EU-HYBNET

IDENTIFICATION OF TARGET AREAS FOR IMPROVEMENT AND INNOVATIONS

FIRST INTERIM REPORT MAPPED ON GAPS AND NEEDS

DELIVERABLE 3.1

Lead Author : TNO

Contributors: TNO, RISE, MTES, UCSC, HCoE, NL MoD, ZiTIS, Laurea/UTU, KEMEA

Deliverable classification: PUBLIC

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

D3.1 IDENTIFICATION OF TARGET AREAS FOR IMPROVEMENT AND INNOVATIONS: *FIRST INTERIM REPORT MAPPED ON GAPS AND NEEDS*

Deliverable number	3.1	
Version	V1.0	
Delivery date	Ultimately 31/08/2021 while submitted to EC already on 14/07/2021	
Dissemination level	Public	
Classification level	Public	
Status	Final	
Nature	Report	
Main authors	Rick Meessen, Okke Lucassen	TNO
Contributors	Rolf Blom	RISE
	Michael Meisinger	ZiTIS
	Maria Kampa	KEMEA
	Margriet Drent	NL MoD
	Päivi Mattila	Laurea
	Emma Lappalainen	HCOE
	Antoine-Tristan Mocilnikar, Geraldine Ducos	MTES
	Rachele Brancaleoni	UCSC

DOCUMENT CONTROL

Version	**Date**	**Authors**	**Status and Changes**
V0.1	28 April 2021	Rick Meessen, Okke Lucassen	V01 is an initial and not complete version that serves as an intermediate report in which the most relevant results and recommendation for the kickstart of WP4 are described.
V0.2	10 June 2021	Rick Meessen, Okke Lucassen	V02 is the official version to be reviewed by assigned partner reviewers.
V1.0	14 July 2021	Rick Meessen, Okke Lucassen	Reviewed by: Maria Kampa (KEMEA), Rachelle Brancaleoni (UCSC), Paivi Mattila (Laurea, PM), Isto Mattila (Laurea, IM), Angela Kwaijtaal (TNO). All review comments have been processed.

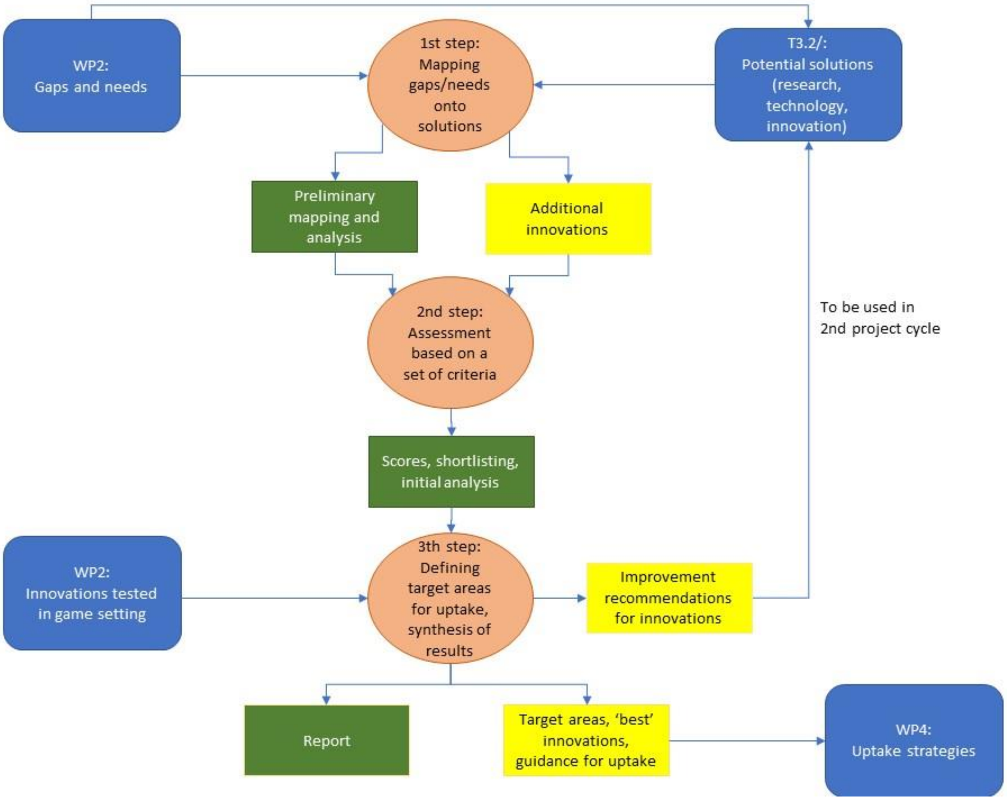
DISCLAIMER

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.

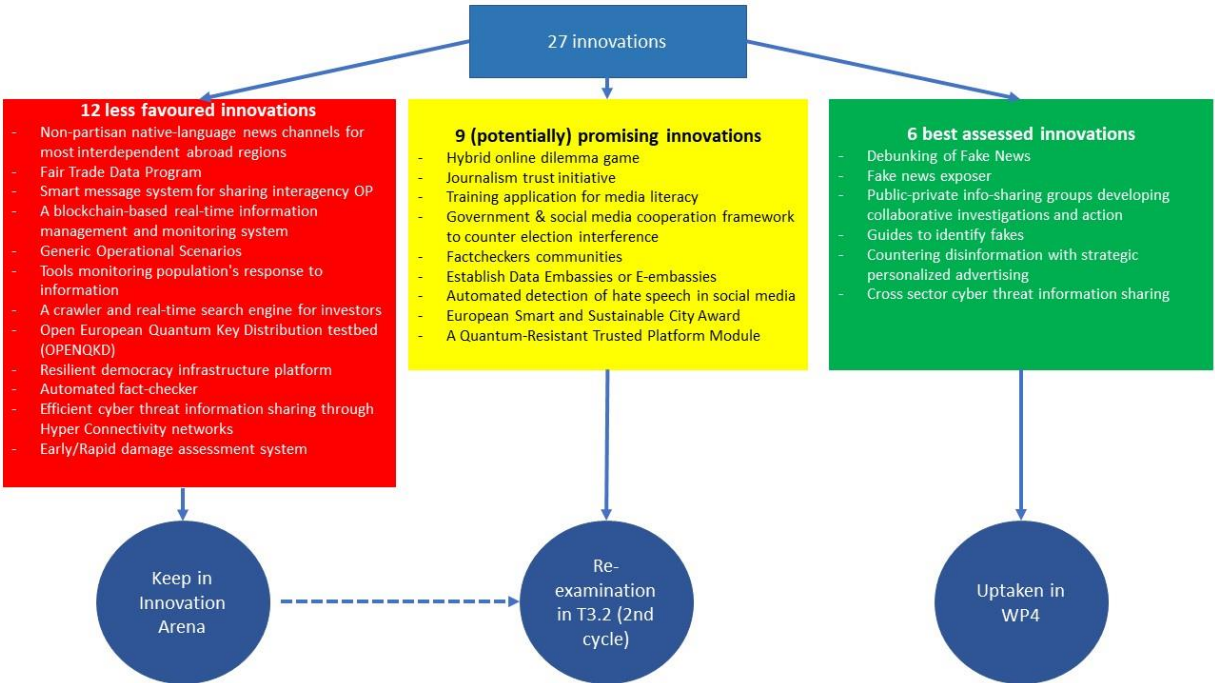
EXECUTIVE SUMMARY

This deliverable (D3.1) is the first interim report of Task 3.1 (Definition of Target Areas for Improvement and Innovations). The objective of Task 3.1 and hence of this deliverable, as defined in the DoA, is to identify target areas in which improvements and innovations for countering hybrid threats need to be taken up. In addition, it is Task 3.1's role to review, complement and assess the innovations that have been identified in Task 3.2 and 3.3. Finally the formulation of target areas and the assessment of innovations are used to prioritise innovations and feed these 'selected' innovations into WP4 for further processing and uptaking. The figure below shows the Task 3.1 process and flow.



A methodology has been developed to assess the innovations. The main criteria and drivers of assessment are: Excellence, Impact and Implementation. Excellence refers to how well the innovations are described as well the credibility and soundness of the innovations. Impact relates to how well suited innovations are in countering hybrid threats, and more specifically against which threats and what (societal) vulnerabilities are protected by those innovations. Finally, implementation cover the difficulty to get innovations implemented and working. The criterium of implementation also considers the required efforts in resources, restrictions for use, and cost drivers like development, acquisition and exploitation. In addition to these criteria a scoring system including thresholds has been defined.

A total of 27 innovations have been processed and assessed in Task 3.1. These 27 innovations have been divided up in 3 categories: 12 innovations that are less favoured and that for the time being will not be followed-up on, 9 innovations that are potentially promising but requires some additional effort to leverage their potential, and 6 innovations that get high assessments and that will integrated into WP4 that deals with the uptake of those innovations. The figure below provides an overview of all 27 innovations and their prioritisation.



27 innovations

12 less favoured innovations

- Non-partisan native-language news channels for most interdependent abroad regions
- Fair Trade Data Program
- Smart message system for sharing interagency OP
- A blockchain-based real-time information management and monitoring system
- Generic Operational Scenarios
- Tools monitoring population's response to information
- A crawler and real-time search engine for investors
- Open European Quantum Key Distribution testbed (OPENQKD)
- Resilient democracy infrastructure platform
- Automated fact-checker
- Efficient cyber threat information sharing through Hyper Connectivity networks
- Early/Rapid damage assessment system

9 (potentially) promising innovations

- Hybrid online dilemma game
- Journalism trust initiative
- Training application for media literacy
- Government & social media cooperation framework to counter election interference
- Factcheckers communities
- Establish Data Embassies or E-embassies
- Automated detection of hate speech in social media
- European Smart and Sustainable City Award
- A Quantum-Resistant Trusted Platform Module

6 best assessed innovations

- Debunking of Fake News
- Fake news exposer
- Public-private info-sharing groups developing collaborative investigations and action
- Guides to identify fakes
- Countering disinformation with strategic personalized advertising
- Cross sector cyber threat information sharing

Keep in Innovation Arena

Re-examination in T3.2 (2nd cycle)

Uptaken in WP4

In addition to the prioritisation of the 27 innovations according to their scoring on excellence, impact, and implementation, the innovations have also been categorized according to 4 target areas. A target area is considered to be a cluster of comparable and coherent innovative solutions for a specific domain and/or vulnerability. Target areas serve as a guidance for WP4 to look for standards and best practices in order to foster the development and implementation of like-wise innovations. The 4 identified target areas are: (1) Citizen and Governmental Resilience, (2) Critical Infrastructure and Flows, (3) Disinformation, and (4) Cyber and Quantum security. It is envisaged that during the second cycle of the project additional target areas might pop up.

When reflecting on the innovations we were able to draw many conclusions and provide useful recommendations for follow-on activities in other WPs and the next project cycles. Three observations and conclusions stand out:

- 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 problem of disinformation is considered to be an essential threat in the hybrid domain, resulting in a high need and medium-high impact of solutions against disinformation.
- Innovations in the target area Critical Infrastructure and Flows get relatively lower scores than the other three target areas. This might resultant from these innovations being considered as crisis management provisions rather than specifically aimed at hybrid threats.
- For many innovations some implementation and exploitation problems are foreseen. Most of the problems, leading to potential restrictions for using and applying these innovations, refer to ethical, legal and public acceptance issues. So, apart from defining and designing innovations that can contribute to counter hybrid threats, it is essential and critical to also consider whether these innovations are also feasible to be employed, from legal, ethical, and public acceptance perspectives.

TABLE OF CONTENT

TABLES

FIGURES

1 INTRODUCTION

1.1 BACKGROUND

The "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) project Description of Action (DoA) (European Commission, 2020) document describes this deliverable (D3.1) as a report on the "Identification of Target Areas for Improvement and Innovations".

The EU-HYBNET "Identification of Target Areas for Improvement and Innovations" report (D3.1) is part of WP 3 (Surveys to Technologies, Research and Innovations). WP 3 has the following objectives:

- To **map current and future needs** for innovations across the different operational areas, focusing on practitioners and relevant actors.
- To monitor and **select currently available innovative solutions** for measures against hybrid threats also with a view of possible standardisation.
- To **arrange events where projects partners will meet innovation** (technical and social, non-technical) **providers** that are invited outside the project consortium to explain and demonstrate innovative solutions that match with the event theme and to interact with practitioners.
  The events will highlight what kind of innovations (existing or future) are needed and exist already.

The figure below shows WP3 in relation to the other WPs and to the overall EU-HYBNET project. The starting point for WP3 is based on the gaps and needs provided by WP2. In this context, WP3 identified solutions (research technology and innovations) to cover these gaps and needs, and then proceeded with an assessment of the most promising areas of solutions, which will be later fed into WP4.

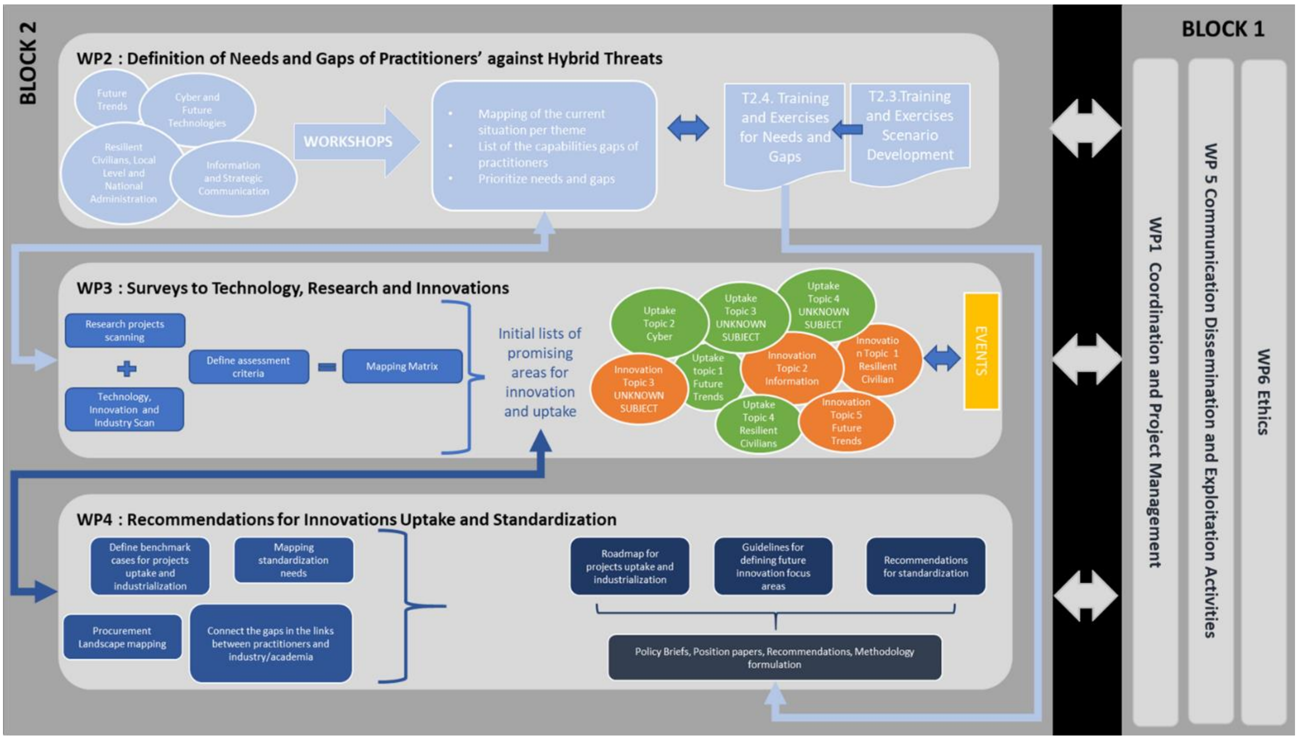

BLOCK 2
BLOCK 1
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the 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 1 Resilient Civilian
Innovation Topic 3 UNKNOWN SUBJECT
Uptake topic 1 Future Trends
Innovation Topic 2 Information
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
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

1.2 OBJECTIVE OF THE TASK

This deliverable is the first interim report of Task 3.1 (Definition of Target Areas for Improvement and Innovations).

The objective of Task 3.1 and hence of this deliverable, as defined in the DoA, is **to identify target areas in which improvements and innovations for countering hybrid threats need to be taken up.**

The following deliverables are the starting point for Task 3.1:

- Task 2.2: Short list on Gaps and Needs (D2.9)
- Task 3.2: Technology and Innovations Watch (D3.3)
- Task 3.3: Innovation and Research Project Monitoring (D3.7)

In addition, the following deliverables were consulted during the execution of Task 3.1:

- Task 2.3: Training and Exercises Scenario Development (D2.17)
- Task 2.4: Training and Exercises for Needs and Solutions for Gaps (D2.20)

One of the purposes of Task 3.1 is to connect the demand side, being the gaps and needs that have to be covered to counter hybrid threats effectively, onto the supply side, being the identified research, technology and innovations that might lead to useful solutions for countering hybrid threats. This seems to be a simple mapping process, but in reality, this requires an in-depth analysis and assessment of both the demand and supply side and in particular the connection between these two. So why is that needed?

Hybrid threats are one of the main challenges Western democracies currently struggle with. Hybrid threats are in the news, mostly framed or wrapped in specific 'hybrid' phenomena like disinformation, foreign meddling in elections, cyber hacks and so on. Governments warn us about them. Institutions like NATO and the EU write policy papers and organize symposia and workshops to discuss them. Various security providers are in the process of defining strategies and developing capabilities to counter hybrid threats, mostly in a particular incarnation rather than across the board. The ultimate response to hybrid threats has not been found yet and in all likelihood does not exist. Countering those threats will remain a very challenging task as long as hybrid threats will evolve due to technological advances, new ways of hybrid campaigning and new opportunities (vulnerabilities and attack vectors) that will be identified by hybrid actors.

Therefore, we must proceed thoughtfully when identifying promising solutions. All too often we see in daily life that the value of new technologies and innovations are overestimated. In a socially and technologically changing society, the pressure to innovate, is increasing rapidly. This makes it all the more important to know the risks and pitfalls of innovative solutions, and to avoid mistakes in practice that do not necessarily arise from theoretical considerations. The willingness to innovate and take risks is indispensable if we want to be effective in protecting our society against hybrid threats. We need to come up with break-through solutions. However, we must not blindly chase after supposed innovations, but must keep an eye on the overall concept and, last but not least, head for the goal by assessing all feasibilities and risks to steer along the right path.

Task 3.1 therefore performs a thorough assessment of the might-be solutions (identified in Task 3.2 and 3.3) in the context of what is really needed (stated by the gaps and needs as identified in Task 2.2). The analysis of Task 3.1 is further complemented by the results from Task 2.3 and Task 2.4 which examined the operationalisation of selected potential innovations. Task 3.1 assessment includes the quality and excellence of the proposed solutions, their impact and effectiveness in countering hybrid threats, and the potential of successful implementation. The latter is very important since innovative solutions often require social and organisational changes and provisions in order to succeed.

Finally target areas for promising innovative solutions will be identified. A target area is considered to be a cluster of comparable and coherent innovative solutions for a specific domain and/or vulnerability. A target area will serve as guidance for WP4, which will develop uptake plans for these target areas and their corresponding innovations.

1.3 TASK ACTIVITIES

In order to meet the Task objective, the following 3-step approach has been performed:

Step 1: Mapping, which includes:

- Mapping the potential solutions derived from research, technology and innovations onto the identified gaps and needs;
- Performing an initial analysis of the produced mapping;
- Looking for additional innovative solutions, based on presumed white spots.

Step 2: Assessment, which includes:

- Assessing availability and quality of data for each innovative solution;
- Reviewing and refining all solutions, driven by the outcomes of the data check;
- Assessing the potential solutions based on the criteria of Excellence, Impact and Implementation (see section 3.2 for further explanation), leading to scores and shortlisting of the most interesting solutions;
- Collecting and synthesizing recommendations for improving innovative solutions that are not on the shortlist and that will be fed back to Task 3.2 to proceed with in the 2nd project cycle (project months 18-34).

Step 3: Defining target areas, which includes:

- Defining target areas (clusters) of solutions, based on this assessment and shortlisting. These target areas serve as input and guidance for WP4 (plans and recommendations for uptake);
- Writing a synthesis of the main assessment findings that will support WP4 in their follow-on actions, and that will be input for WP3 tasks in the next cycle. The synthesis will also include some results and findings from T2.4, in which several innovations have been tested in a game setting.
- Delivering (interim) report.

This 3-step approach is characterised by an iterative process, in which WP2, WP3 (in particular T3.2 and 3.3) and WP4 are being involved, since some innovations, gaps and needs, or the combined mappings might require further consideration (e.g. adding and reviewing data) before we can pull these through the assessment.

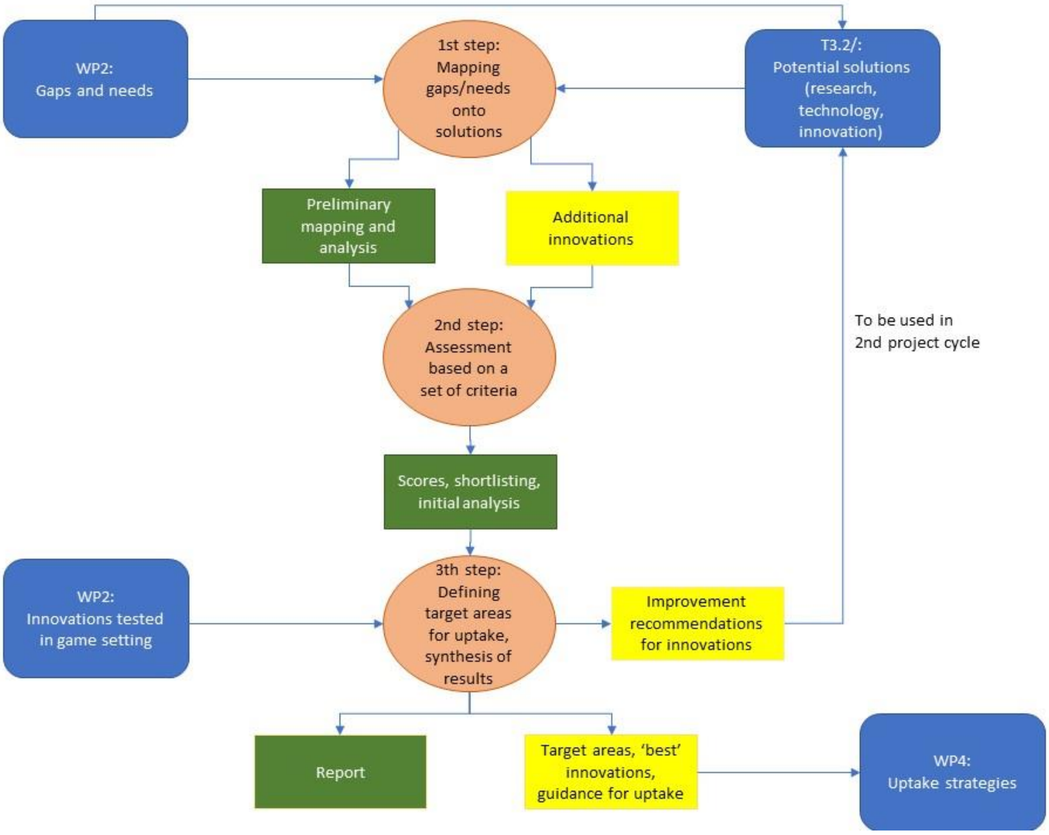


Figure 2: Task 3.1 activities and their interrelations with other WPs and Tasks

1.4 STRUCTURE OF THE DELIVERABLE

The overall structure of the deliverable is as follows:

- Section 1 – Introduction: task background, objective and approach.
- Section 2 – Mapping process and results: mapping the gaps & needs onto the identified innovations, analysing the results of this mapping and developing some additional innovations.
- Section 3 – Assessment: the methodology used for assessing the innovations and the assessment results.
- Section 4 – Game play results: in Task T2.4 several innovations have been tested in a game setting; additional results (complementary to the assessment results in section 3) are included in section 4.
- Section 5 – Target Areas: categorizing the best assessed innovations in target areas for improvement and take up.
- Section 6 – Recommendations: the results of T3.1 will be used by WP4 and WP3 (next cycle), therefore this section provides the recommendations for those WPs.
- Section 7 – Final downselection: all innovations have been assessed and prioritized.
- Section 8 – Lessons learned: identifying lessons learned in the first project cycle about the mapping and assessment process of innovations.
- Section 9 – Contribution to Project Objectives and KPIs: provides assessment of how the results contribute to the agreed and defined project objectives and KPIs as stated in the DoA.

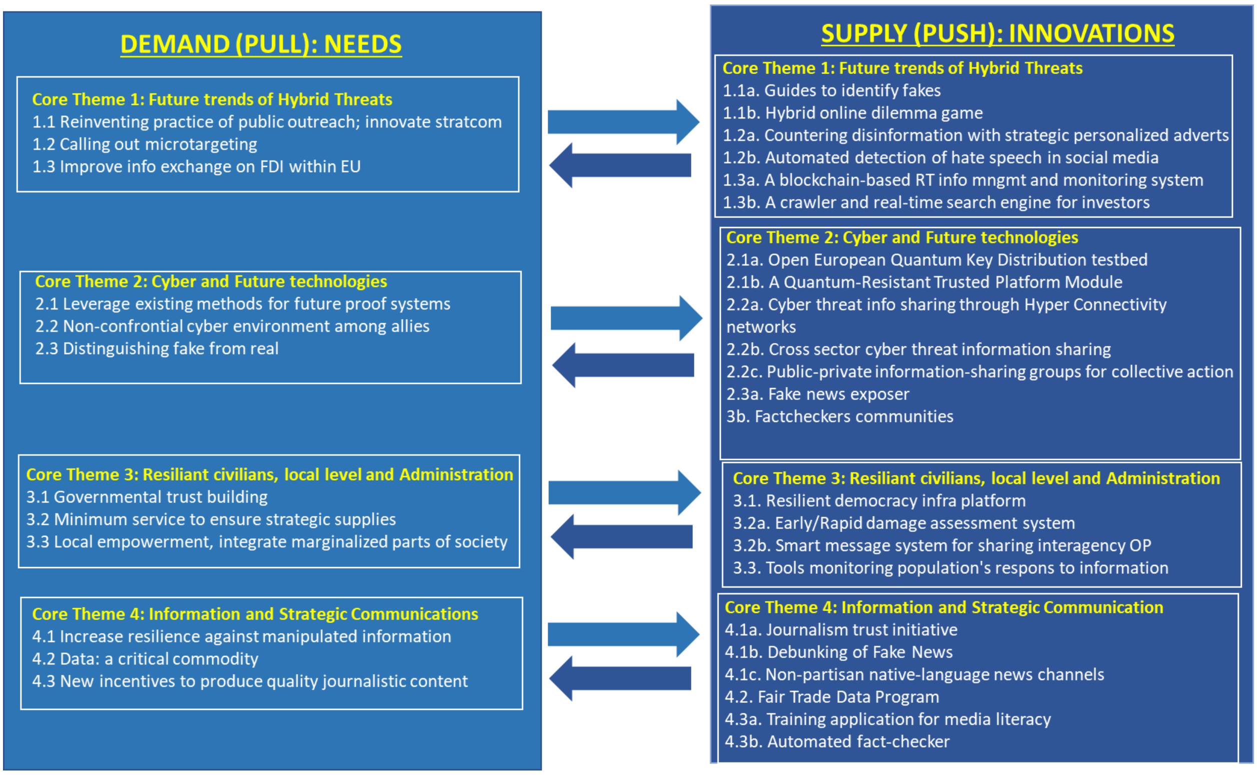
- Section 10 – Conclusions and Recommendations: short summary of the most important takeaways and recommendations for process improvement for the next cycle.

2 MAPPING PROCESS AND RESULTS

2.1 STARTING POINT

Task 3.2 has used the shortlist of gaps and needs (output of Task 2.2, Deliverable D2.9) as a starting point for their technology and innovation watch. Consequently, all identified innovations (see Deliverable D3.3) have been related to specific gaps and needs. As a result, we did not end up with gaps and needs that have not been covered by any innovation, or the other way around, innovations that do not contribute to a specific gap and need.

For Task 3.1 the synthesis of the outcomes of Task 2.2 and Task 3.2 led to a 'matrix' of 12 gaps and needs that correlate with 23 innovations. The figure below shows this matrix. Both the gaps and needs, and the innovations are clustered in the 4 core themes that are the backbone of the EU HYBNET project. Note that the numbering in the figure represents following: the first number refers to the core theme, the second number refers to the innovations related to the specific gaps and needs within that specific Core Theme; e.g. 1.2a and 1.2b refer to the innovations related to Core Theme Future trends of Hybrid threats and specifically to Gap and Need number 2 within this Core Theme. In other words, these two innovations are considered to be (partial) solutions for calling out microtargeting.



DEMAND (PULL): NEEDS

Core Theme 1: Future trends of Hybrid Threats
1.1 Reinventing practice of public outreach; innovate stratcom
1.2 Calling out microtargeting
1.3 Improve info exchange on FDI within EU

Core Theme 2: Cyber and Future technologies
2.1 Leverage existing methods for future proof systems
2.2 Non-confrontial cyber environment among allies
2.3 Distinguishing fake from real

Core Theme 3: Resiliant civilians, local level and Administration
3.1 Governmental trust building
3.2 Minimum service to ensure strategic supplies
3.3 Local empowerment, integrate marginalized parts of society

Core Theme 4: Information and Strategic Communications
4.1 Increase resilience against manipulated information
4.2 Data: a critical commodity
4.3 New incentives to produce quality journalistic content

SUPPLY (PUSH): INNOVATIONS

Core Theme 1: Future trends of Hybrid Threats
1.1a. Guides to identify fakes
1.1b. Hybrid online dilemma game
1.2a. Countering disinformation with strategic personalized adverts
1.2b. Automated detection of hate speech in social media
1.3a. A blockchain-based RT info mngmt and monitoring system
1.3b. A crawler and real-time search engine for investors

Core Theme 2: Cyber and Future technologies
2.1a. Open European Quantum Key Distribution testbed
2.1b. A Quantum-Resistant Trusted Platform Module
2.2a. Cyber threat info sharing through Hyper Connectivity networks
2.2b. Cross sector cyber threat information sharing
2.2c. Public-private information-sharing groups for collective action
2.3a. Fake news exposer
3b. Factcheckers communities

Core Theme 3: Resiliant civilians, local level and Administration
3.1. Resilient democracy infra platform
3.2a. Early/Rapid damage assessment system
3.2b. Smart message system for sharing interagency OP
3.3. Tools monitoring population's respons to information

Core Theme 4: Information and Strategic Communication
4.1a. Journalism trust initiative
4.1b. Debunking of Fake News
4.1c. Non-partisan native-language news channels
4.2. Fair Trade Data Program
4.3a. Training application for media literacy
4.3b. Automated fact-checker

Figure 3: Mapping of 23 innovations (Task 3.2) on 12 gaps and needs (Task 2.2)

Additionally, results from Task 3.3 (Innovation and Research project monitoring, Deliverable D3.7) have also served as a starting point for Task 3.1. These monitoring results were not linked to specific gaps and needs but to the core themes, and to primary contexts within these core themes. A primary context indicates an area of vulnerability that can be exploited by an adversary by employing hybrid threats.

In Task 3.1 an aggregation and summary of the Task 3.3 results has been compiled. This is used in the assessment activity of Task 3.1. In Annex I the brief summary of the Task 3.3 results is provided.

2.2 DATA COLLECTION

The gaps and needs as identified in Task 2.2 showed a myriad of complex gaps and needs that need to be addressed by the innovations and solutions, to be identified in Tasks 3.2 and 3.3. In our discussions with the Tasks 2.2 and 3.2 partners, an expectation was brought forth that the variety of innovations and solutions might prove challenging to integrate in a comparative overview. How would we be able to universally assess the different potential solutions to gaps and needs varying from highly technical ones such as distinguishing fake content from real content compared to more societal dilemma's like empowering communities and integrating marginalized parts of society? In order to improve the consortium's ability to compare such varying potential solutions amongst each other, we developed in Task 3.1, in close coordination with WP3 partners and in particular with Task 3.2, a universal template to be used by Task 3.2. In the Task 3.1 template we wanted to enable the Task 3.2 partners to the largest extent possible to provide relevant details for the identified solutions and innovations. This template became the guiding format in which Task 3.2 would describe its identified potential innovations and solutions, as can be observed in D3.3.

The template was also used for featuring the innovations in the Innovation Arena. The Innovation Arena is a web-based idea management platform that allows participants to add and address existing challenges in the hybrid threat domain by providing ideas, solutions, discussions and so on. The Innovation Arena is created exclusively for the EU HYBNET project consortium, stakeholders and the wider project network. By integrating all innovations developed by Task 3.2 and partly T3.1 in the Innovation Arena, easy access to all innovations for all partners is guaranteed, and moreover, discussions about the innovations can be monitored and can be used to get a better understanding about (some of) the innovations.

Below you can find this template. In Annex IV you may find the instruction manual for the Task 3.1 template in its entirety, including the specific instructions of use and the appendices[1] that were added to the instruction manual.

[1] These appendices refer to external documents, relevant to the understanding of hybrid threats, and the description of innovations: namely the 13 JRC domains as defined by the JRC (Cullen, et al.); the HYBNET core themes (European Commission, 2020)

BOX 1 NAME OF THE IDEA **DESCRIPTION OF THE IDEA**	
BOX 2 REFERENCE TO CAPABILITY GAPs/NEED Describe the use of the solution in reference to the gaps/need Applicable JRC domains as stated by the gaps/need: Applicable core theme(s) as stated by the gap/need	**BOX 3 TYPE OF SOLUTION** • Technical • Social/Human • Organizational/Process
BOX 4 PRACTITIONERS Provide the applicable JRC domains for which the idea 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 end-users of the idea (such as NGO’s, private citizens, private companies, media outlets, police, firefighting departments	
BOX 5 STATE OF THE ART Indication of current Technology Readiness Level (TRL 1-9 index). In which stage is the solution (research, technology, available innovation, proven innovation). Expected time to TRL-9. Expected time to market.	
BOX 6 DESCRIPTION OF USE CASE(S)	
BOX 7 IMPACT ON COUNTERING HYBRID THREATS Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs. Is the idea aiming at resilience or defense or offense against hybrid threats.	
BOX 8 ENABLING TECHNOLOGY Which technologies are critical in fielding the idea?	**BOX 9 RESTRICTIONS FOR USE** Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?

BOX 10 COSTS Indication of costs (differentiate if possible in development, procurement and exploitation).	**BOX 11 COUNTERMEASURES** 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?)
BOX 12 MISCELLANEOUS Any additional remarks/disclaimers/comments/information you might want to provide.	

Figure 4: The template used by Task 3.2 to describe the innovations and used by Task 3.1 for the assessment of innovations

The template as provided above was shared with the Task 3.2 partners who used it in their identification of potential innovations and solutions in respect to the identified gaps and needs. The use of this template allowed the Task 3.2 partners to gather and structure all the information related to the identified innovation or solution in a way that is relevant to the further analysis within Task 3.1.

2.3 MAPPING ANALYSIS

Based on the outcomes and interrelations of Tasks 2.2, 3.2 and 3.3, an initial analysis of the 23 innovations has been completed with the aim to steer the further activities in Task 3.1 and to seek some common denominators that can support both the assessment of the innovations and the selection of target areas.

The initial analysis provided the following observations:

- **Most solutions are hard- or software based**
  Most innovations (85%) offer a solution that is hardware or software based, hence technology is the driving factor behind these solutions. However, to get these innovations successfully implemented, one should keep in mind that respective organizational changes are also needed. For example: the setup of a European quantum testbed (being a combination of hard- and software) also requires new ways of working and cooperation agreements between the partners and nations involved. Therefore we will include the implementation strategy in the assessment (methodology) of the innovations.

- **Most innovations have a strong focus on ICT and Cyber**
  This observation is not that much surprising since the four core themes steer the consortium to search for innovations in that direction. In the next cycles we should consider how we identify and integrate other types of innovations, possibly by expanding the scope of the core themes.

- **Artificial Intelligence is a key enabling technology for a lot of innovations**
  AI is a key, enabling technology for almost 50% of the innovations. Given the central role of AI technology for such applied technology innovations, AI will play a critical role in the development of successful innovations to improve resilience against hybrid threats. Therefore the EU should focus on fostering AI technology within the EU to help develop new innovations to counter hybrid

threats, in addition to many other useful potential applications of AI technology developments.

- **Government role in innovations for citizens**
  Several innovations are meant to be used by citizens. However, a proper use of these innovations will require new legislation and policies. Therefore the role of the government or international institutions as the entity responsible for new policies and legislation is encouraged to be expanded. We will therefore try to stipulate the governmental/institutional role for the innovations that prove to be promising and that will be taken up in WP4.

- **All solutions are directed to increasing resilience and defence against hybrid threats**
  The innovations and solutions identified by Tasks 3.2 and 3.3 were limited to innovations and solutions to enhance resilience and to improve defensive capabilities against hybrid threats. Offensive innovations and solutions, aimed at targeting a hybrid actor in order to prevent or mitigate further hybrid threats, were not identified in this first cycle. Western ethical and legal restrictions might be a limiting factor to the identification of such solutions and innovations. However, in the assessment we will pay attention to the reversed mode, i.e. the robustness of the innovative solutions against (offensive) actions by the opponent. The results of Task 2.4 and the DTAG will further inform this aspect.

- **Many innovations might be available on short notice, probably within 2-3 years**
  The godsend of this is that already in the very near future we could our capabilities to counter hybrid threats. Some innovations are already on the market but not yet fully exploited for countering hybrid threats. Only 2 innovations were estimated to have a time-to-market longer than 5 years. A drawback of this observation is that we might be overlooking the potential of innovations and solutions that could be developed in the long term and that might provide a real breakthrough that can be disruptive in countering hybrid threats. This is especially pertinent to address, in order to be adequately prepared in our defense against the future evolutions of hybrid threats. This will be taken into account during the lessons learned at the end of the 1st project cycle, in order to collectively determine whether the 2nd project cycle should put more emphasis on innovations for the long(er) term.

- **Costing is difficult to specify**
  Although the first objective is to find effective solutions for countering hybrid threats in general and covering the gaps and needs specifically, the costs involved in developing, fielding and employing an innovation is also of importance. However, it proved to be very difficult to provide any cost indications. In some cases the innovation is not developed yet and therefore no figures about costing exist. And in other cases indications about the total life cycle costing of an innovation is not for grasping, especially the costs that relate to the implementation and maintenance are nowhere fully logged. For the assessment we therefore will focus more on qualitative costing indicators (cost drivers).

2.4 ADDITIONAL INNOVATIONS

Despite the tremendous effort that Task 3.2 put into identifying and describing all 23 innovations, especially in the very short time period that was planned for this task, we still pursued the option in

Task 3.1 to identify additional innovations. In the initial analysis we observed that the gaps and needs, and innovations did focus on specific domains like cyber and disinformation. Whilst these domains were addressed extensively, other domains were largely ignored, like space and defence. In order to adhere to the gaps and needs identified in WP2 for the first cycle, we decided to pursue the identification of additional innovations conform the gaps and needs, and thus in the same, corresponding domains emanating from Task 2.2. For the 2nd cycle it might be prudent to emphasize the integration of the domains that were not covered in the 1st cycle.

As a result we requested the participants to Task 3.1 (9 out of 25 consortium partners) to check whether they could find additional innovations that relate to the 12 defined gaps and that are not predominantly cyber or ICT related. This finally resulted in 4 additional innovations, being:

- **Establish Data Embassies or E-embassies**: Establishment of national datacentres in secondary countries or so called Data Embassies in allied countries in order to safeguard essential governmental services and governmental continuity in case digital infrastructure in home countries is no longer operable.
- **European Smart and Sustainable City Award (ESSCA)**: This award assists cities in becoming more sustainable and resilient, and can therefore be used to assess and improve a city's resilience against hybrid threats. It addresses e.g. urban security, resilience of communication networks, societal challenges and citizen inclusiveness.
- **Generic Operational Scenarios (GOS)**: Hybrid threats threaten with a particular acuity the Critical infrastructures. Therefore, private and public players must be intensively trained to handle the systemic crises endangering the countries' vital networks. GOS concerns the innovative use of digital scenarios which would provide a regular training to the involved actors.
- **Government and Social Media cooperation framework in countering election interference**: Cooperation framework in which government practitioners can work with social media companies to counter election interference, for example through mitigating the spread of influence operations on social media platforms during (the run-up to) elections.

Annex V provides a detailed description of all 27 innovations (the 23 original innovations emanating from Task 3.2 and the 4 additional innovations as mentioned above), in the form of the templates that were described in section 2.2.

3 ASSESSMENT

3.1 DATA QUALITY AND COMPLETENESS

In Task 3.2 a huge effort was made to describe all the innovations as completely and in as much detail as possible, in line with the provided templates. However, relevant data in some of the templates (and hence innovations) was still missing, making an adequate and fair assessment of all innovations problematic.

Since the assessment leads to a selection of innovations that will be further explored in WP4, we also wanted to ensure that the data provided in the templates was of sufficient quality. Therefore, we set up a review and refinement process for all innovations, both the 23 initial innovations and the 4 additional innovations.

We used the broad and in-depth expertise that is available in the consortium, and requested 2-3 consortium partners to review and add more specific or missing information (where needed) to the innovation templates. The partner that first introduced the identified innovation in Task 3.2 (the initiator or source) was excluded from the review, to avoid the review being doing by the initiator.

Since most consortium partners are specialized in a specific domain/expertise, we tried to assign (as best as possible) partners to innovations that are within their area of expertise. Therefore, we defined **several clusters of innovations**, based on a combination of core theme, domain, enabling technology etc. By doing so we specifically targeted and identified consortium partners to add and review a cluster (small set) of innovations which are more or less in their comfort zone. This proved to provide a high review quality and also to ensure an efficient and effective approach, which could be executed in a short timeframe.

The table below depicts all 27 innovations categorized in 5 clusters. Annex III provides additional information about the specific contribution of consortium partners to each innovation (the initiator of the innovation, the partners that have reviewed and added data to the innovations, and the partners that have done the assessment).

Clusters of innovations	Specific innovations
Crisis Management & Critical infrastructures protection	Resilient democracy infrastructure platform
	Early/Rapid damage assessment system
	Smart message system for sharing interagency OP
	A blockchain-based real-time information management and monitoring system
	A crawler and real-time search engine for investors
	Establish Data Embassies or E-embassies
	European Smart and Sustainable City Award
Microtargeting and Influencing	Tools monitoring population's response to information
	Non-partisan native-language news channels for most interdependent abroad regions
	Fair Trade Data Program

	Countering disinformation with strategic personalized advertising
Education and training	Training application for media literacy
	Hybrid online dilemma game
	Generic Operational Scenarios
Disinformation	Fake news exposer
	Factcheckers communities
	Journalism trust initiative
	Debunking of Fake News
	Automated fact-checker
	Guides to identify fakes
	Automated detection of hate speech in social media
	Government & social media cooperation framework in countering election interference
Cyber and Quantum security	Open European Quantum Key Distribution testbed
	A Quantum-Resistant Trusted Platform Module
	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

Table 1: Clusters of innovations used for the assignment of assessors

For each cluster we requested one of the T3.1 partners to coordinate the review process for the corresponding innovations. To support the review process, we specified the type of information that was initially missing in the description of the innovation. In addition to these specific information requests, tailored for each innovation, we also defined two general questions that needed to be addressed for all innovations. These two questions were derived from the preliminary analysis of all templates. It showed that especially information regarding potential countermeasures and cost drivers were lacking in most of the innovation templates, or were only very briefly described.

The two general questions were formulated as follows:

1. To review and add information on **potential countermeasures** against the proposed solutions. Are there any potential countermeasures that other actors could field that would be detrimental to the effectiveness of the described idea? Provide a description of how they would degrade the effectiveness of the idea. Provide an estimation of how long the described idea would be effective and useful as a solution to the identified gaps/need.
2. To generate more information about **cost drivers** for all proposed solutions.
   It appeared to be difficult to forecast or assess expected costs for the innovations. Therefore, we are looking for more indirect cost drivers, like the manpower needed to operate the innovation, the time and effort it requires to implement the innovation in an organization, the production time to get the innovation mature etc. In short: anything that helps to make a rough assessment about costing does help.

3.2 METHODOLOGY

3.2.1 METHODOLOGY: DIMENSIONS

The assessment of innovations (solutions) follows a path similar to the way that Horizon 2020 project applications are evaluated. There are three dimensions to be assessed:

- Excellence
- Impact
- Implementation.

EXCELLENCE

In the Excellence dimension there are 3 main aspects to consider in the assessment. This dimension has to do with how clear and pertinent the description of the innovation and its intended use is. All relevant aspects should be clearly described to enable a fair assessment. In particular the scoring should be based on:

1. **Clear definition of intended scope / applicability.** Is the claimed coverage of EU-HYBNET Gaps and Needs, JRC domains, and core themes convincing? Is it clear which groups of practitioners and end-users (NGO's, private citizens, private companies, media outlets, police, firefighting departments) will benefit and how? Who will provide the service?

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

3. **Credibility and soundness of the concept.** Is the proposed innovation viable? Is the solution, based on the innovation, realistic?

IMPACT

In the Impact dimension there are 4 main aspects to consider in the assessment. This dimension has to do with how much impact the innovation will have in detecting and/or countering threats and/or attacks and its coverage of use cases. In particular the scoring should be based on:

1. **The coverage.** Is the solution useful in many domains versus only in a single or a small number of domains? In the covered domains, is this a dearly needed solution or is it a nice to have solution?

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

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

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

IMPLEMENTATION

In the Implementation dimension there are 5 main aspects to consider in the assessment. This dimension has to do with the size of the effort required for bringing the innovation to life, its operational and maintenance cost as well as the time when it can be taken into practical use. In particular the scoring should be based on:

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

2. **Implementation effort:** How high are the expected costs (development cost, capital expenditure and operational expenditure) for bringing the innovation into a practically usable technical and operational solution? If relevant, what is the Technology Readiness Level (TRL) of the key technologies used. What are the difficulties/cost of integration in current organizations and/or processes for the set-up of an operational environment?

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

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

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

3.2.2 METHODOLOGY: SCORING AND THRESHOLDS

The assessment of each dimension is given a score from 0 – 5. Scores must be an integer. The scores reflect the degree in which the innovation fulfils the dimension, which is as follows:

0 — **Fails.** The innovation fails to address the aspects to consider or cannot be assessed due to missing or incomplete information.

1 — **Poor.** The aspects to consider are inadequately addressed, or there are serious inherent weaknesses.

2 — Fair. The innovation broadly addresses the aspects to consider, but there are significant weaknesses.

3 — **Good.** The innovation addresses the aspects to consider well, but a number of shortcomings are present.

4 — **Very Good.** The innovation addresses the aspects to consider very well, but a small number of shortcomings are present.

5 — **Excellent.** The innovation successfully addresses all relevant aspects to consider. Any shortcomings are minor and can be mitigated.

The assessment is documented on a scoring card, which is based on an MS-Excel format. The scoring card contains a request for comments on the assessment procedure in general, like fit-for-purpose and suggestions for improvements. These will be taken into account during the setup of the 2nd project cycle. Furthermore, the scoring card contains a request for comments on how comfortable and well-suited the assessor considers themselves with performing the assessment task. In case of high fluctuations in scores between different assessors, this information might be used to weigh the scores.

To perform on the one hand a fair assessment using as much data as possible and on the other hand keep the level of effort and time within limits, we determined that all innovations had to be assessed by at least 3 consortium partners.

To be able to classify all innovations at the end, and to decide which innovations will be used for further consideration in WP4, we will work with thresholds. For that we use a two-level threshold approach.

The first level, being the **primary threshold,** is set by:

- Each assessment dimension requires an average[2] score of at least 3;
- The overall score, applying to the sum of the three (EII) individual average scores, is at least 10.

All innovations that meet the primary threshold are considered to be promising innovations. However, since WP4 needs to be selective in the first project cycle when it comes to the number of innovations that can be considered for the uptake, we will apply a second level, being the secondary threshold. Applying this threshold will then finally lead to a shortlist of the 'best assessed' innovations.

This **secondary threshold** is set by:

[2] Averaging the scores given by all assessors for a single dimension

- Each assessment dimension requires that all individual scores are at least 3; so that implies that an innovation may not get a score lower than 3 by one of the assessors on one of the dimensions.

The table below illustrates an example in which an innovation meets the primary threshold: the average score for each dimension (Excellence, Impact, Implementation) is 3 or higher, and the total is 10. However, the innovation in this example does not meet the secondary threshold: Assessor B gives a score of 2 for Implementation, which is below the threshold of 3.

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**		

Table 2: Example of additional requirements for passing secondary threshold

The innovations that do not meet both the thresholds will be fed back to Task 3.2 with the aim to try to improve the innovation and/or complete missing data in the 2nd cycle of the EU HYBNET project.

In the figure below the scoring and thresholding methodology is summarized.

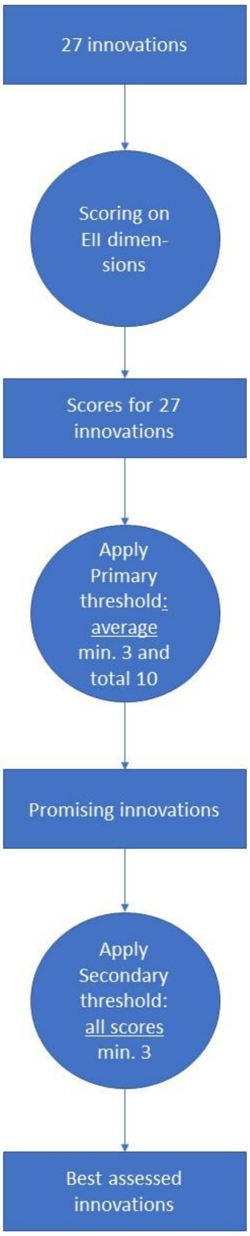

27 innovations
Scoring on EII dimen-sions
Scores for 27 innovations
Apply Primary threshold: average min. 3 and total 10
Promising innovations
Apply Secondary threshold: all scores min. 3
Best assessed innovations

Figure 5: Scoring and thresholding methodology

3.3 RESULTS

All innovations have been assessed by at least 3 consortium partners, and in some cases even 4 partners. In case of 2 innovations one of the assessors did not give a score, either because essential information was lacking or the innovation was not considered relevant in the context of countering hybrid threats (both in the eyes of the assessor). In Annex III the complete assignment of innovation initiator, reviewers and assessors is provided.

Finally, 15 (out of 27) innovations met the primary thresholding criteria, which are a minimum average score of 3 for each of the EII criteria, and an overall minimum average score of 10.

In the table below the **15 'promising' innovations** including their averages are listed, in order of descending total scores.

Promising Innovations	**Total score**	**Excellence score**	**Impact score**	**Implem-entation score**
Debunking of Fake News	13,0	4,5	4,0	4,5
Fake news exposer	12,1	3,7	3,7	4,7
Hybrid online dilemma game	11,6	4,3	3,3	4,0
Public-private info-sharing groups enabling collaborative Investigations & action	11,4	3,7	4,0	3,7
Journalism trust initiative	11,3	3,7	3,3	4,3
Guides to identify fakes	11,3	3,8	3,5	4,0
Countering disinformation with strategic personalized advertising	11,0	4,0	3,3	3,7
Training application for media literacy	11,0	3,5	4,0	3,5
Cross sector cyber threat information sharing	11,0	4,3	3,7	3,0
Government & social media cooperation framework to counter election interference	10,7	3,7	3,3	3,7
Factcheckers communities	10,6	3,3	4,0	3,3
Establish Data Embassies or E-embassies	10,3	3,3	3,3	3,7
Automated detection of hate speech in social media	10,1	3,8	3,3	3,0
European Smart and Sustainable City Award	10,0	3,0	3,3	3,7
A Quantum-Resistant Trusted Platform Module	10,0	3,7	3,3	3,0

Table 3: Promising innovations (passing the primary threshold)

In Annex II all innovations including their scores are included.

If we zoom in on the scores that were given by each assessor, we are able to be more selective and employ the secondary threshold. This secondary threshold (see also section 3.2) states that an innovation may not get a score lower than 3 by one of the assessors.

By applying this secondary threshold to the initial list of 15 innovations, we observe that the **following 9 innovations do not meet the secondary threshold criterium**. See table below, in which the scores lower than 3 are included and marked with an orange color.

Innovations meeting the primary threshold but NOT the secondary threshold	Total score	Excellence scores below 3	Impact scores below 3	Implem. Scores below 3
Hybrid online dilemma game	11,6	none	1x score 2	none
Journalism trust initiative	11,3	1x score 2	1x score 2	none
Training application for media literacy	11,0	none	none	1x score 2
Government & social media cooperation framework to counter election interference	10,7	none	none	1x score 2
Factcheckers communities	10,6	none	none	1x score 1
Establish Data Embassies or E-embassies	10,3	1x score 2	1x score 2	none
Automated detection of hate speech in social media	10,1	none	none	1x score 2
European Smart and Sustainable City Award	10,0	1x score 2	1x score 2	none
A Quantum-Resistant Trusted Platform Module	10,0	none	none	1x score 2

Table 4: Promising innovations NOT passing the secondary threshold

So, by applying both the primary and secondary criteria we are able to come up with a shortlist of innovations that can be considered as the ‘best assessed’ innovations. That does not imply that all other innovations will be dropped. Some of these will be fed back to Task 3.2 including the main recommendations provided by the assessors, and will require an additional effort to see if these innovations can be improved or not. This effort will be done in the second cycle of the project. In Section 5.3 the main recommendations and potential improvements for all non-shortlisted innovations are provided.

Finally, this leaves us with a shortlist of 6 'best assessed' innovations, presented in the table below.

‘Best assessed’ innovations	Total score	Excellence score	Impact score	Implem-entation score
Debunking of Fake News	13,0	4,5	4,0	4,5
Fake news exposer	12,1	3,7	3,7	4,7
Public-private info-sharing groups developing collaborative investigations and action	11,4	3,7	4,0	3,7
Guides to identify fakes	11,3	3,8	3,5	4,0
Countering disinformation with strategic personalized advertising	11,0	4,0	3,3	3,7
Cross sector cyber threat information sharing	11,0	4,3	3,7	3,0

Table 5: Best assessed innovations (passing both the primary and secondary threshold)

3.4 INITIAL ANALYSIS

Although 15 innovations (out of 27) do meet the primary threshold criteria, and are therefore considered to be promising, we still see some differences and variations in scores:

- **Debunking of fake news** gets by far the highest score: it achieves the highest total score (13) and it is the only innovation that scores on all 3 EII criteria above 4 (while 3 was the threshold).
- The 3 lowest scoring innovations on the list of promising innovations (detection of hate speech, Smart City Award, Quantum-Resistant Trusted platform) do meet the primary threshold criteria marginally; their total score is either just 10 (the minimum threshold) and they have at least one EII score at just 3.0 (the minimum threshold). Therefore these 3 innovations are quite comparable with some that scored just below 10 and therefore not made it to the list of 15 promising innovations (e.g. Fair Trade data program, Generic Operational Scenarios). Since the number of assessments is relatively low, we therefore have to be **a bit reluctant in drawing to heavy conclusions on the bottom ones**.
- Another striking observation is that **5 (out of 6) best assessed innovations do meet both the primary and secondary threshold relatively easy**. The only exception is the innovation concerning the cross sector cyber threat information sharing, which has an average score of 3.0 for implementation. This relatively low score requires some follow-up action which is defined as in the recommendations for WP 4 (see section 5.4).
- **3 promising innovations do get a relatively high total score (11 or higher) but do not pass the secondary threshold** (Hybrid dilemma game, Journalism Trust Initiative, Training media literacy). This requires some additional work and clarification in the next project cycle, since we think that these innovations are that promising that these could be lifted up to the list of best assessed innovations.

If we look from another perspective, being the one related to the dimensions (criteria) we see the following:

- The **Implementation criteria** was often scored relatively low (not on average but on single scores) and/or difficult to assess, which was caused by insufficient or too vague information, implementation costs assumed to be high, implementation obstacles foreseen (acceptance, legal and ethical restrictions, multinational alignment).

- The **high Impact scores** were often motivated by short term impact and wide range of use (applicable to many domains). The latter should be handled with care, since a wide range of use might also lead to (potentially) too generic solutions and finally less fit-for-purpose.

A more thorough analysis is done in chapter 5, where we will come up with findings and recommendations that will be useful for WP4 and for the next cycle of WP3.

4 BRIEF OVERVIEW TASK 2.4 SCENARIO-BASED EXERCISE RESULTS

In addition to the assessment of innovations as performed in Task 3.1, some of the innovations have been tested in a scenario-based exercise. Task 2.4 was responsible for this scenario-based exercise, based on the scenario and vignettes as developed in Task 2.3. Although it has not been foreseen in the DoA to include or even integrate the Task 2.4 outcomes in Task 3.1, it was considered to provide some added-value to do so. Therefore this section briefly describes the main outcomes of Task 2.4.

In the first cycle Task 2.4 decided to use a Disruptive Technology Assessment Game (DTAG) as a format for the scenario-based exercise. The scenario formed a central baseline setting for the DTAG, which was further specified through the use of 4 vignettes, each reflecting one of the 4 Core Themes. Every vignette contained 2 injects, representing a turning point within the vignette with a specific crisis for the players to solve[3]. Task 2.4 made a selection of the most relevant innovations and solutions for every vignette. The players were then asked to select the IoS – a representation of the 27 identified innovations and solutions – that they deemed most useful for every inject in their vignette. After the selection of their IoS, the players would further expand upon the operationalization of the IoS within a broader campaign plan to counter the crises that they were faced with within the vignette. The DTAG as such has resulted in complementary information on the potential operational benefits and challenges of the IoS. Given the limited time span and format of the DTAG, not all innovations were tested within the scenario-based exercise.

Below we give an overview of the most relevant findings of the operationalization of the chosen IoS (innovations) per Core Theme, which helps inform the opportunities and challenges towards the operational use of some of the innovations as identified by Tasks 3.2 and 3.3, and analyzed within Task 3.1.

4.1 CORE THEME 1: FUTURE TRENDS OF HYBRID THREATS

IoS card	**Name of IoS**	**Relevant action point**
1	Cross sector cyber threat info sharing platform	Sharing information among services and agencies
	This IoS should find synergies and complementarity as well as continuity / deepening of the CERT-EU model in order to integrate disinformation. H2020 Concordia project has for instance resulted in "Threat Intelligence Platforms for Europe" enabling cross sector collaboration. It is based on a mutual cyber intelligence sharing agreement among partners. Such arrangement would be a way to join up disparate sources of information, based on open source information and partners' information.	

[3] For more information on the DTAG, consult D2.20; for more information on the scenario and vignettes, consult D2.17. A selection of the most relevant innovations and solutions was made for every vignette.

2	Resilient Democracy Infrastructure Platform	Communication online and offline War room for crisis communications
	Benefit in that it would be a bi-directional feedback loop, increasing communication outreach and preventing miscommunication to an extent. The platform would require reliable energy supply while SMS Messages would prove more direct and less costly in terms of energy. A modular system could be envisaged, with different digital configurations according to the level of crisis intensity. An EU cross border perspective is essential.	
3	Early damage assessment system	Sharing information among services and agencies
	Algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event. This would take the form of a Critical Infrastructure Resilience Platform (CIRP) when fed with real time nowcasting or forecasting data instead of a scenario hazard, can be turned into an early or rapid damage assessment system respectively, thus providing the unique capability to initiate efficient response actions, right after (in case of now-cast data) or even before (in case of forecast data) the occurrence of catastrophic events. Long tem investment supporting and enabling other IoSs. Metadata analysis is essential in this loop. The idea is in use within INFRASTRESS H2020 project as well as 7Shield Project and EU-Circle H2020.	

4.2 CORE THEME 2: CYBER AND FUTURE TECHNOLOGIES

IoS card	**Name of IoS**	**Relevant action point**
1	Blockchain real time info management and monitoring system	Close down systems
	This idea of system would be a real time operationalization of EU momentum in addressing the critical character of foreign direct investments monitoring. The main idea of this system would a constantly up to date visualization of transactions based on companies' and governments' information sharing. This idea raises issues in terms of market freedom and privacy and it should therefore be limited to those restrictively defined critical sectors of the economy that affect societal stability and resilience of society. While the information would be verified and transactions authorized based on blockchain technology. Rendering transactions transparent and giving the means of verification. Keeping the system running while tracking transactions, not getting down by threat actors, applied across infrastructures	

2	Quantum key distribution testbed	NIST response / digital rescue package
	Scalable solutions in different infrastructure for protection against quantum computing enhanced attacks. The QKD project consortium should be leveraged in order to have updates on the most relevant advances in terms of quantum secure communications. This could apply in terms of B2C and B2B communication as well as emergency communications in times of crisis. Quantum communication engagement would enhance the security of institutional communications.	
3	Public-private information sharing groups	Communication / *Engagement* / to the population
	Crowd *sourcing for generating ever more complete pictures of an ongoing situation or crisis. This would need to deepen information sharing among institutions coming from the grassroots. Need to estimate a system to flow information in a double feedback loop. Possibility for thematic groups. Consideration on open source to track cyber criminals and hackers, increase the risk of prosecution for them and raise the costs of engaging cyber action.*	
4	Hyper connectivity network	Communication / Closing down systems
	High speed information sharing to be exploited by CERT EU teams. This idea is connecting the NIS Directive article 12 establishment of CSIRT networks in order to exchange information on zera day and other vulnerabilities, including TTPs for cyber threats. This would leverage the hyper connectivity of networks.	

4.3 CORE THEME 3: RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

IoS card	**Name of IoS**	**Relevant action point**
1	Emotional detection tool on SOME and automated detection of hate speech in social media	Social media scans
	Semantic analysis and machine learning are a usual part of the work with big data. By training the used algorithm to map a group of words to the most likely meaning, a detection of a particular topic can be performed. For example, several Github projects provide tools to detect hate speech. Such concepts are already used on Twitter to detect and censor	

	discriminatory contents. Detection and analysis of emojis. Tools subject to spoofing, fake accounts, artificially generated content, large group of bystanders on social media.	
2	Smart messaging routing and notification service	Factchecking
	The service enables the sharing of the information among involved actors at every level of coordination enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. This way relevant information will reach the appropriate persons at every level of coordination in a timely manner. It can be evolved and integrated to share the operational picture to every agency involved in the response at every level of coordination. This idea is implemented in InfraStress H2020 and SATIE H2020 project.	
3	Resilient Democracy Infrastructure Platform	Long term investment
	Medical and scientific experts in line with crisis topic. Generating open and transparent discussion. Modularity of the RDIP based in peace time for specifics of the crisis. Diffusion of important information and expert advice, crowdsourcing the gathering of information.	

4.4 CORE THEME 4: INFORMATION AND STRATEGIC COMMUNICATIONS

IoS card	**Name of IoS**	**Relevant action point**
1	Guides to identify fakes	Centrality of detection
	Debunking fake news using dashboard website, open source debunking platform. Integrate the usual channels of disinformation identified. Ethics and definition questions of a debunking platform are crucial. Citizen engagement and collaboration a major challenge – good faith engagement with platform a big challenge. Frameworks and working methods and definitions on deepfakes. Guide to identify fakes could be used in order to raise awareness on practices that improve abilities to detect fake images and videos online.	
2	Strategic personalized advertising	Debunking fake news
	Ethics issue – no go	

4.5 TAKEAWAYS OF D2.23 FOR TASK 3.1

Information collection and information sharing opportunities: There are some clear trends visible from the players' selection of innovations within the operational setting of the DTAG. Across the 4 Core Themes, the players have shown an express interest in using innovations to improve the information collection and sharing position of governmental entities. This ranges from establishing and expanding dedicated specialized cross-sector cyber threat information sharing platforms, early damage assessment platforms, public-private information sharing groups civilian emotional detection tools, Foreign Direct Investment monitoring platforms, to a more holistic society-wide resilience-improving network in the form of Resilient Democracy Infrastructure Platforms.

Improve technical cyber security position: Reflecting the more specialized and highly technical nature of Core Theme 2 Cyber and Future Technologies, the players in this vignette have shown an express interest in pre-emptively improving cyber security against future quantum computing-enhanced cyber-attacks. The quantum key distribution testbed could help improve societal resilience against such quantum computing-enhanced cyber-attacks for Business-to-Business and Business-to-Consumer collaborations, as well as for crisis-time emergency communications.

Lackluster addressing of legal and ethical challenges: The players flagged some clear operationalization challenges for the fielding of several innovations, with a focus on lackluster solutions to legal and ethical challenges. This reflects similar findings within the work of Task 3.1. Such challenges are to be expected, given the novelty of the identified solutions, and the limited experience in practical implementation of such newly identified innovations. In the future development and experimentation of innovations of interest, such challenges should be better addressed. Without practical guidelines of how innovations would fit within the legal and ethical frameworks of practitioners, innovations will remain unusable.

Blowback risk due to low societal acceptance: The players identified blowback risks for some of the innovations, especially pertaining to Core Themes 3, Resilient Civilians, Local Level and Administration, and 4, Information and Strategic Communication. Innovations related to improving civilian resilience and enhancing governmental strategic communications to citizens are highly dependent on citizens' acceptance of tooling that interacts with, informs, and influences the citizenry. Such tools can only be implemented in settings where a certain threshold of societal acceptance of these tools has been reached. In absence of such community support, tools that are intended to improve citizen resilience and expand accessible and understandable information could have the counter-productive effect of further citizen distrust towards the government, which in turn could further polarize societies.

The aforementioned main observations and takeaways are included and integrated in section 6, which addresses the recommendations for WP4 and WP3 (next cycle).

5 TARGET AREAS

5.1 OBJECTIVE, DEFINITION AND SELECTION

As described in the DoA the main objective of Task 3.1 is to identify and define target areas in which WP4 should look for the uptake of innovations. However, we did not define target areas very detailed in the DoA, so that implied that we had to explore the scoping and use of target areas during this first cycle.

As we have seen in chapter 3 we used five clusters of innovations to smoothen the assessment process. All five clusters have been composed based on a combination of:

- Type of solutions (e.g. training systems)
- Domain of application (e.g. cyber, disinformation)
- Specific vulnerability that needs to be protected (e.g. critical infrastructure)
- Core theme (e.g. civilians resilient against influencing operations)
- Technology involved (e.g. quantum)

After analysing the assessment process and the assessment results, we now can conclude that these clusters function to some degree quite well in analysing coherence and similarities between various innovations. However, there is some overlap between these clusters and some tend to be more types of solutions, while others are more focussing on the application domain. In order to use these clusters as target areas, we need to adapt and comprise these slightly. But first, we need to provide a definition and reason-to-be for target areas.

The **definition** we will use for **target areas** is:
A target area is a cluster of comparable and coherent innovative solutions for a specific domain and/or vulnerability.

Target areas **serve (reason-to-be)** as a guidance for WP4 to look for standards and best practices in order to foster the development and implementation of like-wise innovations.

With the definition and the reason-to-be in mind we recommend to use the following four target areas, which are actually derived from the clusters used for assessment and from the innovations that are promising or even best assessed. We further envisage that during the second cycle of the project additional target areas might pop up.

The **four selected target areas** are:

- Citizen and Governmental Resilience
- Critical Infrastructure and Flows
- Disinformation
- Cyber and Quantum security

Citizen and Governmental Resilience included all means which support firstly that citizens and governmental bodies are aware of hybrid threats and their impact, and secondly, how to cope with these threats in order to mitigate the effects and risks for citizens and their society in general. The latter can range from being educated by the influencing effects of (social) media to being protected against election interference.

Critical Infrastructure and Flows include infrastructures, nodes and flows (e.g. goods, data) that are vital for the wellbeing and welfare of our society and its citizens. Therefore, protecting these against hybrid threats is of eminent importance.

Disinformation is such a powerful tool in current hybrid threats and tactics that it should be considered as a target area itself. This target area is interrelated to citizen resilience (how to make citizens more resilient against e.g. disinformation) and strategic communication and influencing (e.g. countering the narrative that is wrapped up in the disinformation campaign).

Cyber and in the (near) future quantum security is just like disinformation a very powerful tool in current hybrid campaigns. It often is employed to attack critical infrastructures and therefore could be an element in the target area 'Critical infrastructure and flows'. However, due to its omnipresence in hybrid campaigns it also justifies a dedicated target area.

5.2 MAIN FINDINGS

The table below maps the 15 promising innovations (including the 6 best assessed innovations, marked in green) on the four identified target areas.

Target Areas	**Promising innovations [in green the best assessed innovations]**
Citizen and Governmental Resilience	Government & social media cooperation framework in countering election interference
	Training application for media literacy
	Hybrid online dilemma game
	Automated detection of hate speech in social media
Critical infrastructure and Flows	Establish Data Embassies or E-embassies
	European Smart and Sustainable City Award
Disinformation	Fake news exposer
	Factcheckers communities
	Journalism trust initiative
	Debunking of Fake News
	Guides to identify fakes
	Countering disinformation with strategic personalized advertising
Cyber and Quantum security	A Quantum-Resistant Trusted Platform Module
	Cross sector cyber threat information sharing
	Public-private information-sharing groups developing collaborative investigations and collective action

Table 6: Mapping of the 15 promising innovation on the defined Target Areas

This provides some useful insights:

- **The target areas** prove to be, to **some extent, similar to the four core themes** that have been defined in the HYBNET project DoA, which justifies their choice. However, there are **some slight differences**:
    - The target area Critical Infrastructure and Flows is considered to be an area on its own, and requires full attention when identifying the risks posed by hybrid threats and the countermeasures to be taken. This target area may warrant further focus and analysis of additional innovations in future cycles.

    - The core theme Information and StratCom is broader than the current target area Disinformation. However, the innovative solutions that have been identified fully focus on Disinformation and thereby narrow the scope of the current theme. Keep in mind that this counts only (or so far) for the current 1st cycle.
    - Trends that are part of the core theme of Future Trends of Hybrid Threats are currently (1st cycle) well addressed in the four chosen target areas, e.g. the trend of data flows (part of critical infra and flows) and the trend towards quantum technology and communication (part of Cyber and quantum security). For the next cycle we envisage other/new trends that probably will justify another target area (e.g. threats against satellites).
- **Disinformation innovations were assessed relatively high**. With 6 promising innovations (out of 15), of which 4 belonging to the top 6 (best assessed innovations), the target area Disinformation achieves by far the best results. This can be explained by:
    - The implementation is scored 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). And also the problem of disinformation is considered to be an essential threat in the hybrid domain, resulting in a high need and medium-high impact of solutions against disinformation.
    - Also most of the identified solutions are already feasible, some are even available and running on a low scale. Nevertheless, some concerns have been put forward, like the acceptance and resistance by the general public, and the cooperation of social media companies who have financial stakes that will prevail above restricting and checking content.
- **The innovations in the target area Critical Infrastructure and Flows get relatively lower scores** than the other three areas. They offer only 2 promising innovations (out of 15), none of which are part of the best assessed innovations. This might be explained by:
    - Their score on Excellence and Impact is relatively low, which is caused by some doubts whether these two innovations really contribute to countering hybrid threats.
    - Nevertheless, their score on implementation is on average when compared to the others, which implies that it is worthwhile to investigate the take up of these innovations in a later stage, once we have improved (if possible) the description and scoping of these innovations. The scoping might also lead to a higher impact.

6 RESULTS AND RECOMMENDATIONS FOR OTHER WORK PACKAGES

6.1 RECOMMENDATIONS FOR TASK 3.2 IN THE 2ND PROJECT CYCLE

As stipulated in the previous chapters and sections, the 6 best assessed innovations will be taken up for further recommendations in WP4. In the next section we will further elaborate this.

For the other 21 innovations we do recommend the following.

The 9 innovations that meet the primary threshold but not the secondary threshold will be further examined and improved by Task 3.2 during the 2nd project cycle. These 9 innovations proved to be promising and did achieve relatively high average scores but did get also (only) 1 or 2 individual low scores out of 9 total individual scores. The latter implies that there are some minor issues that should be tackled and probably solved in the next iteration (cycle).

The table below include the 9 innovations that should considered once again in Task 3.2 during the 2nd project cycle, and updated accordingly to the improvement areas and recommendations that are provided in the right column of the table. In order to improve innovations, it might be wise to involve practitioners and/or solution providers. They probably can add additional information and specifications to the innovations. Whether these innovations will then be fed back to T3.1 for a renewed assessment is up to Task 3.2. If it is not possible to improve an innovation, then that innovation will be not further processed anymore. Otherwise a re-assessment will take place in Task 3.1 during the 2nd project cycle.

Non-selected innovations that will be fed back into T3.2 during the 2nd project cycle	**Improvement area and recommendations**
Government & social media cooperation framework in countering election interference	This solution is deemed to be useful for the very specific problem of election interference, which could overall improve democratic institutions and enhance societal resilience. However it is very dependent on the cooperation of social media companies. In addition such efforts are strongly limited by the amount of resources that social media companies and governments are able and willing to invest. As such a waterbed effect might occur where the protection of some countries' election processes may be protected at the cost of exposing other countries as relatively more vulnerable. Standardization and international cooperative frameworks could be useful in addressing this shortcoming. Lastly this type of government oversight of social media content may not be accepted by society. This issue of societal acceptance needs to be addressed.
Training application for media literacy	There is a clear European consensus that media literacy needs to be improved. This solution is one amongst many that could help facilitate such improvements. However the descriptions for implementation fall short. Conceptually, the idea is interesting and useful yet concrete ideas on how to implement such a training application amongst the various member states and their citizens remains unclear.
Hybrid online dilemma game	Overall this solution is deemed to be useful and effective, but limited in scope. Given that the hybrid online dilemma game is focused on improving awareness of hybrid threats for practitioners across disciplines

	in a whole-of-society approach, it might be an impetus for follow-up improvements with the relevant practitioners and stakeholders. However the value of the dilemma game itself is expected to be limited, mostly to raising awareness on hybrid threats, rather than a solution to hybrid threat itself. Further specification on the contributions to improving resilience could be useful.
Automated detection of hate speech in social media	The idea of the solution is clear. However there are major ethical, legal, and implementation challenges that are not addressed. Such hurdles include the allocation of powers who gets to decide what might constitute as hate speech versus what is considered to be free speech. The variation of interpretation and definitions of hate speech between the different Member States are not addressed. This type of solution tends to focus on quantity over relative impact of possible hateful speech. Maintenance of keeping such automated detection programs up-to-date is not considered. These are major challenges to any kind of further scrutiny for development and uptake.
Establish Data Embassies or E-embassies	The establishment of Data Embassies is deemed to be a useful solution, but very limited in scope. It only addresses a very narrow set of challenges within the data, information and cyber domains; namely the establishment of data redundancies in case of widespread cyber attacks on a single nation. In addition there are some concerns about the robustness of the solution. The selection of the Host Nation of such Data Embassies could make those specific countries a more interesting target, creating a greater potential vulnerability into a select few countries. Both concerns are somewhat inherent to the proposed solution, which makes the space for improvement limited.
European Smart and Sustainable City Award	Whilst this award could help incentivize the sustainable development of cities, it remains unclear how this progress would then be maintained in the longer run. In addition the proposed solution pertains to a very limited scope of improvement, which in and of itself is unclear how it would improve societal resilience against hybrid threats. As such, whilst the proposed solution might be helpful in improving urban life in cities, the long term applicability to improving resilience against hybrid threats needs to be improved.
Factcheckers communities	There are some methodological flaws and there is a clear potential to be infiltrated and discredited. This makes fact checker communities vulnerable to changes, attacks and trust questions. Discrepancies between responsibility and competences can discredit the whole effect of the solution, the availability of guides or practices criteria could also make information manipulation easier and less counterable. There is a clear potential for this solution to be counterproductive as it could diminish the added value of journalism as a profession. In addition the success of this solution is dependent on public acceptance; as of yet it is unclear what a minimal threshold of public acceptance would be for this platform to be effective, nor how it would reach such a level of acceptance and trust. The question how the internal reporting of fake news of social media platforms like Facebook or Twitter can be structured and assessed remains unanswered.
Journalism trust initiative	Whilst this solution is deemed to be effective in improving journalistic practices and standards, the specific links to improving resilience against hybrid threats needs to improved. This solution in faces general

	challenges when it comes to checking and regulating journalistic content, such as obtaining and maintaining a minimal level of public trust and acceptance.
A Quantum-Resistant Trusted Platform Module	The intended effects of this solution are well defined. Whilst the scope of this solution is rather limited, it could serve as an enabler for further improvements towards societal resilience in related domains. The innovation itself faces some hurdles in available information, given its low TRL and general early stages of research into quantum computing. The impact of this solution for practitioners and end-users should be defined better to clarify the possible implications in relation to improving societal resilience against hybrid threats.

Table 7: Overview of innovations that might get a second chance in the next cycle if improved accordingly.

A total of 12 innovations did not meet both primary and secondary thresholds. However, these 12 might have some potential, and might have even better potential due to ongoing technological developments by the next cycle. **We recommend to keep these 12 innovations in the Innovation Arena, and thereby serving as inspiration when looking for innovations during the 2nd project cycle.** We think that some of these innovations can be improved or adapted by providing more detailed and focused information on one or more dimensions, as well as progression in the development of these innovations. Some of these innovations might even appear to be (when improved) suitable solutions for newly identified gaps and needs during the 2nd project cycle.

In the table below the 12 innovations that are not selected for uptake in WP4 or re-examination in Task 3.2 during the second cycle, but be kept in the Innovation Arena, are listed, including their shortfalls on the assessment criteria.

Non-selected innovations that will be kept in the Innovation Arena for further inspiration	Shortfalls on assessment criteria
Tools monitoring population's response to information	Implementation and overall score
Non-partisan native-language news channels for most interdependent abroad regions	Implementation
Fair Trade Data Program	Overall score
Generic Operational Scenarios	Overall score
Automated fact-checker	Excellence, impact, implementation and overall score
Open European Quantum Key Distribution Testbed	Excellence, Impact, Implementation, overall score
Efficient cyber threat information sharing through Hyper Connectivity networks	Missing essential information
Resilient democracy infrastructure platform	Excellence, Impact, Implementation, and overall score
Early/Rapid damage assessment system	Not considered as specific hybrid solution
Smart message system for sharing interagency OP	Overall score
A crawler and real-time search engine for investors	Excellence and Impact

A blockchain-based real-time information management and monitoring system	Overall score

Table 8: Non-selected innovations but still be kept in the Innovation Arena.

6.2 RECOMMENDATIONS FOR WP4

WP4 will address the uptake of the innovations, which include topics like standards, legal and ethical issues, and procurement strategies. Therefore, in this section we will come up with recommendations that relate to these topics and that will include some other considerations. We will use a synthesis of recommendations made by the assessors for the 6 best assessed innovations. Additionally, we will provide general recommendations for all 4 target areas, which are derived from the analysis of all 15 promising innovations in previous chapters and sections.

For a clear understanding of all 27 innovations, see their description in Annex V.

6.2.1 CITIZEN AND GOVERNMENTAL RESILIENCE

General recommendations

- Although we have built up a lot of experience in election interference, and especially in how to prevent it, this is still a major threat and risk, which can stress our democratic system. Therefore, we should be keen on identifying innovative solutions to strengthen our democracy (systems, processes, structures etc.) and raise awareness at citizen level about the stakes at risk. Although an improved citizen-government relation and trust is the basis for this, we have seen that many innovations that might play a role in this, have their drawbacks. Concerns about privacy, about a too centralised government approach and about influencing temper the value and expectations of these innovations.
- Innovations that might work in improving this very delicate citizen-government relationship and trust building do have some elements in common:
    - The citizen-government relationship is an area of active and productive research but rather fragmented, and needs therefore further research and focus (trust building, societal dialogue, social cohesion, consensus building etc.).
    - Education and training are elementary elements, and should already being started at the primary schools, e.g. about media literacy, democratic values, history, new technology (and its impact on our society).
    - Citizen-involvement is a prerequisite, e.g. in the development of tools like the fair-trade data program, in which citizens become more responsible for sharing (and selling) their own data.

6.2.2 INFRASTRUCTURE AND FLOWS

General recommendations

- Critical infrastructure and flows are vulnerable and therefore hot spot targets for hybrid actors. Most of the vulnerabilities are within the Cyber domain, and therefore require innovative solutions that can deal with cyber-attacks in order to mitigate or even neutralise the effect of such attacks.

For some of these types of innovations we refer to the innovations and recommendations provided in the target area Cyber and Quantum security.

- Apart from the cyber (and quantum) related vulnerabilities, other vulnerabilities and corresponding threats need to be further considered and investigated. Some venues for further research are:
  - Foreign and private investments in critical infrastructure and flows leading to spying, intrusion, hacking and also coercion. Therefore, screening of investments and risk assessment is required.
  - The massive grow of the Internet-of-Things will lead to even smarter but also more vulnerable cities. This requires risk assessment, chain analysis (weak links) and might lead to independent auditing and evaluation to keep cities aware of the risks and the necessary measures.
  - More attention for back-up and graceful degradation alternatives in case of a total system lock down (back up storage of data, alternative routes of supply, etc.) is needed. Better understanding and using supply chain risk management can be very beneficial.
  - And last but not least, in the next cycle we should also look into specific and other domains in which the occurrence of hybrid threats will become more likely in the (near) future. One might think of the space domain and in particular our dependence and hence vulnerability of satellites. But also the mobility and transport sector is a relevant domain, which is already heavily affected by the Covid-crisis and is therefore more vulnerable than ever before.

6.2.3 DISINFORMATION

Innovation “Fake news exposer”

- Privacy, integrity, transparency of algorithms might be an issue. This might hamper the public acceptance of this type of innovation. Therefore, it is advised to do more experimentation, validation and testing in approved laboratories, which ultimately will contribute to more credibility of such tools. Additionally, standards for the aforementioned issues might need to be in place before using these tools.
- There is a potential added value of public-private partnerships for co-creation of these tools. Tools that are only commercially driven might be sensitive to misfunctioning.
- To enhance the wide use of these tools (e.g. within the EU) the linguistic challenge should be addressed. The current scope seems to be directed at text, but a grow path to expose also fake images and videos should be included in the development and procurement strategy.

Innovation “Debunking of fake news”

- To a great extent the recommendations defined for the fake news exposer also apply to this innovation.
- In addition, it should be made clear how and by whom this platform (DebunkEU.org) is funded. It should be independent and therefore clearly associated with a trustworthy organisation.
- The current scope is relatively narrow now, it is very much targeted at one very specific and extremely important problem and region. The solution should be scalable.

- In the development and implementation strategy attention should be paid to the overload problem. The platform could be overwhelmed by a massive amount of disinformation, this sets requirements for its robustness of operation.
- Also the role of the experts / analysts should be considered in more detail: background, training, independency, costs etc.

Innovation "Guides to identify fakes"

- The guide needs to be updated regularly, since the state-of-art and the abuse of fakes evolve. Also, adversarial learning (based on Artificial Intelligent technology) can make the process and the innovation less effective and reliable. Therefore, the development and implementation strategies need to consider how the maintenance is organised and what are the maintenance costs.

Innovation "Countering disinformation with strategic personalized advertising"

- An EU wide solution is preferred but does pose severe challenges to get this implemented at national level. Due to e.g. cultural differences, it will be difficult to find one coherent approach. Hence, this requires a lot of testing and tailoring before ready to use.
- Although the idea is conceptually good ("using Cambridge Analytics for good purposes"), it could face a lot of scepticism and criticism. It even could backfire and diminish trust in government and institutions. Therefore it is recommended to perform more human behavioural research before taking up this innovation.

General recommendations

- No others than the ones already addressed above.

6.2.4 CYBER AND QUANTUM SECURITY

Innovation "Cross sector cyber threat information sharing"

- Acceptance of practitioners and end-users might be a problem due to not willing to share this type of information. It requires a high level of trust amongst partners involved. Probably starting on a small scale (specific nation, domain) with finally showing very good results could lead to a stepping stone for others.
- It is foreseen that the development of this technological solution requires a high amount of resources and funding. Together with the previous recommendation this requires a thorough roadmap in which the technological feasibility, costing and upscaling is described.

Innovation "Public-private information-sharing groups developing collaborative investigations and collective action"

- Actually, the same recommendations apply as for the previous innovation. In addition, the public-private construct even poses extra challenges, like privacy and security concerns. Therefore, this innovation should probably be considered as a next generation innovation once the previous innovation has shown its benefits. This could be included in the roadmap that was recommended for the previous innovation.

General recommendations

- We should stop to treat cyber security as a pure technical topic. Improvement of cyber security throughout our whole society requires more than just technology. The human and organisational dimension is just as important. Therefore, we should take these dimensions into account when designing cyber security solutions.
- We already have to look beyond the traditional cyber security. Although quantum technology is still at low TRL, it will be a future threat to the current encryption. And thus do we need to make systems that use current encryption quantum-safe. Therefore, we should start with thinking and working on guidance and regulations to ensure that critical systems will be quantum-safe in the future.

7 OVERVIEW OF FINAL DOWNSELECTION AND PRIORITIZATION OF INNOVATIONS

The process and methodology of assessment, down-selection and categorization of the initial 27 innovations has led to several recommendations and follow-on activities. In the figure below a clear overview of all steps (including related results) is provided.

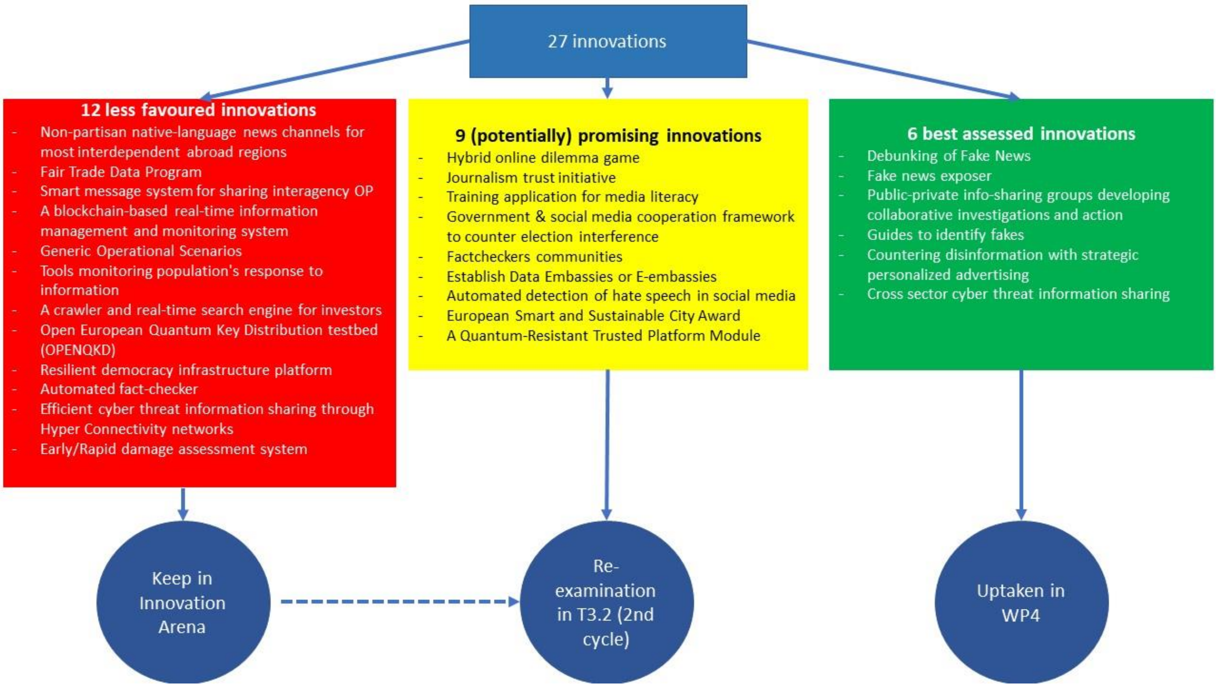

27 innovations
12 less favoured innovations
- Non-partisan native-language news channels for most interdependent abroad regions
- Fair Trade Data Program
- Smart message system for sharing interagency OP
- A blockchain-based real-time information management and monitoring system
- Generic Operational Scenarios
- Tools monitoring population's response to information
- A crawler and real-time search engine for investors
- Open European Quantum Key Distribution testbed (OPENQKD)
- Resilient democracy infrastructure platform
- Automated fact-checker
- Efficient cyber threat information sharing through Hyper Connectivity networks
- Early/Rapid damage assessment system
9 (potentially) promising innovations
- Hybrid online dilemma game
- Journalism trust initiative
- Training application for media literacy
- Government & social media cooperation framework to counter election interference
- Factcheckers communities
- Establish Data Embassies or E-embassies
- Automated detection of hate speech in social media
- European Smart and Sustainable City Award
- A Quantum-Resistant Trusted Platform Module
6 best assessed innovations
- Debunking of Fake News
- Fake news exposer
- Public-private info-sharing groups developing collaborative investigations and action
- Guides to identify fakes
- Countering disinformation with strategic personalized advertising
- Cross sector cyber threat information sharing
Keep in Innovation Arena
Re-examination in T3.2 (2nd cycle)
Uptaken in WP4

Figure 6: Overview of final results and follow-on activities

The 6 innovations that do meet the primary and secondary threshold, implying that the overall score is at least a 10 (on a scale from 0-15), and all individual scores do not get below 3 (on a scale from 0-5) are considered to be the best assessed innovations. Therefore these innovations will be passed to WP4 (in particular Task 4.2) for developing uptake strategies.

The 9 promising innovations (meeting the primary threshold but still achieving 1 or 2 scores below 3) will be re-examined by Task 3.2 during then 2nd cycle, in order to see of some of these innovations can be improved (adding information, detailing descriptions, etc.) and can therefore achieve better assessment results, and lifting them up to the highest category (best assessed innovations).

The 12 innovations that do not meet both thresholds and are assessed as being less favored innovations will be kept in the Innovation Arena during the entire project duration. This might lead to new inspiration and to, possibly, adapting these innovations to newer or better ones. This can be done by everyone who has access to the Innovation Arena. Also the partners working at Task 3.2 can do so in the next cycles (this is illustrated by the dotted line).

8 LESSONS LEARNED

During this first project cycle we have identified the following lessons learned:

- **Analyzing gaps and needs in all 13 JRC domains.** In the first cycle the identified gaps and needs did not cover potential gaps and needs in all 13 JRC domains. Whilst the focus of any project cycle may differ, it is recommended to Task 2.1 to look at the various gaps and needs in all domains, in order to cover all potential vulnerabilities. The Core Themes to some extent give a cross-domain focus, which is somewhat restrictive of in-depth analysis of domains that are not covered as much by these Core Themes.

- **Identifying solutions in all 13 JRC domains.** As with the lack of coverage of all 13 JRC domains in the identification of gaps and needs across all 13 domains, the identified innovations and solutions did not cover all 13 JRC domains. This is a natural consequence of the lack of coverage of all 13 JRC domains in the gaps and needs, given that the identification of potential innovations and solutions was based on the previously identified gaps and needs.

- **The role of Task 3.3 needs to be clarified and integrated.** Task 3.3 focused on the identification of relevant research projects. Some attention was given on specific innovations, which led to some overlap with Task 3.2. This has complicated the distinction between Tasks 3.2 and 3.3, and their respective roles within WP3 and the integration into Task 3.1. The effort to clarify the role of Task 3.3 will need to be done in close coordination with WPs 2 and 3 and Task 4.1.

- **Revision of the Task 3.1 template.** The use of the Task 3.1 template was experienced as a useful format to structure the required information to be collected on the potential innovations and solutions. However, the template did not always lend itself to the types of information that is relevant for the various solutions and innovations. For example the more personnel and organizational solutions are not as easily described in regard to their TRL or costs. Differentiation of templates for the strongly diverging technical, societal, human, and organizational innovations and/or solutions could help tailor enable a better identification of potential solutions and facilitate better information collection. In a similar fashion it might be useful to make a separate template specific to the work on research project monitoring for Task 3.3. Improvements are warranted to optimize the utility of the Task 3.1 template. Such efforts will be done in close coordination with Tasks 3.2, 3.3 and 4.1.

- **The process of collecting information needs to be streamlined**. In chapter 3.1 we explained how the quality and completeness of the filled in Task 3.1 templates differed. It is warranted to clarify the process of information collection to prevent additional workload of requesting additional information. This may be integrated in the improvement of the Task 3.1 template. Given that the partners are now familiar with the process, this issue might be less prevalent in the next cycles.

- **Identifying out-of-the-box innovations and solutions.** In the current process, the identification of gaps and needs determines the types of innovations and solutions to be identified in Task 3.2. This creates a rigid process of finding specific solutions to identified gaps and needs. This enables the identification of solutions fit-for-purpose. However, it mitigates the possibility to identify potential innovations and solutions that are not linked to any gaps and needs, which excludes the potential inclusion of out-of-the-box solutions. The next project cycles could benefit from expanding the process to include the possibility to identify such solutions. The Future Trends Workshops could provide an additional specific avenue for the identification and integration of out-of-the-box innovations and solutions.

- **Terminology of hybrid threats**. In the first cycle of the project and in this specific report, innovations are brought into relation with their potential to provide resilience against hybrid threats as a whole. Whilst the core idea is solid, it might lead to misunderstandings that some narrow solutions to very specific, limited problems might not be broad enough to be deemed as contributing to the conceptually holistic challenge of hybrid threats. It might be useful to re-examine our understanding of and approach to hybrid threats. It could be beneficial to frame specific solutions against threats that may be part of a broader hybrid campaign. This would facilitate an easier integration of more narrow solutions to more limited problems within the broader improvement of societal resilience against hybrid threats.

- **The chronology of evaluation of innovations in Task 3.1 and its relation to Tasks 2.3 and 2.4.** In the first cycle Task T2.4 selected the most relevant innovations and solutions from Tasks 3.2 and 3.3, as related to the specific scenario and vignettes developed by Task 2.3. This has entailed that some innovations have been tested within Task 2.4 that in a subsequent stage within Task 3.1 were evaluated to be less useful than other innovations and solutions. Likewise, some innovations that Task 3.1 deemed to be more useful than other innovations and solutions were not tested within Task 2.4 as it was less applicable to the scenario and vignettes as developed within Task 2.3. It might be useful to re-examine the project planning and execute the Task 3.1 evaluation of the identified innovations from Tasks 3.2 and 3.3 before the development of the scenario and vignettes in Task 2.3 and the testing of innovations within Task 2.4. As such the project could focus on testing the most useful and relevant innovations as concluded in Task 3.1. This could also bring about new challenges, such as overlooking the potential of innovations and solutions that might be at a very low TRL, which would make them score lower within the evaluations of Task 3.1, but could still be very interesting to test within an operational setting in Task 2.4. In addition the preselection of most potent solutions and innovations could give a bias in the development of the scenario's and vignettes within Task 2.3 and the testing of the innovations within Task 2.4. This approach has been suggested during a HOTWASH and was well received. It will require further examination and discussion as to whether this approach would be more beneficial than the one that was followed in the first cycle.

- **Added value of Target Areas.** In the DoA we used the term Target Areas without fully knowing the meaning, implication and use of Target Areas. Although we managed to come up with a proper definition, the overlap and therefore ambiguity between target areas and core themes could complicate our project. It is therefore recommended to re-assess the use of Target Areas, and to decide whether target areas and core themes can co-exist. One reason for co-existence might be that Target Areas can be flexibly defined during the project and could therefore provide additional room and inspiration for identifying relevant innovations that do not fit in one of the 4 core themes.

9 CONTRIBUTION TO PROJECT OBJECTIVES AND LINES OF ACTION

The D3.1 deliverable contributes to some of the overall Project Objectives (OB) defined in the DoA. In the table below the most significant contributions related to OBs and their relevant Key Performance Indicators (KPI) are listed.

OB.4. To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats		
Goal	KPI description and target value	Contribution by Task 3.1
4.1: To compile recommendations for uptake/industrialisation of innovation outputs (incl. social/non-technical); and provide opportunities for greater involvement from public procurement bodies upstream in the innovation cycle	Appraise best innovations (technical/human science based) for standardisation and innovation uptake, especially industrialisation and procurement. Targets: - At least 3 reports targeting areas for improvement (potentially ground-breaking innovations mapped on gaps and needs) - A list of final recommendations for procurement and/or industrialisation	- 4 target areas for new innovations have been identified and described - For each target area recommendations for development, procurement and implementation have been defined - For 6 specific innovations recommendations for development, procurement and implementation have been defined
4.3: To develop a mapping matrix connecting gaps and needs of European actors to areas that highlight the most promising innovations	The matrix is constructed so that innovations match European actors' gaps and needs in different domains Targets: - Mapping matrix is submitted for analysis to support innovations defined precisely to meet requirements for uptake	- The mapping of 27 innovations on the 12 gaps and needs has been established - All 27 innovations have been assessed in such a way that the most promising (15 in total) have been identified - For all innovations recommendations for improvement (description, usefulness and implementation) have been provided

OB5: To establish conditions for enhanced interaction with practitioners, industry and academia for meaningful dialogue and for increasing membership in the network		
Goal	KPI description and target value	Contribution by Task 3.1
5.1: To establish a platform for information exchange through an Innovation Arena, along with an associated web site	Innovation Arena (IA) supporting research and innovation; and a website for networking Targets: - At least 30 new users of the Innovation arena (IA) yearly	- All 27 innovations have been integrated in Innovation Arena - All 25 consortium partners have been involved in the assessment of the 27 innovations, supported by IA and the consortium sharepoint

OB7: To create a basis for establishing effective synergies with existing European, national and sub-national networks of practitioners and other actors countering hybrid threats		
Goal	KPI description and target value	Contribution by Task 3.1
7.2: To empower European practitioners, industry, SME and academic actors to recognise important innovations/trends	Events are organised on innovations and future trends Targets: - At least 2 events yearly where information on innovations and future trends is shared	- During the IKEW (Information and Knowledge Exchange Workshop) in January 2021 the mapping of the innovations on gaps and needs including a preliminary analysis has been presented

Table 9: Deliverable 3.1 contribution to project objectives and KPIs.

Next to the OBs the EU HYBNET consortium decided on request of the EC to also report on three Lines of Action. Each deliverable should therefore state its contribution to these Lines of Action in order to highlight the importance of the work conducted in the deliverable to the whole success and proceeding of the project. In the table below D3.1's contribution to the three Lines of Action is provided.

Lines of Action	**D3.1 contribution**
Monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results	• Task 3.1 has drawn from the work of Tasks 3.2 and 3.3 which were responsible for the identification of solutions, innovations, research, and innovation projects that might have potential to help counter hybrid threats. As such Task 3.1's work is founded on this Line of Action and builds on it for the research and innovations projects that are monitored to be leveraged, recommended for uptake and eventually exploited by the EU and its member states to improve their resilience against hybrid threats. • 27 innovations (or innovative solutions) for countering hybrid threats have been identified and reviewed. All 27 innovations have been integrated in the Innovation Arena platform and are accessible to the consortium partners and stakeholders. • Out of these 27 innovations 15 innovations have been assessed as promising based on assessment and review input from different experts and stakeholders. Out of these 15 innovations 6 have been selected and recommended for further processing and uptake in WP4.
Common requirements as regards innovations that could fill in gaps and needs	• Although many innovations do have significant potential in countering hybrid threats, some implementation and exploitation problems are foreseen. Most of the problems, leading to potential restrictions for using and applying these innovations, refer to ethical, legal and public acceptance issues. So, apart from defining and designing innovations that CAN contribute to counter hybrid threats, it is essential and critical to also consider whether these innovations are also legally ALLOWED to be employed, and whether member states and the EU are WILLING to employ these based on ethical considerations. For those innovations that face these challenges, the D3.1 deliverable has indicated the specific concerns, which need to be further addressed in WP4 and probably the next cycles.

Priorities as regards of increasing knowledge and performance requiring standardisation	• Based on the first cycle of identifying innovations it has become clear that specific target areas get a high priority when looking into the combination of gaps and needs and potential solutions for those gaps and needs. T3.1 has therefore identified and prioritised the following target areas when it comes to increasing knowledge and performance: (1) Citizen and Governmental Resilience, (2) Critical Infrastructure and Flows, (3) Disinformation, and (4) Cyber and Quantum security. • For the next cycle it is recommended to envisage other/new trends that probably will justify another target area (e.g. threats against satellites), reflecting the coverage of other domains that were not extensively covered in the first cycle.

Table 10: Deliverable 3.1 contribution to Lines of Action

10 CONCLUSIONS AND RECOMMENDATIONS

The focus of task 3.1 has been on identifying target areas and selecting specific innovations, which are very promising in countering hybrid threats. The selection of both target areas and innovations has been based on a down-selection and assessment process and methodology. In order to support WP4 in the further uptake of the selected target areas and innovations, recommendations with respect to procurement and implementation strategies, legislation and costing have been provided.

Summarizing the main conclusions and recommendations can be split up in 4 elements:

- Assessment and selection of innovations;
- Definition of target areas;
- The process and methodology used;
- Improvements for next cycle.

<u>Assessment and selection of innovations:</u>

- The following 6 innovations have been assessed as high potential innovations and will be forwarded to WP4 for further uptake:
    - Debunking of Fake News
    - Fake news exposer
    - Public-private info-sharing groups developing collaborative investigations and action
    - Guides to identify fakes
    - Countering disinformation with strategic personalized advertising
    - Cross sector cyber threat information sharing
- There are 9 other innovations that seem to be promising but do require some additional information and examination. It is expected that some of these innovations will have experienced some progress in their development to the extent where they will be evaluated at a better level in the next project cycle. This will be done in Task 3.2 during the 2nd project cycle. The ones that can be improved to such a level that they will pass the requirements and criteria, will then be part again of a broader assessment and down-selection in Task 3.1 during the 2nd project cycle.
- There are 12 innovations that have some major insufficiencies. These innovations still have potential for use in future project cycles, but would require a limited evaluation in the next cycle as to how far these innovations have progressed and whether these innovations can be deemed to have progressed to such an extent that they should be included into the full examination and evaluation in the 2nd project cycle. Irrespective of the outcome, these innovations will be kept in the Innovation Arena platform, and might serve further inspiration in the next cycles.
- It is observed that innovations that contribute to debunking and countering fake news (disinformation) score very high and seem to have the highest potential for uptaking.
- For many innovations some implementation and exploitation problems are foreseen. Most of the problems, leading to potential restrictions for using and applying these innovations, refer to ethical, legal and public acceptance issues. So, apart from defining and designing innovations that can contribute to counter hybrid threats, it is essential and critical to also consider whether these innovations are also legally allowed to be employed, and whether member states and the EU are willing to employ these based on ethical considerations.

<u>Definition of target areas:</u>

- A target area is considered to be a cluster of equivalent and coherent innovative solutions for a specific domain and/or vulnerability. Target areas serve (reason-to-be) as a guidance for WP4 to look for standards and best practices in order to foster the development and implementation of like-wise innovations.
- The following 4 target areas have been identified during this first cycle:
    - Citizen and Governmental Resilience
    - Critical Infrastructure and Flows
    - Disinformation
    - Cyber and Quantum security
- It is recommended for the next cycle to look for additional target areas. It is expected that gaps and needs and corresponding solutions can be identified in other domains and/or for other vulnerabilities. Some cues to look into other/new directions are:
    - Current focus was strongly on Cyber and ICT innovations, we should also look for other innovations, e.g. related to human factors, space.
    - Most innovations tend towards short term availability. We should not forget to look at more disruptive innovations, using technology that is still under development.

The process and methodology:

- The process used for assessment, which included a scoring methodology on Excellence, Impact and Implementation in combination with thresholds as minimum requirements, proved suitable to rank and select innovations.
- In the process all consortium partner have been involved, leading to a balanced set of scores, and next to that, to a better familiarisation of all innovations amongst all partners.
- Nevertheless, some improvements for the process and methodology might be useful. First of all, the templates used for describing all the innovations will be slightly adapted, so that more focussed and meaningful information can be extracted (e.g. data concerning cost drivers and robustness of innovations were difficult to get). And secondly, it is worthwhile to increase the number of partners that do assess a single innovation. This was now 3-4, but we should try to raise this up to 5.

Improvements for the next cycle:

- The interrelation and alignment on both input/output and time synchronization between Tasks 2.3, 2.4, 3.1, 3.2 and 3.3 might be improved. Innovations that have been tested in 2.4 did not fully make use of the assessment and recommendations that were produced in 3.1, since the timing did not allow this. The parallel execution of 3.2 and 3.3 did made it difficult for 3.1 to align the results from both tasks and in particular to fully exploit the 3.3 results.
- The template developed in 3.1 for describing and characterising the innovations needs to be improved to some extent. This would enable a better description and hence assessment of the innovations. Additionally it would streamline the collection of information much better and thereby making this activity and process more efficient.
- In the DoA we used the term Target Areas without fully knowing the meaning, implication and use of Target Areas. Although we managed to come up with a proper definition, the overlap and therefore ambiguity between target areas and core themes could complicate our project. It is therefore recommended to re-assess the use of Target Areas, and to decide whether target areas and core themes can co-exist.

11 ANNEXES

11.1 ANNEX I: BRIEF SUMMARY OF INNOVATION AND RESEARCH MONITORING

In the table below a brief summary of the Task 3.3 (Innovation and Research Project Monitoring) results is provided. For a detailed overview of the results, see Deliverable D3.7.

Core Theme: Resilient civilians, local level and administration	
Primary Context	**Observations/ findings**
Distrust and stress in political decisionmaking	• The field of Governmental trust building, and situational awareness is rather active and productive, but rather fragmented. • trust building, societal dialogue and consensus building are primary focus areas for further research of phenomena and provision of methods and tools. • Multi stakeholder situational awareness building and protected, well informed and unified decision making is much more advanced and gains more attention in research and implementation domains.
Resilience on critical services and tech systems	• Better understanding of Supply chain risk management (SCRM) requires multilevel modelling approach: combination of Discrete Event Simulation and System Dynamics is used at the different levels of the simulation model. • The main problem of this situation is that cyber security is still usually treated as a technical aspect or technology which can be easily implemented inside the organization and this implementation will guarantee cyber security. This attitude must change, because cyber security nowadays is something more than just the technology. • E-commerce is reshaping business practices and education, yet many have expressed concern over the e-commerce education and training provided to students.
Globalization vs localization	• Inclusiveness of minorities: Ensuring easy access to health services, especially mental health care services for ethnic minorities is seen critical to ensure that minorities are not forgotten in the societies' basic services. • The main observation is that many initiatives are dedicated to helping cities around the world become more resilient to the physical, social and economic challenges that current societies face. There is growing evidence that social infrastructure, as opposed to physical and economical infrastructure, drives social resilience. Fostering social cohesion in cities means creating societies where people can live together with all their differences. A solution is a framework to characterize social cohesion and help promote resilient cities, i.e. to help identify levels and possible factors related to cohesion, which need to be taken into account to help design interventions for cities to become more sustainable and resilient. • More positive inter-group contact in local level is to diminish lack of trust between different actors and decrease intolerance. The

	cohesion reduces attempts to destabilize local communities. This provides more stable basis for national administration to work as well. • Civil-military cooperation is seen as a key to resilience against hybrid threats; especially in the case to prevent citizens to be targeted as actors who destabilize coherence in society. In the context of the civil-military cooperation, one can also refer to the concept of “total defense” where the citizens are an important actor next to military to provide security in national level. In this case civilians are seen as active actors to provide defense and security to state next to military.
General	• In this research context innovations that can be considered as solutions for the need are more often non-technical/ social science based, policy initiatives and concepts rather than technical. Still the technical solutions may have significant role especially in information sharing, information analysis and delivering services.
Core Theme: Cyber and Future Technologies	
Primary Context	**Observations/ findings**
Game changers: Quantum as disruptive technology	• the field of post quantum cryptography research is very active and productive, international standardization bodies recognize need and considerable maturity of the post quantum cryptography, so standardization efforts are well on the way. • that there is a clear lack of widely available guidance and regulations, which would govern how to ensure that critical applications built today would-be quantum-safe (or upgrade-ready). • Our research and innovation scanning revealed no research on post-quantum protection of the legacy systems.
Hyperconnectivity as impact multiplier of cyber	• In this orientation, development of a European cybersecurity crisis cooperation framework is still a work in progress. The EU’s scope to act to cyberattacks at the operational and political level in the happening of a large-scale, cross-border incident has been characterized “limited”, partly because cybersecurity is not yet integrated into existing EU-level crisis response coordination mechanisms. • From the academia side, models are analyzed to foresee zero-day vulnerabilities. These models are formulated into three noticeable forecast model suites, and they are currently being applied at the global and category (web browser, operating system, and video player) levels. The accomplishment of some of these forecast models have been assessed and the outcomes display promise for future use of these models. Future development of these models will include a consensus forecast model that integrates the individual models into a larger model with better long-term accuracy. These models should also be extended and adapted to forecast vulnerabilities at the software application and be applied also to level multi-version software.

Individual as digital entity	• To conclude, the problem of detecting a deep fake is an active research area, but as deep fake technologies evolve so must the detection methods. Working methods have been developed and are used in practice but there are no published standards or generic services. The problem of relating a deep fake to its original media is an area where less information has been found, but this problem may be of less importance in a fake news context as trust will gone if it becomes known that the content is doctored.

Core theme: Information and StratCom	
Primary Context	**Observations/ findings**
Going viral	• Missing of a general concept to reduce the spread of manipulated information. Fundamental questions: how do we create the news ecosystem and culture that values and promotes truth? Need for an international action rather than a national action • Future research should further explore the various impacts of manipulated information. The negative impact is currently assumed, rightly so, but a closer examination of the various negative effects of manipulated information can better guide initiatives to combat it. For example, while manipulated information derives part of its ability to fool individuals by mimicking the look and feel of real information, no systematic analysis of its effect on real information perceptions has been conducted.
Digital monopolies and massification of data	• The problem of controlling collection and use of big data must be seen as more of a regulatory problem than a technical one. Possible means to limit which data is collected, how it is used, for what purpose, and how it is traded should be researched.
Deterioration of the quality of Content	• The research scan revealed that main efforts in the journalistic content evaluation is dedicated to fact-checking claims. A number of organizational and technical solutions were deployed and are functioning, using mix of technical solutions (e.g. natural language processing, artificial intelligence, machine learning, etc) and human intervention. At the present time it is a quite mature field both organizationally and technologically. • Still the impact of fact-checking to public opinion remains the object of discussion. Some studies indicate that fact-checks can reduce misperceptions, but most often fact-checking has no significant impact on vote choice or candidate selection. So more of the research and practical testing is needed to: o further elaborate techniques for automated fact-checking, approaching near-real-time fact-checking, o ensure unbiased result of fact-checking, o tracing real source of the claim

	○ understand better how fact-checking impacts or fails to impact consumers' perceptions
Core theme: Future Trends of Hybrid Threats	
Primary Context	**Observations/ findings**
Official StratCom losing power	• Overall the subject as is described is very complex, built of numerous phenomena and influencing factors. So research is not addressing the phenomena as such, but rather focusses into specific areas (like relationship between transparency and efficiency of organization). Application of research in the political communication is even less common.
Big data as new power source	• As a discussion point, the matter of data-driven micro-targeting, especially connected to political campaigning has gained prominence in recent years, both academically and in the wider public domain. The criticism of Social Media and tech giants; namely Facebook, Twitter and Google are central to the dialogue. Papers and research have been growing since the aforementioned elections of 2016, but the release of The Social Dilemma and The Great Hack has pushed the topic higher on the agenda of public issues and concerns. • From the initial analysis, there does not appear to be many tools aimed at countering micro-targeting. Although, as we have seen, there are efforts to counter malicious content, misinformation, fake news, etc. However, there isn't a direct correlation between micro-targeting and the former threats, although micro-targeting, viral content and advertising exacerbate their impact. • Review of the scientific publications and research projects reveal that most of the publications concern the political micro-targeting which is threatening media pluralism and democracy at a global level.
Increasing strategic dependency of critical services	• From the initial research, there are no clear tools that support the ongoing analysis of the risks associated with FDI. Much of the discussion around FDI relates to the need for reciprocal relations and the avoidance of market imbalances. Also, with the increased scrutiny of foreign investments; better transparency and awareness of events related to the three risk framework (Moran) mentioned above, could be useful to conceptualize the changing landscape.

11.2 ANNEX II: INNOVATION SCORES

In the table below all 27 innovations including their scores are presented.

All 27 Innovations	Total score	Excellence score	Impact score	Implem-ent. score
Debunking of Fake News	13,0	4,5	4,0	4,5
Fake news exposer	12,1	3,7	3,7	4,7
Hybrid online dilemma game	11,6	4,3	3,3	4,0
Public-private info-sharing groups developing collabor. Investigations & action	11,4	3,7	4,0	3,7
Journalism trust initiative	11,3	3,7	3,3	4,3
Guides to identify fakes	11,3	3,8	3,5	4,0
Countering disinformation with strategic personalized advertising	11,0	4,0	3,3	3,7
Training application for media literacy	11,0	3,5	4,0	3,5
Cross sector cyber threat information sharing	11,0	4,3	3,7	3,0
Government & social media cooperation framework to counter election interference	10,7	3,7	3,3	3,7
Factcheckers communities	10,6	3,3	4,0	3,3
Establish Data Embassies or E-embassies	10,3	3,3	3,3	3,7
Automated detection of hate speech in social media	10,1	3,8	3,3	3,0
Non-partisan native-language news channels for most interdependent abroad regions	10,1	3,8	3,8	2,5
European Smart and Sustainable City Award	10,0	3,0	3,3	3,7
A Quantum-Resistant Trusted Platform Module	10,0	3,7	3,3	3,0
Fair Trade Data Program	9,8	3,5	3,0	3,3
Smart message system for sharing interagency OP	9,7	3,0	3,7	3,0
A blockchain-based real-time information manage-ment and monitoring system	9,7	3,7	3,0	3,0
Generic Operational Scenarios	9,6	3,3	3,0	3,3
Tools monitoring population's response to information	9,3	3,3	3,3	2,7
A crawler and real-time search engine for investors	8,7	3,0	2,7	3,0
Open European Quantum Key Distribution testbed (OPENQKD)	7,9	2,3	2,8	2,8
Resilient democracy infrastructure platform	7,7	2,7	3,0	2,0
Automated fact-checker	7,3	2,5	3,0	1,8
Efficient cyber threat information sharing through Hyper Connectivity networks	N/A	N/A	N/A	N/A
Early/Rapid damage assessment system	N/A	N/A	N/A	N/A

11.3 ANNEX III: CONSORTIUM PARTNER CONTRIBUTIONS

Clusters of innovations	Specific innovations	Innovation 'initiator'	Partners assigned to Review and Data completion	Assigned assessors
Crisis Management & Critical infrastructures protection Coordination by MTES	Resilient democracy infrastructure platform	ICDS	MTES, SATWAYS, UiT	ESPOO (FI), DSB (NO), TNO (NL)
	Early/Rapid damage assessment system	SATWAYS	MTES, ICDS, UCSC	DSB (NO), TNO (NL), COMTESSA (DE)
	Smart message system for sharing interagency OP	SATWAYS	MTES, ICDS, UCSC	DSB (NO), COMTESSA (DE), KEMEA (GR)
	A blockchain-based real-time information management and monitoring system	COMTESSA	MTES, ZITIS, L3CE	PLV (ES), KEMEA (GR), TNO (NL)
	A crawler and real-time search engine for investors	COMTESSA	MTES, ZITIS, L3CE	PLV (ES), KEMEA (GR), TNO (NL)
	Establish Data Embassies or E-embassies	TNO	MTES	ESPOO (FI), COMTESSA (DE), TNO (NL)
	European Smart and Sustainable City Award	MTES	SATWAYS	ESPOO (FI), TNO (NL), PLV (ES)
Microtargeting and Influencing Coordination by TNO	Tools monitoring population's response to information	SATWAYS	TNO, URJC, UiT	ZITiS (DE), ICDS (EE), LAUREA (FI)
	Non-partisan native-language news channels for most interdependent abroad regions	L3CE	TNO, URJC, MALDITA	ICDS (EE), ZITiS (DE), UiT (NO)
	Fair Trade Data Program	SATWAYS	TNO, L3CE, URJC	LAUREA (FI), UiT (NO), ZITiS (DE)
	Countering disinformation with strategic personalized advertising	ZITIS	TNO, URJC, MALDITA	LAUREA (GE), ICDS (EE), TNO (NL)
Education and training	Training application for media literacy	ICDS	HCOE, URJC, MALDITA	UCSC (IT), MoD (NL), EOS (BE)

Coordination by HCOE	Hybrid online dilemma game	TNO	HCOE, URJC, PPHS	UCSC (IT), MoD (NL), EOS (BE)
	Generic Operational Scenarios	MTES	HCOE	UCSC (IT), MoD (NL), EOS (BE)
Disinformation Coordination by ZITIS	Fake news exposer	KEMEA	ZITIS, MALDITA	MTES (FR), URJC (ES), L3CE (LT)
	Factcheckers communities	KEMEA	ZITIS, MALDITA, UiT	HCOE (FI),JRC (BE), URJC (ES)
	Journalism trust initiative	SATWAYS	ZITIS, KEMEA, UiT	HCOE (FI), Maldita (ES), URJC (ES)
	Debunking of Fake News	L3CE	ZITIS, URJC, MALDITA	ABW (PO), MTES (FR), JRC (BE)
	Automated fact-checker	ICDS	ZITIS, MALDITA, URJC	HCOE (FI),L3CE (LT), ABW (PO)
	Guides to identify fakes	ZITIS	ZITIS, L3CE, URJC	HCOE (FI), Maldita (ES), MTES (FR)
	Automated detection of hate speech in social media	ZITIS	ZITIS, L3CE, URJC	ABW (PO),JRC (BE), Maldita (ES)
	Government & social media cooperation framework in countering election interference	HCoE	ZITIS	JRC (BE), MTES (FR), L3CE (LT)
Cyber and Quantum security Coordination by KEMEA	Open European Quantum Key Distribution testbed	L3CE	KEMEA, COMTESSA, ZITIS	RIA (EE), RISE (SE), PPHS (PO)
	A Quantum-Resistant Trusted Platform Module	L3CE	KEMEA, COMTESSA, ZITIS	RIA (EE), RISE (SE), PPHS (PO)
	Efficient cyber threat information sharing through Hyper Connectivity networks	KEMEA	KEMEA, L3CE, ZITIS	MVNIA (RO), PPHS (PO), RISE (SE)
	Cross sector cyber threat information sharing	KEMEA	KEMEA, ICDS, L3CE	MVNIA (RO), PPHS (PO), RIA (EE)

	Public-private information-sharing groups developing collaborative investigations and collective action	KEMEA	KEMEA, PPHS, ZITIS	MVNIA (RO), RISE (SE), RIA (EE)

11.4 ANNEX IV: INNOVATION TEMPLATE AND INSTRUCTIONS MANUAL

Below the template used for Task 3.1 innovation assessment, is provided. Following the template you will find a more specific description and explanation for each highlighted box.

BOX 1 NAME OF THE IDEA **DESCRIPTION OF THE IDEA**	
BOX 2 REFERENCE TO CAPABILITY GAPs/NEED **Describe the use of the solution in reference to the gaps/need** **Applicable JRC domains as stated by the gaps/need:** **Applicable core theme(s) as stated by the gap/need:**	**BOX 3 TYPE OF SOLUTION** **Technical** **Social/Human** **Organizational/Process**
BOX 4 PRACTITIONERS **Provide the applicable JRC domains for which the idea 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 end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**	
BOX 5 STATE OF THE ART **Indication of current Technology Readiness Level (TRL 1-9 index)**: **In which stage is the solution (research, technology, available innovation, proven innovation):** **Expected time to TRL-9.** **Expected time to market.**	
BOX 6 DESCRIPTION OF USE CASE(S)	

BOX 7 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**	
BOX 8 ENABLING TECHNOLOGY **Which technologies are critical in fielding the idea?**	**BOX 9 RESTRICTIONS FOR USE** **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
BOX 10 COSTS **Indication of costs**: **Differentiate if possible in development, procurement and exploitation**	**BOX 11 COUNTERMEASURES** **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?)**
BOX 12 MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide**	

Box 1:

- State the name/reference of the idea in question that is being evaluated in this template
- Give a short description of the idea

Box 2:

- Refer to the capability gaps/need, as they are delivered by the short list, long list, or master excel file
- State the JRC domains that the capability gaps/need lists as applicable domains, see the JRC domains in appendix 1 of this Annex.
- State the applicable HYBNET core themes that the capability gaps/need lists as applicable core themes, see the HYBNET core themes in appendix 2 of this Annex.

Box 3:

- State what type of solution the idea is. You may fill in 1 or more, according to need.
  - Technical solution types include software, hardware and other types of technical solutions.
  - Social/human solution types refer to solutions like training, education, behavioral sciences, etc.
  - Organizational/process solution types refer to solutions like organizational, bureaucratic or process solutions such as information sharing, coordination mechanisms, or transparency initiatives.

Box 4:

- Provide the JRC domains that the idea could be valuable, see the JRC domains in appendix 1.
- Provide as detailed as possible which level of practitioners are relevant for the use/implementation of the idea, and how they could use it. See appendix 3 of this Annex for the definition as stated in the DoA.
- Provide the expected or possible end-users that would use the idea upon acquisition and implementation, including how they would use this idea.

Box 5:

- Give an indication of the current Technology Readiness Level, see also appendix 4 of this Annex. This may be less applicable to non-technological ideas. In this case you may write “not applicable” and fill in the subsequent section within box 5 instead, see also directly below.
- Give an indication of what conceptual research stage the idea is in (exploratory research, conceptual research, trial phase, etc.).
- Provide an estimation of how long it would take for the idea to reach TRL-9, please use a range as listed below:
    - 0 (already available)
    - 0-2 years
    - 3-5 years
    - 6-10 years
    - 10-15 years
    - 20+ years
- Provide an estimation of how long it would take for the idea to become available upon the market, and thus be ready for acquisition. Please use a range as listed below:
    - 0 (already available)
    - 0-2 years
    - 3-5 years
    - 6-10 years
    - 10-15 years
    - 20+ years

Box 6:

- Provide some contemporary use cases of the idea in its current TRL. This may be less applicable for lower level TRL ideas.

Box 7:

- Provide a description of how the idea does or may contribute to countering hybrid threats, with a specific reference to the identified gaps/need.
- Can the idea be used in an offensive or defensive way to counter hybrid threats? Does it contribute to enhancing societal resilience instead? Please be as clear as possible.

Box 8:

- Are there any technologies that are critical in the fielding of this idea? If the relevant critical technology is currently available, describe how and why it is a critically enabling technology. If the technology is not yet available, describe why it is a critically enabling technology that needs to be developed prior to the fielding of this idea.

Box 9:

- Provide any possible restrictions, like judicial demands, ethical objections, financial constraints, technological limitations, security concerns, etc.

Box 10: Costs

- Provide an indication of costs. There will be a great spread in the ranges of costs between ideas. Please give an indication of the range of costs. If possible and applicable, please differentiate in costs of:
    - Research
    - Development
    - Exploitation
    - Procurement
- In your indications of costs, please provide a range:
    - 0-50k
    - 50k-100k
    - 100-200k
    - 200k-500k
    - 500k-1M
    - 1M-2M
    - 5M+

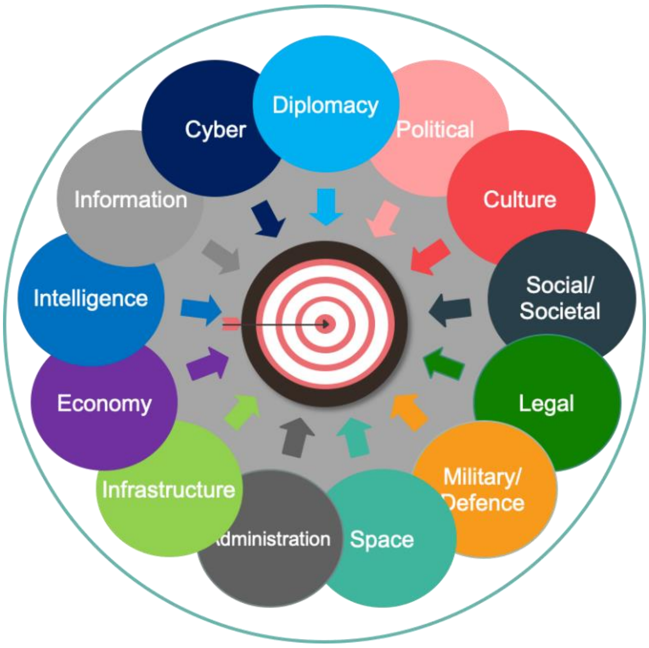
Box 11: Countermeasures

- Are there any potential countermeasures that other actors could field that would be detrimental to the effectiveness of the described idea? Provide a description of how they would degrade the effectiveness of the idea.
- Provide an estimation of how long the described idea would be effective and useful as a solution to the identified gaps/need.

Box 12: Miscellaneous

- Here you may provide any additional information you deem relevant in the description of the idea.

Appendix 1: The 13 JRC domains



Appendix 2: The HYBNET Core Themes

- CT1: Future Trends of Hybrid Threats
- CT2: Cyber and Future Technologies
- CT3: Resilient Civilians, Local Level and National Administration
- CT4: Information and Strategic Communications

Appendix 3: Definition of Levels of practitioner (DoA part B, page 32)

EU-HYBNET follows to the European Commission definition of practitioners which states that "A practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection." In addition, practitioners in the hybrid threat context are expected to have a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats. Accordingly, EU-HYBNET practitioners are categorised as follows: I) ministry level (administration), II) local level (cities and regions), III) support functions to ministry and local levels (incl. Europe's third sector). EU-HYBNET includes practitioner partners from all of these levels and, in keeping with the Commission practitioner definition above and the demands of the GM-01 call, EU-HYBNET's primary focus will be on civilian security issues. In addition, the varied backgrounds of practitioner partners will allow them to make unique contributions to the project.

Appendix 4: Technology Readiness Levels (TRL)[4]

TRL 1 – basic principles observed

TRL 2 – technology concept formulated

TRL 3 – experimental proof of concept

TRL 4 – technology validated in lab

TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)

TRL 6 – technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)

TRL 7 – system prototype demonstration in operational environment

TRL 8 – system complete and qualified

TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

[4] Mihaly, Heder, "From NASA to EU: the evolution of the TRL scale in Public Sector Innovation", The Innovation Journal 22, pages 1–23, October 11, 2017.

11.5 ANNEX V: DESCRIPTION OF ALL 27 INNOVATIONS

Annex III provides a detailed description of all 27 innovations, using the templates that were already described in section 2.2.

11.5.1 INNOVATIONS AS IDENTIFIED IN TASK 3.2

NAME OF THE IDEA

AUTOMATED DETECTION OF HATE SPEECH IN SOCIAL MEDIA

DESCRIPTION OF THE IDEA

Hate speech in an extreme form can lead to hate criminality. To prevent and prosecute crimes connected to that and avoid distrust in society and state an efficient tool to identify hate speech on the internet especially on social media is needed. To improve such a tool different algorithms of machine learning and semantic analysis must train on a sufficient amount of data.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**
  Detecting hate speech automatically to intervene earlier against disinformation, distrust and destabilization
- **Applicable JRC domains as stated by the gaps/needs:**
  Information, social, cyber
- **Applicable core theme(s) as stated by the gap/need:**
  - CT1: Future Trends of hybrid threats CT2: Cyber and Future Technologies
  - CT3: Resilient Civilians, Local Level and National Administration
  - CT4: Information and Strategic Communications

TYPE OF SOLUTION

- **Technical**
  software application with human (analyst) operators/supervisors
- **Social/Human**
  n/a
- **Organizational/Process**
  n/a

PRACTITIONERS

Provide applicable domains for which the solution is valuable:

The base of that concept can be used in every domain, where a training on big data is needed to achieve better results. Here the focus is the use for governmental (local, national and institutional like EU) as well as non-governmental organizations to detect hate speech and intervene appropriately.

- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level* (administration):** expertise needed
  - **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)**
  Governmental organizations with help of experts on the subjects datamining, machine learning and semantic analysis as administration and police for observation and execution in case of prosecution

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 6-9
  Researches and technology available, partially in use (sometimes on other topics) but less for governmental purpose

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  There are different researches that deal with semantic analysis and machine learning algorithms to categorize texts on social media. The efficiency of the concept depends on the quality of the training data. Since there are different approaches and datasets for training, only an appropriate implementation is needed. Therefore, a concept for the handling of results afterward is required.
- In the future, also audio and video can possibly be scanned for hate speeches
- **Expected time to TRL-9.**
  Expected time to market.

DESCRIPTION OF USE CASE(S)

For governmental organizations detecting hate speech can help to identify reasons for a negative attitude of a person/ a group towards others. For example, a disinformation can lead to a negative attitude. By rectifying this information the conflict could be weaken. Concerning terrorism prevention, suspicions arising from hate speeches could be investigated earlier, so that timely intervention could prevent worse.

For non-governmental organizations like the social media companies it offers the chance to censor discriminatory contents.

Semantic analysis and machine learning are a usual part of the work with big data. By training the used algorithm to map a group of words to the most likely meaning, a detection of a particular topic can be performed. For example, several Github projects provide tools to detect hate speech. Such concepts are already used on Twitter to detect and censor discriminatory contents.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to use big data as training to detect hate speech and influence social media in a positive way.
- **Resilience/defensive/offensive**
  By detecting hate speech and weaken discriminatory content, it is possible to improve societal resilience. That can be done by clarifying or censoring disinformation or discriminatory content or, if necessary with police actions.

ENABLING TECHNOLOGY

- Semantic analysis
  Machine learning
  Sentiment analysis
  Artificial intelligence

- Critical technologies for the automated detection of hate speech similarly involves the ability to classify text or other media content online in the category of hate speech.
  This involves sophisticated language recognition algorithms that can conduct sentiment analysis with sufficient speed and certainty. It is crucial for the

RESTRICTIONS FOR USE

- It is important to differentiate between hate speech and expression of opinion. A free expression of opinion is a component of human rights and important to protect. In general, content is classified as discriminatory as soon as it attacks or harms others by insulting, spreading rumors or threating violence. The line between hate speech and free speech is heavily discussed. Therefore, a definition for this is needed as well as supervision of the results delivered by a program.

background technology to dispose of enough computing resources for efficient processing. This is especially important in the beginning of the spread of this type of information so that a potential source of hate speech can be identified swiftly and further outreach be stopped accordingly.	- A solution could be that potential hate speeches are automatically detected, and the final decision to act is left to a human Additionally, it is important to emphasize that only the use of the detection and observation on public areas of the internet can be considered, since the privacy of a person needs to be protected.
COSTS - **Indication of costs**: There are cost for permanent use as long as supervision is needed to ensure whether further actions are required. Since the technology is partly already available, here lower costs are expected. With regards to steadily changing technologies and connected possibilities in programming the costs of research may increase with the amount of social media platforms that should be considered - **Differentiate if possible in development, procurement and exploitation** permanent costs for operation and update	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? The available programs only run on the current versions of technology. Therefore, it is possible that later versions of social media applications are not supported anymore and the programs need to be adapted. Since the trust into government is not as strong as needed everywhere, an intervention of governmental organizations can be seen critically. The responsibility for censoring content on social media lies on the operators of the platforms. Therefore, a very tolerant attitude towards hate speech or the rejection of censoring such content would weaken the effectiveness of the detection of hate speech. - **How durable is the idea (how long is the idea expected to be effective/useful?)** As long as there is the possibility of accessing to social media platforms and using machine learning algorithms on the contents published there.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** Consider not only automated detection but also the machine-human interaction with trained practitioners that can modify taxonomies according to new trends in hate speech wording, and refine the tool and most suitable queries. Specification of the Internet segment this automated detection tool would look at might have implications for the design and use of the innovation.	

NAME OF THE IDEA

Automated fact-checker

DESCRIPTION OF THE IDEA

Disinformation and misinformation have been (sometimes these two are named fake-news) at the core of the deterioration of the quality of online content. The solution for overcoming it so far is checking facts from other trustworthy sources and there A relevant solution has been proposed in the same section. However, since cross-checking is a time consuming process if performed by humans, it could be assisted in this process by AI, using available open (and some password-protected or paid content) sources, finding the way to original source through the tangled web of cross-referencing and reducing language barriers by use of advances in the field of automatic translation.

REFERENCE TO CAPABILITY GAP/NEED

Describe the use of the solution in reference to the gap/need

- Deteriorating quality of content.

Applicable JRC domains as stated by the gaps/needs:

Applicable core theme(s) as stated by the gap/need:

CT1: Resilient Civilians, Local Level and National Administration
CT3: Information and Strategic Communications
CT4: Future Trends of Hybrid Threats

TYPE OF SOLUTION

Technical
Social/Human
Organizational/Process

PRACTITIONERS

- **Provide disciplines for which the solution is valuable:**
  StratCom
  Debunking
- **Provide the level of practitioners in the same discipline:** Would affect all levels in contact with media or communicating with public.
  - I) ***ministry level*** **(administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe’s third sector):**

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: **1**
  In which stage is the solution (research, technology, available innovation, proven innovation): The solutions are not on the market, yet.
  Expected time to TRL-9. Three to five years.
  Expected time to market: Six years.

DESCRIPTION OF USE CASE(S)

The primary users would be the journalists, especially those editing online news under time pressure. The secondary users would be members of academia and think-thankers also influencing the quality of content. The same way it could be used by public servants or political advisers making sure that distorted facts do not penetrate public or internal memos or public speeches.

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**

  The automated fact-checker would have no offensive capacity. It would contribute to the social cohesion (or resilience of society) and defend against hostile information attacks.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the solution?**

  IT mainly, some input from social scientists, humanities, media experts and linguists is needed, especially in setting the original trustworthiness levels of sources.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

  There are no special restrictions known at the time of writing, however, it depends on the reliability of the solution – misjudgements by the system may cause confusion.

  It must be kept in mind that the tool would be assisting its users in checking that can be checked from other sourece and it would not provide useful in giving on estimates, judgements, assasments, etc. Nor would it be useful as a tool for analysing different kinds of artistic self-expression like sarcasm or humor and for evaluating fiction.

  There are ethical considerations to the proposed solution, starting with the name "automated fact-checker". A technological solution to find the primary source is welcome and there are technological tools that can help detection but it's not in any way ready to ascertain with a high enough level of confidence humor, sarcasm, irony and other factors that are crucial to label something as disinformation. It could be construed as censorship and lacking human re view. It is also open to manipulation. There can be automation to provide fact-checks for some topics and work it through databases such as Google Claim Review, but automation has its limits as of today.

COSTS

- **Indication of costs:**

  Estimated EUR 2.3 Million (highly dependent on the advances in AI, quantum technologies and translation software)

COUNTERMEASURES

- **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution?**

  There is the possibility of hostile cyber-attacks, however, since the application is not time critical and if it is down for shorter periods of time does not cause much harm,

<table>
<tr>
<td>- <b>Differentiate if possible in development, procurement and exploitation</b>
The cost indicated above is meant solely for development. The procurement and exploitation (maintenance) costs are rather low (if not foreseen constant feedback to users by system handlers), although this all depends on how the content will be upgraded in the future.</td>
<td>it is not a major problem.

There is a low possibility that counter-technology is developed by hostile actors to remain undetected, however, such technologies do not exist now. Careful study of the algorithms used in the tool and/or infiltrating false information into databases used for fact check my hindrance the operation of the tool, however, developing such countermeasures would require resources and time.

Automated fact-checking might struggle with content that is ambiguous or partially true and partially false.

- <b>How durable is the idea (how long is the idea expected to be effective/useful?)</b>
It is durable in the foreseeable future (5-10 years) and the need could disappear only in the case of major changes in (social)media landscape unforeseeable future. If implemented successfully, the use of automated fact-checker could become as common as using Internet for searching information, maybe even integrated into more common search engines.</td>
</tr>
<tr>
<td colspan="2"><b>MISCELLANEOUS</b>
<b>Any additional remarks//disclaimers/comments/information you might want to provide</b>
There has been some theoretical work conducted in the field, see e.g.
https://www.aclweb.org/anthology/C18-1283.pdf
The proposed solution could be web-based, a browser plugin, or even a smartphone app.

This solution could benefit from related proposed solutions, like factchecker communities and debunking platforms. Their output could be used for a shared database on fake news.</td>
</tr>
</table>

NAME OF THE IDEA

A BLOCKCHAIN-BASED REAL-TIME INFORMATION MANAGEMENT AND MONITORING SYSTEM

DESCRIPTION OF THE IDEA

According to a definition by Nofer et al. (2017), "A blockchain consists of data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions" [5]. The keyword to tackle the problem mentioned above is "information." Real-time information management and monitoring systems can help to prevent future critical foreign investments. All organizations (companies and governments) should contribute to these systems by sharing their

[5] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187. Chicago

information; this information can be partly anonymized. The investment transactions in the system should be verified based on blockchain technology. Each system member has two main tasks: sharing the information and demonstrating the investments based on the system's data. Only verified investments are allowed then to be executed. Government/EU officials can do the verification. The system's information should always be updated and visualized/monitored so that the member of the network can easily access important information.

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gap/need** Access to necessary information The community with enough information verifies the investments - **Applicable JRC domains as stated by the gaps/needs:** Can be applied to all the 13 domains - **Applicable core theme(s) as stated by the gap/need:** Can be applied to other core themes. It depends on the context	- **Technical** Blockchain technology Information management and monitoring tool - **Social/Human** Verify the investments - **Organizational/Process** Sharing information

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**

Real-time information management and monitoring system, where the community verifies the inside information, can be used in any organization (governmental and non-governmental) to improve the information's accuracy and support the decision-making process.

- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level*** **(administration):** related to national security interests, and therefore, this is of concern to the ministry level
  - **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**

Mostly the companies because they are the ones who own the information, which is needed to verify the investments. They are also the ones who will get the most benefit from this system.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**

There are many research publications about the application of blockchain technology on information systems. However, some challenges of these kinds of systems are discovered, for example, Data validation and transaction integrity, the system's efficiency, and third parties' access. These challenges should be mustered before a blockchain-based information management system, becoming a minimal viable product.

- **Expected time to TRL-9.**
- **Expected time to market.**

In 1 or 2 years

DESCRIPTION OF USE CASE(S)

As part of recent legislation, the Medicaid Information Technology Architecture (MITA) aims to increase interoperability between healthcare systems. There is certainly a willingness to change the underlying information system's underlying architecture for large, complex, and disparate systems. This concept can only be realized under the common standards that the blockchain would provide. Perhaps an incremental blockchain as an implementation of a single architecture could solve the data access problem, data protection, and interoperability in public and private health information systems[6].

In another effort to expand its use, Francisco and Swanson suggest severe ethical concerns and serious human rights violations in several companies that are implementing supply chain implementations in all areas (Francisco & Swanson, 2018) [7]. They suggest that the supply chain has the capacity and potential to provide an alternative means by which audits and human rights organizations can verify that an institution is operating in full compliance with laws and regulations on this type of behavior. By creating a transparent supply chain, the intention is to highlight such violations and ensure that they are addressed quickly.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Real-time verification of information
- **Resilience/defensive/offensive**
  Increase the resilience of the investment community by avoiding critical investors. Improve society resilience by avoiding the not verified investments on critical infrastructure.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Blockchain: With blockchain, a trustable and fair platform can be created, where the members can share and verify the information.
  Real-time Information processing and visualization: some investment decision needs to be made rapidly. So there is a need for a real-time system.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Security: the system needs to be highly secured so that no one can modify the correct information. The members of the system also need to use the system with their highest responsibility.
  Anonymity: the information within the system needs to be anonymized. If not, the member may not really want to share their knowledge.
  Legal: Applying blockchain is still a very new trend. The system needs to be implemented to comply with the law of different countries.

[6] Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. *Journal of Health & Medical Informatics*, *8*(3), 8-11.

[7] Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2.

COSTS

- **Indication of costs**:
  high cost for tool development because of the key technologies and the security of the system.
- High cost for getting enough members for the system: the system can only work if there are enough member with enough information. Sharing information has never been an easy decision for a company so getting them into the system is a very difficult task
- High operation cost: to extend the network, to maintain the system and to keep it realizable for all the member
- **Differentiate if possible in development, procurement and exploitation**

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  The critical investor could hide behind a verified company/ another verified investor, but this problem can be solved if there is enough information. With enough qualified details, the system can automatically detect the abnormal behaviour of an investor.
- **How durable is the idea (how long is the idea expected to be practical/useful?)**
  very durable

MISCELLANEOUS

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

NAME OF THE IDEA

A CRAWLER AND REAL-TIME SEARCH ENGINE FOR INVESTORS

DESCRIPTION OF THE IDEA

A crawler is a computer program that automatically searches for files and information on the web. Crawlers are programmed primarily for repetitive behavior, so browsing is automatic. Search engines most often use crawlers to browse and index the Internet.

Building a unique crawler and a real-time search engine only for the investors' information can provide a quick overview of the investor, which results in a better evaluation of investors. It can also help to build a database of investors or detect connections between investors.

The database created with the crawler can be used as the input for the first idea described above.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

Provide an overview of investment quickly

Detect hidden connections

- **Applicable JRC domains, as stated by the gaps/needs:**
  Can be applied to all the 13 domains

- **Applicable core theme(s) as stated by the gap/need:**

Future trends of hybrid threats

Resilient civilians, local level and administration

Information and strategic communications

TYPE OF SOLUTION

- **Technical**

Crawling, search engine

- **Social/Human**

n/a

- **Organizational/Process going**

n/a

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
- **Provide the level of practitioners in the same discipline:**
    - I) ***ministry level*** **(administration):** The ministry level is the authority that can decide on foreign direct investment approval and should therefore be the primary user and operator of these type of crawling/searching tools.
    - **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**

Governments, companies, police

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 7

Some well-known crawlers:
TwitterEcho: a distributed focused crawler to support open research with Twitter data
DeepBot: a focused crawler for accessing hidden web content
HAWK: A Focused Crawler with Content and Link Analysis

- **In which stage is the solution (research, technology, available innovation, proven innovation):**

Crawler and search engine are very well-known research problems. Focused crawlers extract information about one predefined topic from web content and stores the data in a structured format. However, the Internet's data is highly unstructured and in many different forms such as text, images, audio, video. There is still a need to continue researching and developing a highly efficient, focused crawler.

- **Expected time to TRL-9.** In 2 years

- **Expected time to market.** In 3 years

DESCRIPTION OF USE CASE(S)

Google and other well-known search engines are used for "general" purposes.
A novel design of the focused crawler based on the genetic and ant algorithms is proposed by Zheng et al. in their paper[8]. The genetic and ant algorithms were combined to improve the performance of the focused crawler. The selection operator, the crossover operator and the mutation operator are optimized. The whole improved framework is based on a new URL analysis model. And the experimental results show the effectiveness of the new algorithm.

IMPACT ON COUNTERING HYBRID THREATS

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

A focused web crawler can provide enough important information for political decision making or verify the truth of information about an investor.

- **Resilience/defensive/offensive**
  Improves resilience by detecting possible high risk/malign investments.

[8] Zheng, S. (2011, December). Genetic and ant algorithms based focused crawler design. In 2011 Second International Conference on Innovations in Bio-inspired Computing and Applications (pp. 374-378). IEEE. Chicago

<table>
<tr><td><b>ENABLING TECHNOLOGY</b>
- <b>Which technologies are critical in fielding the idea?</b>
Natural language processing (NLP) is a subfield of linguistics, computer science, and artificial intelligence that deals with computers and human language interaction. In particular, how computers can be programmed to process and analyze large amounts of natural language data. The crawler needs to apply NLP to study a massive amount of text data, the web's main content.
Computer vision: besides text, webs can also contain images. With computer vision, a web crawler can extract information from these images.
Information retrieval is the science of searching for information in documents. It involves searching for the documents themselves and metadata describing the data and databases of text, images, and sound.</td><td><b>RESTRICTIONS FOR USE</b>
- <b>Are there any restrictions with respect to using the solutions, e.g., legal, ethical, security, etc.?</b>
The best language for a crawler is English because of the developer community. Other languages are more difficult to be crawled and analyzed. The different structures and syntax of the website code make the development a little bit more complicated, but there are enough code examples in this field.</td></tr>
<tr><td><b>COSTS</b>
- <b>Indication of costs</b>:
Development cost is not so high because the key technologies are not difficult to be implemented.
Operation cost is also not so high because crawling is an automatic process
- <b>Differentiate if possible in development, procurement and exploitation</b></td><td><b>COUNTERMEASURES</b>
- <b>Are there any potential countermeasures that could degrade the effectiveness of the solution</b>?
Legal: Crawling content from the web may not be allowed in some specific situations or by some websites.
- <b>How durable is the idea (how long is the idea expected to be effective/useful?)</b>
very durable</td></tr>
<tr><td colspan="2"><b>MISCELLANEOUS</b>
<b>Any additional remarks/disclaimers/comments/information you might want to provide</b></td></tr>
</table>

NAME OF THE IDEA

Cross sector cyber threat information sharing platform

DESCRIPTION OF THE IDEA

Even where there is relative maturity in sectors for information sharing, trust and barriers to collaboration remain between regions. Many information-sharing groups have emerged from, or are associated with, national legislative or regulatory authorities. Consequently, specific jurisdictions might be absent from some information-sharing groups due to wider considerations. This is the case where there are restrictions on jurisdictions collaborating.

The greatest progress on promoting cyber-information sharing has emerged out of the most cyber-mature sectors and countries, in particular the US and European Financial Services (FS-ISAC) and in frameworks, such as provided by NIST. In less developed markets and sectors, however, greater progress is needed. For example, in Africa, just eight countries have a national strategy on cybersecurity and only 13 have a Government-Computer Emergency Response Team, which typically act as vehicles for establishing national information sharing programmes. Cross-sector collaboration as an issue was specifically part of US President Barack Obama’s Executive Order 1369, which looked to establish new Information Sharing and Analysis Organizations (ISAOs) as a way of promoting more sectorial collaboration.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution about the gap/need**

  Cyber security and cyber defence against common and zero-day vulnerabilities, through sharing among actors from different sectors.

- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all 13 domains.
- **Applicable core theme(s) as stated by the gap/need:**

  - CT2: Cyber and Future Technologies
  - CT3: Information and Strategic Communications

TYPE OF SOLUTION

- **Technical**

  - Information Sharing Platform

- **Organizational/Process**

  - **Several organisations from different sectors participate.**

PRACTITIONERS

- **Provide applicable domains for which the solution is valuable:** All sectors
- **Provide the level of practitioners in the same discipline:**

  - ***Ministry level* (administration):** policymakers 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.
  - **Provide the expected end-users of the solution:**

  Computer security incident response teams (CSIRTs) system and network administrators,

  cybersecurity specialists,

  privacy officers,

technical support staff,
chief information security officers (CISOs),

chief information officers (CIOs),

computer security program managers, and
others who are key stakeholders in cyber threat information sharing activities.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: TRL6-7
- **In which stage is the solution (research, technology, available innovation, proven innovation):** Under development
- **Expected time to TRL-9.** Not available
- **Expected time to market.** Not available

DESCRIPTION OF USE CASE(S)

CONCORDIA is a H2020 European Union-funded project comprising 55 industry and academic partners. Its goal is to build a secure, resilient and trusted ecosystem. Information sharing is one of the most important aspects to address. This has resulted in the creation of "Threat Intelligence Platforms for Europe", which has enabled cross-sector (telecommunications, finance) collaboration in a wide variety of data sets and requirements. The respective project activity recognized that effective information sharing between different organizations in disparate sectors is not trivial and, as a result, a comprehensive plan was designed to overcome this. A mutual cyber intelligence sharing agreement was first drafted that allowed users of institutions to define the data they wanted to share, with whom, duration of the intelligence sharing, spatial and temporal characteristics (e.g. only shared in a specific country or for a specific period) and the definition of roles for accessing and controlling the information. This foundational model and way of working also allowed more mature organizations to then build federated machine learning approaches, leveraging the data sets of different participants, but preserving the privacy of data to enhance security.

The CONCORDIA platform is a way of joining up information from disparate data sources and sectors, thereby presenting a single view over Open-Source Intelligence (OSINT) information, based on financial services information and telecommunications-related data. The platform was built on existing, freely available open-source components, including the Malware Information and threat Sharing Platform (MISP) and the Incident Clearing House developed during the project "Advanced Cyber Defence Centre" (ACDC). With this platform in place, different use cases can be more easily applied, which assist with the defensive posture of participants. This includes incident response and automated exchange of attack information.

IMPACT ON COUNTERING HYBRID THREATS

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

Cyber information-sharing among domains and sectors will provide a single view for security.

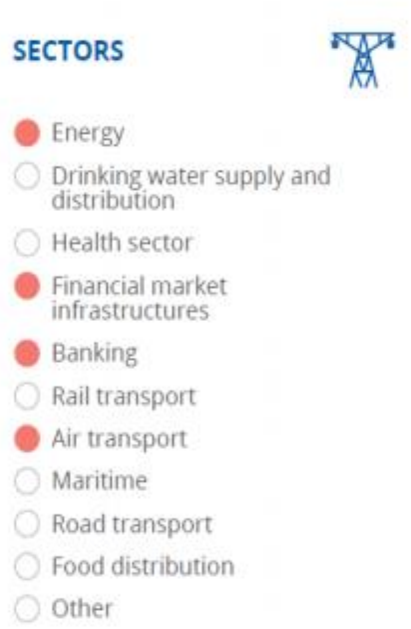
• **Resilience/defensive/offensive** Resilience and defensive aspects will be covered.	
ENABLING TECHNOLOGY • **Which technologies are critical in fielding the idea?** ○ **AI, ML and Privacy Enhancing Technology.** More research and deployments are needed to make AI and ML more operationally accessible as a defensive and information sharing capability	**RESTRICTIONS FOR USE** • **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** Security measures should be taken since sensitive information will be shared. Restriction to use this solution may be found in the reluctancy of the end users to share sensitive information with other organisations. Data sharing can introduce a new set of challenges for users, including: Aligning the integration of data across separate organization-specific data systems. Sharing a data system that was not developed with sharing in mind. Formatting and collecting data using disparate or incompatible methods. Partners from different sectors may use the same words to mean different things and use sector-specific terminology to describe similar ideas. Partners may use differing definitions for variables, which may lead to inconsistent data collection. There are a variety of data sharing barriers (e.g., data consistency, interoperability), but legal barriers are among the most significant. Laws pose a significant barrier to cross-sectoral data sharing primarily because the personal data protection framework that protect data differently depending on the

	type of data, who has it, why it was initially collected, and what they intend to do with it. Moreover, legal variations exist at state levels, frustrating efforts to understand how laws apply to proposed data sharing activities.
COSTS **Indication of costs**: Integrated data systems can be expensive to develop and require upfront planning and significant resources. • For decision-makers and industry leaders looking to reap the rewards of participating in an information-sharing ecosystem, estimating the costs and targets for tangible investments is often difficult due to the array of options and lack of agreed standards from which to measure the benefits of such investment. Even where information-sharing programmes are available, participation costs act as a barrier • **Differentiate if possible, in development, procurement and exploitation** N/A	**COUNTERMEASURES** **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Cross sector information sharing is hampered by fears about giving competitors an advantage, as well as concerns about sharing sensitive internal data. More specifically, some sectors, due to their specificity and cybersecurity maturity, are more willing and eager to participate than others. Free cross border information sharing is additionally complicated by the possible threats to human rights protections when information is shared with states that have a weak rule of law and or a history of systemically violating human rights. The lack of sector specific guidance tools, which map preexisting privacy principals, responsibilities, harms and remedies to the creation and management of cross sector information sharing has caused uncertainty. This in turn, delays efforts to build cross sectoral programmes. There is a current lack of alignment and harmonization across jurisdictions – and in many cases conflicting regulations in relation to the sharing of cyber information – especially with regard to concerns over the disclosure of what could be considered as sensitive proprietary information by an organization. **How durable is the idea (how long is the idea expected to be effective/useful?)** The main idea of the solution using legacy networks is in place many years before, so the advanced solution is also going to last and be effective as long as vulnerabilities and zero days exists.

MISCELLANEOUS

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

.Sectors which have created or launched an initiative to create such initiatives on the European level



SECTORS

● Energy

○ Drinking water supply and distribution

○ Health sector

● Financial market infrastructures

● Banking

○ Rail transport

● Air transport

○ Maritime

○ Road transport

○ Food distribution

○ Other

are:

NAME OF THE IDEA

DebunkEU.org

DESCRIPTION OF THE IDEA

DebunkEU.org is a digital platform and an independent crowdsourced analytical centre, whose main task is to research disinformation in the public space and execute educational media literacy campaigns. By employing artificial intelligence, Debunk EU carries out detailed research on disinformation in the Baltic states and with crowdsourced local experts involvement spots and identifies disinformation within 2 minutes from real time.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  Manipulated information in the disinformation media, social media, disinformation and misinformation analysis.

- **Applicable JRC domains as stated by the gaps/needs:**

  Information
Social/Socie
tal Cyber

- **Applicable core theme(s) as stated by the gap/need:**

  Information and Strategic Communications

  Disinformation / misinformation large scale analysis

TYPE OF SOLUTION

- **Technical, cloud based platform**
- **Organizational/Process automation**

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:** Cross domain

- **Provide the level of practitioners in the same discipline: Strong involvement and impact:**
  - ○ **I) *ministry level* (administration):**
  - ○ **II) *local level* (cities and regions):**
  - ○ **III) *support functions to ministry and local levels* (incl. Europe's third sector):**

Cooperation on disinformation analysis with the Lithuanian Ministry of Foreign Affairs:

https://www.debunkeu.org/post/incidents-at-the-belnpp-are-being-covered-up-using-falsehoods-mockery-and-made-up-facts

https://www.debunkeu.org/post/kremlin-media-lithuania-risks-baltic-unity-by-forbidding-allies-to-import-energy-from-belarus

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments)**

- The Intended users are media organisations, StratComs and the general public.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: TRL9

In which stage is the solution (research, technology, available innovation, proven innovation):

Fully operational

- **Expected time to TRL-9.**
  0 years
- **Expected time to market.**
  0 years

DESCRIPTION OF USE CASE(S)

Using an AI powered system, we are able to monitor more than 2000 domains which are known for spreading mis/disinformation, and scan through 1M pieces of content every month. Based on the filters and keywords created by our analysts, the AI selects the most harmful content, which is then reviewed by our team of experts and volunteer fact-checkers 'elves'.

The content to review is based on a "infometer" tool which showcases the relevancy score of each piece. The relevancy score consists of three variables: importance (based on keywords and narratives within the text), social interaction (shows to what extent the article was commented on, liked and shared on Facebook), and reach (indicates popularity of a website the article was published on).

The total relevancy score shows the impact of the content piece with false information in it. For example, if the piece of content has a lot of harmful narratives in it, but the social interaction and reach is low, it is considered not to be that damaging. However, if the piece of content has just a couple of harmful narratives but was actively shared on social media and has reached a wide audience, it is considered to be more dangerous.

Analysed data is then put together into concise reports, which are published on our own platform debunkeu.org, shared with various groups of stakeholders (other disinformation-countering organizations, strategic communication units, ministries of defence and foreign affairs, and embassies around the world), and also disseminated as press releases in national and international media. This way, we are reaching not only the expert communities, but also keep the members of the general public well informed about attempts to manipulate their opinion.

- **Please elaborate on the organizational/process challenges for the use of the proposed solution. Is it embedded/utilized to an effective extent? Are the results used by the general public?**

In order to implement the Debunk EU system, it is necessary to train the users so they understand how it works and the methodology behind it.

The system is fully operational and utilized to its full potential. Debunk EU analysts use it in their daily work to analyse data for their reports.

The findings from our analyses are available for the general public on our own website; they are also being distributed as press releases to national and international media outlets.

IMPACT ON COUNTERING HYBRID THREATS

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

  The proposed solution allows to carry out data driven analysis of emerging disinformation threats based on the most common narratives, techniques, and sources. The findings from our analyses provide a bigger picture of the disinformation issue and contribute towards expanding the knowledge about it. Our reports are shared with various stakeholder groups, who in turn can make informed decisions when developing disinformation countering strategies.

  Moreover, to increase public resilience to disinformation, we are communicating the findings from our analyses in press release form to national and international media outlets.

- **Resilience/defensive/offensive**

Resilience

The platform is intended for countering disinformation through increasing civil resilience. By disclosing and analysing the most harmful stories, presenting narratives and techniques used to deceive audiences, we contribute towards informing citizens in the Baltic countries and Poland about disinformation targeting citizens of those states. Well informed society lessens the impact of disinformation greatly, because when people are aware of the ways false and misleading content is being spread and used to try and manipulate their opinions, it is way harder to deceive them - hence the effect of disinformation is also lower.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**

1. Process automation using Machine learning and AI.
2. Training disinformation analysts.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

Cloud based platform has no scalability restrictions. Which means that there are no significant language barriers, the system is adaptable with some technical work. To be able to use it, employees need to pass a certain training.

Public authorities may face difficulties in organizing debunking platforms. Private Social media platforms, threated by such a solution, can accuse government's authorities of attempting to manipulate news feeds. This could result in their noncompliance leading to a useless tool (since no content will be provided for analysis).

Wider society may perceive the usage of the debunking platform as an attempt to manipulate the news feed. People involved in such communities should be trusted in order to avoid infiltration of the fact checking communities. In this context a baseline level of trust should be considered between communities and media.

- **What is the role of (non-)compliance by private (social media) companies?**

Debunk.eu analyse only publicly available data sources. If platform users need to

	analyse some non-public data, this will require consent from the social media so that they provide the data.
COSTS	COUNTERMEASURES
- **Indication of costs**: Cost per project, depends on scope. Cost per use goes down with an increased number of users. - **Differentiate if possible, in development, procurement and exploitation** What influences the cost of adaptation is wider scope of monitoring. The wider the scope, the higher the number of automation processes and features which will have to be implemented. Additionally, with a broader scope of research the need for API requests to machine learning algorithms increases, since every API call (request for data) costs.	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Control over mainstream media outlets in some countries is often so thinly veiled that audiences are sceptical even towards quality journalism. This kind of solution is open to manipulation and its results are methodologically flawed and pose reputational risks for those involved. Large scale production of fake news content may create problems to the effectiveness of the solution due to the large amount of fake news that needs to be debunked. Moreover, the creation of fake news is by default a more easy process than their identification and exposure. The aforementioned could deteriorate the quality of results and report real news as fake ones, creating lack of trust to the overall solution. - **How durable is the idea (how long is the idea expected to be effective/useful?)** As long as the platform will be supported by the community - **How could mass production and flooding of fake news impact the efficacy of the proposed solution?** The analysis is semi-automatic; it can hold as much information as necessary. However, if the stream of disinformation increases, we might need more human resources, since the final call whether the article is true or false is made by the analysts. - **Producing and disseminating fake news is less**

	time- and resource-consuming than the identification, evaluation and exposing of fake news; How does this impact the effectiveness of the proposed solution? To increase the effectiveness of our platform, every article which was debunked previously can be identified. With our database of debunked content growing, the system finds similar cases more easily and faster - therefore, the automation of the whole process progresses.

MISCELLANEOUS

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

How are the enabling technologies critical in the fielding of the proposed solutions? Elaborate.

Regretfully, the world-wide response to disinformation is still too slow, too fragmented and relying on an outdated 2G approach, where the first G stands for Google search (manual monitoring) and second G – for Gut feeling (no data-based evidence). Because the problem is complex, it requires complex solutions.

We are using a cloud based solution, which is accessible through a secure browser connection. Our system is to automate the process of debunking disinformation as much as possible to make it faster, fool-proof and wide reaching. Using AI we are able to teach the system to recognize more and more disinformation narratives, techniques and sources; moreover, since it is highly adaptable, we can add necessary features as new disinformation threats emerge. As mentioned earlier, disinformation spreads fast, therefore, the response to it has to be as rapid as possible, and it can only be achieved by applying tech-based solutions.

Please read more about our work and methodology behind it on our website:

https://www.debunkeu.org

https://www.debunkeu.org/about

https://www.debunkeu.org/methodology

NAME OF THE IDEA

Early or Rapid Damage Assessment System

DESCRIPTION OF THE IDEA:

Rapid damage assessment enables operators to assess in real-time the expected structural damage and identify possible expected impacts. The algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event i.e. propose automated reaction, optimize response (areas in green can continue to operate, areas in yellow integrity can be assessed automatically, whereas the red areas should be investigated in detail before entering operational mode). A Critical Infrastructure Resilience Platform (CIRP) when fed with real time nowcasting or forecasting data instead of a scenario hazard, can be turned into an early or rapid damage assessment system respectively, thus providing the unique capability to initiate efficient response actions, right after (in case of now-cast data) or even before (in case of forecast data) the occurrence of catastrophic events.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  Primary Need No2: [Minimum service for ensuring strategic supplies.] Provides the capability to initiate efficient response actions right after or before a catastrophic event.

- **Applicable JRC domains as stated by the gaps/needs:**
  Economy, Infrastructure, Administration

- **Applicable core theme(s) as stated by the gap/need:**
  Resilient civilians, local level and administration

TYPE OF SOLUTION

- **Technical**
- Software application, simulation program. The calculated impact assessment results can be presented to the users through an intuitive graphical user interface
- Potential users are the CI operators, CI and safety response planners, safety engineers and managers in Civil Protection agencies, etc

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  Infrastructure, Administration
  Provide the level of practitioners in the same discipline:
    - I) ***ministry level*** **(administration): The Ministry of Civil Protection**
    - Ii) local administration . The municipalities could also be involved in this
    - **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**
  Private companies, police, firefighting departments, civil protection ministries

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: TRL6
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
- **Expected time to TRL-9.** The innovation will reach TRL 7 by autumn 2021
- **Expected time to market.** 4 years

DESCRIPTION OF USE CASE(S)

1) The solution is currently being implemented for a big refinery case in Greece, where the impact of natural hazards (e.g. earthquake) is studied with respect to the resilience of the critical infrastructures (InfraStress H2020 project)
2) The same application will be used for ground satellite stations. The impact of Natural hazards (earthquakes, extreme winds, floods) will be studied on buildings, and more specifically ground satellite station (7shield project). Based on the results, risk assessment will be conducted.
3) The application has been used for the study of the impact of climate change on Cis (EU-Circle H2020 project)

IMPACT ON COUNTERING HYBRID THREATS

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

The innovation is particularly relevant to the Primary Gaps No. 1 and 2, because if in times of crises critical infrastructures are not available, there would be disruptions in the delivery and global supply of necessary goods and services. All the above are critical for the essential functioning of society.

Resilience/defensive/offensive

The innovation reinforces Critical Infrastructures with the capability to assess in real-time the expected structural damage after a catastrophic event and identify possible expected impacts. Additionally, the algorithms for an automated rapid damage assessment system can automatize the reaction process during a severe event. Some examples include proposing automated reaction, optimizing response (areas in green can continue to operate, areas in yellow integrity can be assessed automatically, whereas the red areas should be investigated in detail before entering operational mode.

ENABLING TECHNOLOGY	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** GIS and Computational Probabilistic techniques. GIS is used for geographic representation of the critical infrastructure. CPT is used in order to execute the calculations	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** Not applicable The solution can be purchased by public and private CIs. There are no legal or ethical concerns . No personal data are used.
COSTS	**COUNTERMEASURES**
- **Indication of costs**: Depending on the magnitude of the deployment. Software development and after sales costs (for support, if needed)	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?

are the main cost parameters that depend on the magnitude of the CI. - **Differentiate if possible, in development, procurement and exploitation** Development is an important part of the cost	Incomplete representation of the structural details of the CI Low resolution input data Inaccurate estimation of hazards All the above can degrade the solution Results will not be accurate and they will not represent the real impact to the Critical Infrastructure - **How durable is the idea (how long is the idea expected to be effective/useful?)** Configuration of the algorithm will be needed if there are changes in the structural details

MISCELLANEOUS

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

What-if scenarios can be used for impact and risk assessment that will be used by the practitioners for preparedness and training purposes.

NAME OF THE IDEA

FACTCHECKERS COMMUNITIES

DESCRIPTION OF THE IDEA

The most prominent approach to combating misinformation is the use of professional fact-checkers. This approach, however, is not scalable: professional fact-checkers cannot possibly keep up with the volume of misinformation produced every day. In this regard, capitalizing on crowds of regular people at moderating fake news as professional fact-checkers is considered as a good alternative. Unlike professional fact-checkers, who are in short supply, it is easy (and inexpensive) to recruit large numbers of laypeople to rate headlines – thereby allowing scalability. By creating fact checkers communities, best practices and exchanges in this field can be further promoted.

REFERENCE TO CAPABILITY GAP/NEED - **Describe the use of the solution in reference to the gap/need** - Improve societal resilience against disinformation. **Applicable JRC domains as stated by the gaps/needs:** It can be related to helping countering disinformation across all 13 domains. - **Applicable core theme(s) as stated by the gap/need:** CT2: Cyber and Future Technologies CT3: Information and Strategic Communications	**TYPE OF SOLUTION** - **Technical** - **N/A** - **Social/Human** - **N/A** - **Organizational/Process** Yes

PRACTITIONERS

- **Provide disciplines for which the solution is valuable**
  The solution can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry, NGO) organizations. However, the primary focus seems to be directed to governmental organizations and on specific topics (elections, political debates, etc.). The governmental focus covers are applicable for all 13 JRC domains.
- **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).

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: N/A

- **In which stage is the solution (research, technology, available innovation, proven innovation):** N/A

- **Expected time to TRL-9.** N/A

- **Expected time to market.** N/A

DESCRIPTION OF USE CASE(S)

1/One such example is VERIZON which on its website (https://www.verizon.com/info/technology/fake-news-on-social-media/) has published a guide for identifying fake news on social media networks. It is mentioned in more detail to:

- Reliability of sources
- How Social Media Users Are Contributing to Misinformation
- How to Recognize Fake News and Misinformation
- How to Handle Fake News and Misinformation and
- How to Report Fake News and Misinformation

2/Facebook is using crowdsourcing as a promising approach for helping to identify misinformation at scale.

3/ The International Fact-Checking Network is a unit of the Poynter Institute dedicated to bringing together fact-checkers worldwide. The IFCN was launched in September 2015 to support a booming crop of fact-checking initiatives by promoting best practices and exchanges in this field.

4/ Finland's government has launched an anti-fake news initiative in 2014 – two years before Russia meddled in the US elections – aimed at teaching residents, students, journalists and politicians how to counter false information designed to sow division. (https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/)

5/BBC Academy for reporting, education and training related to Fake news (https://www.bbc.co.uk/academy/en/collections/fake-news)

6/Related EU projects/ initiaves/ strategies

- https://ec.europa.eu/digital-single-market/en/media-literacy
- https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to the need for exposing and countering disinformation and increasing societal resilience.
- **Resilience/defensive/offensive**

Such a guide is improving societal resilience against fake news and is also a defensive capability against hybrid state actors using disinformation campaigns.	
ENABLING TECHNOLOGY - **Which technologies are critical in fielding the idea?** n/a	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** There are some ethical considerations for fact checking however no restrictions are imposed Public authorities may face difficulties in organizing regular people in communities with the specific task to moderate fake news. Private Social media platforms, threated by such a solution, can accuse government's authorities of attempting to manipulate news feed. This will result to their noncompliance leading to a useless tool (since no content will be provided for analysis) Wider society may perceive the usage of the fact checker communities as an attempt to manipulate the news feed. People involved in such communities should be trusted in order to avoid infiltration of the fact checking communities. In this context a baseline level of trust should be considered between communities and media Fact-checkers are human beings who live in the real world and have specific believes that may influence their work. In this context we should abandon the pretense of objectivity and design a system of adversarial fact-checking that places the evidence for competing claims front and center. There is a clear ethical concern in using the term "fact-checking communities" for people and organizations who are not trained or have the same standards as real fact-checking organizations. Either you invest in preparing those communities to do

	proper fact-checking (and thus scalability concerns remain) or you solve scalability by removing precisely the qualities that make a fact-checker effective in fighting disinformation.
COSTS - **Indication of costs**: No costs - **Differentiate if possible in development, procurement and exploitation** n/a	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Guides can be bypassed in order to manage and distribute fake news and personal opinions may influence the quality of results. Citizens may accuse the government of attempting to manipulate information flow under the cover of community fact checking Obtaining reliable, authoritative information to debunk misinformation is another challenge that affects even well-funded fact-checkers in relatively open societies. Not all such information is readily available, and only a fraction of it exists in the form of structured datasets that are easily searchable. Control over mainstream media outlets in some countries is often so thinly veiled that audiences are skeptical even towards quality journalism. This kind of solution is open to manipulation and its results are methodologically flawed and pose reputational risks for those involved. - **How durable is the idea (how long is the idea expected to be effective/useful?)** Certainly for the next years. It can create long term impact.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** This idea could work in a similar way as Wikipedia, I the sense that it is maintained by a community of individuals. Another idea, complementary to this one would be the training of the civil society on how to identify fake news and formulating a trusted to the wider public community could be an important step towards winning the war on misinformation	

NAME OF THE IDEA

Fair Trade Data Program[9]

The California Consumer Privacy Act of 2018 secures new privacy rights for California consumers, including, besides the right to know, the right to delete and the right to non-discrimination, the right to opt-out of the sale of their pesonal information. It was a definite start in helping consumers understand that they are the owners of their data, and are therefore the ones to decide if, when and to whom they will give them.

The next step was for citizens to realise that they can actually sell their data, if they wish to, to whoever they wish. A company that allows that was formed in 2018. With Killi, companies are able to purchase first-party compliant data while users are able to profit from their data for the first time ever.

DESCRIPTION OF THE IDEA

Fair Trade Data program allows all Killi users to be fairly compensated for their data. Whenever one joins a platform, information about the person is collected – from personally identifiable information down to financial information. While most sites require this information, the person is not compensated for it. With the Killi Fair Trade Data Program, the user is given a share of funds for the data he/she provides. Besides that, there are other ways to compensate the user, as The Profile Reward, The Location Reward(Android only), The Shopping Reward, Surveys, Videos (Android only), Completing your profile, Refer A Friend.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  In order to reduce the power of digital monopolies, their source of income should be challenged. Such an application can help citizens understand the way digital monopolies operate
- **Applicable JRC domains as stated by the gaps/needs:**

  Information
  Economy
  Cyber
  Social/Societal
- **Applicable core theme(s) as stated by the gap/need:**

  Information and strategic communications

TYPE OF SOLUTION

- **Technical**
- **Social/Human**
- **Organizational/Process**

This is a technical solution that would have broad societal implications on how people behave online. Their consumer behavior and interaction with data and advertising would drastically change.

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**

  Information
  Economy
  Cyber
  Social/Societal
- **Provide the level of practitioners in the same discipline:**

Strong involvement and impact:

- **ministry level (administration)**
- **support functions to ministry and local levels (incl. Europe's third sector)**

Some involvement

- **local level (cities and regions)**

[9] Name of the idea 'Fair Trade Data Program' is used in the company webpage of 'Killi'

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
  Citizens

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:
  9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Proven innovation
- **Expected time to TRL-9.**
  n/a
- **Expected time to market.**
  Operating since 2018

DESCRIPTION OF USE CASE(S)

Already being used by the company Killi, and companies are able to purchase first-party compliant data while users are able to profit from their data for the first time ever

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  The use of the idea could have important impact in countering hybrid threats, especially with respect to digital monopolies as the main source of their income would be challenged.Resilience/defensive/offensive
  defensive

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  No special technology needed, the use is similar to purchasing online

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Attention should be paid to this application being used by non-adults.

COSTS

- **Indication of costs**:
  No particular costs needed, just the cost of updating the tax collection authority with the citizen's profits
- **Differentiate if possible in development, procurement and exploitation**

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Not at the moment
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  As long as e-commerce is used by citizens, this idea is useful

MISCELLANEOUS

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

NAME OF THE IDEA

FAKE NEWS EXPOSER

DESCRIPTION OF THE IDEA

Software tool that gives insights that makes it easy to follow, analyze, and report on what's happening with public content on social media posts and assists users to identify fake news and disinformation.

To do this, the tool analyzes both content and metadata and some tools also have the ability to classify the article as fake or not by evaluating the article based on predefined external and internal indicators.

The research is now heading to automate the whole procedure by solutions that mainly focus on the source of the news.

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gap/need** - Improve societal resilience against disinformation. **Applicable JRC domains as stated by the gaps/needs:** It can be related to helping countering disinformation across all 13 domains. - **Applicable core theme(s) as stated by the gap/need:** CT2: Cyber and Future Technologies CT3: Information and Strategic Communications	- **Technical** software - **Social/Human** n/a - **Organizational/Process** n/a

PRACTITIONERS

- **Provide disciplines for which the solution is valuable**
  The fake news exposer can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry, NGO) organizations. However, the primary focus seems to be directed to governmental organizations and on specific topics (elections, political debates, etc.). The governmental focus covers are applicable for all 13 JRC domains.
- **Provide the level of practitioners in the same discipline:**
  - I) *ministry level* (administration): primary focus seems to be directed to governmental organizations and on specific topics (elections, political debates, etc.).
  - II) *local level* (cities and regions):
  - III) *support functions to ministry and local levels* (incl. Europe's third sector).

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index):** TRL 9
  To date, several tools have already been developed. Most tools are platform-based or web-based. Recently the big social media companies are developing and using it for their own sake in order to analyse social media content as quickly as possible.
- **In which stage is the solution (research, technology, available innovation, proven innovation):** To the market.

- **Expected time to TRL-9.** Not applicable, solutions have already been implemented

- **Expected time to market.** Already in use

DESCRIPTION OF USE CASE(S)

The RAND organization has performed a survey on disinformation tools, which resulted in 84 identified tools, see https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html

Moreover, from a market survey the following have been identified :

- TinEye which provides advanced image identification for content moderation and fraud detection.
- Trendsmap, Trendolizer, Google Trends and Newswhip to keep track trends by location
- Google Reverse Image Search helps find images that are similar to the one being verified.
- CrowdTangle to search across Facebook or Instagram for content relevant to their reporting.
- Botswatch to map bot networks.
- CoFacts is a collaborative fact-checking project that combines a chatbot with a hoax database, integrated within LINE, a popular instant messenger app in Asia.
- Fraunhofer Software that can automatically detect fake news: A new tool developed by the Fraunhofer FKIE for the automated detection of so-called "fake news" can be seen as an early-warning system. It scans social media news feeds and filters out news items with specific characteristics. However, the system does not perform an automated fact check, and it certainly does not conduct censorship. The final assessment of news stories flagged as potential fake news is left up to the user. The point is to detect conspicuous news items and quickly draw attention to them so that their further dissemination can be monitored, if necessary. The tool is thus a preselection and alert system that helps users evaluate and monitor the news situation
- Truly media: a web-based collaboration platform. It has been designed to support the verification of digital (user-generated) content residing in social networks and elsewhere. Truly Media was developed in very close collaboration with journalists and human rights investigators, taking their demands and requirements fully into account.
- Text gain: Natural Language Processing tools for GDPR-compliant user profiling, content extraction and sentiment analysis.
- ANSAcheck solution : The ANSAcheck solution works by assigning a unique hash ID to every ANSA-created news story and posting the hash to Ethereum, the world's largest public blockchain platform. If even one letter in the story is changed, the system will detect that it is not an identical copy to the original story. Story IDs are batched and posted multiple times each day to Ethereum. If ANSA updates the story, another entry is recorded on the blockchain and linked back to the original entry to form a chain of provenance. Each ANSA story posted on its website is accompanied with an ANSAcheck sticker to signal its authenticity to readers. Readers can click on the ANSACheck sticker to query the blockchain about the source of the story.
- "Hoax-News Inspector"(https://link.springer.com/article/10.1007/s12652-020-02698-1) for the detection of fake news that propagates through the web and social media in the form of text. To distinguish fake and real reports on an early basis, prominent features were identified by exploring two sets of attributes that lead to information spread: Article/post-content-based features, Sentiment based features and the mixture of both called as Hybrid features. The proposed algorithm is trained and tested on the self-generated dataset as well as one of the popular existing datasets Liar. It has been found that the proposed algorithm gives the best results using the Random Forest classifier with an accuracy of 95% by considering all sets of features. Detecting and verifying news have many practical applications for news consumers, and time-sensitive services, which generally help to minimize the spread of false information. The proposed system Hoax News-Inspector can automatically collect fabricated news data and classify it into binary classes Fake or Real, which later benefits further research for predicting and understanding Fake news.

IMPACT ON COUNTERING HYBRID THREATS

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

  This contributes to the need for exposing and countering disinformation and increasing societal resilience.
- **Resilience/defensive/offensive**

  Such a tool supports improving societal resilience against fake news and is also a defensive capability against hybrid state actors using disinformation campaigns.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**

  AI powered analytics
  Machine Learning
  Blockchain
  Language technologies
  Deep neural networks

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

  Probably one caveat might be that justified information could accidentally be categorized as fake news, which could lead to legal issues and claims.
  Private Social media platforms, threated by such a solution, can accuse government's authorities of attempting to manipulate news feed. This will result to their noncompliance leading to a useless tool (since no content will be provided for analysis)
  Wider society may perceive the usage of the fake news exposer as an attempt to manipulate the news feed.

  In terms of security considerations, a potential hack on the algorithm of such tool could also deteriorate its results. High security considerations should be in place during its implementation.

  Automation and crowdsourcing efforts can be effective in helping detection of disinformation, but if professional expertise by fact-checkers is removed, the result of the process can be called into question.

  AI is not in any way ready to ascertain with a high enough level of confidence humor, sarcasm, irony and other factors that are crucial to label something as disinformation. It is also open to manipulation. There can be automation to provide fact-checks for some topics and work it through databases such as Google Claim Review, but automation has its limits as of today.
-

COSTS	COUNTERMEASURES
- **Indication of costs**: These tools tend to be quite cheap or even free and are used with a subscription model. - **Differentiate if possible in development, procurement and exploitation** Most of the cost lies in the use and exploitation of it, and imbedding it in governmental organizations.	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Smart algorithms that circumvent the fake news exposer. The content identified by the tools then needs to be analyzed by a group of journalists in order to verify eventually if the content is fake. A counter automated production of fake news content may create problems to the effectiveness of the solution due to the large amount of data received. Moreover, the creation of fake news is by default a more easy process than their identification and exposure. The aforementioned could deteriorate the quality of results and report real news as fake ones, creating lack of trust to the overall solution. In addition language barriers could defeat the usage of AI tools to counter disinformation given the extensive training required to cover all languages and potential slang wording use. The same counter impact in the effectiveness of the solution could be released with the usage of semantic language. The predicted flaws in the solution point to a very possible backfire effect after identifying as disinformation contents that are not. - **How durable is the idea (how long is the idea expected to be effective/useful?)** Certainly for the next years, however when it becomes obvious that disinformation does not strike anymore, people and actors probably will shift to new tactics. We already see that there is a shift towards deep fakes (using fake videos instead of fake textual / written information). It can be useful for the next years as it mainly lies to journalists' analysis. Moreover, closed groups with encrypted communication can be easy targets for disinformation campaigns.

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

NAME OF THE IDEA

GUIDES TO IDENTIFY FAKES

DESCRIPTION OF THE IDEA

Several existing tools can help to detect fakes in images and videos, but they are rarely noticed by society. To raise the attention for the use of such tools, public guides to inform the citizens about the possibilities in the verification of visual materials are needed. This includes a guidance as well as a list of several public tools that can support the user identifying fakes by providing for example an online analysis of suspicious objects. Therefore, an extensive research on existing tools, as well as their functionality and reliability are required.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**
  Support media literacy of citizens to increase trust in official communication
- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all 13 domains**.**
- **Applicable core theme(s) as stated by the gap/need:**
  - CT1: Future Trends of Hybrid Threats
  - CT3: Resilient Civilians, Local Level and National Administration
  - CT4: Information and Strategic Communications

TYPE OF SOLUTION

- **Technical**
  - Devise a type of hashing or fingerprinting algorithm in order to identify copies or further instances of fake information as posted on the various social networks and websites. These algorithms will be based on machine learning technologies. Appropriate algorithms and feature extraction methods need to be identified and tested.
  - Potential issues can be the resources necessary (in terms of processing speed and memory) to execute these methods on the web data.
- **Social/Human**
  - Guides/ guidelines
- **Organizational/Process**
  - Furthermore, the accuracy of the selected machine learning procedures needs to be reliable enough to warrant flagging information as fake information. Providing additional information that provide explanations is necessary to increase effectiveness particularly if the flagging and explanation come from an already trustworthy sources in the eyes of the information recipients.

	○ Review processes with trusted reviewers may need to be implemented

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  A guidance to identify fakes can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry) organizations as well as citizens. However, the primary focus here seems to be directed to citizens to get a better understanding of the methods governmental and non-governmental organizations use in a more extensive dimension.
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):** guides are mainly intended for citizens, however also at ministry level these can be useful, although one might expect that these practitioners are more skilled in distinguishing fake from real
  - **II) *local level* (cities and regions):** The same as above, although at local level awareness about disinformation is probably lower
  - **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**
  Citizens can use a guide or a tool to verify by themselves if there might be doubts concerning the authenticity of an image or a video. As a result, statements given by governmental sources become more comprehensible**.**

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:
  Solution is already available; TRL 9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  To date, several suppliers offer a supportive guidance on specific themes or a web-based tool that can be used by a non-expert to identify fakes. These need to be evaluated, so the most promising can be summarized in a guide that governmental organizations can provide to the citizens.
  Expected time to TRL-9.
  Already available.
  Expected time to market.
  Already available.

DESCRIPTION OF USE CASE(S)

There are already many guides on the internet, which explain how to identify fakes in images and videos. Some of them include tools to do a short analysis of suspected objects without further knowledge on the subject. In some cases, a guidance or an analysis done by oneself can help to understand decisions by building up a better comprehension of the evidences that have contributed to this.
Some examples for already existing guides/ web tools are http://fotoforensics.com/ for the analysis of images and https://citizenevidence.org/, which offers several guides on digital verification.

Most existing guides provided by governmental organizations do not include recommendation of tools as can be seen in the following guides:

- https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams
- https://sharechecklist.gov.uk/,
- https://www.bundesregierung.de/breg-de/themen/mythen-und-falschmeldungen/corona-falschmeldungen-erkennen-1750146

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to the need for strengthening the trust in political/ governmental statements and making decisions about authenticity comprehensible.
- **Resilience/defensive/offensive**

Such a guide can improve the societal resilience against fake news and the defensive capability against hybrid state actors using disinformation campaigns.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Depending on the exact tool, the critical field can vary. In some cases, there might be machine learning as a critical technology. Depending on the suspicious material there could be problems with the protection of personal data.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
- Concerning the public use of these tools and data there should not be any restrictions.

COSTS

- **Indication of costs**:
  Depending on the amount of existing tools that can be found and their provided functionalities, the main part of the costs will be in research. Every suggested tool should perform reliable and provide correct results, which is why each tool needs to be tested extensively. This must then be summarized in the guide. As technology constantly changes, the results must be regularly reviewed and updated. The actual costs of the guide itself might be very low, the only foreseen costs are in the staffing procedures (leading to person hours) at institutional, governmental and local level.
- **Differentiate if possible in development, procurement and exploitation**
  Many tools tend to be available for free, probably most of the cost lies in the exploitation of them and summarizing the most promising in a guide.

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Some of the tools might not work as well as announced or might be manipulated, so it is important to test them regularly.

  One main problem is the constant improvements on both sides. Just as the goal of a guidance is to enable a better identification of fakes, the counterparts try to make fakes more believable. Since most algorithm rely on artificial intelligence (AI) to detect or disguise fakes, there is a kind of constant battle between the algorithms. This phenomenon is called a Generative Adversarial Network (GAN).

  Adversaries could use these same guides to improve their fakes.

  How durable is the idea (how long is the idea expected to be effective/useful?)
- As long as the manipulation of images and videos is used to disseminate disinformation and technology is able to identify fakes.

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

NAME OF THE IDEA

HYBRID ONLINE DILEMMA GAME

DESCRIPTION OF THE IDEA

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. The dilemma game can be designed to respond to a specific hybrid threat related issue, but as the threats evolve, their main value is in educating on the complex nature of the hybrid threats.

REFERENCE TO CAPABILITY GAP/NEED

- To improve awareness and understanding of the complexity and cross-sectoral impact of hybrid threats
- **Applicable JRC domains as stated by the gaps/needs**
  Applicable to all domains, depending on the scenarios that is used. However these games address mainly cross-domain challenges.
- **Applicable core theme(s) as stated by the gap/need**
  CT1: Future Trends of Hybrid Threats
  CT3: Resilient Civilians, Local Level and National Administration
  Dilemma games can improve players' situational understanding of current and future hybrid threats, and enhance decision-making capabilities.

TYPE OF SOLUTION

- **Technical**: a software tool
- **Social/human**: to be used for training, the dilemma online game can be part of a broader training session / program
- **Organizational/process**: can be widely used, within a specific sector/organization but also cross-sectoral/organization; the highest value is gained when using it for a better awareness and understanding at (inter-) governmental level

PRACTITIONERS

- **Provide disciplines for which the solution is valuable:**
  Can and should be used by practitioners across all disciplines in a whole-of-society approach. Current focus of end-users is within government administration.
- **Provide the level of practitioners in the same discipline:**
  - ***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).

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: The tool is already available and limitedly in use, TRL=9
- **In which stage is the solution (research, technology, available innovation, proven innovation):** proven innovation. Dilemma games have to some extent been developed, implemented and been proven useful.
- **Expected time to TRL-9.** Not applicable, solution has already been implemented.

- **Expected time to market.** Can be quickly and widely rolled out once it is commercialized
  Use cases: COVID-19, Hybrid threats against EU/NLD posed by RF and China, National and local crisis management

DESCRIPTION OF THE USE CASE(S)

TNO has to date developed various dilemma games. Some of the use cases include: COVID-19; Hybrid threats against EU/NLD posed by RF and China; National and local crisis management.

Meanwhile dilemma game for hybrid threat awareness have also been used and co-developed by other actors (CAN, UK, FIN) in the hybrid domain.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  To counter hybrid threats it is of utmost importance to understand the nature of hybrid threats and the challenges they pose for western democracies. Dilemma games contribute to enhance this understanding and to think about counteractions from different perspectives (DIMEL, PMESI, 13 JRC domains, etc.)
- **Resilience/defensive/offensive**
  Dilemma games enhance players' situational awareness and understanding of hybrid threats and improve the end-users' resilience.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the solution?**
  Basic IT is currently used to facilitate digital (online) dilemma games.
  Newer versions could make use of AI and big data to enhance the generation of scenarios and dilemma's, to make the advisory roles more realistic and interactive, and to improve data analysis.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc?.**
  If using classified scenarios, then some restrictions apply for the online use (internet). However, it is possible to use it in a controlled IT environment.
- Dilemma games pose thought experiments and insight into dilemma challenges for a very specific audience and case study. As such it is prudent that dilemma games are tailored to the audience's organization, their tasks and responsibilities and (topic) expertise).
- Sharing the methods and definitions of hybrid threats and the recommended strategies for countering them could be a risk. Due to the wide coverage required for this solution, it will be difficult to determine who is accessing the content and whether they are the instigators of the attacks.

	- If the solutions are to be used widely, it will be a challenge to maintain up to date versions that are validated and evaluated against the most recent threats – especially if the game is used in local languages
COSTS - **Indication of costs** **Differentiate if possible in development, procurement and exploitation** Indication of procurement costs is assessed as low; driven mostly by the appointment of subject matter experts, the development of the game, and the training of facilitators. The production of the dilemma game content (scenario, dilemma's, advice) can be done in +/- 100 person-hours. Subject matter expertise is essential for both the quality of content and the speed of development. Exploitation costs are assessed as very low; dilemma games require a digital facilitation space for the game(s) to be run. The post-game discussion can be facilitated in a physical environment, or through a digital teleconference platform (MS Teams, Skype, Zoom, etc.). Physical on-site facilitation enjoys the preference due to improvements in the facilitation of discussion.	**COUNTERMEASURES** - **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution**? - The tool can be hacked, which is not very plausible. A hack would lead to data tapping or temporarily out-of-service. If hostile actors obtain the (outcome of) dilemma games, they could exploit this knowledge to their advantage by targeting the identified vulnerabilities. - Likewise, the hostile actors could predict reactions and responses based on the steps in the game making it easier for them to plan around them. - **How durable is the idea (how long is the idea expected to be effective/useful?)** The use of dilemma games is not restricted in time, it is always valuable to think about hybrid threats and the dilemmas they pose. The challenge will be to think about new types of hybrid threats and/or the evolution of hybrid campaigns. - Hybrid threats are characterized by its flexibility and rapid ability to adapt to circumstances and (counter-)actions. As such, dilemma games can give insight into specific dilemmas for known hybrid threats. Yet the unknown manifestation of hybrid threats always looms around the corner. The development, training and utilization of dilemma

	games is as such dependent on a solid foundation of up-to-date understanding and intelligence of the hybrid threat landscape.

<table>
<tr><td colspan="2"><b>NAME OF THE IDEA</b>
Efficient cyber threat information sharing through Hyper Connectivity networks
<b>DESCRIPTION OF THE IDEA</b>
Cyber threat information sharing is not a cure-all solution, but it is a critical step toward improving cyber defenses especially against zero-day vulnerabilities. The benefits of information sharing through hyper connectivity, are numerous. High speed sharing enables organizations to enhance their cyber defenses by leveraging the capabilities, knowledge, and experience of a broader community. It can provide better situational awareness of the threat landscape, including a deeper understanding of threat actors and their tactics, techniques, and procedures (TTPs), and greater agility to defend against evolving threats. It can improve coordination for a collective response to new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors.</td></tr>
<tr><td><b>REFERENCE TO CAPABILITY GAP/NEED</b>
- <b>Describe the use of the solution about the gap/need</b>
Use hyper connectivity as a multiplier of cyber security and cyber defense against common and zero-day vulnerabilities, through sharing.
- <b>Applicable JRC domains as stated by the gaps/needs:</b>
It can be related to helping countering disinformation across all 13 domains.
- <b>Applicable core theme(s) as stated by the gap/need:</b>
○ CT2: Cyber and Future Technologies
○ CT3: Information and Strategic Communications
○ CT4: Future Trends of hybrid threats</td><td><b>TYPE OF SOLUTION</b>
- <b>Technical</b>
○ Information Sharing Platforms
- <b>Social/Human</b>
○ Information Security Collaboration programs
- <b>Organizational/Process</b>
○ Security Operation Centers
○ CSIRTS
○ Information Sharing and Analysis Centers (ISACs)
○ Financial Services Information Sharing and Analysis Center (FS-ISAC)
○ Electricity Sector Information Sharing and Analysis Center (ES-ISAC)</td></tr>
<tr><td colspan="2"><b>PRACTITIONERS</b>
- <b>Provide applicable domains for which the solution is valuable:</b>
○ Private sector / Financial Services / Critical Infrastructures / Public Sector – Organizations / Military Sector / Ministries / Media / Personal and local services / Transportation / Healthcare
- <b>Provide the level of practitioners in the same discipline:</b>
○ <b><i>Ministry level</i> (administration):</b> policymakers and decisionmakers at (for hybrid) relevant ministries: Economy, Security, Defense, Internal affairs, External affairs, Critical Infra, Intelligence services
○ <b><i>Local level</i> (cities and regions):</b> Mayors, regional boards.
○ <b><i>Support functions to ministry and local levels</i> (incl. Europe's third sector):</b> industry participation in game sessions might be useful in relation to the protection of critical.</td></tr>
</table>

- **Provide the expected end-users of the solution:**

  Computer security incident response teams (CSIRTs)
  system and network administrators,
  cybersecurity specialists,
  privacy officers,
  technical support staff,
  chief information security officers (CISOs),
  chief information officers (CIOs),
  computer security program managers, and
  others who are key stakeholders in cyber threat information sharing activities.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: Sharing Platforms between organization are is already available and limitedly in use, TRL=9
- **In which stage is the solution (research, technology, available innovation, proven innovation):** Available innovation.
- **Expected time to TRL-9.** Not applicable, solutions have already been implemented.
- **Expected time to market.** Already in use

  Use cases: NATO CERT / EU CERT / ISACS / Eu members CSIRT-CERT network

DESCRIPTION OF USE CASE(S)

Technology is becoming more segmented but also more hyperconnected. You can see that in the evolution of the private, public, and hybrid cloud and with a combination of infrastructure-as-a-service, platform-as-a-service, and software-as-a-service providers clamoring to support new growth.

In order to take advantage of this hyperconnectivity it can be used as multiplier in sharing fast and on time cyber threats and new exposed zero-day vulnerabilities.

The NIS Directive in Article 12 establishes the **CSIRTs Network** “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation” (Full text of the NIS Directive**)**. The CSIRTs Network is a network composed of EU Member States’ appointed CSIRTs and CERT-EU (“CSIRTs Network members.

The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents.

IMPACT ON COUNTERING HYBRID THREATS

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

  Through hyper connectivity networks cyber information-sharing partnerships will proliferate, especially regionally, and the diversity of the domains and sectors they serve will increase. Shared information using hyper connectivity networks incorporate adversary behaviour elements and behavioural analytics, which are designed to detect real-time behavioural patterns of an unfolding cyber-attack (zero-day indicators). In this context, MS will be prepared for next attacks.
- **Resilience/defensive/offensive**

  Information Sharing tacking advantage hyper connectivity networks, mainly support and increase defensive capabilities and especially:

  - Internet of Things consortia will begin to rapidly form to share cyber information associated with the intersection of device security and safety (e.g., medical devices, autonomous vehicles, on-board avionics, zero-day network attacks).

○ Sharing will increasingly occur as machine-to-machine transactions that are managed by trust contracts and chronicled as transactions on blockchain infrastructures. ○ Shared information using hyper connectivity networks will increasingly incorporate adversary behavior elements and behavioral analytics, which are designed to detect real-time behavioral patterns of an unfolding cyber-attack (zero-day indicators).	
ENABLING TECHNOLOGY - **Which technologies are critical in fielding the idea?** ○ Open IOC, ○ STIX, ○ IODEF ○ TAXII model	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** ● Organizational information sharing, security is one of the biggest barrier. At the same time legal and ethical restrictions are also applicable.
COSTS - **Indication of costs**: Development of a security concept and implementing that 24/7 Service for the Platform 24/7 Server/Data center with fail-safe operation and high performance - **Differentiate if possible, in development, procurement and exploitation** - N/A	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? The downside to hyperconnectivity is unquestionably hyper-vulnerability. Hyper connectivity vastly improves how we communicate and share information. However, it is also bringing in new security risks and compliance requirements. Some security (best practices) protocols might mitigate this potential vulnerability, but would also decrease the effectiveness of such hyperconnectivity : ● Perform automated analyses and technical mitigations to delete personal data that is not directly related to a cyber threat. ● Minimise the amount of data included in the shared threat intelligence – focusing only on content hat is directly related to a cyber threat. ● Retain only information needed to address cyber threats. ● Ensure any information collected is used only for network defence or limited law enforcement purposes. Competitive advantage in hyperconnectivity vulnerability will be driven by volume and usage of Fast Data — data that is collected

	and analyzed in real time to support decision processes in real time, early warning systems based on opinion mining, awareness and real-time feedback. Investment in security will be required from the outset to facilitate this. Countermeasures. Cyber attacks? Flooding of signals/information to the networks? A flood of hyperconnected information might lead to an information overload where the context or initial question/problem is lost in translation. - **How durable is the idea (how long is the idea expected to be effective/useful?)** The main idea of the solution using legacy networks is in place many years before, so the advanced solution is also going to last and be effective as long as vulnerabilities and zero days exists.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** o CISA uses the Traffic Light Protocol (TLP) according to the FIRST Standard Definitions and Usage Guidance. TLP was created in order to facilitate greater sharing of information. o Cyber Information Sharing, and Collaboration Program (CISCP) which enables information exchange and the establishment of a community of trust between the Federal Government and critical infrastructure owners and operators. o Sector-specific Information Sharing, and Analysis Centers (ISACs) which are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry. o European CSIRT /CERTS network (National / Military /Private / Academic) for information sharing mainly through MISP	

NAME OF THE IDEA

Journalism Trust Initiative

DESCRIPTION OF THE IDEA

JTI is a collaborative standard setting process according to the guidelines of CEN, the European Committee for Standardization. More than 120 experts have contributed to this CEN Workshop Agreement (CWA) that was published on 19 December, 2019

This tool is process-focused. It evaluates how information is produced and disseminated.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  Manipulated information in the social media
- **Applicable JRC domains as stated by the gaps/needs:**

  Information
  Social/Societal
  Cyber
- **Applicable core theme(s) as stated by the gap/need:**

  Information and Strategic Communications

TYPE OF SOLUTION

- **Technical**
- **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
- **Provide the level of practitioners in the same discipline:**

  Strong involvement and impact:
  - 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**

  The Intended users are Journalists and the General Public

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:

  TRL9

  In which stage is the solution (research, technology, available innovation, proven innovation):

  Fully operational
- **Expected time to TRL-9.**

  0 years
- **Expected time to market.**

  0 years

DESCRIPTION OF USE CASE(S)

This tool is focused on promoting trustworthy journalism and reducing disinformation through the development of standards of transparency, journalistic methods, and ethics. The aim is for these standards to be used as a self-regulatory mechanism and eventually could lead to certification processes for media outlets. In addition to being used by journalists and the general public, the standards are relevant for tech companies and for advertisers as well as those in media development.

IMPACT ON COUNTERING HYBRID THREATS

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

  Increases societal resilience to fake news

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY - **Which technologies are critical in fielding the idea?** Machine learning and AI	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** No, it is free of charge and available to the public
COSTS - **Indication of costs**: Free of Charge - **Differentiate if possible, in development, procurement and exploitation**	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Not possible as the stakeholders are involved - **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** Founding organizations are European Broadcasting Union (EBU), the Global Editors Network (GEN), Agence France Presse (AFP); facilitated and published by Association française de normalization (Afnor), Deutsches Institut für Normung (DIN) and the European Committee for Standardization (CEN) Google and Facebook participated in the development of standards.	

NAME OF THE IDEA

Non-partisan native-language news channels for most interdependent abroad regions

DESCRIPTION OF THE IDEA

Establishing non-partisan local-language (Russian, Arabic, Mandarin) Media, TV News channels to offer foreign language-speaking communities in the EU an independent news source as an alternative to Abroad officially approved news broadcasts. The problems are on various scales as this phenomena can be addressed to national or sub-national levels:

- On the national level, it is based on national minorities tightly related with neighbourhood countries to ensure the freedom of speech and critically selected and presented information based on ethical journalistic principles is accessible for all ethnical groups. The major instrument is a national television and news broadcasters, providing the ability for foreign language speaking groups to have access to a wide spectrum of information or different views to create an adequate context understanding of situations.
- The European Union is open to external threats and negative narratives creation and manipulation of the information. Europe wide propaganda facilitating radicalization, extremism and targeted situation interpretation of minorities. There are several initiatives in the European Union in progress. The decision was made on the EU parliament level to respond to disinformation and propaganda on the union level by launching and developing activities supporting by German, France and other countries, with broadcasters like “Deutsche Welle” providing the news line in the Russian language, another minorities language for a whole European Union and abroad region.

  In a May 2015 joint statement by the Foreign Ministers of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, and Sweden expressed support for initiatives targeting Russian-speakers with 'alternative sources of information, to ensure a 'pluralistic media landscape, where all people have easy access to independent information. Ministers agreed to look into a 'mechanism to counter disinformation and expressed their support for the efforts undertaken by the European Endowment for Democracy with respect to supporting Russian-language media in the Eastern Partnership States and beyond. https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/559471/EPRS_BRI(2015)559471_EN.pdf

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  Manipulated information in the social media, Fake News, Propaganda
- **Applicable JRC domains as stated by the gaps/needs:**

  Media
  Information
  Social/Societal
- **Applicable core theme(s) as stated by the gap/need:**

  Information and Strategic Communications

TYPE OF SOLUTION

- **Organizational/Process**

  It requires clear context understanding and awareness by monitoring the marginal media ecosystem and per language group to understand language-specific narratives' dominants and plan a timely response to counter them. Marginal media, due to a limited number of citizens is economically self not sustainable and therefore requires political supporting and targeted additional financing from national recourses.

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**

  Administration
  Culture
  Information
  Social/societal
- **Provide the level of practitioners in the same discipline:**

  Strong involvement and impact:
  - 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**

  The Intended users are foreign language speaking communities and the Abroad General Public of State controlled media environments

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:

  TRL9

  In which stage is the solution (research, technology, available innovation, proven innovation):

  Operational and should scale up
- **Expected time to TRL-9.**

  0 years
- **Expected time to market.**

  0 years

DESCRIPTION OF USE CASE(S)

Provide alternative trusted information source for limited languages speaking societal groups to increase resilience and exposure for radicalization, polarization and other manipulated effects mostly for Russian, Arabic and Mandarin speaking societies

IMPACT ON COUNTERING HYBRID THREATS

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

  Increases societal resilience to fake news and propaganda, provide alternative source of news and media built on democratic journalism principles
- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**

  Multilingual news and media content

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

  Legal – relates to national media regulation. Ethical or cultural alignment is a very sensitive point where it should be carefully balanced cultural values of the minority with a national perspective's values line. Its a highly important credibility aspect not only information wise but also institution like a media broadcaster and representative spokesman as a person. Ethically – it will present the usual challenges of building a trusted news source that can present itself as independent and not widely considered an instrument of foreign influence. It would be useful, rather than building an organization from scratch, to build on existing organizations that have a track record of honesty and existing bonds with the community they serve. Another security-related or practical concern to have in mind is the ability of such organization to operate inside some countries and how that could affect its capability to build a rapport with the intended audience.

COSTS

- **Indication of costs**:

  Resources required for trusted broadcasting channels to support alternative languages.

  Technical costs related to broadcasting to other regions. Additional broadcasting licenses for these regions.

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?

  Will vary on country legislation and broadcasting possibilities. Undermining of trust in the situation.

  Broad regions having only manipulated and propaganda-based information spread in their

- **Differentiate if possible, in development, procurement and exploitation** Development of new or adapted content to meet marginal audiences profiles, needs and interests.	native language ensures a wide population and citizens support due to limited access to the presented context. One of the backfire instruments is to provide alternative news streams on their language broadcasted from the European Union. Countermeasures for this solution – limited access to the source, it has numerous way to discredit the information is being spread or even closed. It certainly looks that this approach will bring on countermeasures that could significantly degrade the effectiveness of the solution: a nationalistic campaign painting the solution as foreign meddling and other attacks to its core credibility. Also more practical measures to jeopardize its reach: blocking access for users inside the country, restrictions to operate inside said country etc. **How durable is the idea (how long is the idea expected to be effective/useful?)** As long as media channels supported.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** N/A	

NAME OF THE IDEA **Open European Quantum Key Distribution Testbed (OPENQKD project)** **DESCRIPTION OF THE IDEA** OPENQKD brings together a multidisciplinary team from 13 countries to reinforce Europe's position at the forefront of quantum communication capabilities globally.	
REFERENCE TO CAPABILITY GAP/NEED - **Describe the use of the solution in reference to the gap/need** Primary Context No. 1.: Game changers: Quantum as a disruptive technology Primary Gaps No. 1.: Weak level of digital security: digital security architecture, numerical technologies and encryption protocols - **Applicable JRC domains as stated by the gaps/needs:** Cyber / Infrastructure / defence - **Applicable core theme(s) as stated by the gap/need:** CT2: Cyber and Future Technologies	**TYPE OF SOLUTION** - **Technical:** the testbed itself is a technical solution - **Social/Human** - **Organizational/Process:** the cooperation between the 13 countries is an organizational measure (building an ecosystem) which has not only value for developing a testbed but also for sharing information, knowledge, training etc.

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  cybersecurity, risk management, policy making
- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level* (administration):** policy making, risk management
  - **II) *local level* (cities and regions):** cybersecurity
  - **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)**:
  Quantum computing in general is +/- TRL 4
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Research
- **Expected time to TRL-9.**
  +/- 5 years
- **Expected time to market.**
  +/- 5 years

DESCRIPTION OF USE CASE(S)

The project will create an open QKD testbed to promote network functionality and use-cases to potential end-users and relevant stakeholders from research and industry. Over 25 use-case trials have already been determined and will be complimented by open calls for funding third parties. OPENQKD will develop an innovation ecosystem and training ground as well as helping to grow the technology and solution supply chains for quantum communication technologies and services

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Understanding of vulnerabilities and scope of potential impact
- **Resilience/defensive/offensive**
  resilience and defensive

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Telecommunication equipment manufacturers, end-users and critical infrastructure providers, network operators, QKD equipment providers, digital security professionals and scientists

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  System operational security of the quantum computers.

  Given the sensitive nature of quantum computing, trust needs to be built between the various partners within the project.

  Very high costs of quantum computing (at this stage)

	Slow growth of the quantum computing community and general knowledge related to quantum computing
COSTS - **Indication of costs**: Cost drivers include Equipment: costs of a quantum computer and related physical hardware In the development process, the developer needs to have access to quantum computers, mostly not freely available. The technologies in quantum computing are still not ready yet. - **Differentiate if possible in development, procurement and exploitation** N/A	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Espionage stealing (the access to) the keys Transitioning from legacy to quantum systems will entail a period of specific vulnerabilities, especially to quantum-capable nations. - **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 is to be considered as input providers on the subject for further discussions and knowledge building	

NAME OF THE IDEA Tool that monitors and detects the population's response to the information being published (e.g., when an event is in progress and information has been shared with population) and is able to identify the dominant emotion occurring in social networks**.** **DESCRIPTION OF THE IDEA** Tool with the capability to detect/analyze emojis in order to improve the understanding of user's perceptions, sentiment, and emotion	
REFERENCE TO CAPABILITY GAP/NEED **Describe the use of the solution in reference to the gap/need** The solution can be used to grasp the citizen's response to the outreach strategies in order to capture responses and evaluate the success of the communication campaign **Applicable JRC domains as stated by the gaps/needs:** Administration (Education) Social/Societal Culture **Applicable core theme(s) as stated by the gap/need:**	**TYPE OF SOLUTION** - **Technical** Organisational Probably the central government could be involved to facilitate the implementation on local level

Resilient civilians, local level and administration	
PRACTITIONERS - **Provide applicable JRC domains for which the solution is valuable:** Administration (Education) Social/Societal Culture Public Administration - **Provide the level of practitioners in the same discipline:** **Strong involvement and impact** ○ 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** NGO's	
STATE OF THE ART - **Indication of Technology Readiness Level (TRL 1-9 index)**: TRL7 **In which stage is the solution (research, technology, available innovation, proven innovation):** Research is ongoing **Expected time to TRL-9.** Not known to the author **Expected time to market.** Not known to the author	
DESCRIPTION OF USE CASE(S) The tool (developed by INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS) has been applied in the National Portuguese project MISNIS (Intelligent Mining of Public Social Networks' Influence in Society, 2013—2015)	
IMPACT ON COUNTERING HYBRID THREATS - **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.** The solution can be used to capture the society's response to outreach strategies designed to fight social inequality and injustice, and can help in the society's resilience to hybrid threats - **Resilience/defensive/offensive**	
ENABLING TECHNOLOGY - **Which technologies are critical in fielding the idea?** - **Social media analytics**	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - To be discussed

COSTS - **Indication of costs**: Not known to the author - **Differentiate if possible, in development, procurement and exploitation**	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? As long as emojis are used, the effectiveness of the solution remains important - **A malicious actor can give directions to a large group to respond to the communication campaign in an organised manner, in order to direct the public opinion.** - - **How durable is the idea (how long is the idea expected to be effective/useful?)** The solution will remain effective as long as the cause remains the same, that is, as long as social media are widely used

MISCELLANEOUS

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

According to a study by WordStream[10], using an emoji in a Tweet can increase engagement by 25% compared to messages without emoji. The total use of emoji is increasing which facilitates the use of this innovation.

NAME OF THE IDEA

Public-private information-sharing groups developing collaborative investigations and collective action[11]

DESCRIPTION OF THE IDEA

Cyber information sharing can also drive collective investigations and actions between the public and private sectors. Cybercrime cannot be addressed without creating a more effective deterrence model by confronting the source of cybercriminal activity, reducing the return on investment and making the risk of prosecution real.

The most successful information sharing models that are emerging in the global community and which can detect and disrupt cybercrime are between law enforcement and the private sector. Unlike traditional crime, the skills, data and capabilities to detect and disrupt cybercrime often reside within the private sector. More are required, but these emerging models have been difficult to scale up. Sharing information between parties is fraught with potential privacy and security concerns. It also poses the challenge of ensuring protections for free expression rights and political participation. Incentive models remain nascent, as groups try to understand who bears the cost and responsibility for driving collective action.

[10] Kim. L, 'The Stupid-Simple Secret Ingredient to Better Engagement on Twitter', WordStream, 2018 link

[11] Many information are from the report : Information Sharing and Analysis Centres (ISACs) Cooperative models, ENISA report

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution about the gap/need**
  Use of information sharing can increase resilience for common and zero-day vulnerabilities.
- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all 13 domains.
- **Applicable core theme(s) as stated by the gap/need:**
  - CT2: Cyber and Future Technologies
  - CT3: Information and Strategic Communications

TYPE OF SOLUTION

- **Technical**
  - Information Sharing Platforms
- **Organizational/Process**
  - **Several organization participate in this innovation**

PRACTITIONERS

- **Provide applicable domains for which the solution is valuable:**
  - Private sector / Financial Services / Critical Infrastructures / Public Sector – Organizations / Military Sector / Ministries / Media / Personal and local services / Transportation / Healthcare
- **Provide the level of practitioners in the same discipline:**
  - ***Ministry level* (administration):** policymakers and decisionmakers at (for hybrid) relevant ministries: Economy, Security, Defense, 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.
  - **Provide the expected end-users of the solution:**

    Computer security incident response teams (CSIRTs)
    system and network administrators,
    cybersecurity specialists,
    privacy officers,
    technical support staff,
    chief information security officers (CISOs),
    chief information officers (CIOs),
    computer security program managers, and
    others who are key stakeholders in cyber threat information sharing activities.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: Sharing Platforms between organization are is already available and limitedly in use
- **In which stage is the solution (research, technology, available innovation, proven innovation):** Available innovation.
- **Expected time to TRL-9.** Not applicable, solutions have already been implemented.
- **Expected time to market.** Already in use

DESCRIPTION OF USE CASE(S)

1. European Cybercrime Centre (EC3): Europol set up the EC3 in 2013 to strengthen the law enforcement) response to cybercrime in close collaboration with the private sector. EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds of on-the-spot operational deployments resulting in hundreds of arrests
2. The National Cyber-Forensics and Training Alliance was established in 2002 as a non-profit partnership between private industry, government and academia, with the purpose of providing a neutral trusted environment that enables two-way collaboration. To date, the NCFTA has enabled its community to prevent more than one billion dollars in potential losses, identify critical threats and tackled more than 2,500 law enforcement cases.
3. Microsoft Digital Crime Unit (DCU): The DCU is an international team of attorneys, investigators, data scientists, engineers, analysts and business professionals based in 30 countries, working together to fight digital crime. Since 2010, the DCU has collaborated with law enforcement and other partners on 22 malware disruptions, resulting in more than 500 million devices rescued from cybercriminals.
4. Cyber Defence Alliance (CDA): The CDA, with its headquarters in London, is a cyber defence and anti-fraud group consortium of financial institutions originally founded by Barclays, Santander, Standard Chartered and Deutsche Bank in 2015. The CDA works with member organizations and law enforcement agencies in a co-located space to share information and turn it into actionable intelligence to prevent malicious activity and identify threat actors for criminal investigation.
5. Information Sharing and Analysis Centres (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector. ISACs have created communities within the private sector. They could be oriented on a specific critical sector (e.g. finance, energy, health) or serve as a focal point on the national level to gather information about cyber incidents and analyse it. ISACs involve stakeholders from both the private and the public sector (56% - 44% ratio). The status of PPPs in Europe is covered in a report which constitutes part of the same project: Public Private Partnerships (PPPs) Cooperative model (https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/). The main difference is that ISACs are generally more formal than any other types of PPPs in the field of cybersecurity. With each industry sector free to set up their ISAC, the ISAC differ wide in quality, structure and in how they are funded, managed and operated (Prieto, 2006). The whole concept of this kind of cooperation is connected with sharing information and analysis concerning cybersecurity incidents. This reason increases formality in this cooperative model as the actors/stakeholder involved in the process need to follow a clearly defined framework for sharing both information and analysis.

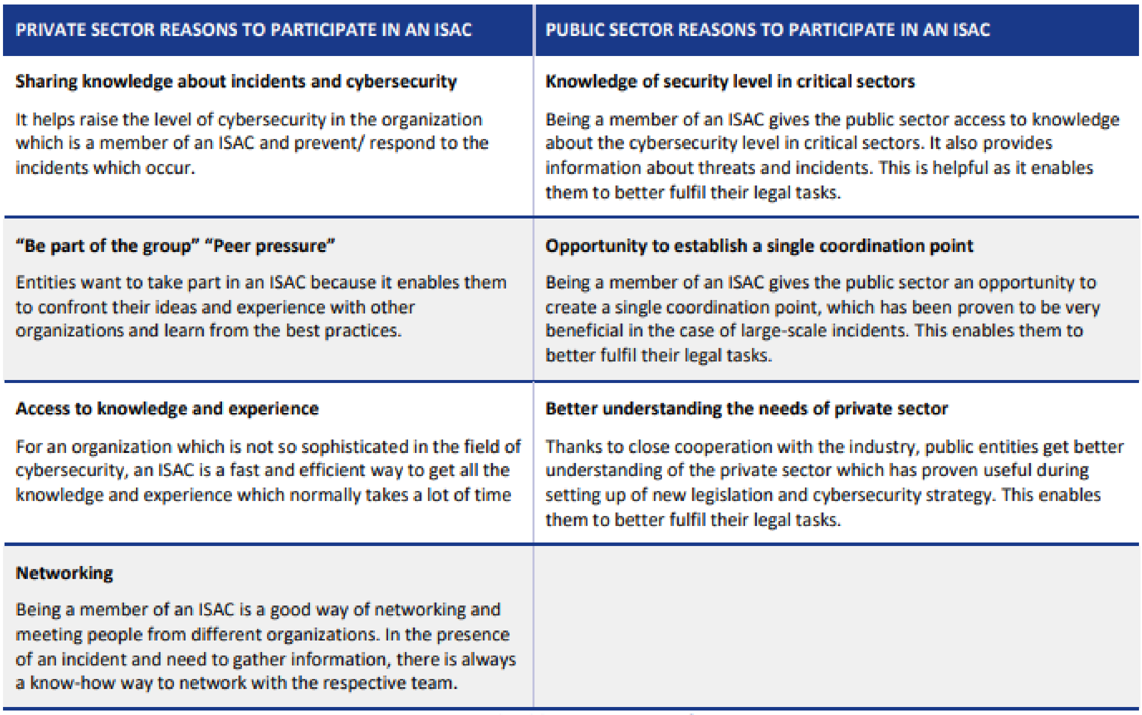
IMPACT ON COUNTERING HYBRID THREATS

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

Increase resilience and cyber threats intelligence by:

- Information sharing
- Analysis
- Trust building
- Capacity building

Reasons to participate in ISAC:



PRIVATE SECTOR REASONS TO PARTICIPATE IN AN ISAC	PUBLIC SECTOR REASONS TO PARTICIPATE IN AN ISAC
Sharing knowledge about incidents and cybersecurity It helps raise the level of cybersecurity in the organization which is a member of an ISAC and prevent/ respond to the incidents which occur.	**Knowledge of security level in critical sectors** Being a member of an ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It also provides information about threats and incidents. This is helpful as it enables them to better fulfil their legal tasks.
"Be part of the group" "Peer pressure" Entities want to take part in an ISAC because it enables them to confront their ideas and experience with other organizations and learn from the best practices.	**Opportunity to establish a single coordination point** Being a member of an ISAC gives the public sector an opportunity to create a single coordination point, which has been proven to be very beneficial in the case of large-scale incidents. This enables them to better fulfil their legal tasks.
Access to knowledge and experience For an organization which is not so sophisticated in the field of cybersecurity, an ISAC is a fast and efficient way to get all the knowledge and experience which normally takes a lot of time	**Better understanding the needs of private sector** Thanks to close cooperation with the industry, public entities get better understanding of the private sector which has proven useful during setting up of new legislation and cybersecurity strategy. This enables them to better fulfil their legal tasks.
Networking Being a member of an ISAC is a good way of networking and meeting people from different organizations. In the presence of an incident and need to gather information, there is always a know-how way to network with the respective team.	

- **Resilience/defensive/offensive**

Resilience capabilities will be offered

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  - **n/a**

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Not really, only regulatory requirements including data protection concerns for their establishment exist

COSTS

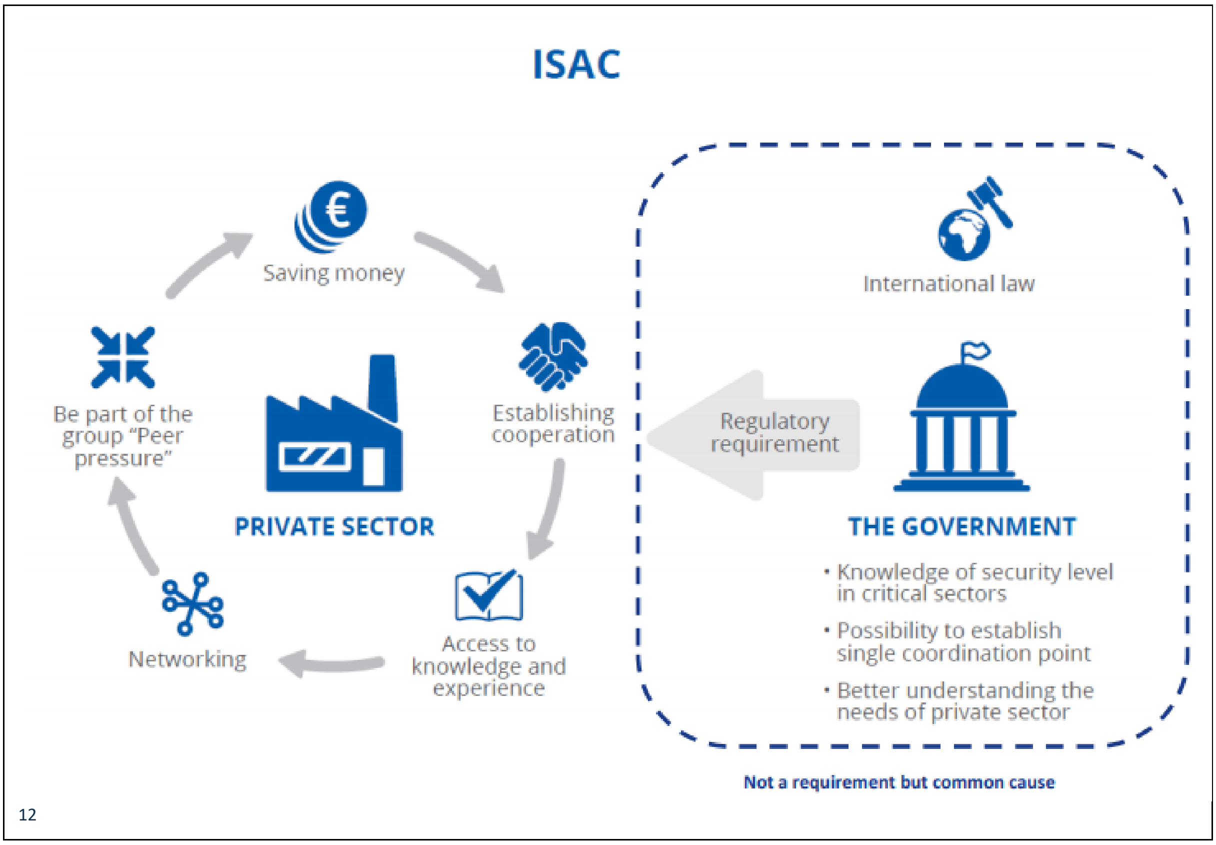
- **Indication of costs**:
  While there are no-cost and open-source technologies such as MISP, The Hive, Cortex
  and IntelMQ, there are still significant technical resources required to implement technology to create and/or participate in cybersecurity information-sharing communities. This can reduce the overheads of producing information and/or refining others' information into actionable intelligence, or allow easy integration between threat information sharing feeds and the range of security/investigation tools used by defenders.
- **Differentiate if possible, in development, procurement and exploitation**
  N/A

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  - There is a lack of trust between key players at operational and governmental levels, which needs to be developed to facilitate information sharing. Geopolitical drivers and fragmentation in international co-operation can affect public-sector enthusiasm for data exchange programmes. The private sector is often reluctant to share information with governments for fear of regulatory impact, to avoid complicity in any privacy and rights violations and because they often see no benefit to doing so.

	○ Lack of resources. The biggest challenge for both the public and the private sector is lack of (human) resources. Firstly, because the overall lack of cybersecurity experts on the market, especially in the area of information analysis, but also the high value of the existing resources. Because of this, the industry is not willing to share experts and appoint them to work for ISACs. Secondly, in the case of the public sector, there are not enough people to support the industry. This concerns not only the secretarial role but also the ability to involve experts who could support the industry on the policy level (e.g. create recommendations, standards) ○ Duplication of information. It is clearly underlined by experts that due to the existence of many information sharing-groups, the same information is usually passed through different sources. It results in the fact that multiple groups are processing information and acting in parallel. There is often a general lack of coordination ○ IT tools affecting data integrity The choice of the right tools to use to ensure data integrity is also a challenge for many ISAC. If the ISAC doesn’t have enough funding it is difficult to acquire specialised tools for information sharing and for data analysis. In some cases, ISACs build tools in-house but these kind of solutions are not interoperable and cannot ensure highest level of security. The community however has understood this challenge and more specialised tools are shared between the stakeholders involved (e.g. MISP is offering a complete toolbox for information sharing and analysis). ○ It is often perceived as financially advantageous for the victims of cybercrime to negotiate and deal directly with the attacker; as the social and brand impact can have

	greater long-term consequences than an initial hack. Thus, a company favours brand reputation of consumer perception over the financial obstacles created by a cyberattack. ○ Victims can have reduced appetite to trigger the traditional processes of law enforcement due to a perceived lack of LEAs’ resources, training and experience to deal with cybercrime. Therefore, criminals can exploit this by lowering payment demands and increasing volume. - **How durable is the idea (how long is the idea expected to be effective/useful?)** The main idea of the solution using legacy networks is in place many years before, so the advanced solution is also going to last and be effective as long as vulnerabilities and zero days exists.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** **Law requirements:** They are being created because there is a specific law which obliges the industry to share information (with the public administration) or they are created to support the implementation of the law as an advisory body e.g. European aviation ISAC, European Energy ISAC, Banking Cybersecurity Centre in Poland. **Economic interests :** For the private sector this is usually the most common reason to establish ISACs. Usually the growing number of threats and incidents demonstrate that sectorial cooperation is essential to strengthen one’s defence. **Social interests.** Beside economic interests, social interests are the second most common reason to establish ISAC. This is mainly the reason for entities with huge experience and know-how in terms of cybersecurity **Public relations.** When an organisation is the critical operator (e.g. banking sector, energy sector), it is important to communicate that the company is safe and will deliver services even if an incident occurs. Therefore, positive public relations could be a reason for the top management to invest in cybersecurity.	



ISAC

Saving money

Establishing cooperation

Access to knowledge and experience

Networking

Be part of the group "Peer pressure"

PRIVATE SECTOR

Regulatory requirement

International law

THE GOVERNMENT

- Knowledge of security level in critical sectors
- Possibility to establish single coordination point
- Better understanding the needs of private sector

Not a requirement but common cause

[12]

NAME OF THE IDEA

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

DESCRIPTION OF THE IDEA

FutureTPM will provide a new generation of TPM-based solutions, incorporating robust and formally verified QR cryptographic primitives. The goal is to enable a smooth transition from current TPM environments, based on existing widely used and standardized cryptographic techniques, to systems providing enhanced security through QR cryptographic functions, including secure authentication, encryption and signing functions. (see also https://futuretpm.eu/)

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gap/need** - Primary Context No. 1.: Game changers: Quantum as a disruptive technology - Primary Gaps No. 1.: Weak level of digital security: digital security architecture, numerical technologies and encryption protocols - - **Applicable JRC domains as stated by the gaps/needs:**	- **Technical: T**PM based solutions including cryptographic tools/algorithms - **Social/Human** - **Organizational/Process**

[12] Information Sharing and Analysis Centres (ISACs) Cooperative models, ENISA

- Cyber / Infrastructure / defence

  Applicable core theme(s) as stated by the gap/need:

  CT2: Cyber and Future Technologies

PRACTITIONERS

- **Provide disciplines for which the solution is valuable:** cybersecurity, risk management, policy making
- **Provide the level of practitioners in the same discipline:**
  - **I) ministry level (administration):** policy making, risk management
  - **II) local level (cities and regions):** cybersecurity
  - **III) support functions to ministry and local levels (incl. Europe's third sector):**

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:

  TBD , not certain, probably 4-6
- **In which stage is the solution (research, technology, available innovation, proven innovation):**

  Technology
- **Expected time to TRL-9.**

  +/- 5 years for quantum computing in general

  Expected time to market.

  +/- 5 years for quantum computing in general

DESCRIPTION OF USE CASE(S)

The goal of FutureTPM is to design a Quantum-Resistant (QR) Trusted Platform Module (TPM) by designing and developing QR algorithms suitable for inclusion in a TPM. The algorithm design will be accompanied with implementation and performance evaluation, as well as formal security analysis in the full range of TPM environments: i.e. hardware, software and virtualization environments. Use cases in online banking, activity tracking and device management will provide environments and applications to validate the FutureTPM framework

IMPACT ON COUNTERING HYBRID THREATS

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

  Understanding of vulnerabilities and scope of potential impact.
- **Resilience/defensive/offensive**

  Resilience and defensive

- **ENABLING TECHNOLOGY**
- **Which technologies are critical in fielding the solution?**

  QR crypto and Trusted Platform Module (TPM) developers

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

  Operational system security remains

	paramount for any quantum computing systems.
COSTS - **Indication of costs**: Cost drivers include: High development cost for quantum computing High costs for quantum computing hardware Expensive personnel costs (small and slow growing quantum computing community) - **Differentiate if possible in development, procurement and exploitation** N/A	- **COUNTERMEASURES** - **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution**? N/A - **How durable is the idea (how long is the idea expected to be effective/useful?)** N/A
MISCELLANEOUS **Any additional remarks//disclaimers/comments/information you might want to provide** This is to be considered as input providers on the subject for further discussions and knowledge building.	

NAME OF THE IDEA

Resilient Democracy Infrastructure Platform

DESCRIPTION OF THE IDEA

It is an organizational structure integrating various essential crisis response mechanisms into a single digital platform. Dimensions include:

- Awareness Rising;
- StratCom;
- Risk Communication;
- Crisis Communication;
- Early Warning;
- Civilian Preparedness, Resilience of Individuals and Households;
- Cyclical Capability-Planning and Readiness Improvement.

The *whole-of-society* resilience should ensure sufficient level of civil preparedness – households, communities, industries, infrastructure(s) and government(s) – to resist and (quickly) recover from crises. The resilience is multi-level and should comprehensively binding together all societal resources available to withstand and recover from large-scale shocks.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need:**

Awareness raising, monitoring online and offline security risks and sharing this information with target audiences, as well as providing technical support while even offering direct protection against the most severe threats.

- **Applicable JRC domains as stated by the gaps/needs:**

Resilient civilians, local level and administration.
Infrastructure, Public Administration.

- **Applicable core theme(s) as stated by the gap/need:**

Resilient civilians, local level and administration.

TYPE OF SOLUTION

- **Technical**
- **Social/Human**
- **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC disciplines for which the solution is valuable:**

Infrastructure, Public Administration.

- **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)**

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 3.
- **In which stage is the solution (research, technology, available innovation, proven innovation):** Some similar protypes as "Be Prepared!" *app* or "Propastop" platforms are tested and in use in Estonia.
- **Expected time to TRL-9.** 2-3 years.
- **Expected time to market.** 3-5 years.

DESCRIPTION OF USE CASE(S)

The integrated platform should contain:

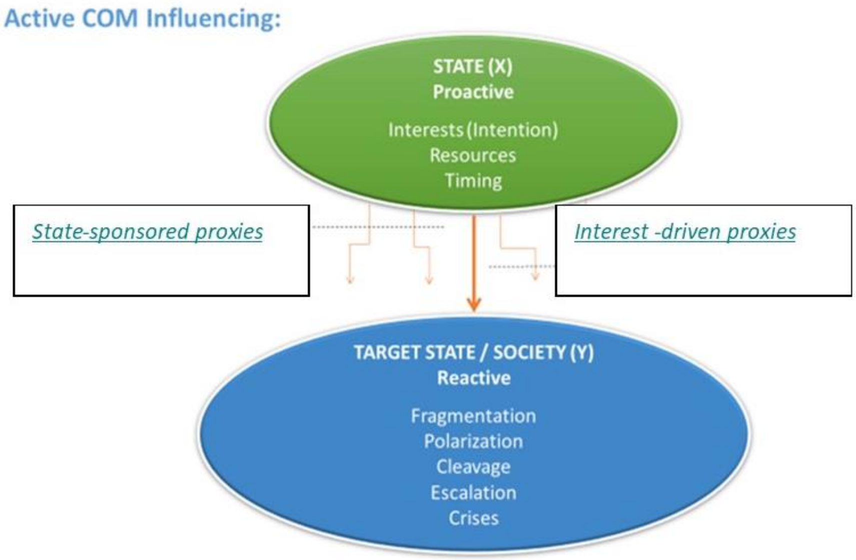
- Official announcements *all-in-one-place online* to the public by the governmental agencies and local authorities;
- Expert advise on how to behave in different emergency and crises situations, incl. what to do in the event of pandemic, a power outage, how to provide first aid, information about fire and water safety, natural disasters, disruption of vital services, food supplies, cyber threats and other safety and security issues;
- Official information and availability of essential public services such as energy, medical, food and other supplies, hospitals, functionality of public transport, etc.;

- Disclosure and alarming of fake-news and dis- and desinformation with expert-explanations and professional guidance;
- List of home and evacuation supplies with what one should be able to cope independently or in households, incl. e-learning and test applications on supplies level;
- All useful emergency numbers directly to public authorities in the MS and European-wide;
- Citizen`s early warning, emergency alerts and quick feedback applications.

IMPACT ON COUNTERING HYBRID THREATS

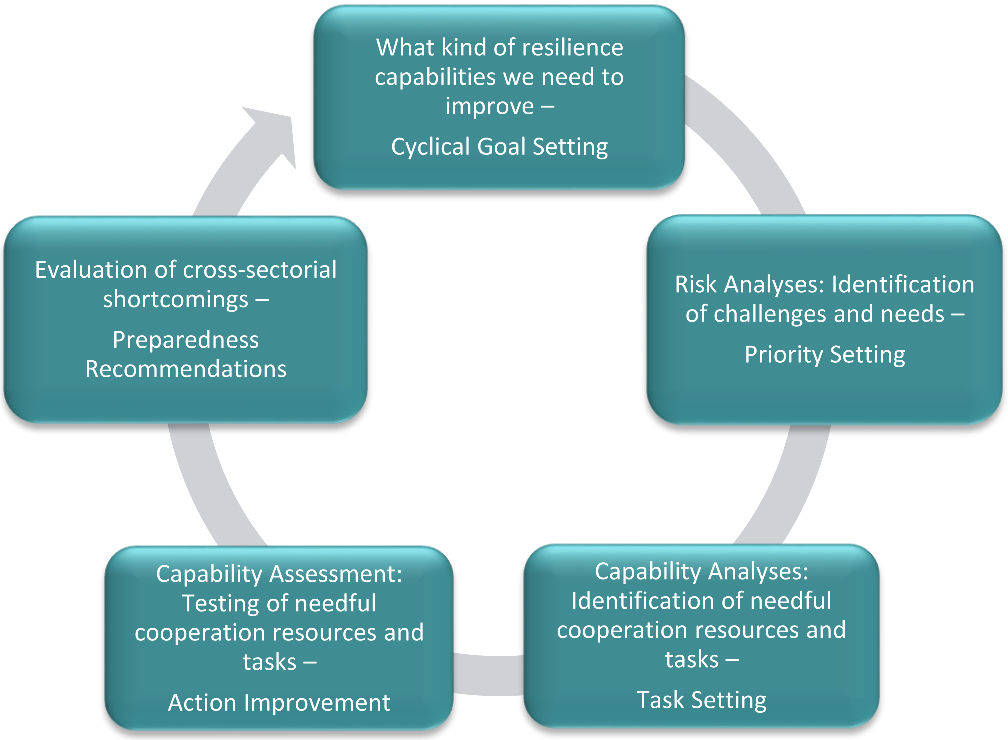
- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**

The *hybrid tools* are designed to target socio-political vulnerabilities, including via using active communication measures to (re-)escalate crises and deepen insecurity, as characterized above.



Hence, the early warning, coherent communication, civil preparedness on all levels and timely response to the crises is key to effectively tackling emerging safety challenges and to mitigate the risks for further escalation up to major political crises and collapse of the democratic order as the "darkest" optional scenario.

- **Cyclical capability-planning resilience-building process:**


What kind of resilience capabilities we need to improve –
Cyclical Goal Setting
Risk Analyses: Identification of challenges and needs –
Priority Setting
Capability Analyses: Identification of needful cooperation resources and tasks –
Task Setting
Capability Assessment: Testing of needful cooperation resources and tasks –
Action Improvement
Evaluation of cross-sectorial shortcomings –
Preparedness Recommendations

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the solution?**

Highly secured IT standards and CERT services.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

High level of security standards and need to permanent expertise-based cyclical improvement and coherent capability-building management.

COSTS

- **Indication of costs**:

Depending on exact national functionalities and security resolutions. Question of the public tender.

- **Differentiate if possible in development, procurement and exploitation:**

Public procurements in MS.

COUNTERMEASURES

- **Are there any foreseen / potential countermeasures that could degrade the effectiveness of the solution**?

Misfit of relevant platforms.

Hacking.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**

No “best before” date.

The idea is expected to remain effective and useful without time limits.

MISCELLANEOUS

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

This is a "on-your-pocket" technical solution that requires organizational management, local customization and social embedding. The platform needs careful expertise-based content design and analytic features for developers.

NAME OF THE IDEA

Smart message routing and notification service for sharing the operational picture to every agency involved in the response at every level of coordination. (A smart information sharing mechanism)

DESCRIPTION OF THE IDEA:

The service enables the sharing of the information among involved actors at every level of coordination enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. Based on the Emergency Message Content Router (EMCR) that will be capable of sharing the operational picture (information related to the management and response to an emergency situation) among involved responding teams by routing messages. This way relevant information will reach the appropriate persons at every level of coordination in a timely manner. It can be evolved and integrated to share the operational picture to every agency involved in the response at every level of coordination.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**

  Primary Need No2: [Minimum service for ensuring strategic supplies.]
- **Applicable JRC domains as stated by the gaps/needs:**
  Economy, Infrastructure, Administration

- **Applicable core theme(s) as stated by the gap/need:**

TYPE OF SOLUTION

- **Technical**
  A routing service that enables the exchange of information related to emergency situations among involved actors.

  Interoperability standards are supported.

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  Infrastructure, Administration
  Provide the level of practitioners in the same discipline:
  - I) ***ministry level*** **(administration):** ministry of civil protection
  - II) **local level (cities and regions):** municipalities and prefectures
  - **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**
  Private companies, police, firefighting departments, civil protection ministries, all involved response teams (for example first responders)

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: **TRL6**

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  research

- **Expected time to TRL-9.** The innovation will reach TRL 7 by autumn 2021

- **Expected time to market.** 4 years

DESCRIPTION OF USE CASE(S)

The tool, developed by Satways, is being tested for the case of a big refinery in order to route information to the responsible public safety agencies (InfraStress H2020 project)

It Is also being tested in the case of airports (SATIE H2020 project) in order to enable the communication (exchange of operational picture, collaboration) between airport operators and the public safety agency.

The tool can be used for various use cases, for both natural and man-made disasters.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  It is vital that, in times of crises, practitioners need to be involved in and remain constantly updated on the protection of Critical Infrastructures and supply chains from cyber and physical events. This will allow them to take appropriate actions and initiate strategically planned processes.

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Distributed event streaming technology

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Access to this operational disseminated information is restricted to relevant security practitioners

  Exchange of information is based on security mechanisms in order to avoid unauthorized access
  Users may be reluctant to share their operational information to other involved agencies/actors

COSTS

- **Indication of costs**:
  Depending on the magnitude of the applications
- **Differentiate if possible, in development, procurement and exploitation**
  Development is the key cost parameter

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?

  All involved registries must be registered and authenticated in the system to be able to communicate with other agencies. Therefore, a malicious party pretending to be an agency cannot exchange information or have access to communication between authorized agencies.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  No limitations as long as the Interoperability standards remain updated and fitted to the operational needs of the agencies

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

NAME OF THE IDEA
COUNTERING DISINFORMATION WITH STRATEGIC PERSONALIZED ADVERTISING
DESCRIPTION OF THE IDEA

Personalized advertising is well known to suggest a subject related to the interests of a user by using data that was collected while the user visited other websites or locations. Based on the collected data it is possible to create a profile of interest and opinions. In order to fight disinformation an effective way is to raise the attention for the correct information from a trustworthy source. By adverting, the related statement given by a trustworthy organization to a topic the user was interested in, disinformation can be weakened. In fact, as a trustworthy channel provides the user with the requested information, the user will not search for other sources. In addition, the observation of questions that were mentioned enables governmental organizations to adjust the provided information to fit the current needs.

REFERENCE TO CAPABILITY GAP/NEED
- **Describe the use of the solution in reference to the gap/need**
  Fighting disinformation by personalized advertisement
- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all domains.
- **Applicable core theme(s) as stated by the gap/need:**
  - CT1: Future Trends of hybrid threats CT2: Cyber and Future Technologies
  - CT3: Resilient Civilians, Local Level and National Administration
  - CT4: Information and Strategic Communications

TYPE OF SOLUTION
- **Technical**
  software
- **Social/Human**
  Personalized adverts based on interests
- **Organizational/Process**

PRACTITIONERS
- **Provide applicable JRC domains for which the solution is valuable:**
  Personalized advertising is already in use by non-governmental (media, industry) organizations. For governmental organizations, the benefit of advertising information on a popular topic is to lead the user to the right information.
- **Provide the level of practitioners in the same discipline:**

- I) ***ministry level*** **(administration):** expertise needed
- **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)**
  Governmental organizations with help of experts on the subjects datamining and marketing for the administration
  Personalized advertisement for private citizens

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 9

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  There are different researches that deal with the effects of personalized advertising. It was already used to manipulate decisions or to take action for disinformation in other countries. To realize this solution the development of an appropriate concept and a technical solution in consideration of the official operation by governmental organizations is needed.
- **Expected time to TRL-9.** N.a.
  Expected time to market. N.a.

DESCRIPTION OF USE CASE(S)

As can be seen in the following personalized advertisement can be used offensive or defensive. There are many examples for using personalized advertisement to influence or weaken other states. For example, Cambridge Analytica, a private political consultancy working on behalf of various political organizations and lobby groups used data mining and analysis to create advertisement that influenced the voting behavior for example while US presidential election and Brexit.
On another case the Internet Research Agency (IRA), a private media firm operating on the Russian, used such strategies on social media platforms to amplify social discontent during the 2016 presidential campaign.
The intended use here is to influence the behavior of citizens in a positive ways by leading them with helps personalized advertisement to the right information provided by a trustworthy source. Concerning disinformation, it is expected that the delivery of related information on the right point can help stabilize the social comprehension.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to use big data for a personalized advertisement in order to deliver trustful information and countering disinformation.
- **Resilience/defensive/offensive**
  Such a concept can improve societal resilience against fake news and raise the defensive capability against hybrid state actors using disinformation campaigns. On the other hand, as mentioned in the use cases it also can be used to destabilize the information environment in other states.

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Personalized advertisement relies on big data methods. Therefore, Machine Learning algorithms and Natural	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** Responsible handling of personal data is very important. It must not be used to

Language Processing is used. Based on statistic evaluations a heat map on popular questions/topics can be created and predictions can be derived.	influence elections or manipulate other authorities. Regarding to the General Data Protection Regulation GDPR there are already conditions for the use of data. Additional legislation might be needed, although not certain. As seen on the use cases it can be used for defense as well as for offense. The following processes could improve the implementation of the proposed solution, and should therefore be considered: Formulate transparent information about desired and achievable goals Regular short, understandable reports on progress and results already achieved Continuous review of whether the desired goals are still in the current focus Adjustment of the goals to current circumstances and situations with explanations and reasons why an adjustment is taking place. Avoiding the impression of arbitrary decisions Offer a history of how the development of a strategic vision is developing Implementation of control mechanisms to avoid manipulation Preparation of different message formats related to different target groups.
COSTS - **Indication of costs**: The technology is already available, it only needs to be implemented for governmental use. Therefore, the elaboration of a detailed concept is needed as well as supervision of the collected data and information in order to be able to identify trends and adapt that to the advertised information. - **Differentiate if possible in development, procurement and exploitation** Development of concept, realization, permanent costs for operation and update	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Especially regarding societies with low trust in government the intrusion of governmental organizations in private areas of personal life may be seen as a violation of privacy. The fear of citizens of being spied on or influenced in an unwanted way could lead to the opposite effect and weaken the trust in governmental organizations. Adblockers and other advertisement-circumventing plugins and tools could

mitigate the effectiveness of the suggested solution.

To avoid backfire this solution needs to use content sources that are as independent as possible, those that are less easily painted as propaganda. It will also need to be conservative when it comes to targeting, using only interest and language-based segmentation and not delving into more complex demographic profiles.

There is an small chance that this develops into an online advertising "arms race" with competing narratives, degrading the level of confidence in promoted content as a whole.

Malicious actors could try to mitigate the effects of the proposed solution. They could influence the strategic advertisements through specifically reformulated messages, either on the content of these strategic advertisements themselves, or on the results and goals. This could be done through the reformulation of the message and/or the integration of false information.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  As long as personalized advertisement technically and ethnically is possible.

MISCELLANEOUS

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

Because of the General Data Protection Regulation GDPR there are already regulations for the use of personal data. Furthermore, it is needed to elaborate a detailed concept of the use and evaluation of data and the possible ways for using it for personalized advertisement. Likewise, the prevailing circumstances of a society should be taken into account to decide about the scope of the measures.

It might be interesting to explore how this idea will work with existing practices like branded content/native advertising published in news outlets by sources considered to be independent.

NAME OF THE IDEA

Training application for media literacy

DESCRIPTION OF THE IDEA

While dealing directly with the quality of content is complicated, the problem could be more effectively addressed by how the low-quality content is perceived by target audiences. While need for better skills in media literacy are generally acknowledged, the innovation in the field remains meagre. The application would enhance critical thinking on (social) media content (in the academic field of history it is named ‘source criticism’). However, the desired impact would be gained only over longer period and if the application is highly attractive for target audiences (it is something obviously lacking in currently available applications)

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**
  Deteriorating quality of content.
- **Applicable JRC domains as stated by the gaps/needs:** information

- **Applicable core theme(s) as stated by the gap/need:**
  CT1: Resilient Civilians, Local Level and National Administration
  CT3: Information and Strategic Communications
  CT4: Future Trends of Hybrid Threats

TYPE OF SOLUTION

- **Technical**
- **Social/Human**
- **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  StratCom
  Debunking
  Trust in democratic processes and government authorities

- **Provide the level of practitioners in the same discipline:**
  Generally, it should be supposed the higher levels of administrators have already now better skills in the field, therefore, the lower the individuals are in the hierarchy the higher the impact.
  - 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**
  Field-level government employees in the beginning of their career. The application could be part of their training to the office. Also providing this training to for example NGOs and university students would increase the societal resilience.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 9

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Some rather primitive solutions are already operational.

- **Expected time to TRL-9.** 0. Already available.

- **Expected time to market.**
  0. Already available.

DESCRIPTION OF USE CASE(S)

The application could be used as part of school curricula or part of training curricula of government, private and third sector employees, depending on the maturity of the content. The general idea is pushing students into making decisions on the (social)media content they face in their daily lives under time-pressure and providing feedback in realistic way, showing that such decisions do have their impact.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Increasing social media literacy strengthens societal resilience and mitigates the effect of disinformation campaigns and fake information, which might be targeted to junior employees of government offices.

- **Resilience/defensive/offensive**
  Application would have no offensive capacity. It would enhance societal resilience and defend against hostile information attacks.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  IT only.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  There are no special restrictions, however, cultural (and religious) awareness, legal aspects on copyright etc. have to be kept in mind while producing content.

COSTS

- **Indication of costs**:
  Highly dependent on the target audience – while the costs for application meant for children may be rather limited (under EUR 100 000), the application meant for practitioner of the field or senior managers would be considerably higher (possibly around EUR 500 000). The users would use it in their own devices.

- **Differentiate if possible in development, procurement and exploitation**
  The cost indicated above is meant solely for development. The procurement and exploitation (maintenance) costs are rather low (if not foresee constant feedback to users by system handlers), although depends on how the content will be upgraded in the future.

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  There is the possibility of hostile cyber-attacks, however, since the application is not time critical and if it is down for shorter periods of time does not cause much harm, it is not a major problem.

  If applied widely as a part of general training of government officials, for example, the hostile actor could try to get the results and learn from them to make the future campaigning even more efficient. It would be of importance to keep the results of the training classified.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  It is durable in the foreseeable future (5-10 years) and the need could disappear only in the case of major changes in (social)media landscape unforeseeable future.

MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** There are some existing applications going in the same direction, most notably: **Get Bad News Game** developed in collaboration of Cambridge University (Cambridge Social Decision-Making Lab, Department of Psychology), the Dutch media collective DROG and graphic design agency Gusmanson. https://www.getbadnews.com/#intro **Go Viral Game** developed by Tapps Games. https://www.goviralgame.com/en/play Both are available for users free of charge.	

11.5.2 ADDITIONAL INNOVATIONS AS IDENTIFIED IN TASK 3.1

NAME OF THE IDEA Establish Data Embassies or E-embassies **DESCRIPTION OF THE IDEA** Establishment of national datacenters in secondary countries or so called Data Embassies in allied countries in order to safeguard essential governmental services and governmental continuity in case digital infrastructure in home countries is no longer operable.	
REFERENCE TO CAPABILITY GAP/NEED - **Describe the use of the solution in reference to the gap/need** Primary Gap2: [Minimum service for ensuring strategic supplies]- while this scheme does not focus on the critical continuation of strategic supplies it does focus on the continuity of government and governmental functionality. - **Applicable JRC domains as stated by the gaps/needs:** Administration, economy, infrastructure, Social/Societal, cyber - **Applicable core theme(s) as stated by the gap/need:**	**TYPE OF SOLUTION** - **Technical** hardware - **Social/Human** - **Organizational/Process** Organizational, bureaucratic processes, information storing

Cyber and Future Technologies	

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  Administration, economy, infrastructure, Social/Societal, cyber
-
- **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**
  Embassy staff, governmental authorities

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:
  Currently being demonstrated in relevant environment (TRL 6)

- **In which stage is the idea (research, technology, available innovation, proven innovation):**
  Available innovation
- **Expected time to TRL-9.**
  3-5 years
- **Expected time to market**
  N/A

DESCRIPTION OF USE CASE(S)

- Since the Russian DDOS attack against Estonia in 2007, and annexation of Crimea, Estonia has determined a need to back up its critical (digital) infrastructure in order to ensure the continuity of governmental capabilities. It has done so by establishing a Data Embassy in Luxembourg where it has stored datasets critical for its functionality. Thus if Estonia's systems are ever compromised it has a backup center and no longer needs to operate from within their own borders. Critical information stored include: Court system, treasury information system, land registration, taxable persons registry, business registry, population registry, identity documents, land cadastral, national pension insurance registry.

- Monaco has also been in talks with setting up a data embassy in Luxembourg as of 2019 and Luxembourg will begin hosting their new data embassy as of 2021.

IMPACT ON COUNTERING HYBRID THREATS

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

Contributes to tackling reliance on critical services and technological systems as well as in tackling distrust in democratic systems and government.

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY - **Which technologies are critical in fielding the idea?** As the technologies already exist this new method of establishing data embassies interconnects allied digital infrastructure with one another therefore paving the way for further digitalization of societies. (Sorry Okke wist niet helemaal wat ik hier kon zetten)	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** Legal agreements and bilateral agreements with foreign countries need to be established. As well as implementation of new laws on a local/national level in primary and secondary country. -
COSTS - **Indication of costs.** **Differentiate if possible in development, procurement and exploitation.** Current costs for hosting are between 200,000 – 300,000	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? If enemies manage to take down both the countries own datacenters as well as those located at the data embassy this solution will not be viable. - **How durable is the idea (how long is the idea expected to be effective/useful?)** As long as adversaries do not yet have the capabilities to simultaneous destroy heavily encrypted data centers in multiple countries the idea will still be effective and useful.

MISCELLANEOUS

Estonia to open the world’s first data embassy in Luxembourg — e-Estonia (e-estonia.com)
E-embassies in Luxembourg - Luxembourg (public.lu)

EUROPEAN SMART AND SUSTAINABLE CITY AWARD (ESSCA)

The European Smart and Sustainable City Award Award developed by Efficacity, Cerema and Fraunhoher (Morgenstadt initiative), with the support of an experts advisory board, complements the European Energy Award to address the other topics (Innovation, Quality of life, Economic development, Resilience) of sustainable development. It is aiming at assisting cities :

- to implement transverse and systemic evaluation of their key policies,
- to build sustainable development strategies and roadmaps,
- to reconcile sustainable city and smart city approaches,
- to promote exchanges of good practices between local authorities,
- to foster the visibility and attractiveness of cities,
- to facilitate the access to national or European funding.

This award is including 50 objectives which are including urban security, resilience of communication networks, societal challenges and citizen inclusiveness, which are based on many contributions coming from international reference frameworks including ISO standards on sustainable Cities and Communities (TC268), Sustainable Development Goals and the Morgenstat City Index.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gap/need**
  Improve citizen inclusiveness, local empowerment, integrate marginalized parts of society, government trust building

- **Applicable JRC domains as stated by the gaps/needs:**
  The ESSCA is dealing with the following JRC domains at local scale : social/societal, administration, infrastructure, economy, cyber, political, culture
- **Applicable core theme(s) as stated by the gap/need:**
  CT4: Resilient Civilians, Local Level and Administration

TYPE OF SOLUTION

- **Technical**
  n/a
- **Social/Human**
  Evaluate objectives of the cities in the field of Innovation, Quality of life, Economic Development and Resilience areas of the Award
- **Organizational/Process**
  promote systemic and inclusive governance to improve sustainable strategies and roadmap

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  The ESSCA is dealing with the following JRC domains at local scale : social/societal, administration, infrastructure, economy, cyber, political, culture
- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level* (administration):**
    n/a
  - **II) *local level* (cities and regions):**
    cities
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
    n/a
- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
  The ESSCA is dealing with all stakeholders who could be included in a sustainable strategy and roadmap

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**: 7
  The V0 version of the ESSCA which was launched on July 2019 with the support of governmental bodies (including French Energy Agency ADEME), cities associations (France Ville Durable, France Urbaine) and companies associations (MEDEF International) was proposed to French cities/local authorities ranging from 30000 to 230000 inhabitants for a field test in order to co-produce a V1 version which will be the commercial version. The pilot phase begun in 2020 with 6 French cities (Paris Vallée de la Marne, Territoire de la Côte Ouest La Réunion, Lorient Agglomération, Communauté Urbaine de Dunkerque, Sète Agglomération, Grand Chalon, Millau Grands Causses). A pilot phase in Germany is being discussed with Fraunhofer, as well as in other European countries.

- **In which stage is the idea (research, technology, available innovation, proven innovation):** Available innovation at pilot phase stage, which commercial version is scheduled for 2022

- **Expected time to TRL-9.** 1 year

- **Expected time to market.** 1 year

DESCRIPTION OF USE CASE(S)

The ESSCA is including several objectives which will contribute to fight hybrid threats :
1.4.1 : develop the use of digital participation mechanisms
1.4.2 : develop the city digital services (e-administration)
1.4.3 : develop an Open Data policy
1.4.4 : foster local innovation with data produced within the local authority’s territory
1.5.1 : set up a digitalization strategy for the local authority physical infrastructure
1.5.2 : map and manage the local authority’s digital assets (data, technologies, information networks)
2.1.1 : help and protect the most vulnerable and reduce inequalities
2.1.3 : foster digital inclusion
2.2.1 : support and look after youths leaving school prematurely
2.3.3 : promote access to sports for all
2.3.4 : promote leisure for all
2.5.1 : implement an urban security strategy
2.6.1 : make culture and heritage a common good
3.1.3 : support work-related quality of life and fight against discriminations (fair wages, men/women, aso.)
3.2.1 : develop the attractiveness of the territory under the local authority's remit
4.1.1 : implement a risk management for natural and technological disasters
4.2.1 : Guarantee the resilience of water supply and wastewater treatment
4.2.2 : Guarantee the resilience of energy networks
4.2.3 : Guarantee the resilience of transport infrastructure
4.2.4 : Guarantee the resilience of communication infrastructure
The cities/local authorities will be coached in order to improve their performance and scores related to these objectives

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  The ESSCA contributes to counter hybrid threats through the awareness-raising, coaching and scoring process implemented for the above quoted objectives, which are related to the following GAPs/NEEDs : improve citizen inclusiveness, local empowerment, integrate marginalized parts of society, government trust building. The ESSCA will also contribute through the share of good practices in these fields between cities/local authorities involved.
- **Resilience/defensive/offensive**
  The ESCCA is involving both resilience, defensive and offensive aspects

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
- No technological barrier, but availability of data to assess the impacts of the ESSCA objectives could be critical

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No restrictions for use, as the ESSCA is including protection of individual data and information

COSTS - **Indication of costs. Differentiate if possible in development, procurement and exploitation.** Development costs of the ESSCA are financed by Efficacity and Cerema. The cost which will be proposed to cities and local authorities for the deployment phase scheduled in 2022 will be finalized in 2021. The costs of the pilot phase are ranging from 30 to 40 k€ according to the cities and local authorities sizes, 50% of these amounts being co-financed by innovation funds for the French pilot phase.	**COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution**? No real identified countermeasures - **How durable is the idea (how long is the idea expected to be effective/useful?)** As the purposes of the ESSCA are to coach cities and local authorities and assess the objectives in order to improve the scores and good practices implementation, the ESSCA is expected to be deployed for many years (as the European Energy Award which was created 25 years ago and is still deploying and evolving) , as it will be updated according to adapt to the new challenges which cities and local authorities are faced with
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** Power Point presentation of the European Smart and Sustainable City Award	

Generic Operational Scenarios (GOS) Hybrid threats threaten with a particular acuity the Critical infrastructures. Therefore, private and public players must be intensively trained to handle the systemic crises endangering the countries' vital networks. We propose an innovative project of digital scenarios which would provide a regular training to the involved actors. Therefore, the tool is aimed to familiarize the executive managers with hybrid attack situations, by modelling real-life scenarios and adding new elements that make the situations vary from one time to another.	
REFERENCE TO CAPABILITY GAP/NEED - **Describe the use of the solution in reference to the gap/need** Improve Critical infrastructures' actors reactivity against hybrid threats, through a training based on digital scenarios - **Applicable JRC domains as stated by the gaps/needs:** It can be related to improving the resilience of the strategic networks (economy, infrastructure, administration, diplomacy).	**TYPE OF SOLUTION** - **Technical** Software - **Social/Human** The tool models the hierarchic relations into a crisis unit - **Organizational/Process** The tool simulates a crisis unit. Il will therefore lead to a clarification of the hierarchical links and the role of each actor in a crisis situation.

- **Applicable core theme(s) as stated by the gap/need:**
    - CT3: Information and Strategic Communications
    - CT4 : Resilient Civilians, Local level and National Administration

PRACTITIONERS

- **Provide applicable JRC domains for which the solution is valuable:**
  The solution is valuable for the Administration, the military, economic and cyber field.

- **Provide the level of practitioners in the same discipline:**
    - I) ***ministry level*** **(administration):**
      We would provide to ministries' executives scenarios where an attack on critical infrastructure triggers national cascade outcomes that they have to handle.

    - **II) *local level* (cities and regions):**
      The same type of scenarios would be provided to local executives, but on a local level.

    - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
      The same type of scenarios would be provided to the operators of critical infrastructures.

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments)**
  The end-users will be the critical operators and the Administration both at local (prefectures, local executives) and national (Ministries, national agencies) level. Executive managers could train themselves on a regular basis to situations of hybrid threats threatening critical infrastructures, in order to get used to crisis management and make the right decisions in the event of a risk occurrence.

STATE OF THE ART

- **Indication of Technology Readiness Level (TRL 1-9 index)**:
  TRL 4 : Basic principles observed. This type of digital scenarios has been already used in the military field for 20 years.

- **In which stage is the idea (research, technology, available innovation, proven innovation):**
  We do not have developed the tool already, but it will be based on basic technologies, and therefore easy to implement.

- **Expected time to TRL-9 :**
  2 years

- **Expected time to market :**
  3 years

DESCRIPTION OF USE CASE(S)

1) This tool will enable private and public decision-makers to familiarize themselves with situations involving attacks on critical infrastructures. The tool will be based on the modelling of real scenarios (the “standard scenarios”), to which we will add variants (increase in the intensity of attacks, occurrence of additional threats, etc.). This tool will replace or multiply the current practice of physical training, which takes a long time to set up and is limited in scenarios. Our scenarios will be based on models offering scenario variations, which will make it possible to propose an “infinite” number of cases. In addition, the digital scenarios can include the long-term consequences and are easy to set up.

2) In the long run, our tool would also be used as a database to anticipate the crises situations. For example the models would bring to light undetected flaws within our organization.

IMPACT ON COUNTERING HYBRID THREATS

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

  A quick and effective reaction would curb a hybrid attack before it triggers systemic outcomes.

- **Resilience/defensive/offensive**

  The executive managers’ preparedness against hybrid threats is the best way to improve our systemic resilience as they will be able to take the good decisions in the right time.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**

  We will rely on existing technologies, i.e modelling based (decisonal tree….)

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**

  The data collected during the exercises will be confidential insofar as it could highlight organizational shortcomings.

COSTS

- **Indication of costs.**
  Differentiate if possible in development, procurement and exploitation.
  - Demonstrator: 200 k€
  - Operational prototype: 1 M€
  - Operational system: 1.5 M €

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution?**
  Not available

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  Certainly very durable if the tool gets technological improvements with time.

MISCELLANEOUS

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

This project is duplicable for other countries and for other standard scenarios

Government & social media cooperation framework in countering election interference

Cooperation framework in which government practitioners can work with social media companies to counter election interference, for example through mitigating the spread of influence operations on social media platforms during (the run-up to) elections.

REFERENCE TO CAPABILITY GAPs/NEED

Responds to gap of **“Missing cohesion between governed and government”**

- By supporting planning of information environment monitoring by the government
- By creating baseline for determining the threshold for intolerable influencing

Responds to gap of **“Governmental trust building and situational awareness”**

- By providing advice on when it is good to start increasing OSINT capabilities in governments

Responds to gap of **“Addressing the mass of manipulated information in social media”**

- By introducing suggestions to engage with private social media companies

- **Applicable JRC domains as stated by the gaps/need:** Information, society, political

- **Applicable core theme(s) as stated by the gap/need:**

Information and Strategic Communications

TYPE OF SOLUTION

- **Organizational/Process**

PRACTITIONERS

Provide the applicable JRC domains for which the idea is valuable:

Information, as this is about being able to define what information influencing is intolerable and having control over the information environment in order to safeguard elections.

Political, as it requires resources from governments and interest to cooperate with private sector based on shared values.

- **Provide the level of practitioners in the same discipline:**
    - I) ***ministry level*** **(administration):**

- **Provide the end-users of the idea (such as NGO’s, private citizens, private companies, media outlets, police, firefighting departments**

Ministries of interior / home affairs, government organisations responsible for election security

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: The solution is a procedure which could be implemented as is. Procedures are also described in Hybrid CoE paper *Improving cooperation with social media companies to counter electoral interference* https://www.hybridcoe.fi/publications/hybrid-coe-paper-5-improving-cooperation-with-social-media-companies-to-counter-electoral-interference/

- **Expected time to TRL-9.**
  N/A; already available
- **Expected time to market.**
  N/A; already available

DESCRIPTION OF USE CASE(S)

A government-social media cooperation framework will enable planning of action well ahead of elections, and swifter detection of information operations and a more comprehensive response by improving both the exchange of information and cooperation with the private sector.

Social media companies have become a permanent part of the information environment, and governments should consider taking measures to further improve cooperation with them, particularly to counter electoral interference.

Enhancing **situational awareness** within government by creating clear government structures enables both a faster response and an improved exchange of information. **Educating** key stakeholders within government on the threat of influence operations on social media platforms, as well as enhancing broader awareness in government, enables both early detection and a rapid response. **Engaging** with the private sector is important both for understanding their work and for connecting with relevant counterparts.

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 - **Which technologies are critical in fielding the idea?**	**RESTRICTIONS FOR USE** - **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
COSTS - **Indication of costs**: **Differentiate if possible in development, procurement and exploitation** Investing in dedicated points of contact and fusion cells for social media channels inside governments	**COUNTERMEASURES** - **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**	

12 BIBLIOGRAPHY

[1] Joint Framework on Countering Hybrid Threats, Join (2016) 18 Final, European Commission

[2] EU-Hybnet Description of Action, Coordination and Support Action, Grant Agreement No 883054

[3] EU-HYBNET Deliverable 2.1 "Long list of defined gaps and needs", European Centre of Excellence for Countering Hybrid Threats, June 2020 (Consortium Only)

[4] EU-HYBNET Deliverable 2.9 "Deeper Analysis, Delivery of Short List of Gaps and Needs", Joint Research Centre, October 2020 (Consortium Only)

[5] EU-HYBNET Deliverable 2.17 "Training and Exercise, Scenario Delivery", KEMEA, March 2021

[6] EU-HYBNET Deliverable 2.20 "Training and Exercises Delivery on Up-To-Date Topics", L3CE, May 2021

[7] EU-HYBNET Deliverable 2.23 "Training and Exercises Lessons Learned Report", European Centre of Excellence for Countering Hybrid Threats, forthcoming (Classification tbd)

[8] EU-HYBNET Deliverable 3.3 "First Report on Improvement and Innovations", SATWAYS, December 2020

[9] EU-HYBNET Deliverable 3.7 "First Report on Innovation and Research Project Monitoring", L3CE, December 2020

[10] Hybrid Conflicts: The New Normal?, TNO & HCSS publication, December 2018