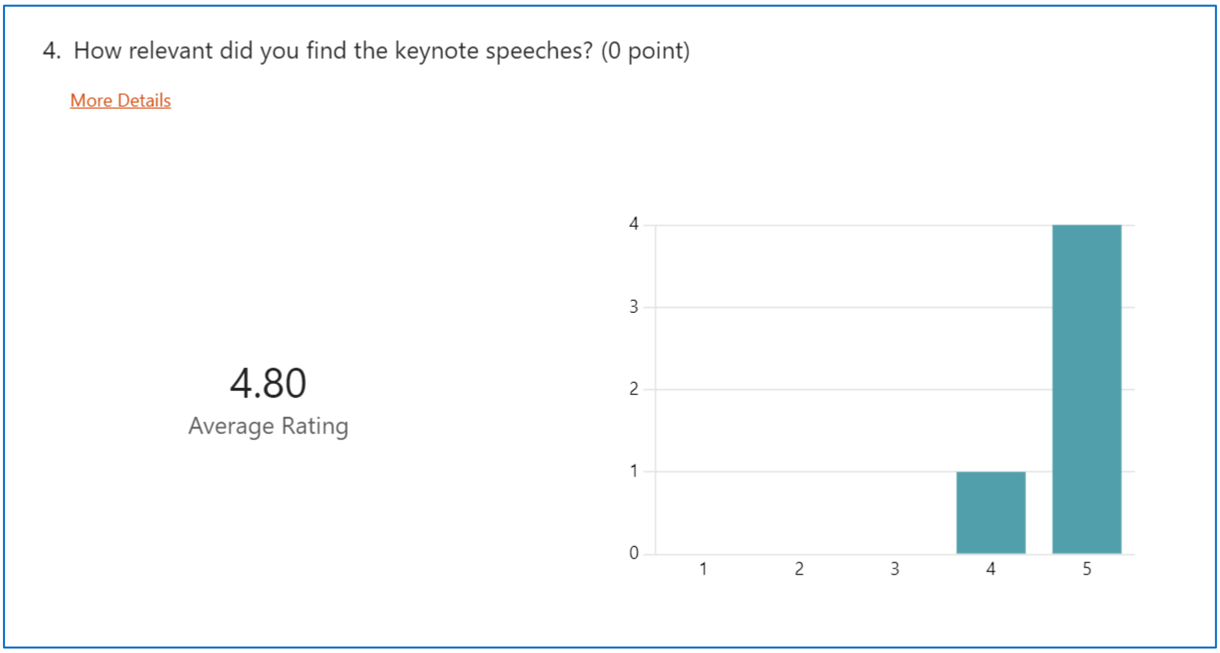
3. How would you assess the event arrangements? (0 point)

More Details

5.00

Average Rating

Figure 8 Evaluation form: event arrangements' assessment



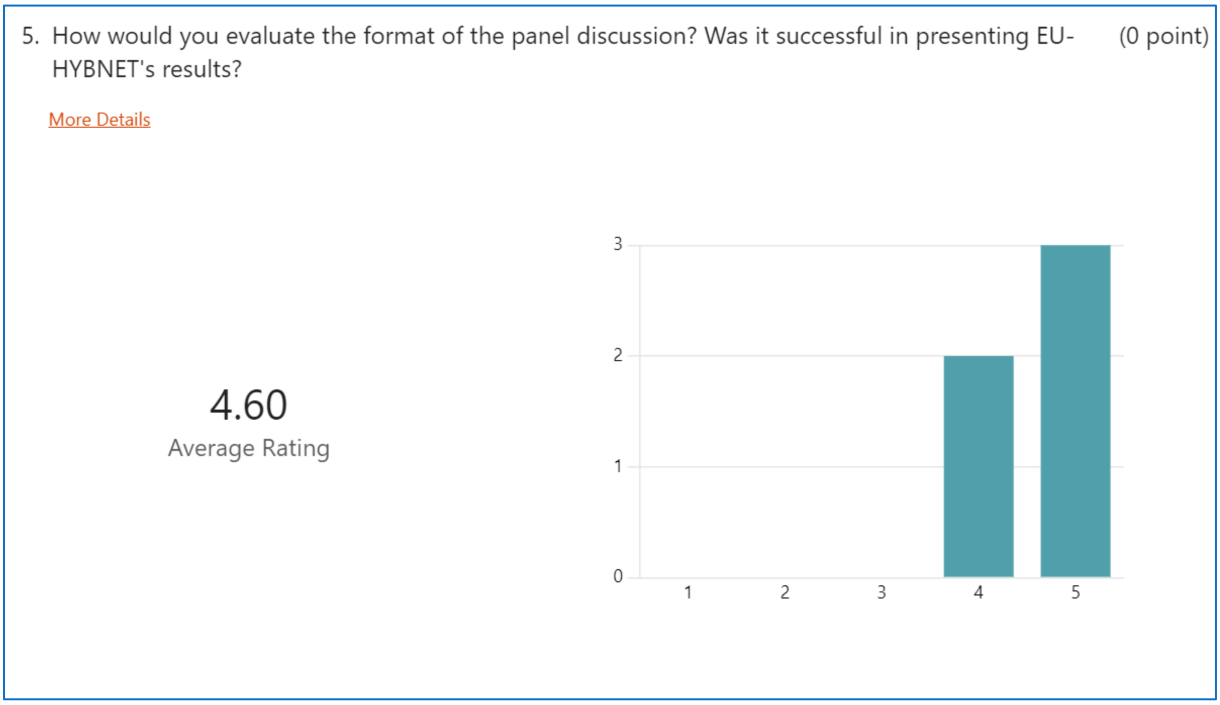
4. How relevant did you find the keynote speeches? (0 point)

More Details

4.80

Average Rating

Figure 9 Evaluation form: keynote speeches' assessment

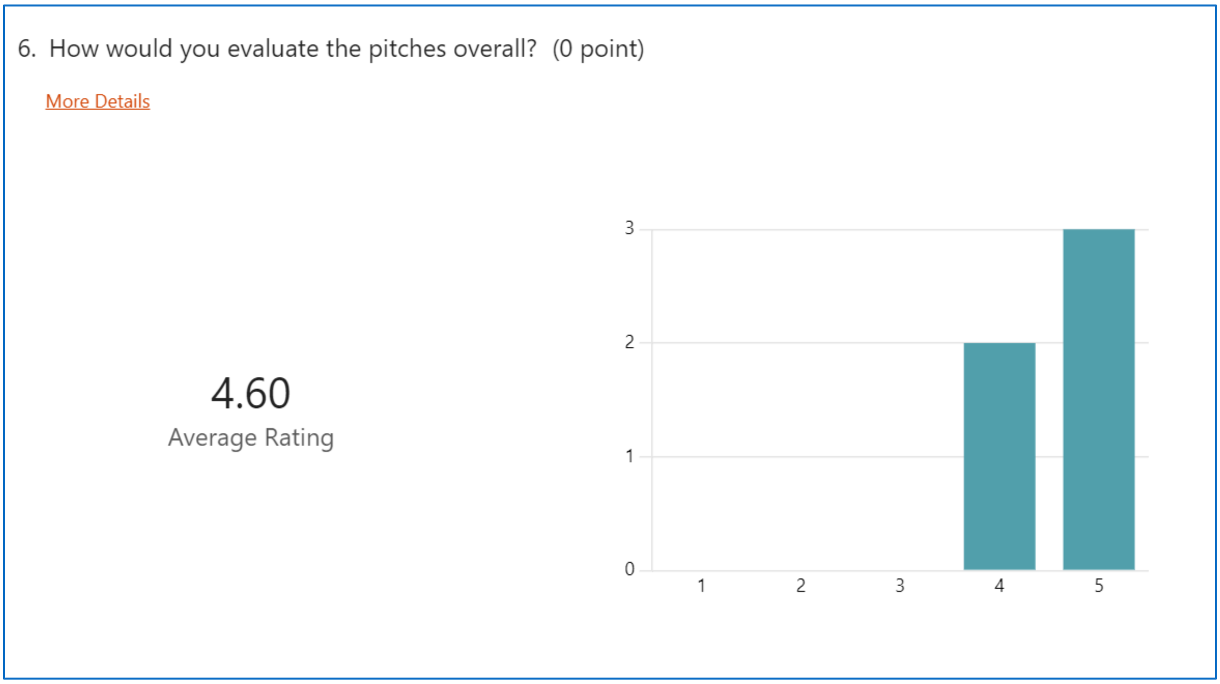


5. How would you evaluate the format of the panel discussion? Was it successful in presenting EU-HYBNET's results? (0 point)

More Details

4.60
Average Rating

Figure 10 Evaluation form: panel discussion’s assessment

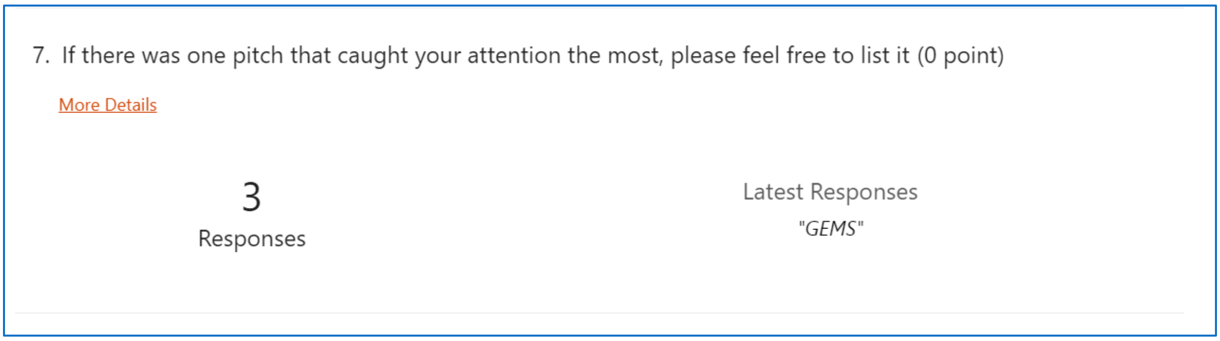


6. How would you evaluate the pitches overall? (0 point)

More Details

4.60
Average Rating

Figure 11 Evaluation form: pitches' assessment



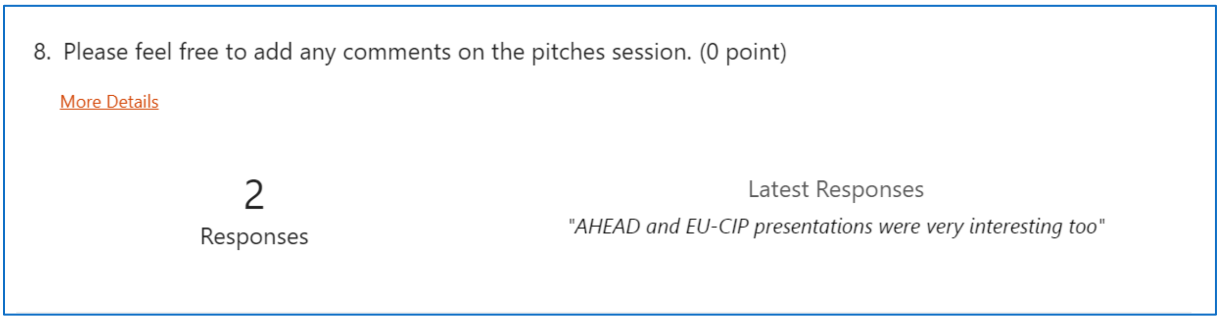
7. If there was one pitch that caught your attention the most, please feel free to list it (0 point)

More Details

3
Responses

Latest Responses
"GEMS"

Figure 12 Evaluation form: question 7



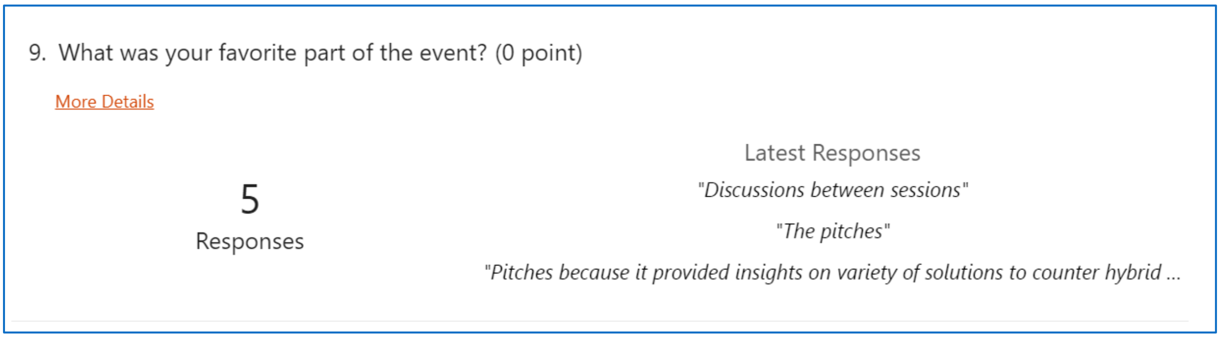
8. Please feel free to add any comments on the pitches session. (0 point)

More Details

2
Responses

Latest Responses
"AHEAD and EU-CIP presentations were very interesting too"

Figure 13 Evaluation form: question 8



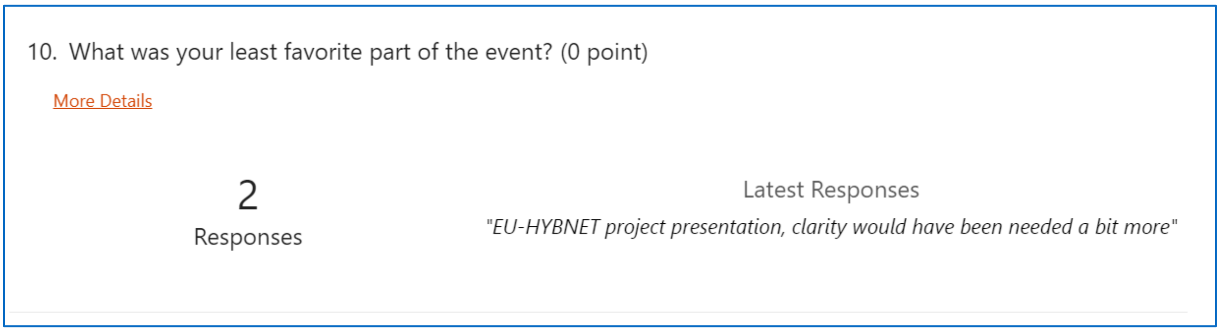
9. What was your favorite part of the event? (0 point)

More Details

5
Responses

Latest Responses
"Discussions between sessions"
"The pitches"
"Pitches because it provided insights on variety of solutions to counter hybrid ...

Figure 14 Evaluation form: question 9



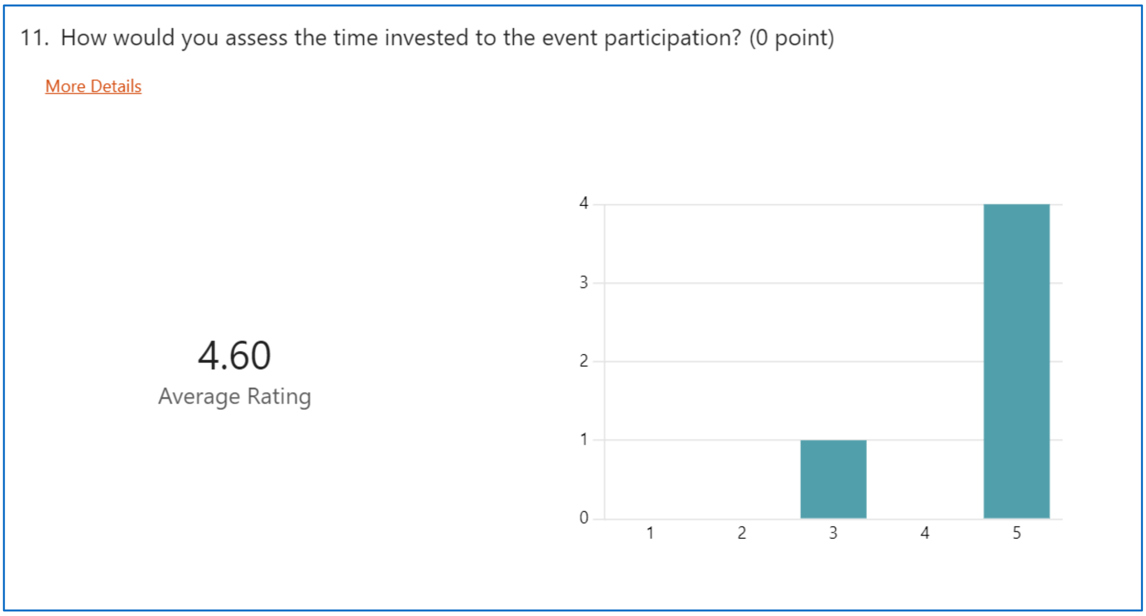
10. What was your least favorite part of the event? (0 point)

More Details

2
Responses

Latest Responses
"EU-HYBNET project presentation, clarity would have been needed a bit more"

Figure 15 Evaluation form: question 10

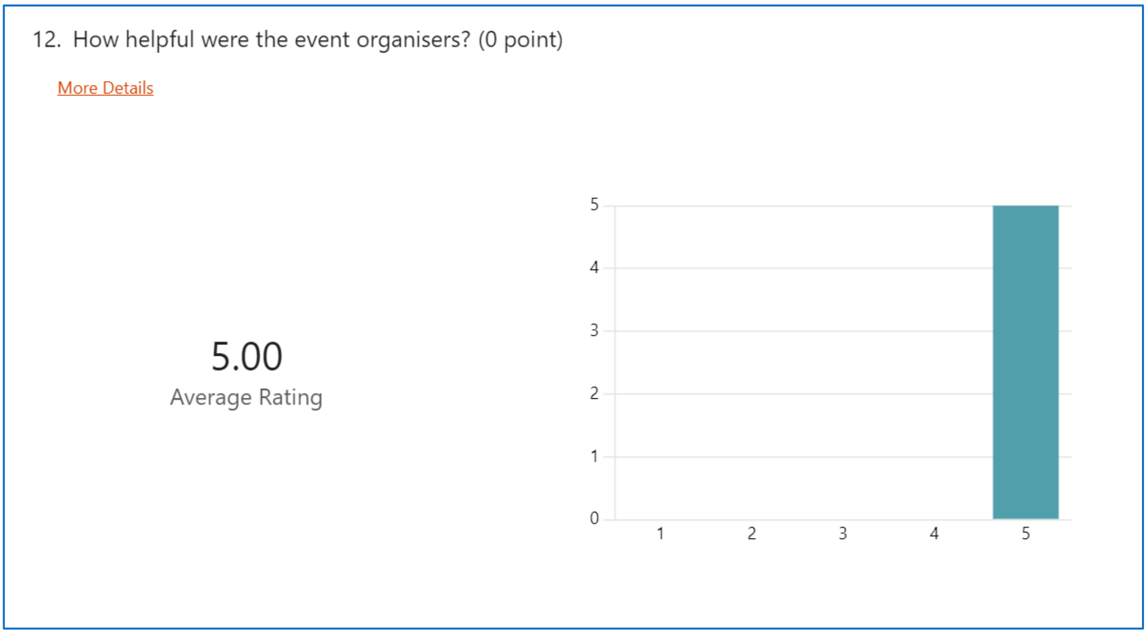


11. How would you assess the time invested to the event participation? (0 point)

More Details

4.60
Average Rating

Figure 16 Evaluation form: invested time's assessment

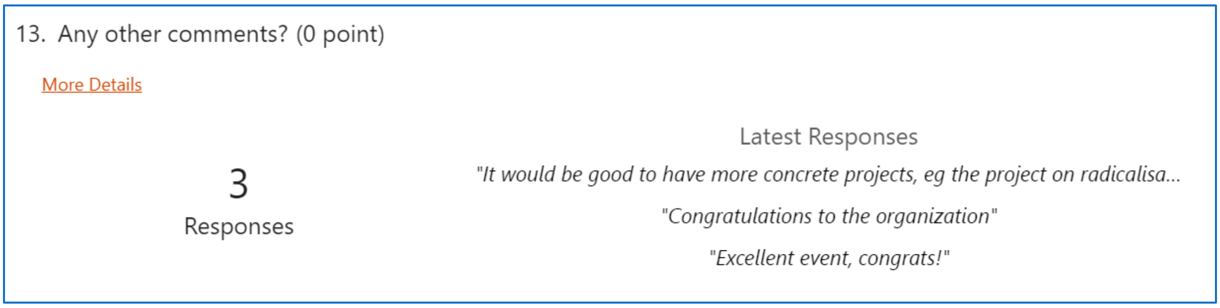


12. How helpful were the event organisers? (0 point)

More Details

5.00
Average Rating

Figure 17 Evaluation form: organisers' assessment



13. Any other comments? (0 point)

More Details

3

Responses

Latest Responses

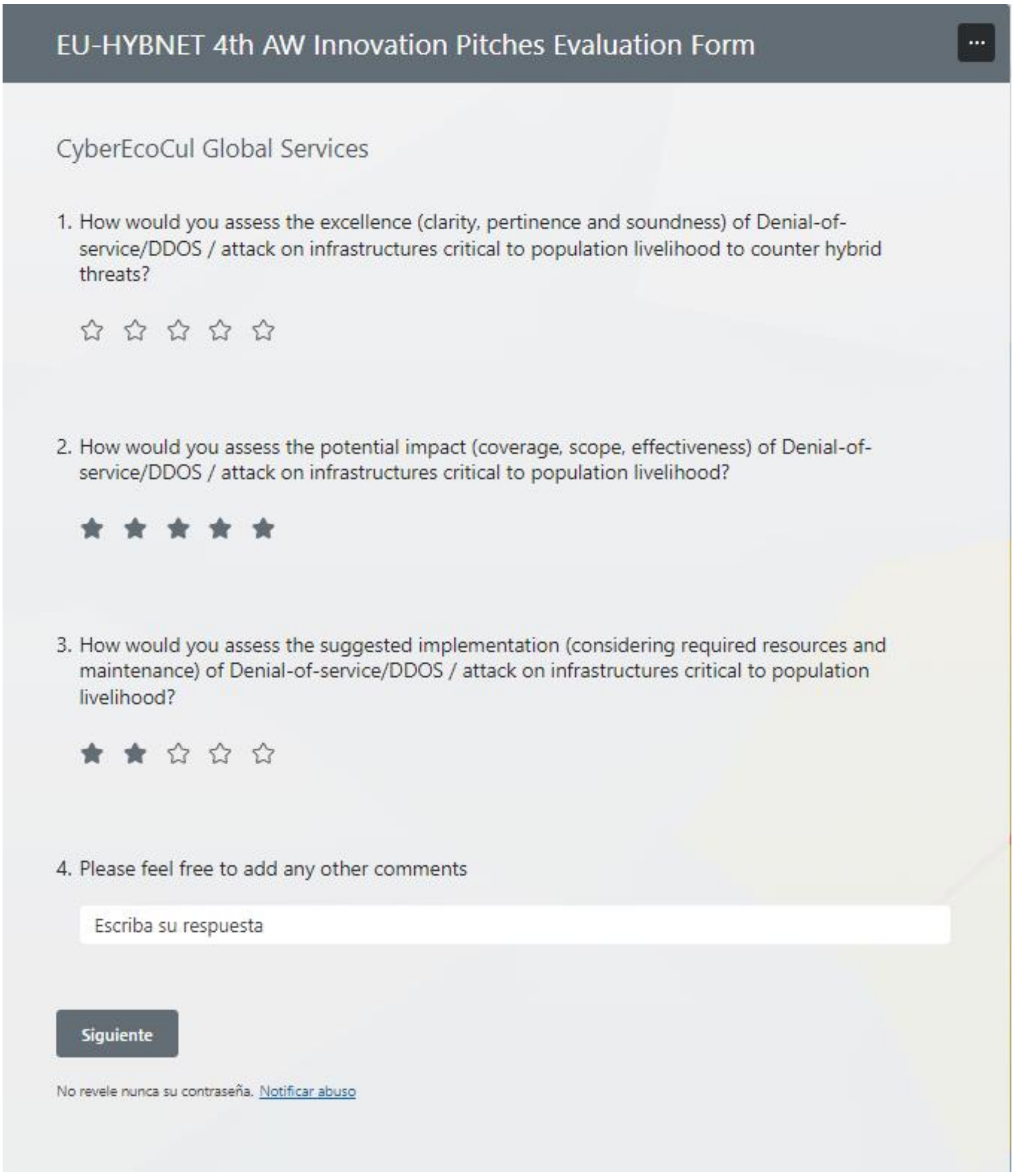
"It would be good to have more concrete projects, eg the project on radicalisa...

"Congratulations to the organization"

"Excellent event, congrats!"

Figure 18 Evaluation form: comments

ANNEX VI. PITCHES EVALUATION FORMS AND ANSWERS



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

CyberEcoCul Global Services

1. How would you assess the excellence (clarity, pertinence and soundness) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood to counter hybrid threats?

☆ ☆ ☆ ☆ ☆

2. How would you assess the potential impact (coverage, scope, effectiveness) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood?

★ ★ ★ ★ ★

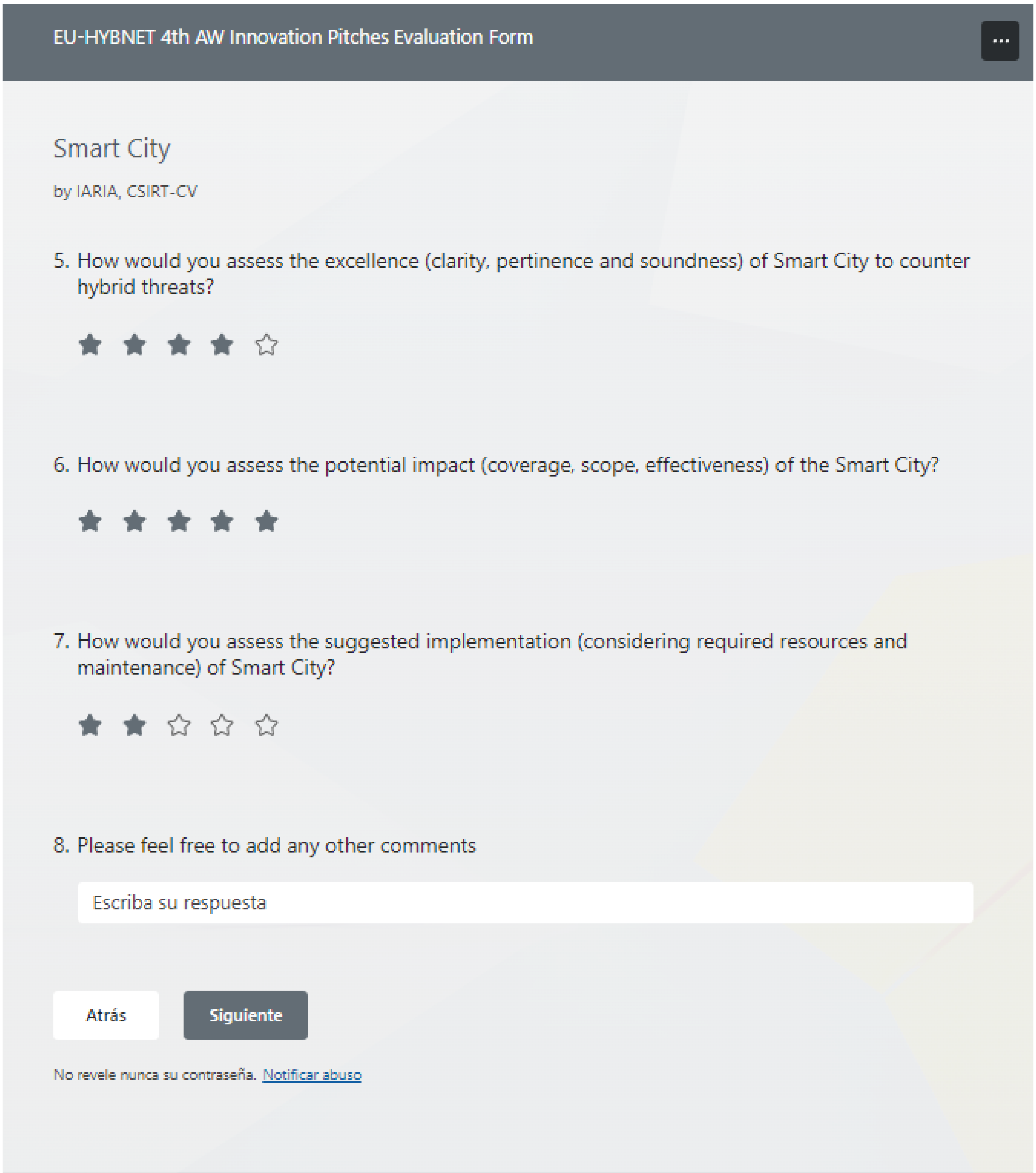
3. How would you assess the suggested implementation (considering required resources and maintenance) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood?

★ ★ ☆ ☆ ☆

4. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

Smart City

by IARIA, CSIRT-CV

5. How would you assess the excellence (clarity, pertinence and soundness) of Smart City to counter hybrid threats?

★ ★ ★ ★ ☆

6. How would you assess the potential impact (coverage, scope, effectiveness) of the Smart City?

★ ★ ★ ★ ★

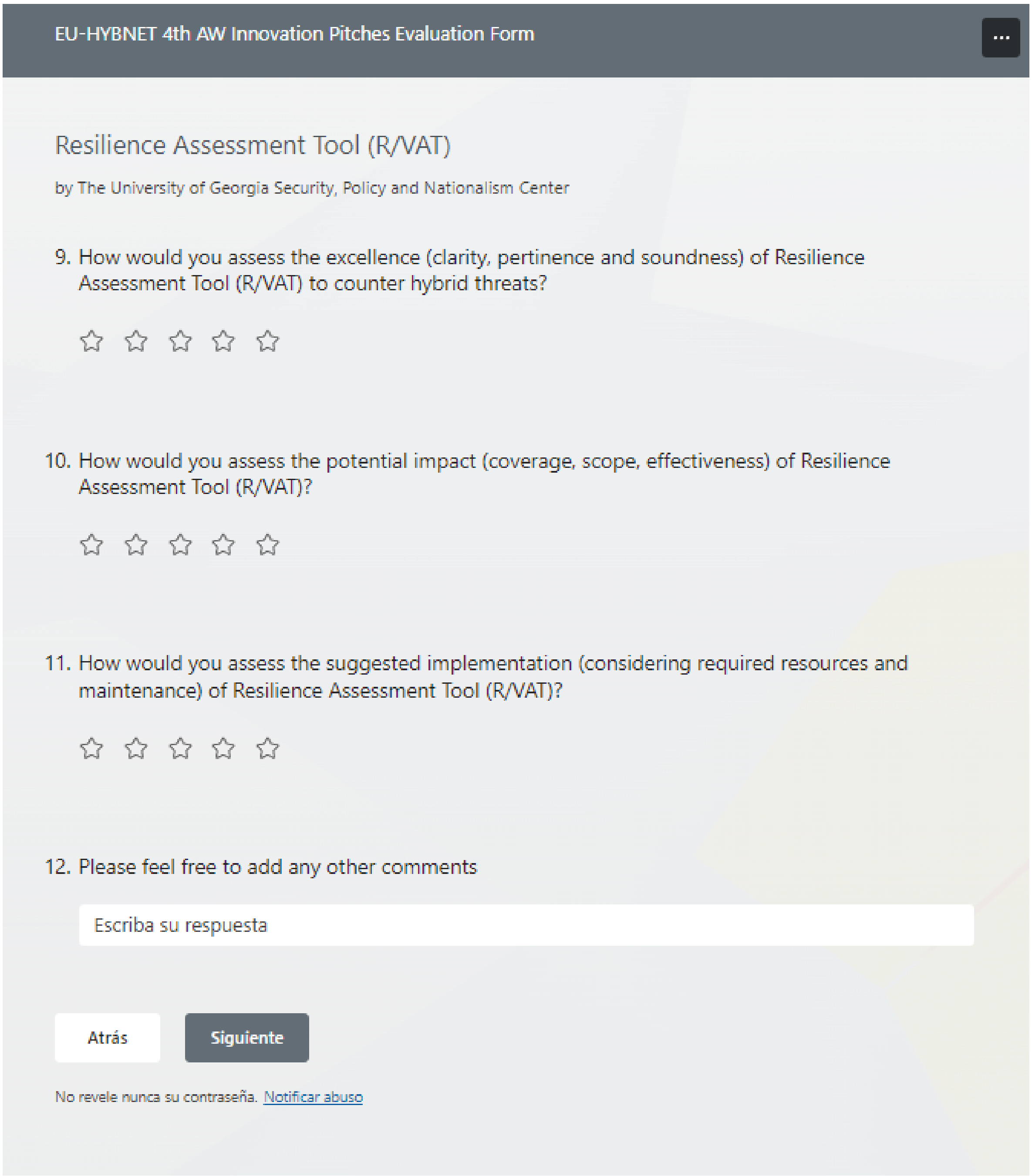
7. How would you assess the suggested implementation (considering required resources and maintenance) of Smart City?

★ ★ ☆ ☆ ☆

8. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

Resilience Assessment Tool (R/VAT)

by The University of Georgia Security, Policy and Nationalism Center

9. How would you assess the excellence (clarity, pertinence and soundness) of Resilience Assessment Tool (R/VAT) to counter hybrid threats?

☆ ☆ ☆ ☆ ☆

10. How would you assess the potential impact (coverage, scope, effectiveness) of Resilience Assessment Tool (R/VAT)?

☆ ☆ ☆ ☆ ☆

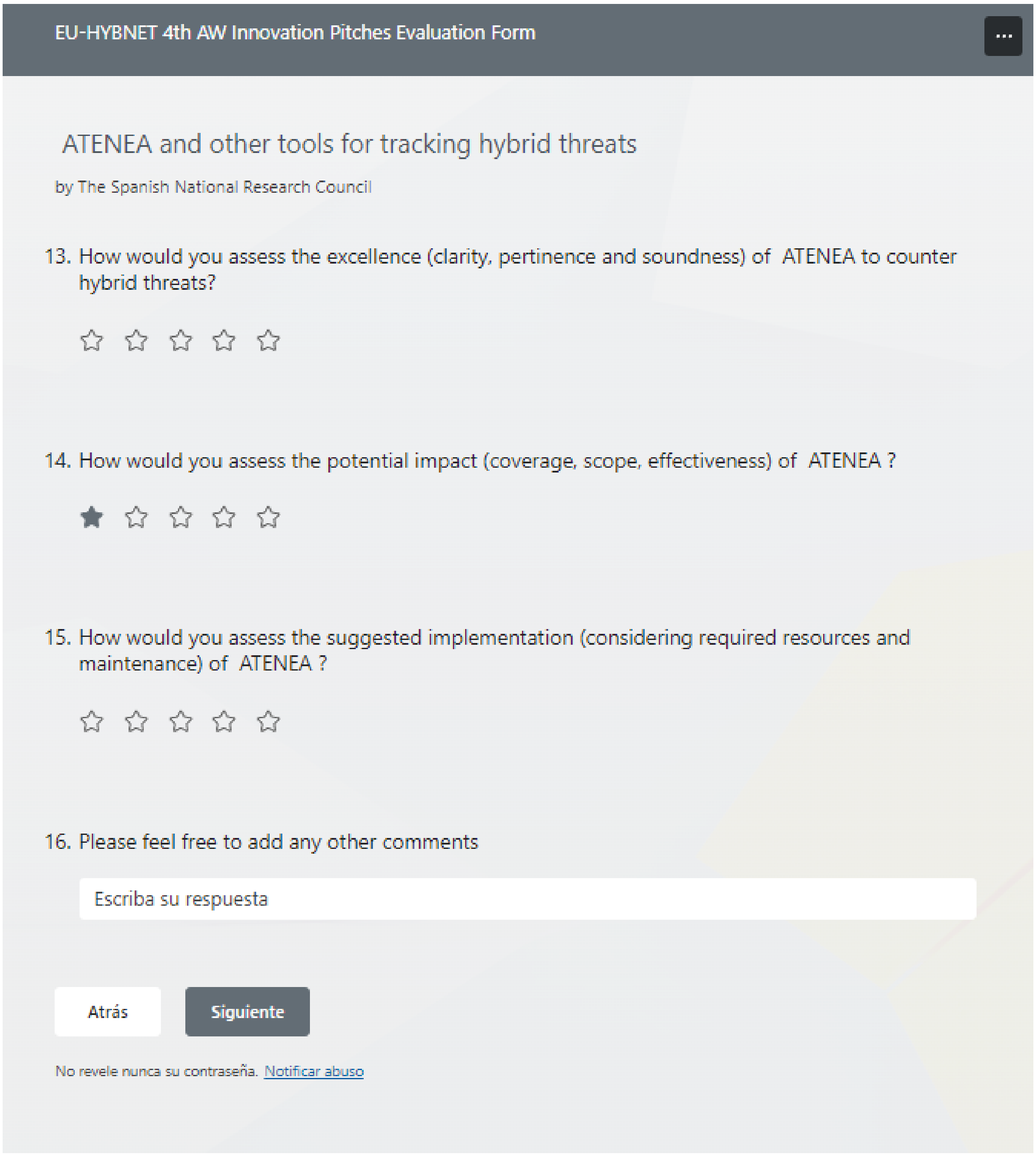
11. How would you assess the suggested implementation (considering required resources and maintenance) of Resilience Assessment Tool (R/VAT)?

☆ ☆ ☆ ☆ ☆

12. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

ATENEA and other tools for tracking hybrid threats

by The Spanish National Research Council

13. How would you assess the excellence (clarity, pertinence and soundness) of ATENEA to counter hybrid threats?

☆ ☆ ☆ ☆ ☆

14. How would you assess the potential impact (coverage, scope, effectiveness) of ATENEA ?

★ ☆ ☆ ☆ ☆

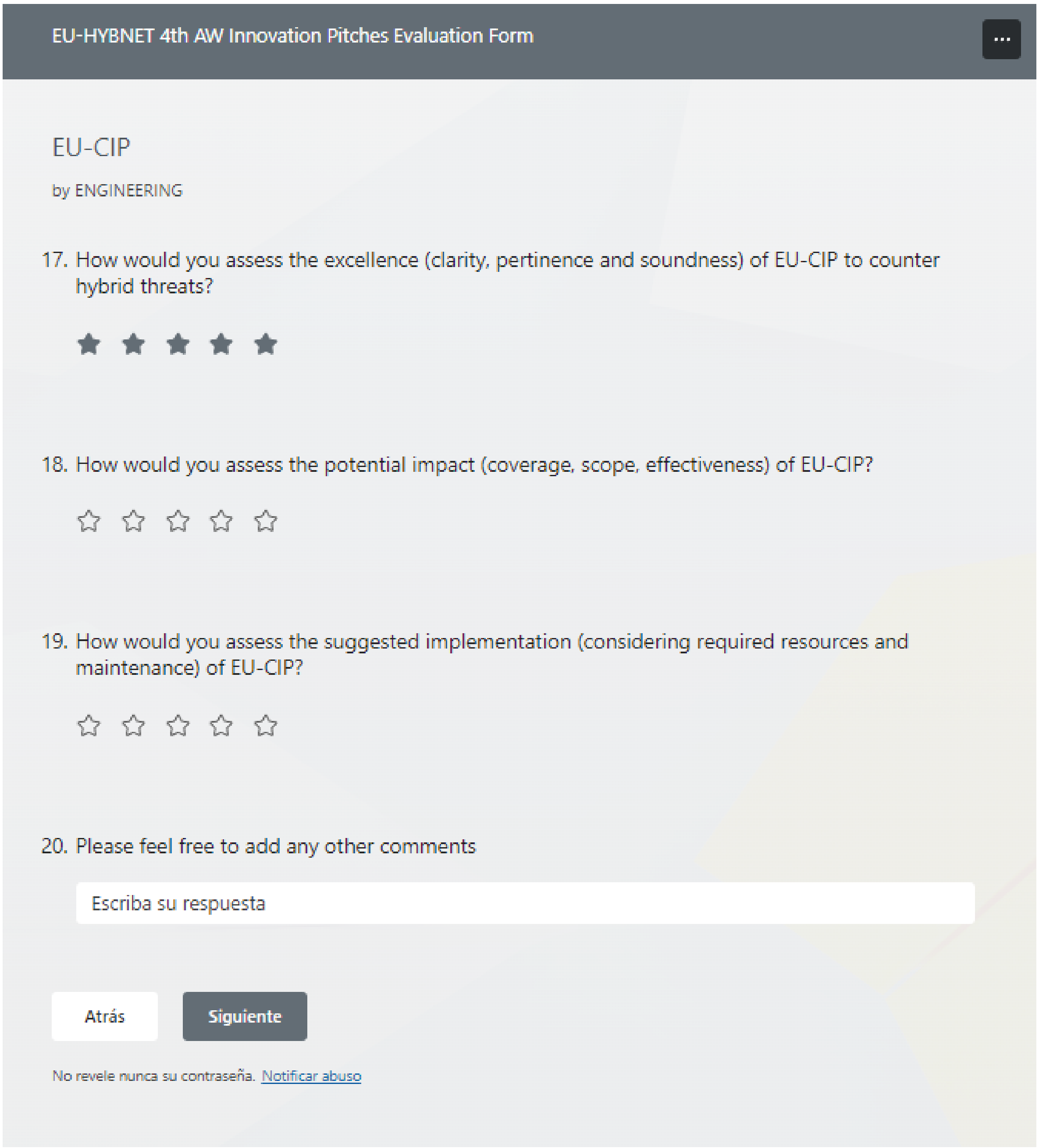
15. How would you assess the suggested implementation (considering required resources and maintenance) of ATENEA ?

☆ ☆ ☆ ☆ ☆

16. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

EU-CIP

by ENGINEERING

17. How would you assess the excellence (clarity, pertinence and soundness) of EU-CIP to counter hybrid threats?

★ ★ ★ ★ ★

18. How would you assess the potential impact (coverage, scope, effectiveness) of EU-CIP?

☆ ☆ ☆ ☆ ☆

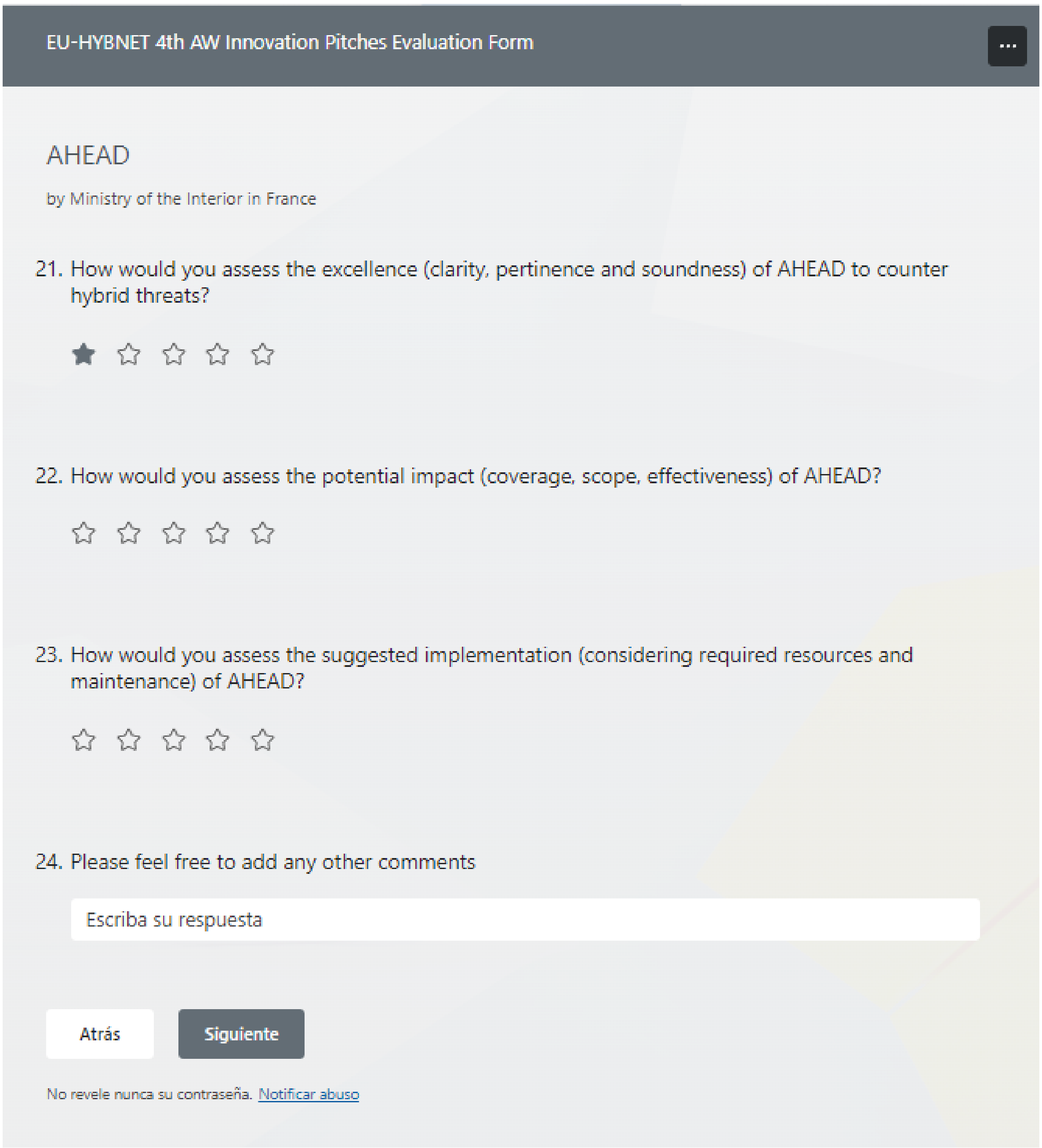
19. How would you assess the suggested implementation (considering required resources and maintenance) of EU-CIP?

☆ ☆ ☆ ☆ ☆

20. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

AHEAD

by Ministry of the Interior in France

21. How would you assess the excellence (clarity, pertinence and soundness) of AHEAD to counter hybrid threats?

★ ☆ ☆ ☆ ☆

22. How would you assess the potential impact (coverage, scope, effectiveness) of AHEAD?

☆ ☆ ☆ ☆ ☆

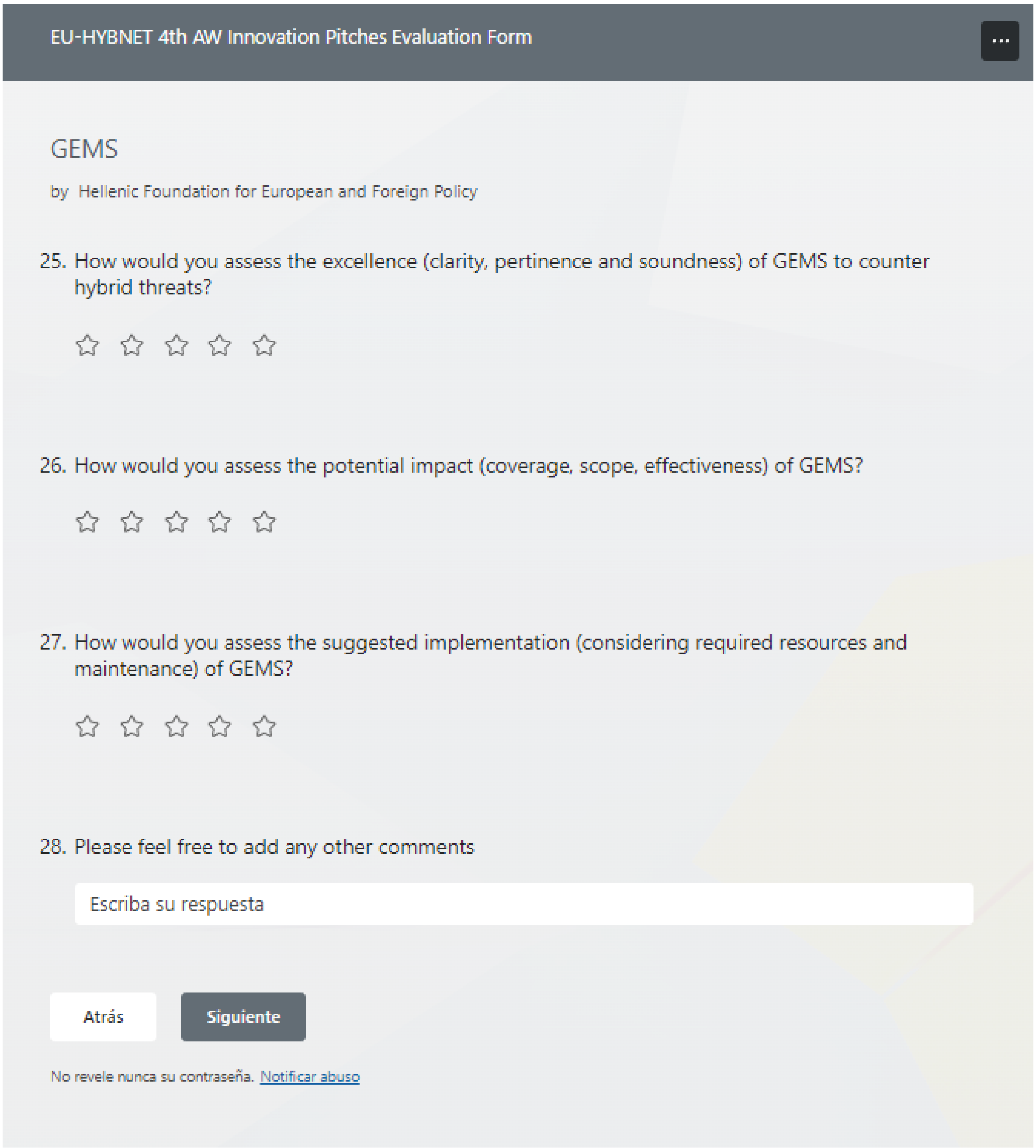
23. How would you assess the suggested implementation (considering required resources and maintenance) of AHEAD?

☆ ☆ ☆ ☆ ☆

24. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

GEMS

by Hellenic Foundation for European and Foreign Policy

25. How would you assess the excellence (clarity, pertinence and soundness) of GEMS to counter hybrid threats?

☆ ☆ ☆ ☆ ☆

26. How would you assess the potential impact (coverage, scope, effectiveness) of GEMS?

☆ ☆ ☆ ☆ ☆

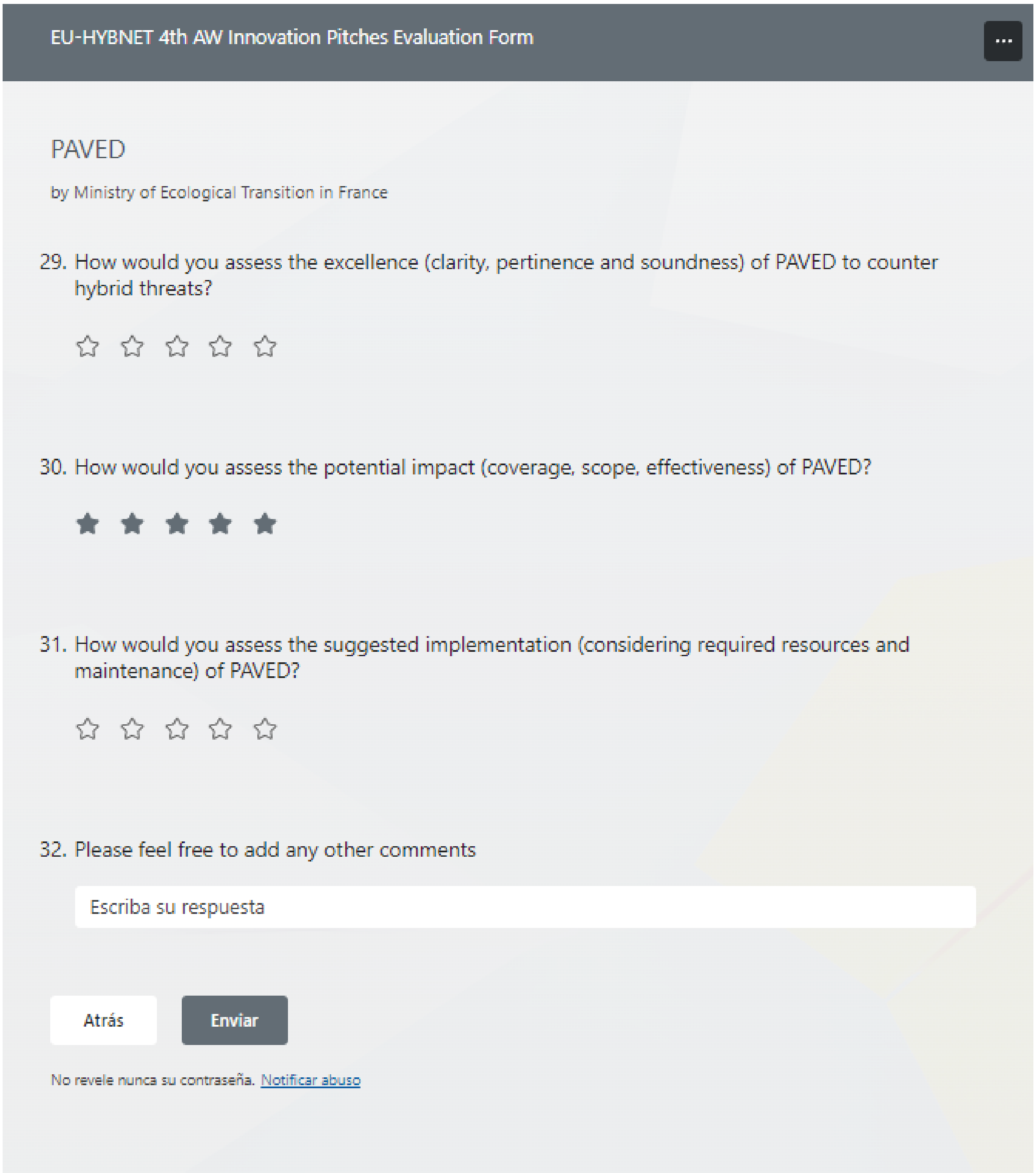
27. How would you assess the suggested implementation (considering required resources and maintenance) of GEMS?

☆ ☆ ☆ ☆ ☆

28. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso



EU-HYBNET 4th AW Innovation Pitches Evaluation Form

PAVED

by Ministry of Ecological Transition in France

29. How would you assess the excellence (clarity, pertinence and soundness) of PAVED to counter hybrid threats?

☆ ☆ ☆ ☆ ☆

30. How would you assess the potential impact (coverage, scope, effectiveness) of PAVED?

★ ★ ★ ★ ★

31. How would you assess the suggested implementation (considering required resources and maintenance) of PAVED?

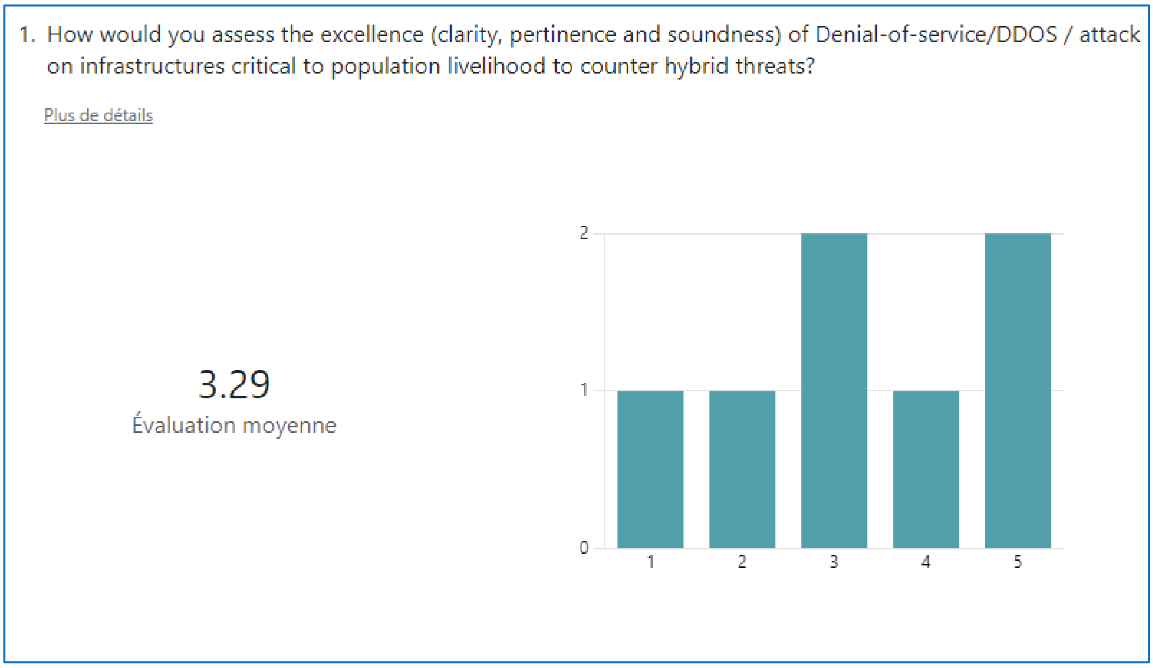
☆ ☆ ☆ ☆ ☆

32. Please feel free to add any other comments

Escriba su respuesta

No revele nunca su contraseña. Notificar abuso

Figure 19 EU-HYBNET 4th AW Innovation Pitches Evaluation Form



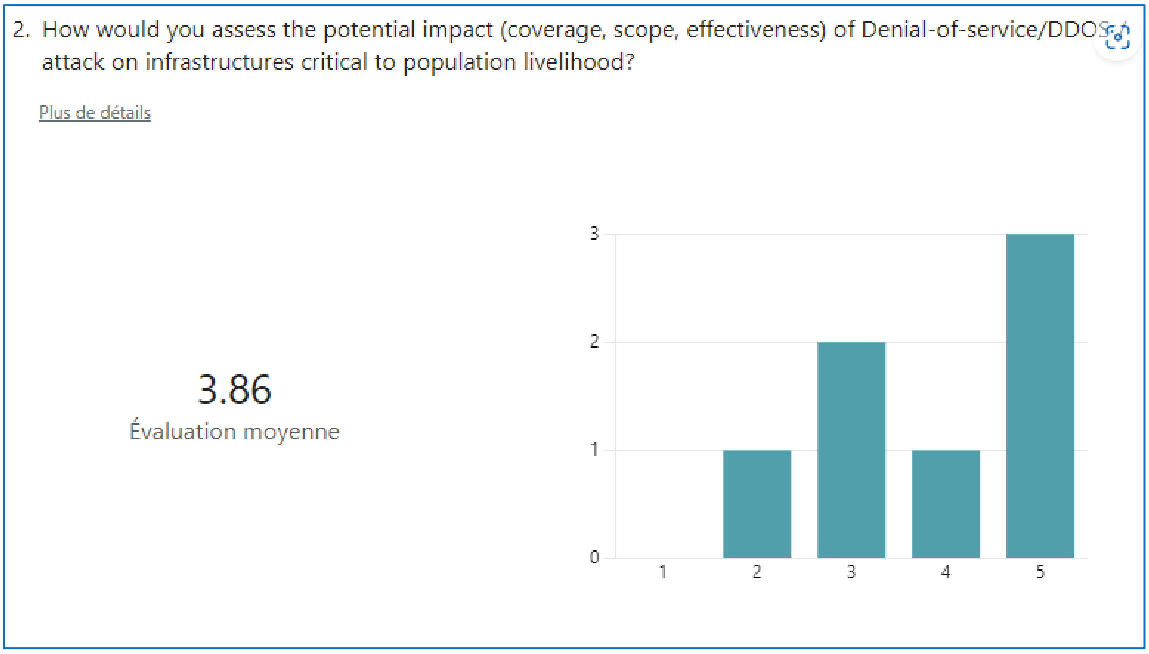
1. How would you assess the excellence (clarity, pertinence and soundness) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood to counter hybrid threats?

Plus de détails

3.29

Évaluation moyenne

Figure 20 Denial-of-service/DDOS excellence assessment



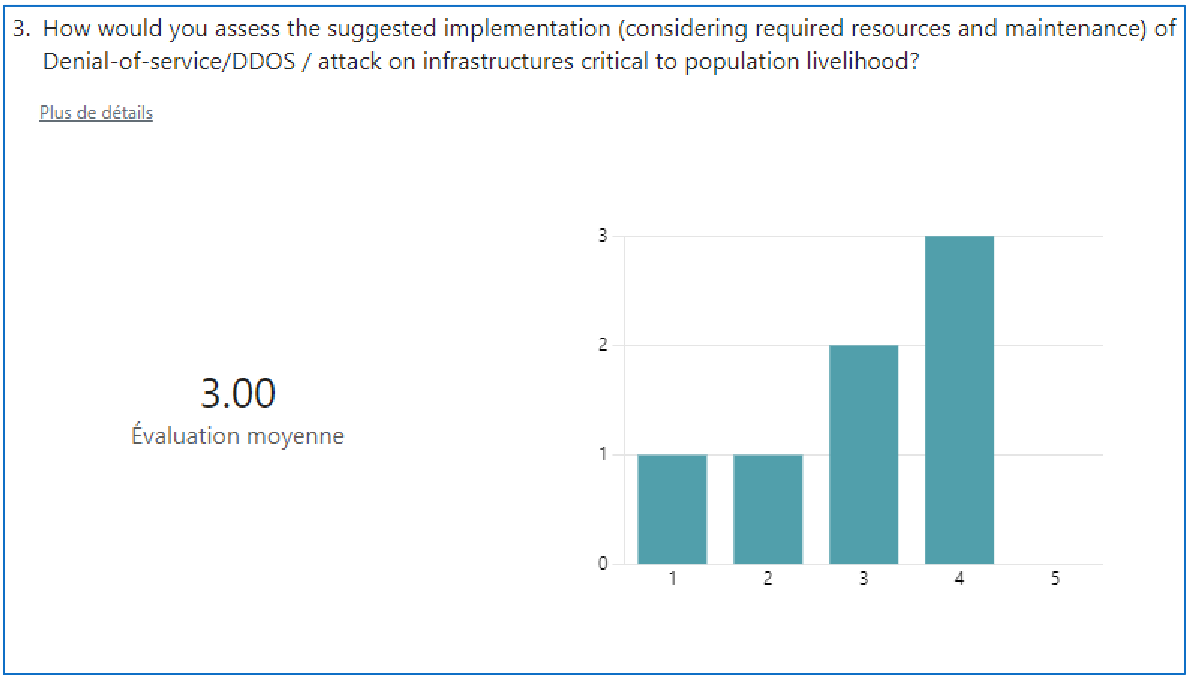
2. How would you assess the potential impact (coverage, scope, effectiveness) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood?

Plus de détails

3.86

Évaluation moyenne

Figure 21 Denial-of-service/DDOS potential impact assessment



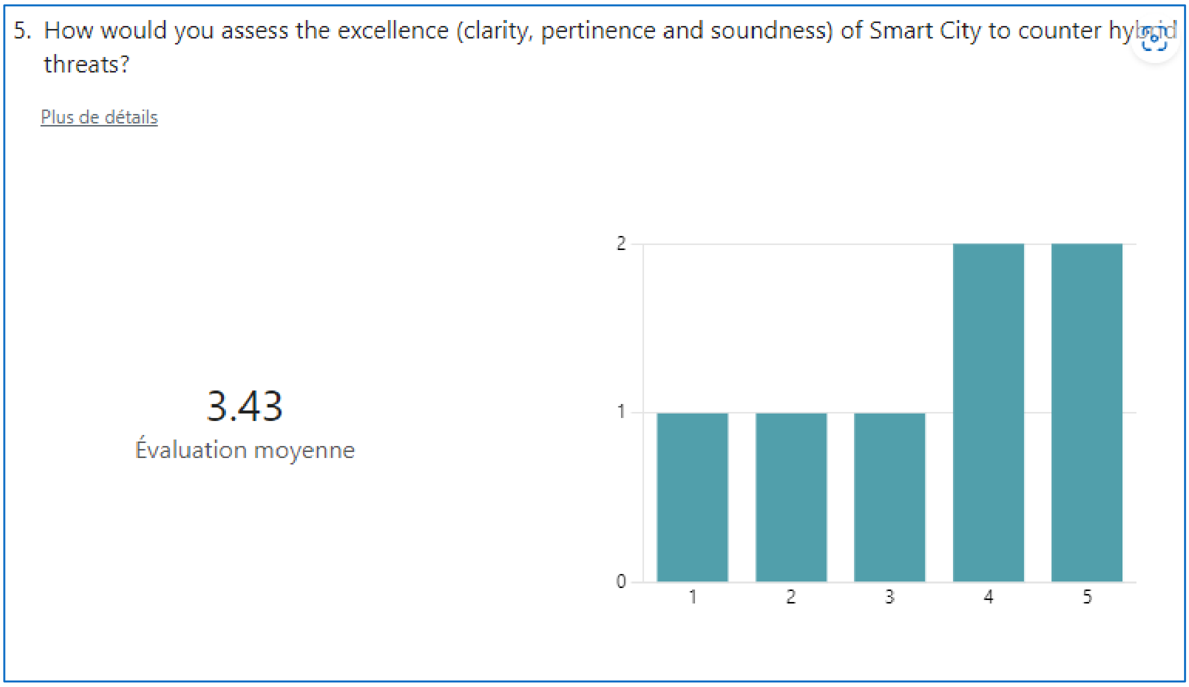
3. How would you assess the suggested implementation (considering required resources and maintenance) of Denial-of-service/DDOS / attack on infrastructures critical to population livelihood?

Plus de détails

3.00

Évaluation moyenne

Figure 22 Denial-of-service/DDOS implementation assessment



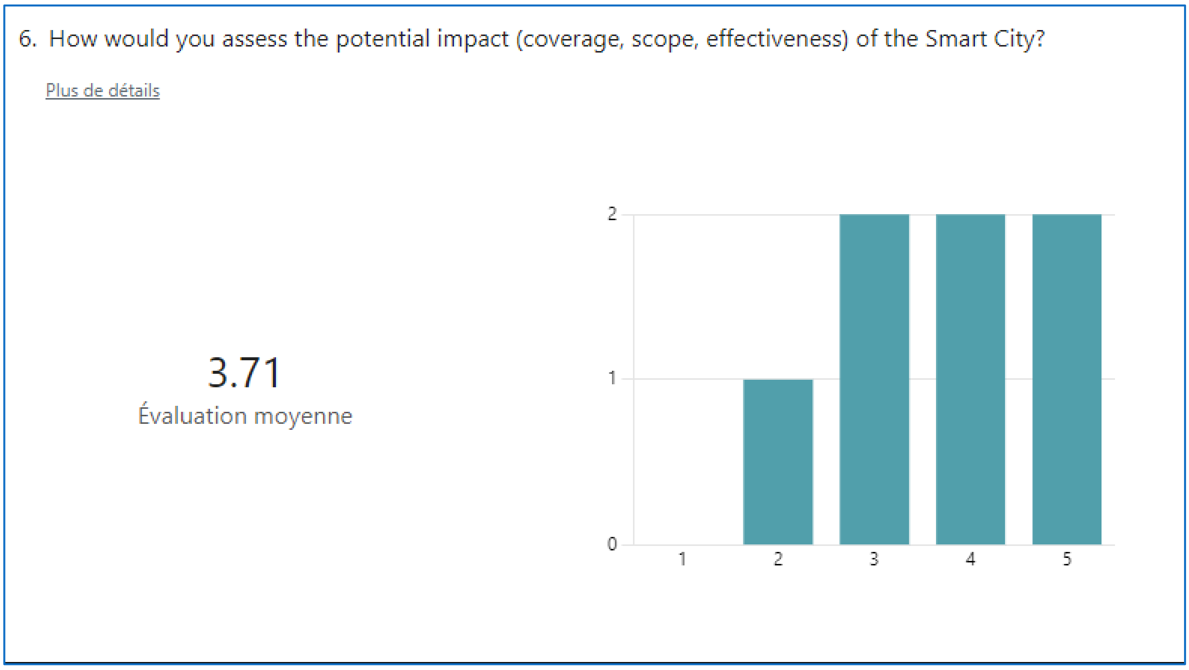
5. How would you assess the excellence (clarity, pertinence and soundness) of Smart City to counter hybrid threats?

Plus de détails

3.43

Évaluation moyenne

Figure 23 Smart City's excellence assessment



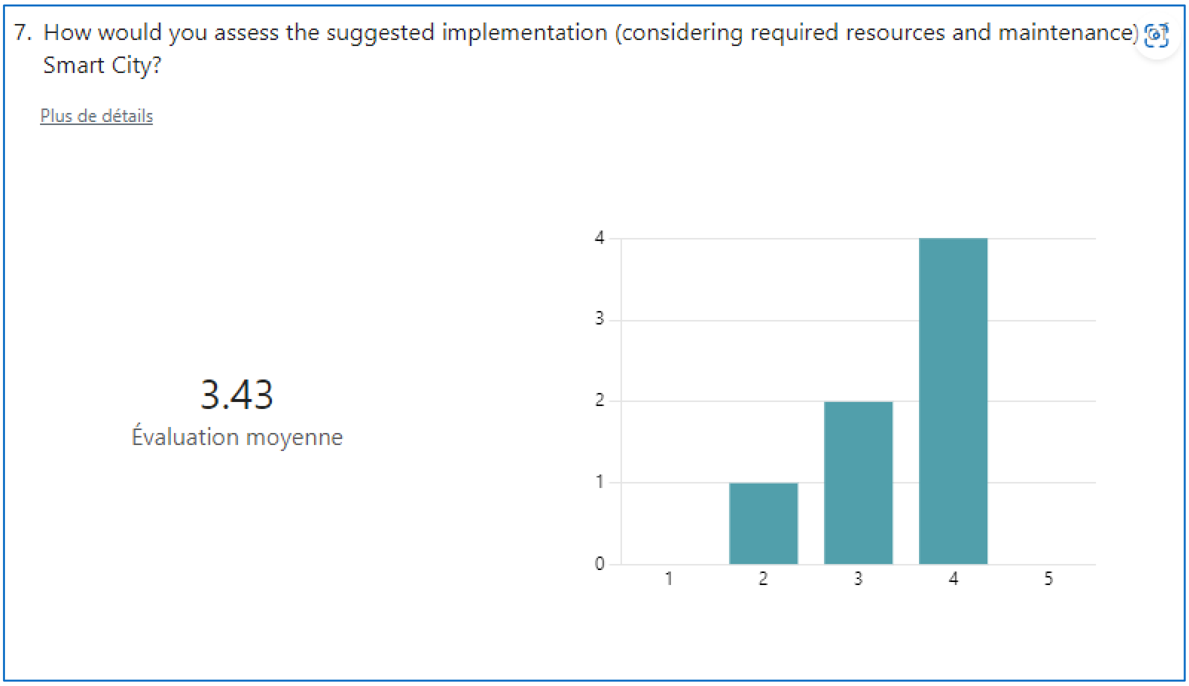
6. How would you assess the potential impact (coverage, scope, effectiveness) of the Smart City?

Plus de détails

3.71

Évaluation moyenne

Figure 24 Smart City’s potential impact assessment



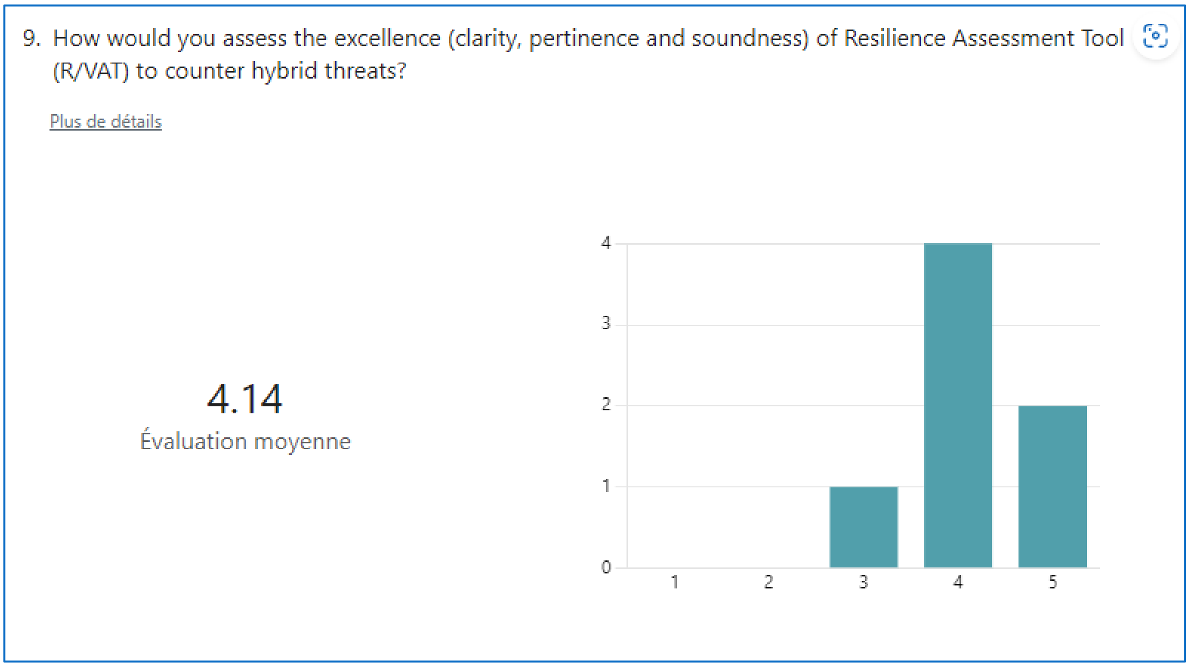
7. How would you assess the suggested implementation (considering required resources and maintenance) Smart City?

Plus de détails

3.43

Évaluation moyenne

Figure 25 Smart City's implementation assessment

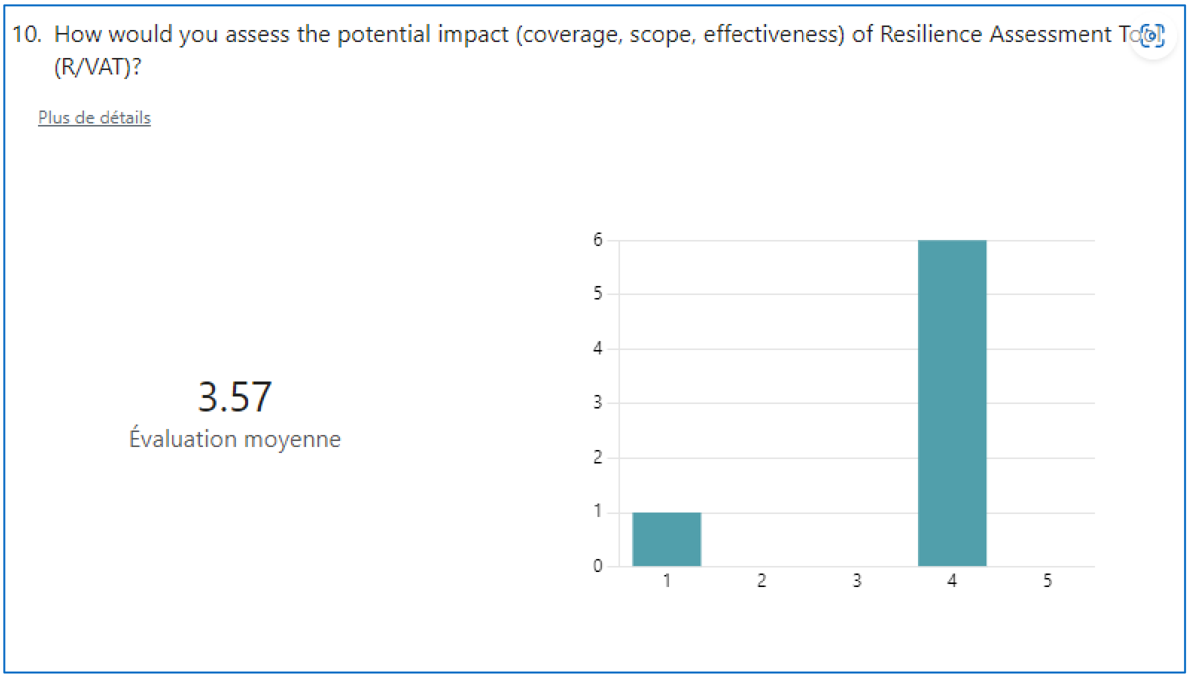


9. How would you assess the excellence (clarity, pertinence and soundness) of Resilience Assessment Tool (R/VAT) to counter hybrid threats?

Plus de détails

4.14
Évaluation moyenne

Figure 26 R/VAT's excellence assessment

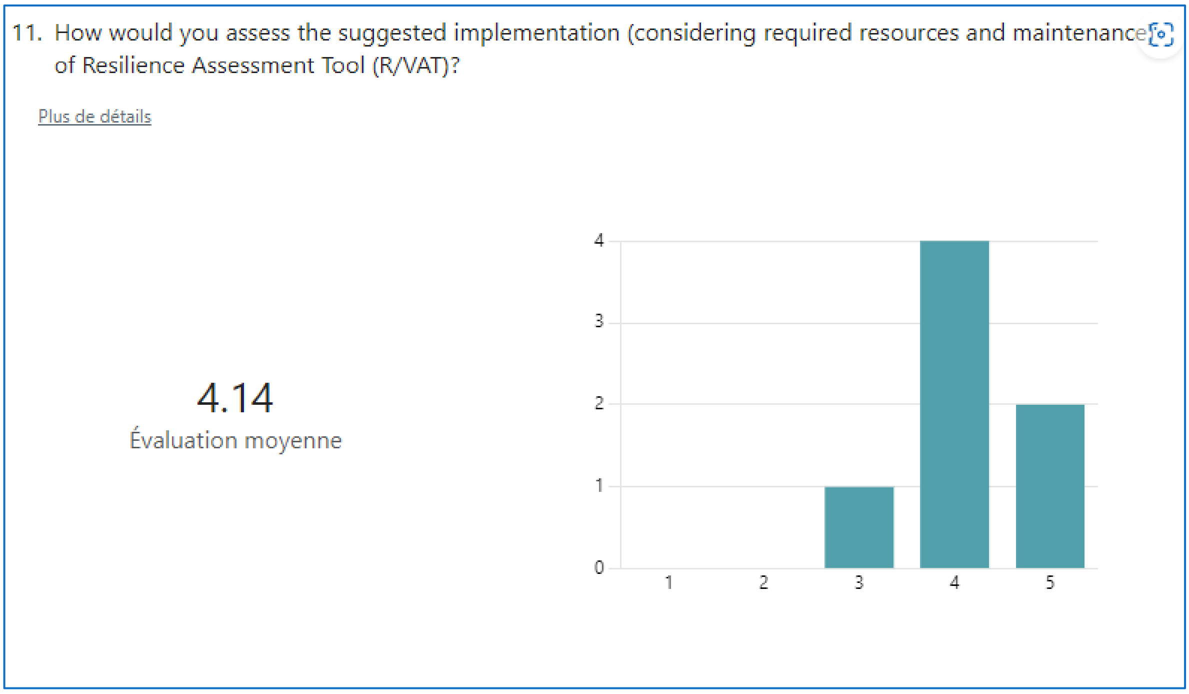


10. How would you assess the potential impact (coverage, scope, effectiveness) of Resilience Assessment To (R/VAT)?

Plus de détails

3.57
Évaluation moyenne

Figure 27 R/VAT's potential impact assessment

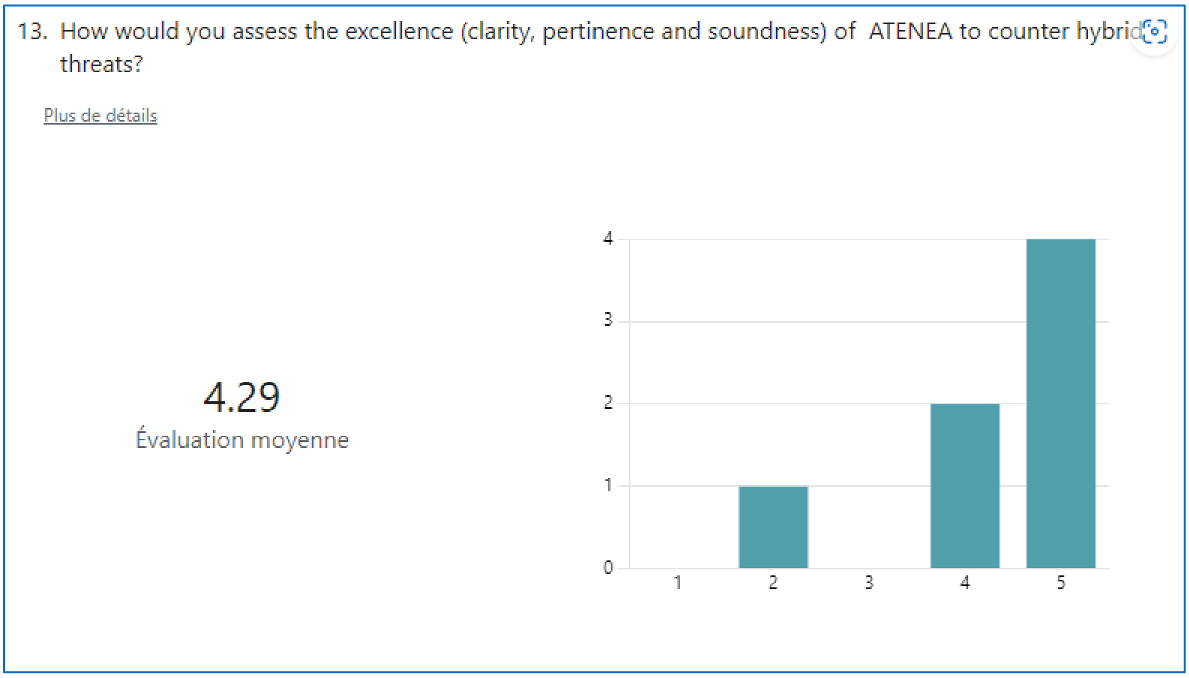


11. How would you assess the suggested implementation (considering required resources and maintenance) of Resilience Assessment Tool (R/VAT)?

Plus de détails

4.14
Évaluation moyenne

Figure 28 R/VAT's implementation assessment

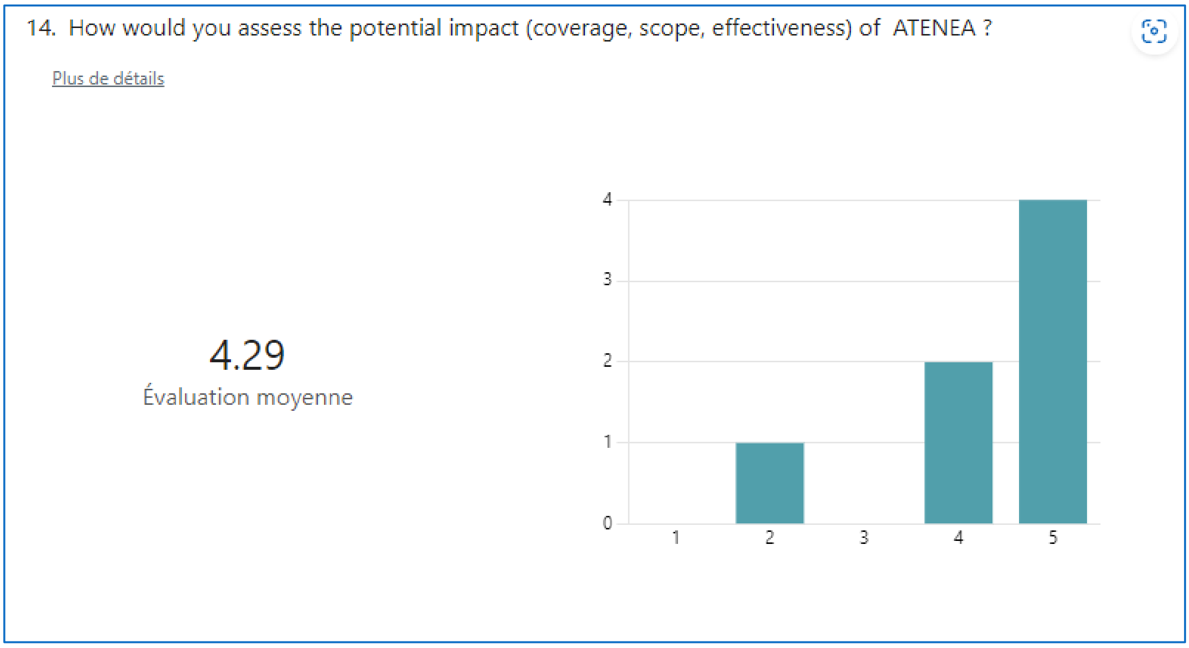


13. How would you assess the excellence (clarity, pertinence and soundness) of ATENEA to counter hybrid threats?

Plus de détails

4.29
Évaluation moyenne

Figure 29 ATENEA excellence assessment

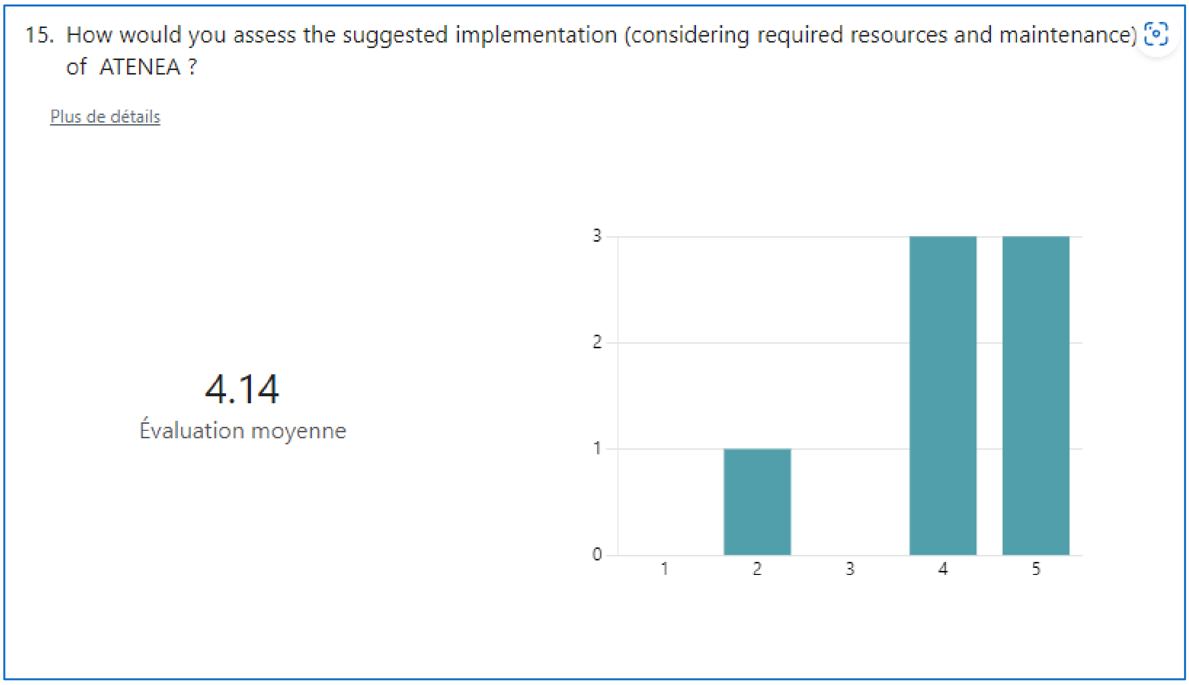


14. How would you assess the potential impact (coverage, scope, effectiveness) of ATENEA ?

Plus de détails

4.29
Évaluation moyenne

Figure 30 ATENEA's potential impact assessment

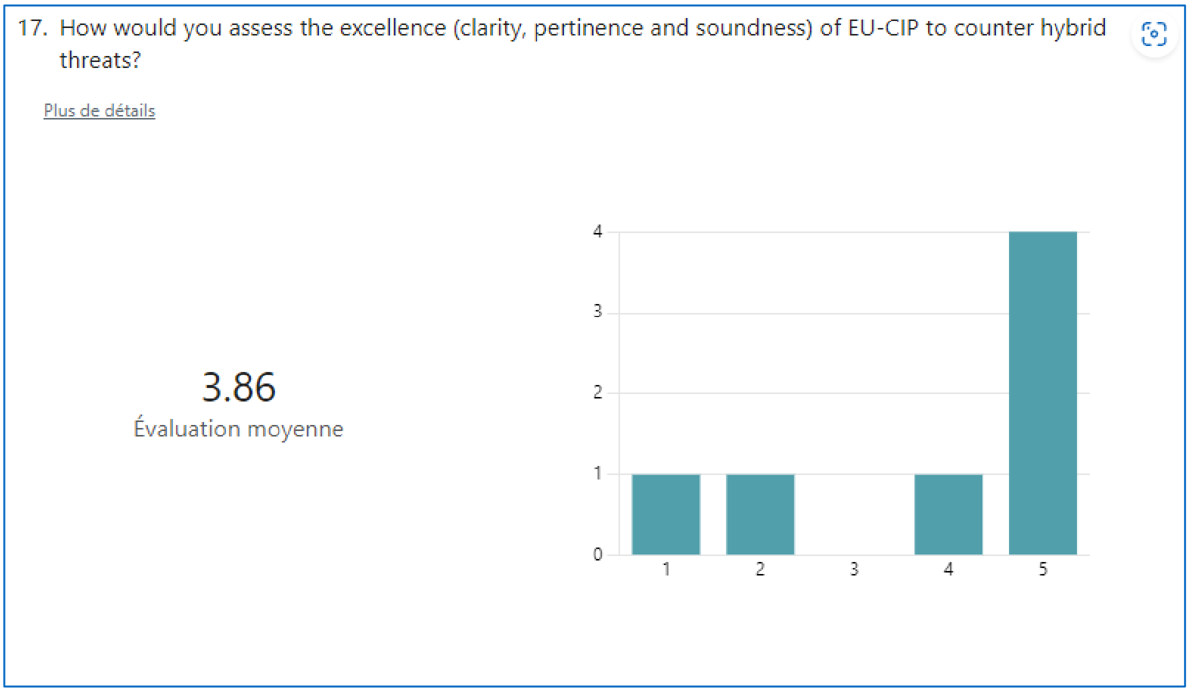


15. How would you assess the suggested implementation (considering required resources and maintenance) of ATENEA ?

Plus de détails

4.14
Évaluation moyenne

Figure 31 ATENEA's implementation assessment

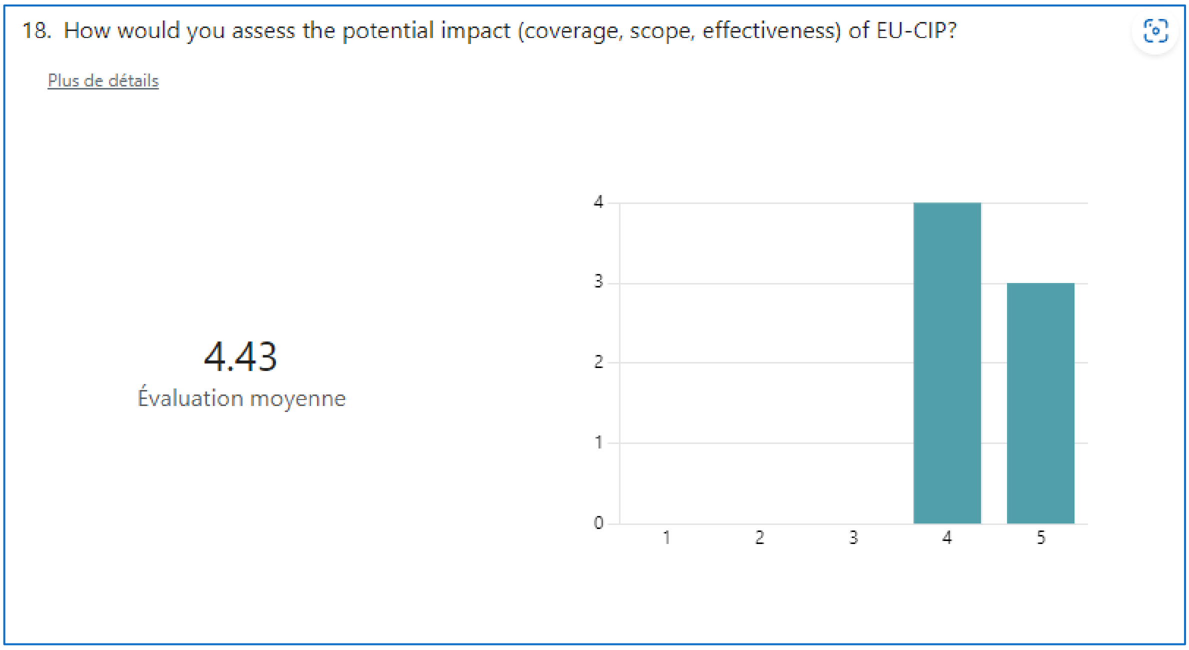


17. How would you assess the excellence (clarity, pertinence and soundness) of EU-CIP to counter hybrid threats?

Plus de détails

3.86
Évaluation moyenne

Figure 32 EU-CIP's excellence assessment

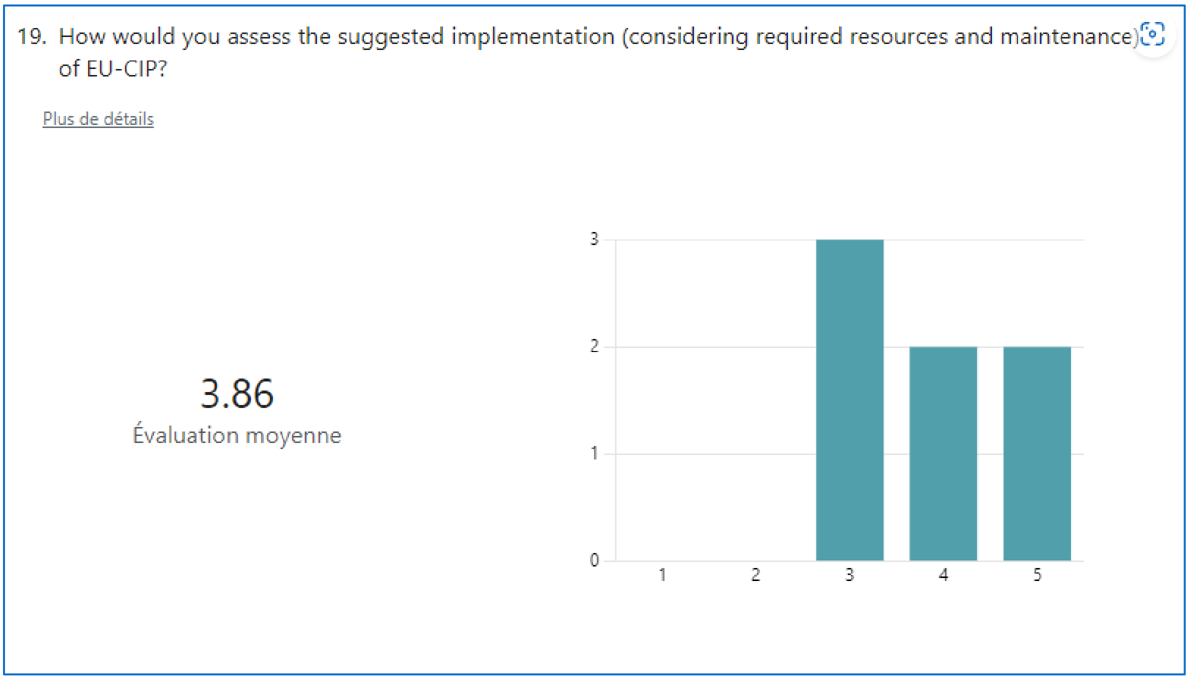


18. How would you assess the potential impact (coverage, scope, effectiveness) of EU-CIP?

Plus de détails

4.43
Évaluation moyenne

Figure 33 EU-CIP's potential impact assessment



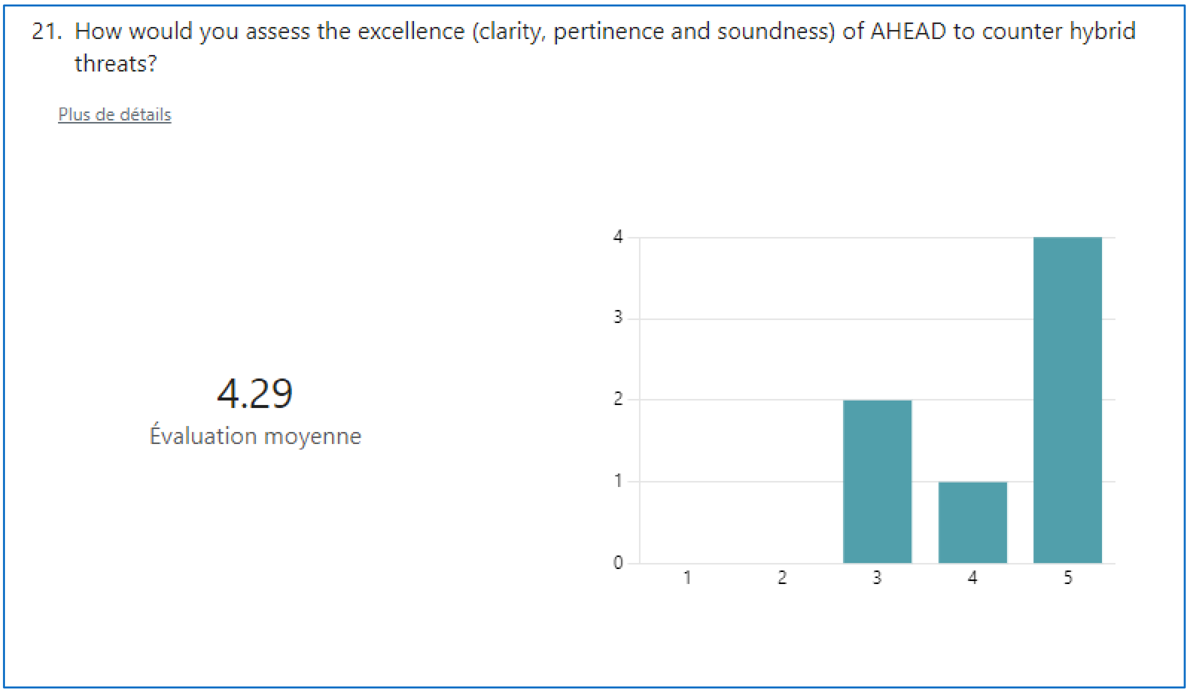
19. How would you assess the suggested implementation (considering required resources and maintenance) of EU-CIP?

Plus de détails

3.86

Évaluation moyenne

Figure 34 EU-CIP's implementation assessment



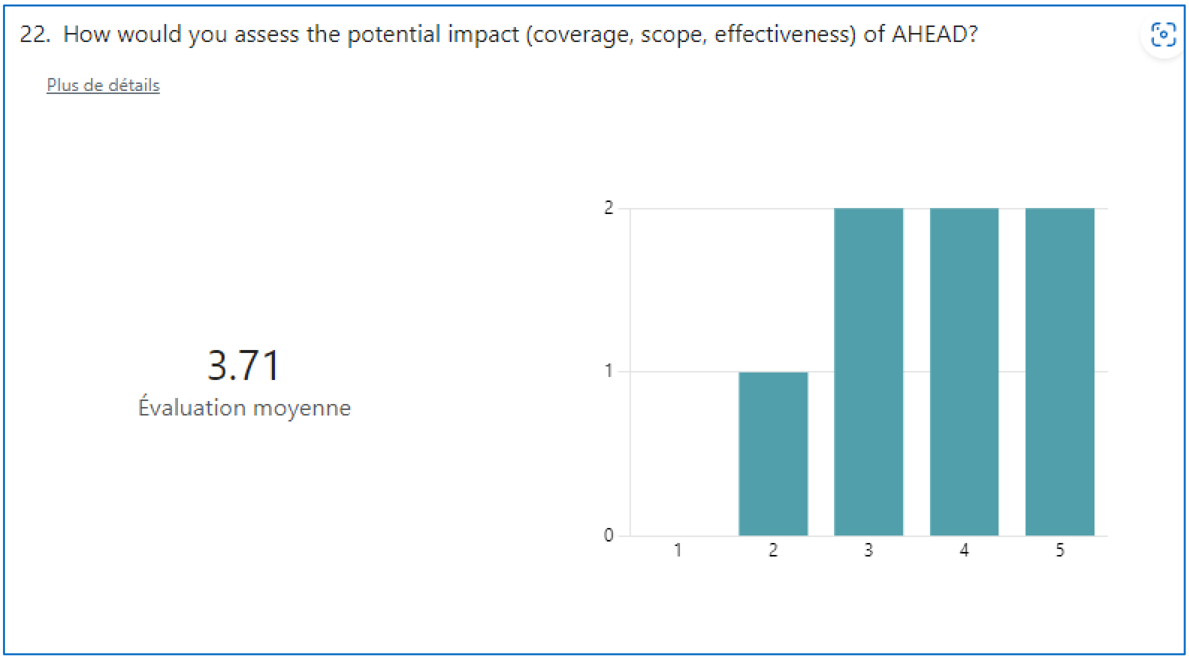
21. How would you assess the excellence (clarity, pertinence and soundness) of AHEAD to counter hybrid threats?

Plus de détails

4.29

Évaluation moyenne

Figure 35 AHEAD's excellence assessment



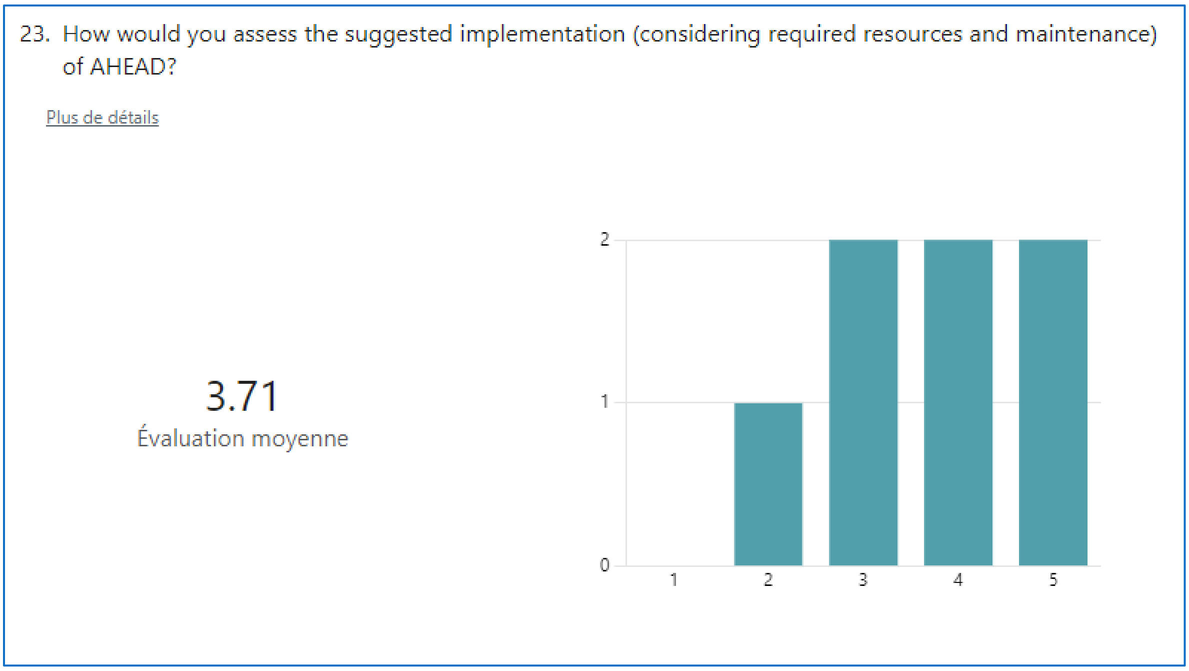
22. How would you assess the potential impact (coverage, scope, effectiveness) of AHEAD?

Plus de détails

3.71

Évaluation moyenne

Figure 36 AHEAD's potential impact assessment



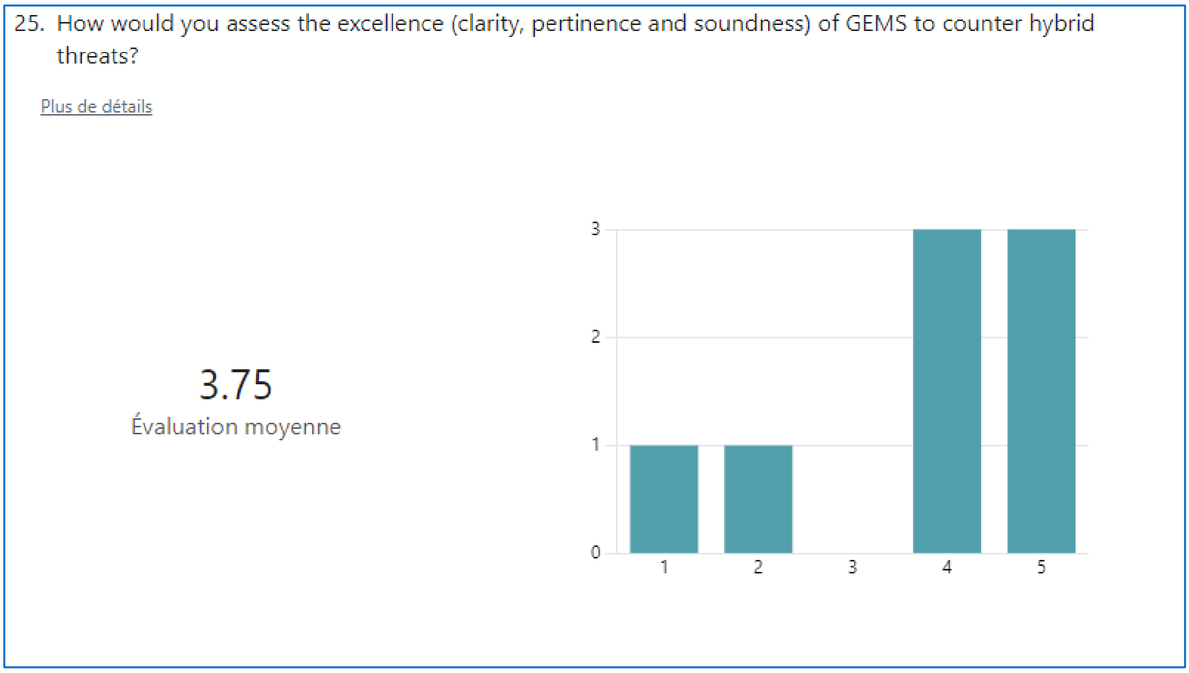
23. How would you assess the suggested implementation (considering required resources and maintenance) of AHEAD?

Plus de détails

3.71

Évaluation moyenne

Figure 37 AHEAD's implementation assessment

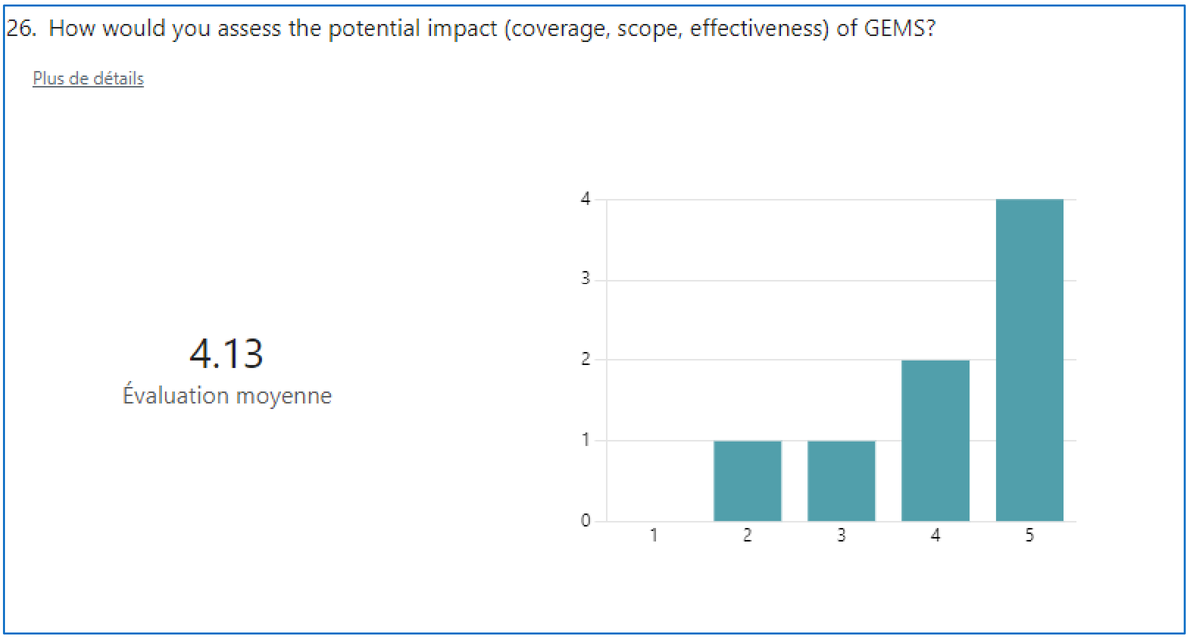


25. How would you assess the excellence (clarity, pertinence and soundness) of GEMS to counter hybrid threats?

Plus de détails

3.75
Évaluation moyenne

Figure 38 GEMS excellence assessment

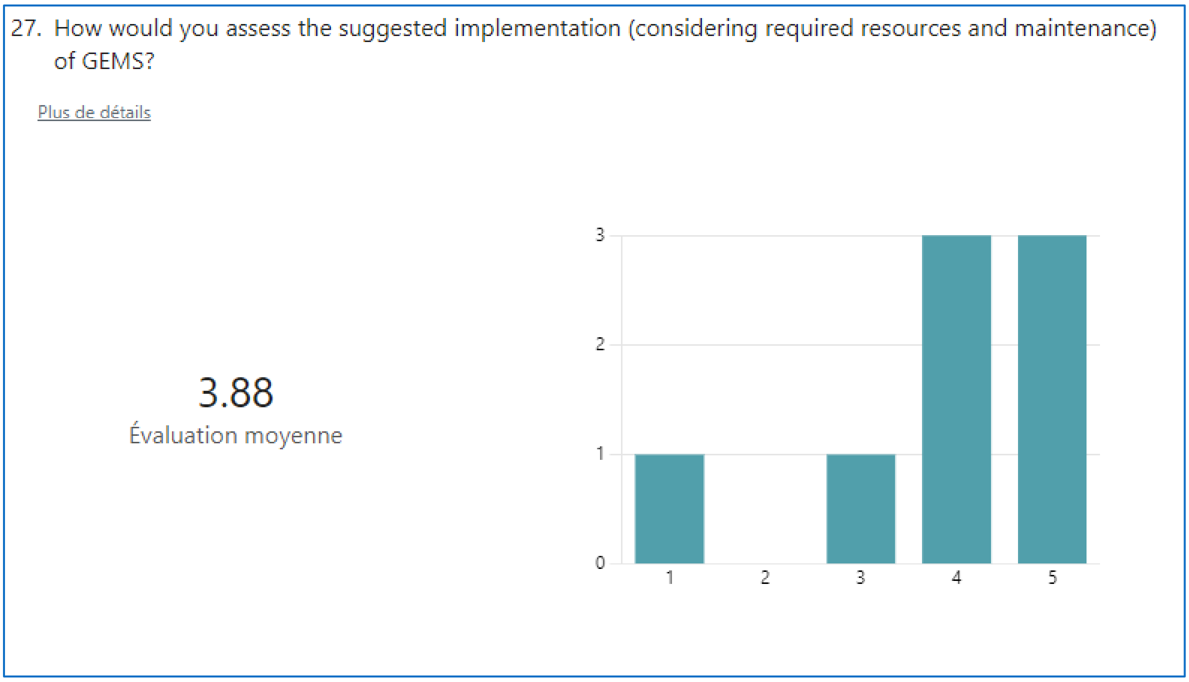


26. How would you assess the potential impact (coverage, scope, effectiveness) of GEMS?

Plus de détails

4.13
Évaluation moyenne

Figure 39 GEMS potential impact assessment



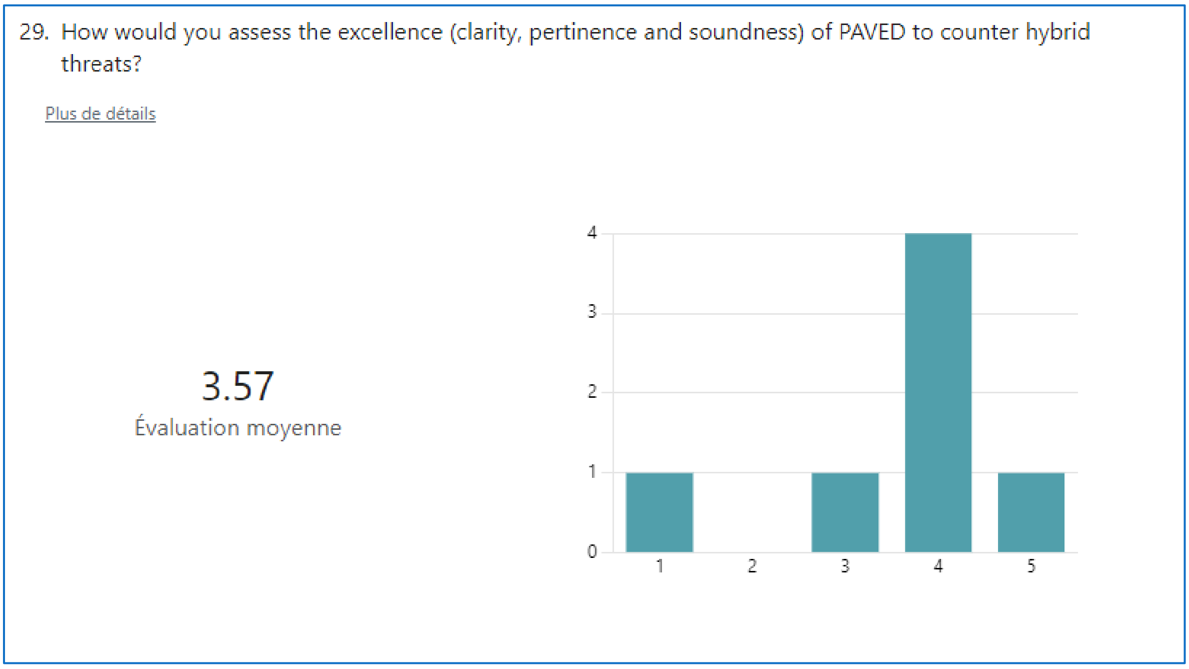
27. How would you assess the suggested implementation (considering required resources and maintenance) of GEMS?

Plus de détails

3.88

Évaluation moyenne

Figure 40 GEMS implementation assessment



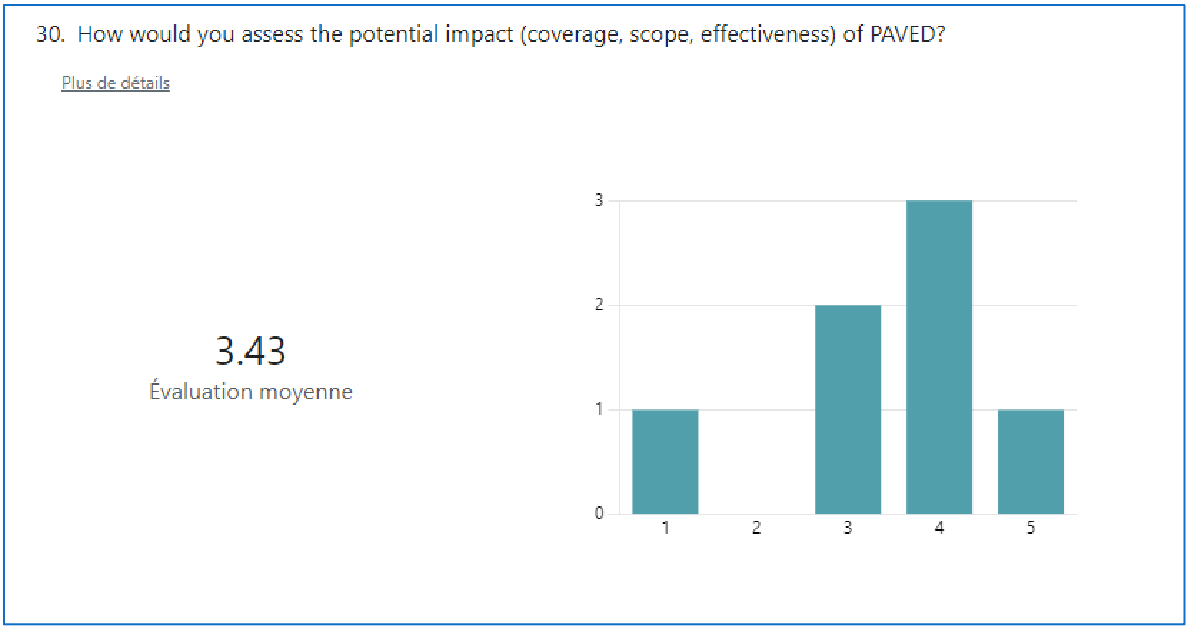
29. How would you assess the excellence (clarity, pertinence and soundness) of PAVED to counter hybrid threats?

Plus de détails

3.57

Évaluation moyenne

Figure 41 PAVED's excellence assessment

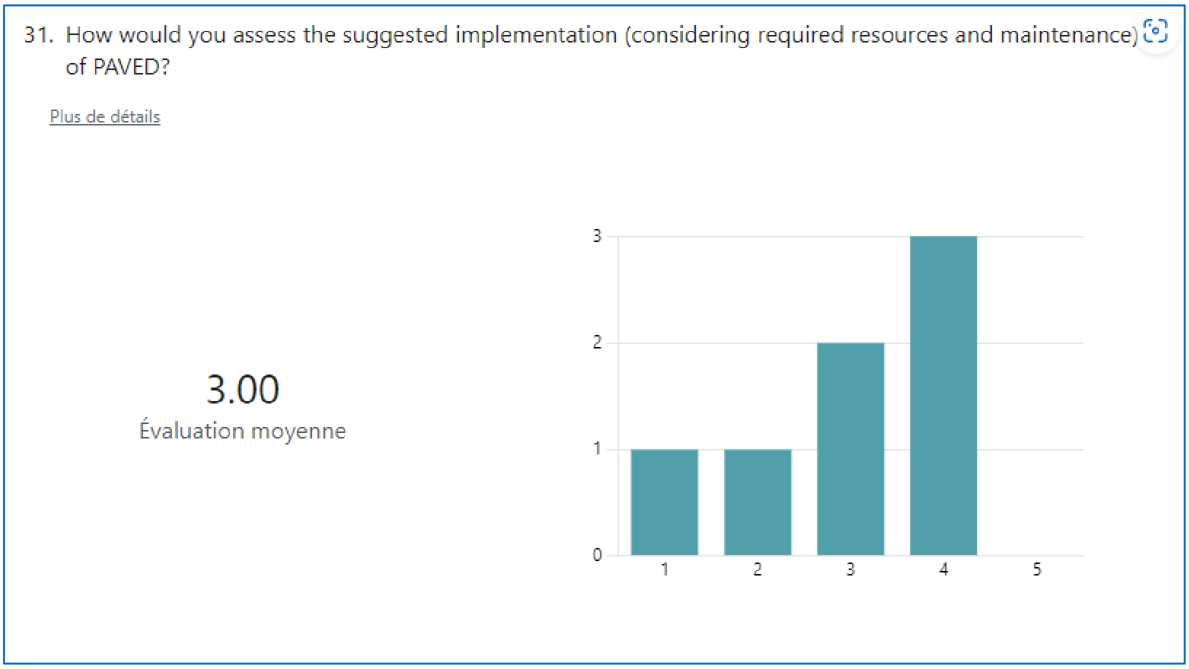


30. How would you assess the potential impact (coverage, scope, effectiveness) of PAVED?

Plus de détails

3.43
Évaluation moyenne

Figure 42 PAVED's potential impact assessment



31. How would you assess the suggested implementation (considering required resources and maintenance) of PAVED?

Plus de détails

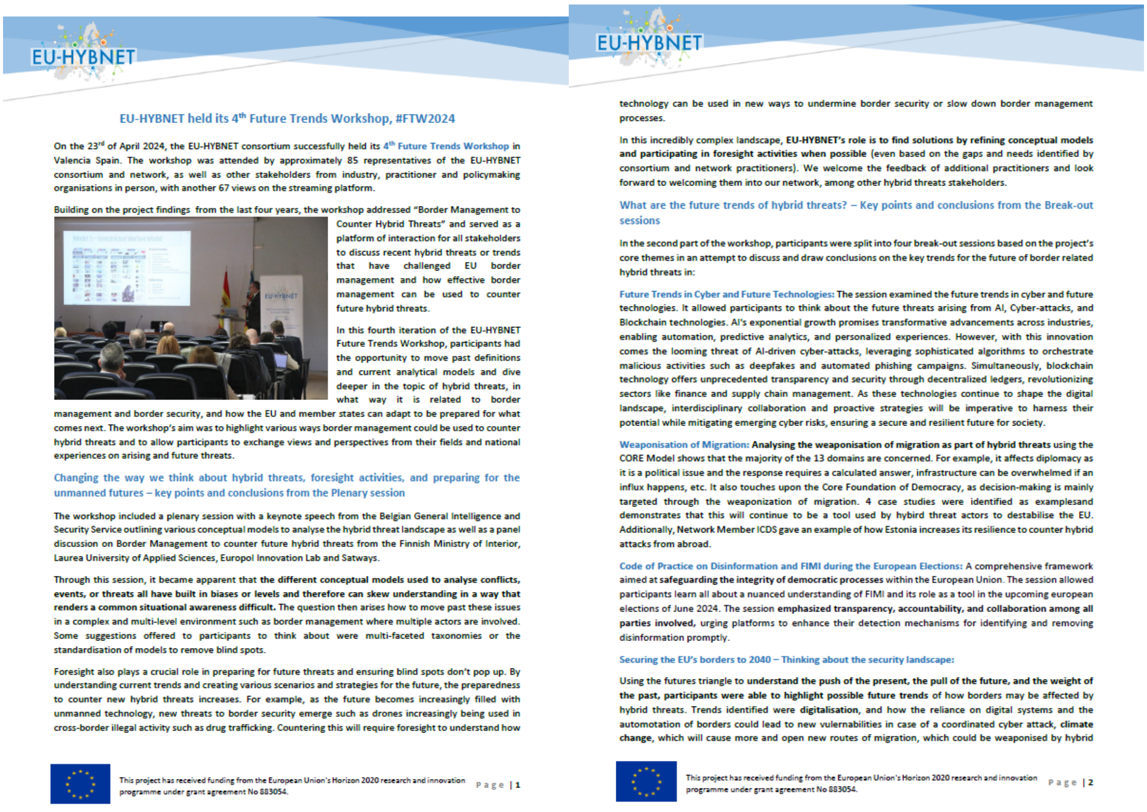
3.00
Évaluation moyenne

Figure 43 PAVED's implementation assessment

ANNEX VII. DISSEMINATION MATERIALS, WELCOME PACKAGE

EU-HYBNET
4th Annual Workshop
&
4th Future Trends Workshop
Save the Date!
23rd & 24th April 2024
Valencia Local Police HQ, Spain
www.euhybnet.eu
@EuHybnet
EU-HYBNET
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054.

Figure 44 AW Invitation



EU-HYBNET held its 4th Future Trends Workshop, #FTW2024

On the 23rd of April 2024, the EU-HYBNET consortium successfully held its 4th Future Trends Workshop in Valencia Spain. The workshop was attended by approximately 85 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations in person, with another 67 views on the streaming platform.

Building on the project findings from the last four years, the workshop addressed "Border Management to Counter Hybrid Threats" and served as a platform of interaction for all stakeholders to discuss recent hybrid threats or trends that have challenged EU border management and how effective border management can be used to counter future hybrid threats.

In this fourth iteration of the EU-HYBNET Future Trends Workshop, participants had the opportunity to move past definitions and current analytical models and dive deeper in the topic of hybrid threats, in what way it is related to border management and border security, and how the EU and member states can adapt to be prepared for what comes next. The workshop's aim was to highlight various ways border management could be used to counter hybrid threats and to allow participants to exchange views and perspectives from their fields and national experiences on arising and future threats.

Changing the way we think about hybrid threats, foresight activities, and preparing for the unmanned futures – key points and conclusions from the Plenary session

The workshop included a plenary session with a keynote speech from the Belgian General Intelligence and Security Service outlining various conceptual models to analyse the hybrid threat landscape as well as a panel discussion on Border Management to counter future hybrid threats from the Finnish Ministry of Interior, Laurea University of Applied Sciences, Europol Innovation Lab and Satways.

Through this session, it became apparent that **the different conceptual models used to analyse conflicts, events, or threats all have built in biases or levels and therefore can skew understanding in a way that renders a common situational awareness difficult.** The question then arises how to move past these issues in a complex and multi-level environment such as border management where multiple actors are involved. Some suggestions offered to participants to think about were multi-faceted taxonomies or the standardisation of models to remove blind spots.

Foresight also plays a crucial role in preparing for future threats and ensuring blind spots don't pop up. By understanding current trends and creating various scenarios and strategies for the future, the preparedness to counter new hybrid threats increases. For example, as the future becomes increasingly filled with unmanned technology, new threats to border security emerge such as drones increasingly being used in cross-border illegal activity such as drug trafficking. Countering this will require foresight to understand how technology can be used in new ways to undermine border security or slow down border management processes.

In this incredibly complex landscape, **EU-HYBNET's role is to find solutions by refining conceptual models and participating in foresight activities when possible** (even based on the gaps and needs identified by consortium and network practitioners). We welcome the feedback of additional practitioners and look forward to welcoming them into our network, among other hybrid threats stakeholders.

What are the future trends of hybrid threats? – Key points and conclusions from the Break-out sessions

In the second part of the workshop, participants were split into four break-out sessions based on the project's core themes in an attempt to discuss and draw conclusions on the key trends for the future of border related hybrid threats in:

Future Trends in Cyber and Future Technologies: The session examined the future trends in cyber and future technologies. It allowed participants to think about the future threats arising from AI, Cyber-attacks, and Blockchain technologies. AI's exponential growth promises transformative advancements across industries, enabling automation, predictive analytics, and personalized experiences. However, with this innovation comes the looming threat of AI-driven cyber-attacks, leveraging sophisticated algorithms to orchestrate malicious activities such as deepfakes and automated phishing campaigns. Simultaneously, blockchain technology offers unprecedented transparency and security through decentralized ledgers, revolutionizing sectors like finance and supply chain management. As these technologies continue to shape the digital landscape, interdisciplinary collaboration and proactive strategies will be imperative to harness their potential while mitigating emerging cyber risks, ensuring a secure and resilient future for society.

Weaponisation of Migration: **Analysing the weaponisation of migration as part of hybrid threats** using the CORE Model shows that the majority of the 13 domains are concerned. For example, it affects diplomacy as it is a political issue and the response requires a calculated answer, infrastructure can be overwhelmed if an influx happens, etc. It also touches upon the Core Foundation of Democracy, as decision-making is mainly targeted through the weaponization of migration. 4 case studies were identified as examplesand demonstrates that this will continue to be a tool used by hybird threat actors to destabilise the EU. Additionally, Network Member ICDS gave an example of how Estonia increases its resilience to counter hybrid attacks from abroad.

Code of Practice on Disinformation and FIMI during the European Elections: A comprehensive framework aimed at **safeguarding the integrity of democratic processes** within the European Union. The session allowed participants learn all about a nuanced understanding of FIMI and its role as a tool in the upcoming european elections of June 2024. The session **emphasized transparency, accountability, and collaboration among all parties involved**, urging platforms to enhance their detection mechanisms for identifying and removing disinformation promptly.

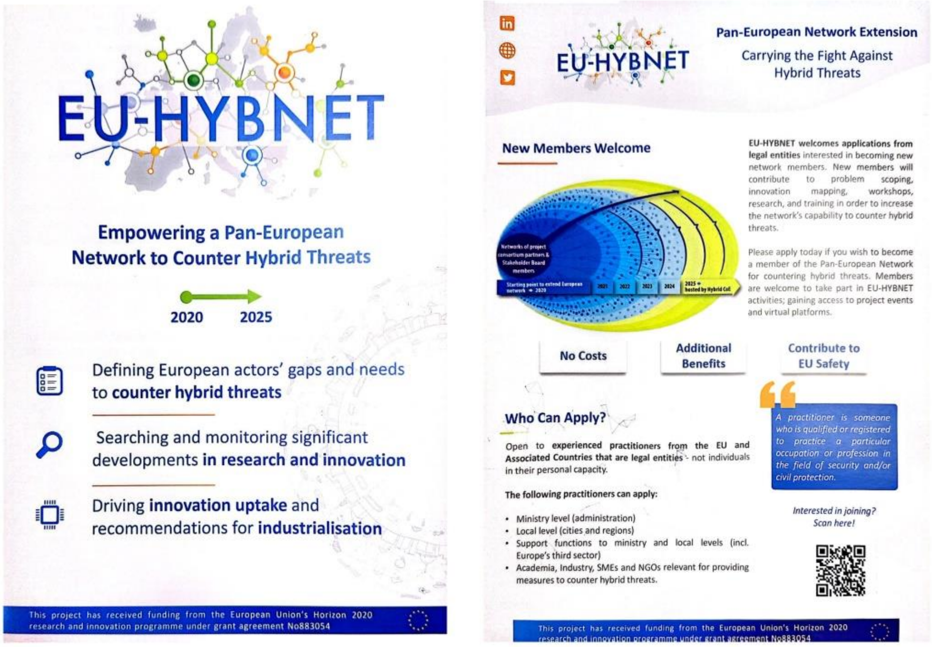
Securing the EU's borders to 2040 – Thinking about the security landscape:

Using the futures triangle to **understand the push of the present, the pull of the future, and the weight of the past, participants were able to highlight possible future trends** of how borders may be affected by hybrid threats. Trends identified were **digitalisation**, and how the reliance on digital systems and the automotation of borders could lead to new vulernabilities in case of a coordinated cyber attack, **climate change**, which will cause more and open new routes of migration, which could be weaponised by hybrid

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054. Page | 1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054. Page | 2

Figure 45 Press release



EU-HYBNET

Empowering a Pan-European Network to Counter Hybrid Threats

2020 2025

Defining European actors' gaps and needs to **counter hybrid threats**

Searching and monitoring significant developments **in research and innovation**

Driving **innovation uptake** and recommendations for **industrialisation**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

EU-HYBNET

Pan-European Network Extension

Carrying the Fight Against Hybrid Threats

New Members Welcome

Networks of project consortium partners & Stakeholder Board members
Starting point to extend European network → 2020
2021
2022
2023
2024
2025 → hosted by Hybrid CoE

EU-HYBNET welcomes applications from legal entities interested in becoming new network members. New members will contribute to problem scoping, innovation mapping, workshops, research, and training in order to increase the network's capability to counter hybrid threats.

Please apply today if you wish to become a member of the Pan-European Network for countering hybrid threats. Members are welcome to take part in EU-HYBNET activities; gaining access to project events and virtual platforms.

No Costs

Additional Benefits

Contribute to EU Safety

Who Can Apply?

Open to **experienced practitioners** from the EU and **Associated Countries that are legal entities** - not individuals in their personal capacity.

The following practitioners can apply:

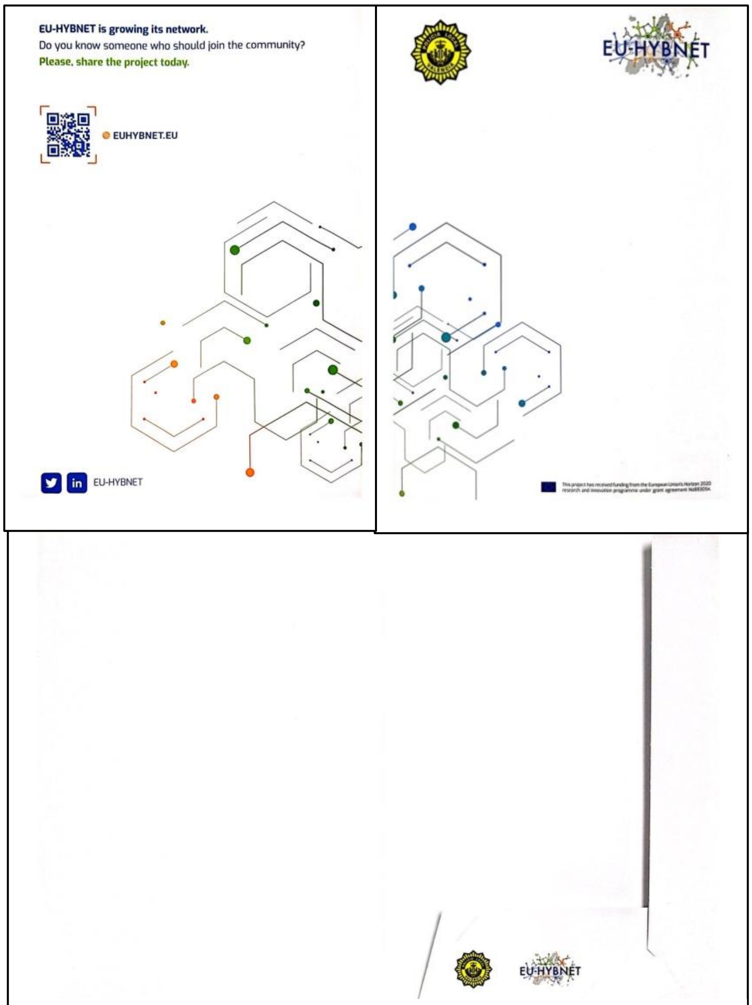
- Ministry level (administration)
- Local level (cities and regions)
- Support functions to ministry and local levels (incl. Europe's third sector)
- Academia, Industry, SMEs and NGOs relevant for providing measures to counter hybrid threats.

A practitioner is someone who is qualified or registered to practice a particular occupation or profession in the field of security and/or civil protection.

Interested in joining? Scan here!

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Figure 47 EU-HYBNET leaflets



EU-HYBNET is growing its network.

Do you know someone who should join the community?

Please, share the project today.

EUHYBNET.EU

EU-HYBNET

Figure 46 EU-HYBNET folder

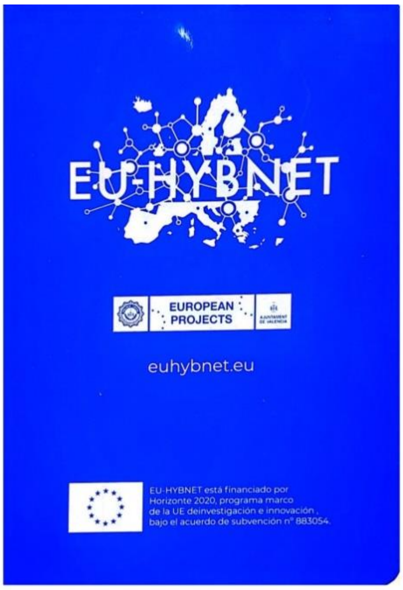

EU-HYBNET
EUROPEAN PROJECTS
euhybnet.eu
EU-HYBNET está financiado por Horizonte 2020, programa marco de la UE deinvestigación e innovación, bajo el acuerdo de subvención nº 883054.

Figure 48 EU-HYBNET notebook

EU-HYBNET
EU-HYBNET está financiado por Horizonte 2020, programa marco de la UE deinvestigación e innovación, bajo el acuerdo de subvención nº 883054.
euhybnet.eu

Figure 49 EU-HYBNET bag

Figure 50 EU-HYBNET pen

Figure 51 EU-HYBNET USB sticks