EU-HYBNET

2° ECSCI Workshop

Empowering a Pan-European
Network to Counter Hybrid-Threats

Innovations to counter hybrid threats

Dr Souzanna Sofou, SATWAYS Ltd

Okke Lucassen, Rick Meessen, TNO

Rimantas Zylius, Evaldas Bružė, L3CE

28/04/2022

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

Work Package 3 –Surveys to Technology, Research and Innovations

Objective: *WP3 aims in monitoring and selecting innovative solutions that can be utilised to counter hybrid threats, based on the priorities identified for the latter in WP2 (presentation by Hybrid CoE in AW2022). Also, WP3 aims in mapping current and future needs for innovations across the different operational areas, focusing on practitioners and relevant actors. A thorough assessment of the results is carried out, and events are also arranged to interact with providers of innovations (of technical and non technical nature).*

Milestones: For the priorities identified in each project cycle, WP3 should create a taxonomy and identify innovations and research projects to counter hybrid threats. Assessment of the results and communication of the main outputs via the Innovation Arena and the annual Innovation and Knowledge Exchange Events.

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

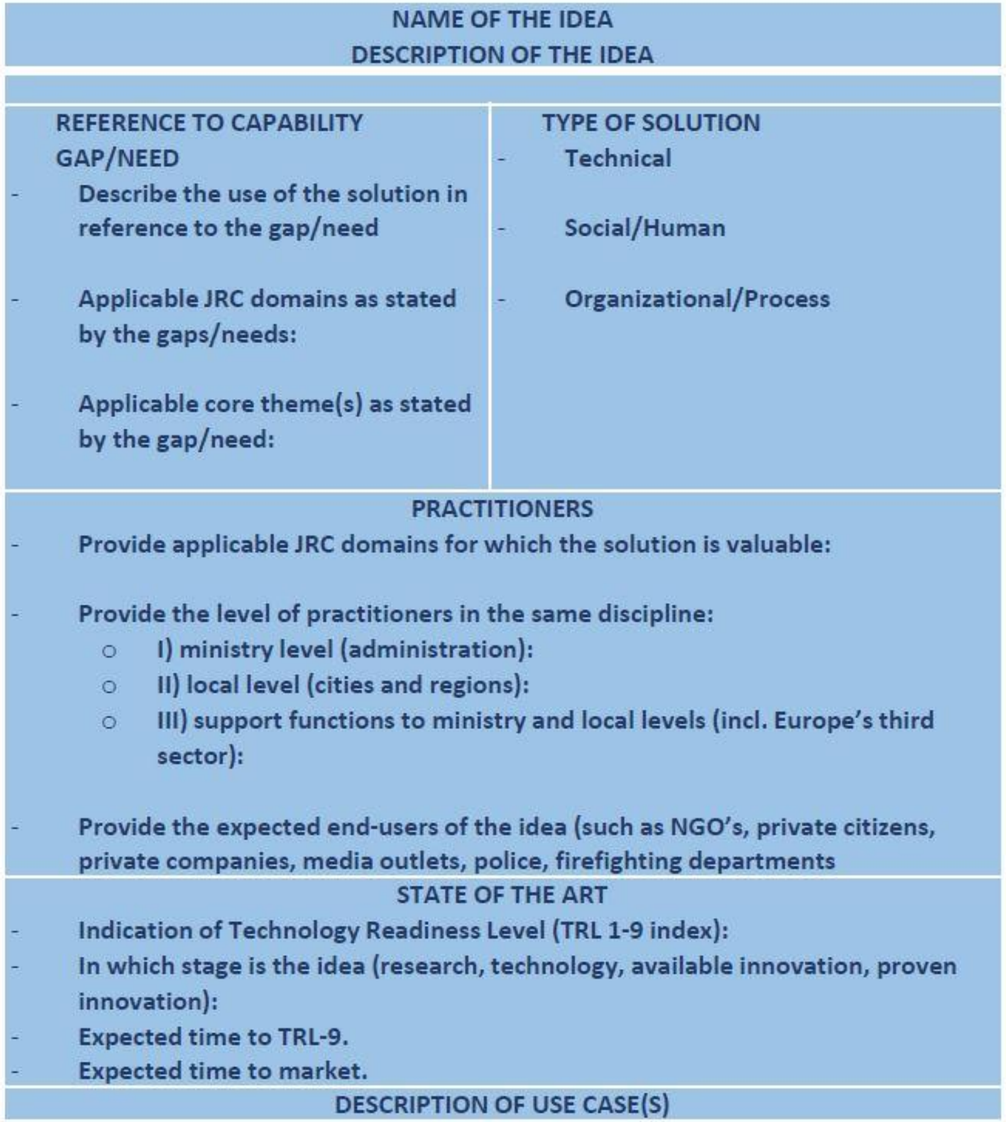
Work Package 3 - Contents

WP3 – Surveys to Technology, Research and Innovations

Task 3.1 Definition of Target Areas for Improvement and Innovations	**Task 3.2 Technology and Innovations Watch**
• Main objective: Defining Target Areas for Improvement • Template for describing innovations, enabling an initial assessment. • Mapping and assessment methodology, based on Excellence, Impact and Implementation. • T3.2 innovations integrated in the Innovation Arena.	• Main Objective: Map and Identify existing Innovations for countering hybrid threats • 23 innovations and ideas have been identified. • Innovations have been identified for and mapped to each of the 4 Core Themes of Hybrid Threats, and to each of the three Primary Contexts of each Core Theme.
Task 3.3 Ongoing Research Projects Initiative Watch	**Task 3.4 Innovation and Knowledge Exchange Events**
• Main objective: Research Projects Monitoring, surveys • Scanning analyzed the scientific research landscape for the gaps and needs identified by practitioners in the hybrid threats field. • Deeper Understanding of the current state of research and its outcomes with respect to filling identified gaps.	• Main objective: Annual Events for information exchange • More than 100 participants registered for the First Innovation Knowledge and Exchange Workshop. • The Future Trend Workshop attracted several stakeholders. • The second IKEW is being planned for June 14th and planning is well underway.

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

Work Package 3 Main Results-Template for presenting Innovations (T3.1)



NAME OF THE IDEA

DESCRIPTION OF THE IDEA

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- Describe the use of the solution in reference to the gap/need - Applicable JRC domains as stated by the gaps/needs: - Applicable core theme(s) as stated by the gap/need:	- Technical - Social/Human - Organizational/Process

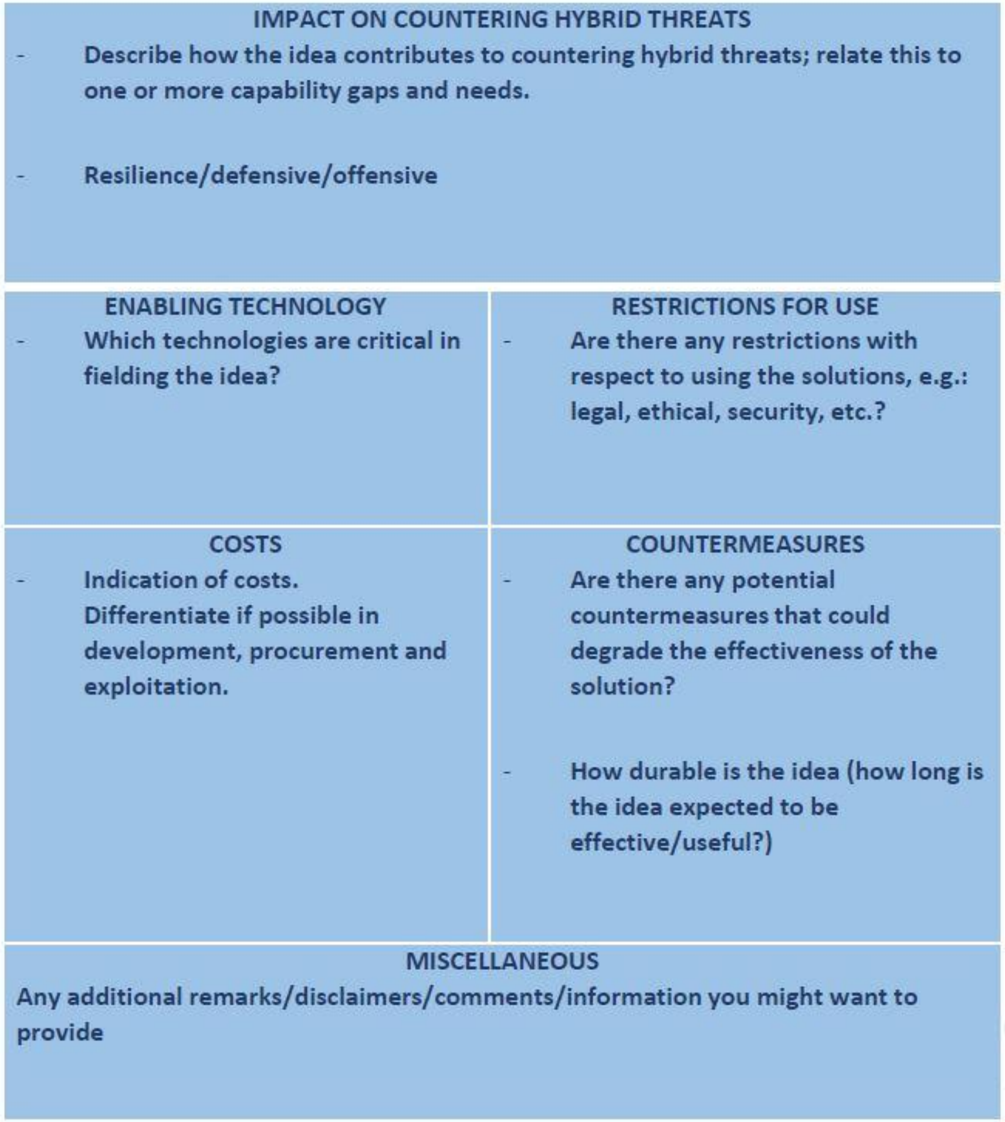
PRACTITIONERS

- Provide applicable JRC domains for which the solution is valuable:
- Provide the level of practitioners in the same discipline:
  - I) ministry level (administration):
  - II) local level (cities and regions):
  - III) support functions to ministry and local levels (incl. Europe's third sector):
- Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments

STATE OF THE ART

- Indication of Technology Readiness Level (TRL 1-9 index):
- In which stage is the idea (research, technology, available innovation, proven innovation):
- Expected time to TRL-9.
- Expected time to market.

DESCRIPTION OF USE CASE(S)



IMPACT ON COUNTERING HYBRID THREATS

- Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
- Resilience/defensive/offensive

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- Which technologies are critical in fielding the idea?	- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?

COSTS	COUNTERMEASURES
- Indication of costs. Differentiate if possible in development, procurement and exploitation.	- Are there any potential countermeasures that could degrade the effectiveness of the solution? - How durable is the idea (how long is the idea expected to be effective/useful?)

MISCELLANEOUS

Any additional remarks/disclaimers/comments/information you might want to provide

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

Work Package 3 Main Results- 23 Innovations mapped to Core Themes (T3.2)

CORE THEME	PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED
1. FUTURE TRENDS OF HYBRID THREATS	1.1 Trend: Official strategic communication losing power	Guides to identify fakes
		Hybrid online dilemma game
	1.2 Trend: Big data as a new power source	Countering disinformation with strategic personalized advertising
		Automated detection of hate speech in social media
	1.3 Trend: increasing strategic dependency of critical services	A blockchain-based real-time information management and monitoring system
		A crawler and real-time search engine for investors
2. CYBER AND FUTURE TECHNOLOGIES	2.1 GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY	Open European Quantum Key Distribution Testbed (OPENQKD project)
		Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module
	2.2 HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER	Efficient cyber threat information sharing through Hyper Connectivity networks
		Cross sector cyber threat information sharing
		Public-private information-sharing groups developing collaborative investigations and collective action
	2.3 THE INDIVIDUAL AS A DIGITAL ENTITY	Fake news exposer
		Factcheckers communities
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1 DISTRUST AND STRESS IN POLITICAL DECISION-MAKING	Resilient democracy infrastructure platform
	3.2 RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS	Early or Rapid Damage Assessment System
		Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination
	3.3 GLOBALIZATION VS. LOCALISATION	Tool that monitors and detects the population's response to the information being published and is able to identify the dominant emotion occurring in social networks
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1 GOING VIRAL	Journalism trust initiative
		Debunking of Fake News
		Non-partisan native-language news channels for most interdependent abroad regions
	4.2 DIGITAL MONOPOLIES AND MASSIFICATION OF DATA	Fair Trade Data Program
	4.3 DETERIORATION OF THE QUALITY OF CONTENT	Training application for media literacy
		Automated fact-checker

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

Assessment methodology (T3.1) RISE + ZITiS + TNO

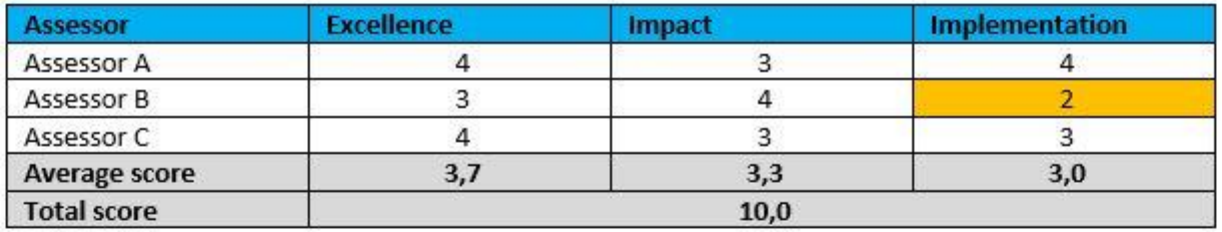
Criteria:

- Excellence: description, scope, credibility
- Impact: coverage, acceptance, effectiveness, robustness
- Implementation: effort, TimeToMarket, preconditions

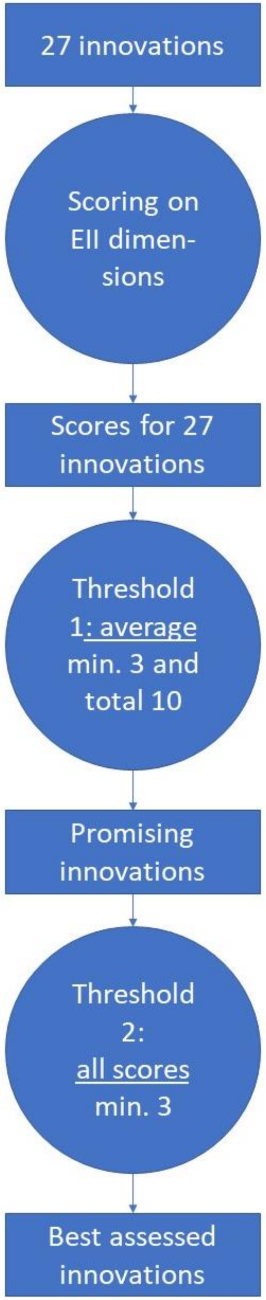
Scoring:

- Scores 0-5, using a score card
- Each innovation assesed by 3-4 consortium partners (after initial review and complementing)
- Primary and secondary thresholds

Table 2: Example of additional requirements for passing secondary threshold



Assessor	Excellence	Impact	Implementation
Assessor A	4	3	4
Assessor B	3	4	2
Assessor C	4	3	3
Average score	**3,7**	**3,3**	**3,0**
Total score	**10,0**		



27 innovations
Scoring on EII dimen-sions
Scores for 27 innovations
Threshold 1: average min. 3 and total 10
Promising innovations
Threshold 2: all scores min. 3
Best assessed innovations

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

Work Package 3 Main Results- Assessment Results (T3.1)

CORE THEME	PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED	ASSESSMENT
1.FUTURE TRENDS OF HYBRID THREATS	1.1 Trend: Official strategic communication losing power	Guides to identify fakes	🟩
		Hybrid online dilemma game	🟨
	1.2 Trend: Big data as a new power source	Countering disinformation with strategic personalized advertising	🟩
		Automated detection of hate speech in social media	🟨
	1.3 Trend: increasing strategic dependency of critical services	A blockchain-based real-time information management and monitoring system	🟧
		A crawler and real-time search engine for investors	🟧
2. CYBER AND FUTURE TECHNOLOGIES	2.1 GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY	Open European Quantum Key Distribution Testbed (OPENQKD project)	🟧
		Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module	🟨
	2.2 HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER	Efficient cyber threat information sharing through Hyper Connectivity networks	🟧
		Cross sector cyber threat information sharing	🟩
		Public-private information-sharing groups developing collaborative investigations and collective action	🟩
	2.3 THE INDIVIDUAL AS A DIGITAL ENTITY	Fake news exposer	🟩
		Factcheckers communities	🟨
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1 DISTRUST AND STRESS IN POLITICAL DECISION-MAKING	Resilient democracy infrastructure platform	🟧
	3.2 RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS	Early or Rapid Damage Assessment System	🟧
		Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination	🟧
	3.3 GLOBALIZATION VS. LOCALISATION	Tool that monitors and detects the population's response to the information being published and is able to identify the dominant emotion occurring in social networks	🟧
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1 GOING VIRAL	Journalism trust initiative	🟨
		Debunking of Fake News	🟩
		Non-partisan native-language news channels for most interdependent abroad regions	🟧
	4.2 DIGITAL MONOPOLIES AND MASSIFICATION OF DATA	Fair Trade Data Program	🟧
	4.3 DETERIORATION OF THE QUALITY OF CONTENT	Training application for media literacy	🟨
		Automated fact-checker	🟧

LEGEND: 🟩 UPTAKEN IN WP4 🟨 DEVELOPMENT RECOMMENDATIONS IN D3.1 🟧 KEEP IN INNOVATION ARENA

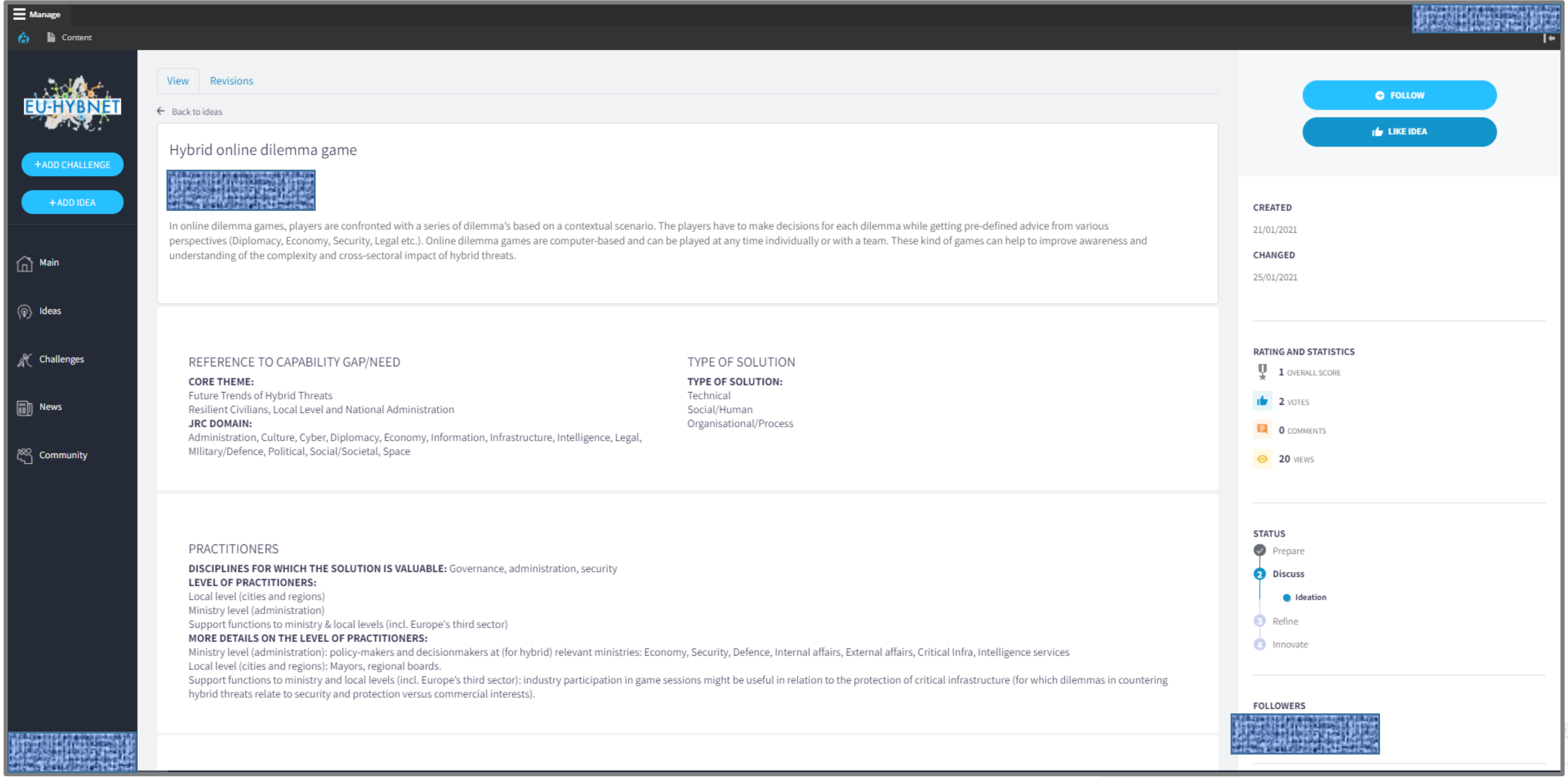
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

Work Package 3 Main Results- Discussion on first year findings

- The scanning analyzed the scientific research landscape for the gaps and needs identified by practitioners in the hybrid threats field.
- The relative report will hopefully contribute to a **deeper understanding** -of the hybrid threats community- regarding the **state of play of the research on the phenomena of interest**. A better understanding is also expected regarding the **outcomes that could be expected** from the scientific research field.
- The report also identified **areas, which apparently lack research of the phenomena**, which is deeply important for hybrid threats better understanding.
- Furthermore, scanning did identify some of the EU research and other projects, which would **contribute, if successful, in filling the identified gaps**.
- **Disinformation innovations were assessed relatively high**. It is estimated that the type of innovations that have been identified can be implemented **cost-effectively** (medium to low impact with fair costs).
- The work conducted so far has served to **identify solutions for different dimensions of hybrid threats**.
- It should be highlighted that **a hybrid threat is multidimensional, time dependent and part of a larger hybrid campaign that targets vulnerabilities, sometimes by occasion and opportunity**.
- Therefore, in order to produce one holistic solution, we should be able to detect and attribute hybrid threats timely across all domains in order to effectively respond.
- Teaching computers how to **respond to a multidimensional and time dependent situation is not yet easy to implement** as hybrid threat patterns are not ready to be described.
- In the future, **Artificial Intelligence tools and quantum technology could be used to help** identify and respond to such threats in a timely manner.
- Besides advanced technologies, **interdepartmental and international cooperation and alignment would be required**.
- For many innovations **implementation and exploitation problems** are foreseen. Most of the problems, leading to potential restrictions to use these innovations, refer to ethical, legal and public acceptance issues. In addition to defining and designing innovations that can mitigate hybrid threats, it is essential to consider these perspectives.

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

Work Package 3 Main Results- Innovations & Ideas integrated in the Innovation Arena



Manage

Content

[redacted]

View Revisions

← Back to ideas

Hybrid online dilemma game

[redacted]

In online dilemma games, players are confronted with a series of dilemma's based on a contextual scenario. The players have to make decisions for each dilemma while getting pre-defined advice from various perspectives (Diplomacy, Economy, Security, Legal etc.). Online dilemma games are computer-based and can be played at any time individually or with a team. These kind of games can help to improve awareness and understanding of the complexity and cross-sectoral impact of hybrid threats.

REFERENCE TO CAPABILITY GAP/NEED

CORE THEME:
Future Trends of Hybrid Threats
Resilient Civilians, Local Level and National Administration
JRC DOMAIN:
Administration, Culture, Cyber, Diplomacy, Economy, Information, Infrastructure, Intelligence, Legal, Military/Defence, Political, Social/Societal, Space

TYPE OF SOLUTION

TYPE OF SOLUTION:
Technical
Social/Human
Organisational/Process

PRACTITIONERS

DISCIPLINES FOR WHICH THE SOLUTION IS VALUABLE: Governance, administration, security
LEVEL OF PRACTITIONERS:
Local level (cities and regions)
Ministry level (administration)
Support functions to ministry & local levels (incl. Europe's third sector)
MORE DETAILS ON THE LEVEL OF PRACTITIONERS:
Ministry level (administration): policy-makers and decisionmakers at (for hybrid) relevant ministries: Economy, Security, Defence, Internal affairs, External affairs, Critical Infra, Intelligence services
Local level (cities and regions): Mayors, regional boards.
Support functions to ministry and local levels (incl. Europe's third sector): industry participation in game sessions might be useful in relation to the protection of critical infrastructure (for which dilemmas in countering hybrid threats relate to security and protection versus commercial interests).

CREATED
21/01/2021
CHANGED
25/01/2021

RATING AND STATISTICS
1 OVERALL SCORE
2 VOTES
0 COMMENTS
20 VIEWS

STATUS
Prepare
2 Discuss
Ideation
3 Refine
4 Innovate

FOLLOWERS
[redacted]

[redacted]

▨ Private information

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

WP 3 Current Challenges: Innovations mapped to Core Themes (T3.2 preliminary results)

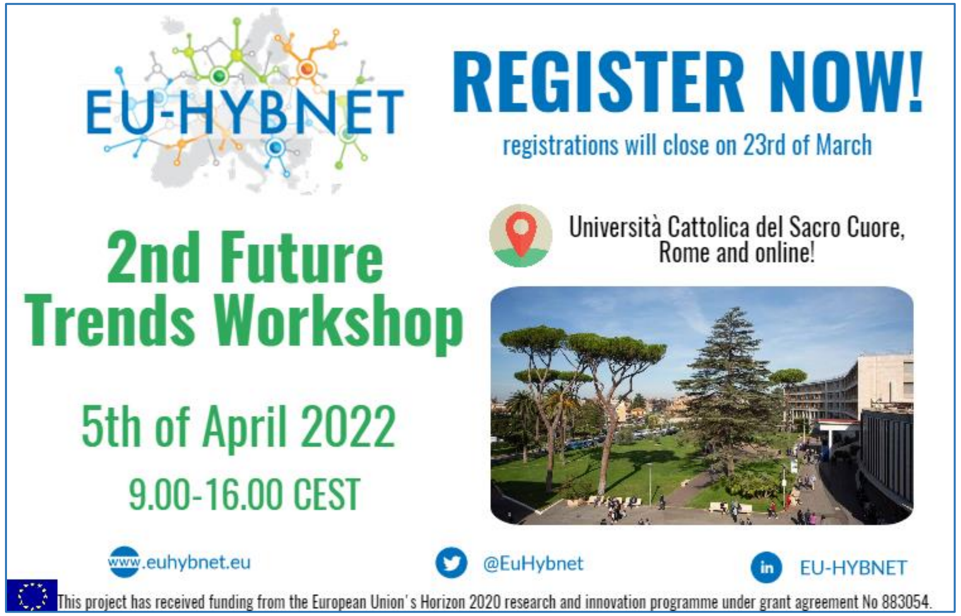
CORE THEME	PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED
1.FUTURE TRENDS OF HYBRID THREATS	Geopolitical heavyweight of domestic policy	DOMESTIC POLICY FORUMS
	Digital escalation and AI-based exploitation	Digital connected security in response to hybrid tactics
		Commitment to Validating and Verifying AI
	Rise of populism	Establishment and reinforcement of political education of democratic values
		Installation of rules for mandatory declarations
2. CYBER AND FUTURE TECHNOLOGIES	Space interference and counterspace weapons	7SHIELD : a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats
		ResilienceTool (incl. RiskRadar)
	Offensive cyber capabilities	The Development of a Proactive Defensive Framework based on ML and cloud
		A fully automated incident response solution based on CT Intelligence
	Disruptive innovation	The Development of a Deepfake Detection System
		Counter-Unmanned Aircraft Systems
3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	Exploitation of existing political cleavages	Detection of Disinformation Delivery Proxy Actors
	Exploitation of critical infrastructure weaknesses and economic dependencies	Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach
		PRECINCT: Resilience Methodological Framework for Cascading cyber-physical Threats on Multiple Critical Infrastructure Modes
	Exploitation or investment in companies by foreign actors	
4. INFORMATION AND STRATEGIC COMMUNICATIONS	Information manipulation with the aim of destabilization	Increasing capabilities to systematically assess information validity throughout the lifecycle
		Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications
		DDS-alpha
	Foreign interference in key information institutions	Integrated Monitoring System Against Malware-Based Cyber Operations
	Promoted ideological extremism and violence	Collection and sentiment analysis of targeted communication
		Identify and safeguarding vulnerable individuals

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

WP3 Main Results: Innovation & Knowledge Exchange Events (T3.4)

2nd Future Trends Workshop

- Hosted in Rome by the UCSC on April 5th, 2022
- Topic: Democracies on the Edge divided into three breakout sessions
  - Changing populism
  - Instrumentalization of social media networks
  - Constitution of International Groups
- The goal of the workshop was to address expected future manifestations of hybrid threats, and how current innovations and solutions may or may not apply in tomorrow's world



EU-HYBNET

REGISTER NOW!

registrations will close on 23rd of March

Università Cattolica del Sacro Cuore,
Rome and online!

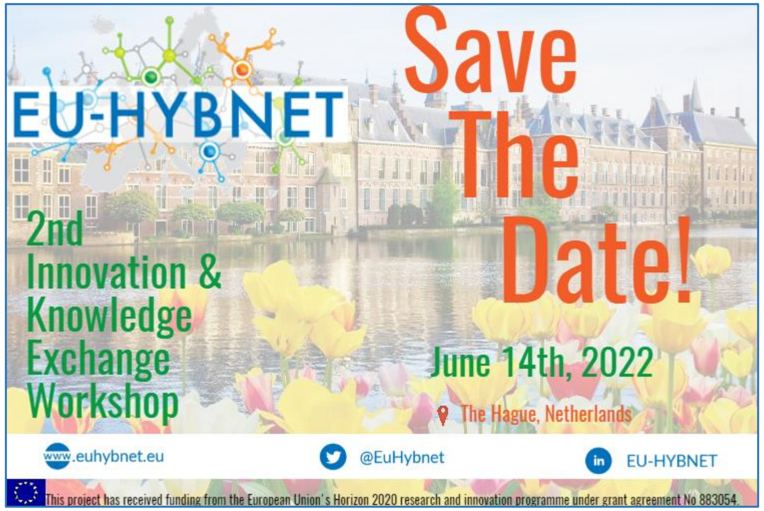
2nd Future Trends Workshop

5th of April 2022

9.00-16.00 CEST

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.



EU-HYBNET

Save The Date!

2nd Innovation & Knowledge Exchange Workshop

June 14th, 2022

The Hague, Netherlands

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.

2nd Innovation and Knowledge Exchange Workshop

- Hosted in the Hague by TNO on June 14th, 2022
- The goal of the workshop is to addresss the gaps that have been identified in the second cycle.
- Please join us for this event!

CONTIBUTORS AND PUBLISHED DELIVERABLES

Number	Task Name	Duration	Responsible	Contributors	STATUS
T3.1	Definition of Target Areas for Improvement and Innovations	M1-M57	**TNO**	RISE, MTES, USCS, HCoE, MoD, ZITiS, Laurea, KEMEA	ongoing
T3.2	Technology and Innovations Watch	M1-M58	**SATWAYS**	ICDS, KEMEA, L3CE, ZITiS, COMTESSA	ongoing
T3.3	Ongoing Research Projects Initiative Watch	M1-M58	**L3CE**	LAU, PPHS, RISE, KEMEA	ongoing
T3.4	Innovation and Knowledge Exchange Events	M4-M58	**EOS**	TNO, PLV, UCSC, MVNIA, HCoE, URJC, JRC, MoD, COMTESSA	ongoing

All WP3 deliverables have been accepted and can be found at the project CORDIS page provided by the European Commission: https://cordis.europa.eu/project/id/883054/results

Number	Deliverables	Completed	Responsible
D3.3	First Report on Improvement and Innovations	M7	Satways
D3.7	First Report on Innovation and Research Project Monitoring	M7	L3CE
D3.11	1st Innovation and Knowledge exchange events Report	M10	EOS
D3.14	1st Future Trends analysis Workshop Report	M13	Hybrid COE
D3.1	First Interim – Report mapped on gaps and needs	M16	TNO

The contents of this presentation reflect only the authors' view and the Research Executive Agency and the European Commission are not responsible for any use that may be made of the information it contains.

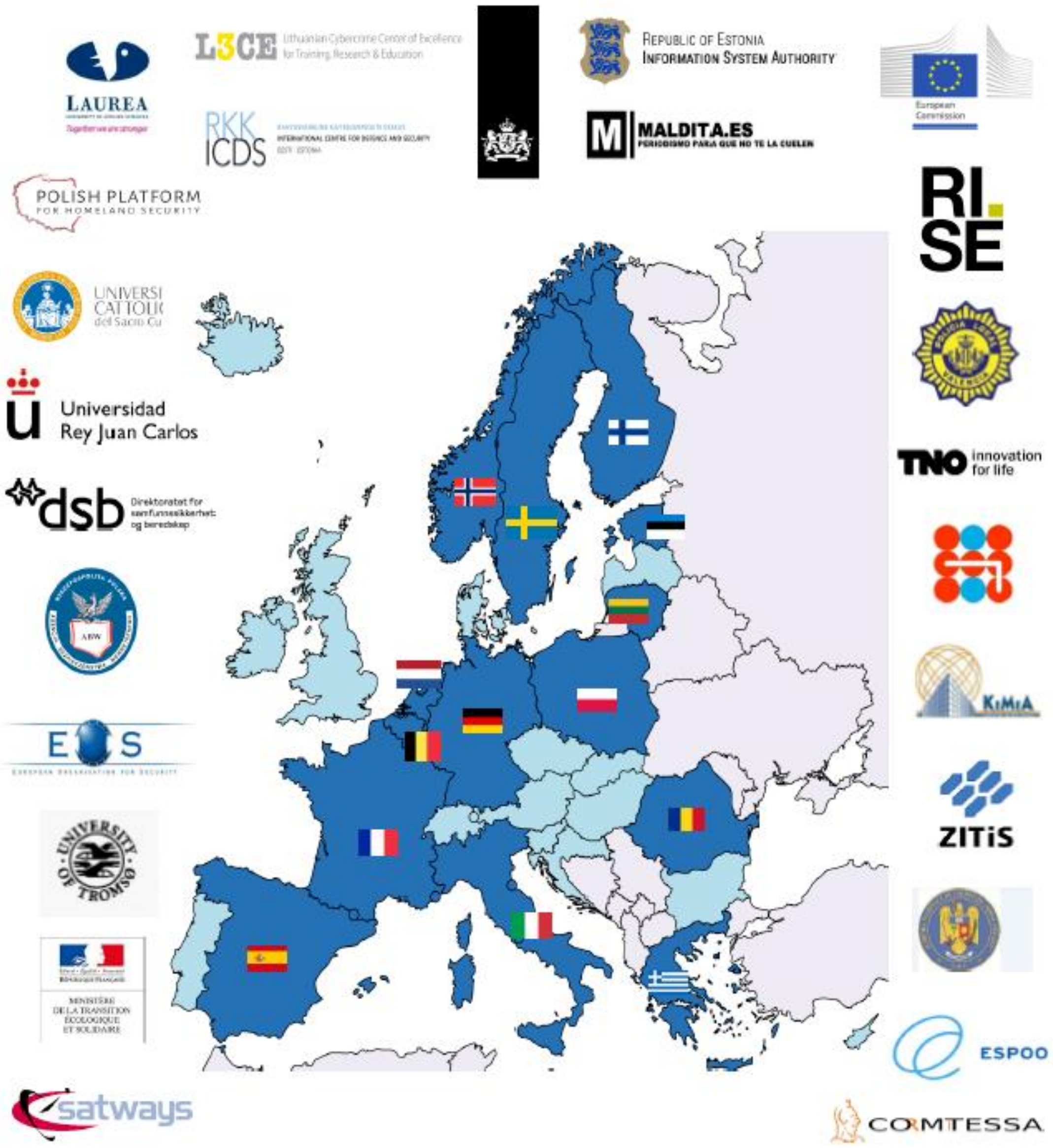
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054

THANK YOU!

Dr. Souzanna Sofou

Satways Ltd

s.sofou@satways.net


LAUREA
L3CE Lithuanian Cybercrime Center of Excellence for Training, Research & Education
RKK ICDS
Republic of Estonia Information System Authority
European Commission
MALDITA.ES
POLISH PLATFORM FOR HOMELAND SECURITY
RI.SE
Universidad Rey Juan Carlos
dsb Direktoratet for samfunnssikkerhet og beredskap
TNO innovation for life
EOS European Organisation for Security
KEMEA
ZITiS
University of Tromsø
Ministère de la Transition Écologique et Solidaire
ESPOO
satways
COMTESSA

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