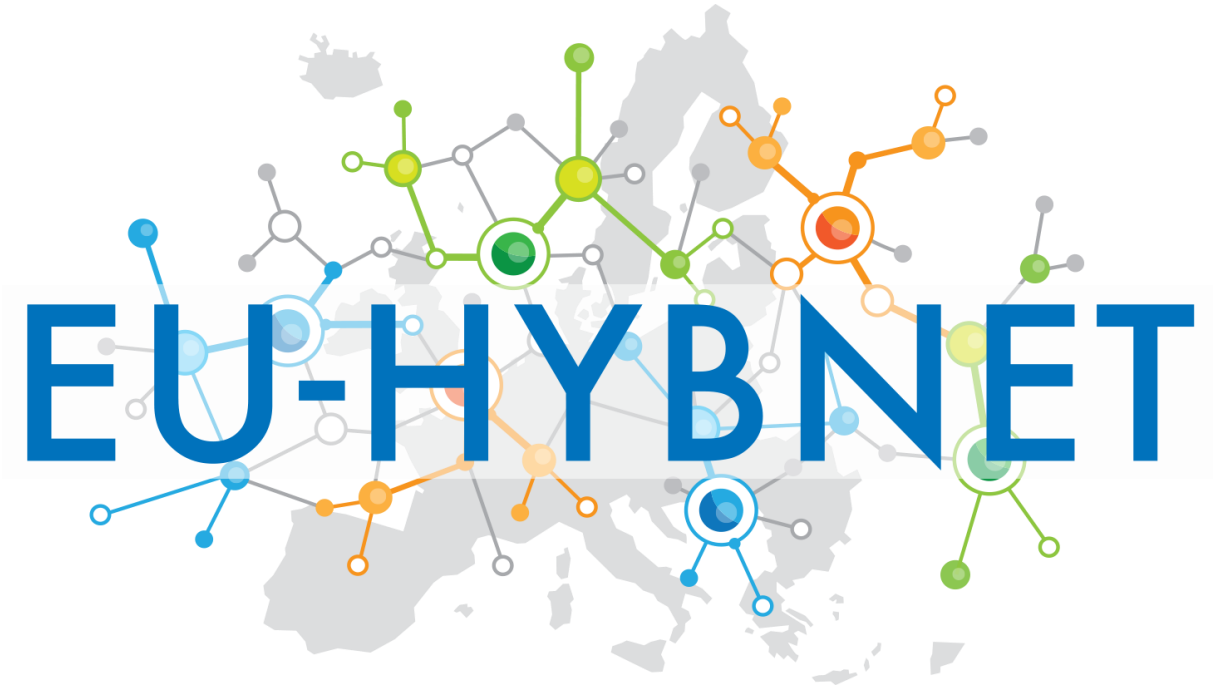


FIRST REPORT ON IMPROVEMENT AND INNOVATIONS

DELIVERABLE 3.3

Lead Author: SATWAYS Ltd

Contributors: ICDS, KEMEA, L3CE, ZITiS, COMTESSA, TNO, Laurea

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

D3.3 FIRST REPORT ON IMPROVEMENT AND INNOVATIONS

Deliverable number	**D3.3**	
Version:	**1.1**	
Delivery date:	**18/12/2020**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Dr. Souzanna Sofou**	**Satways Ltd**
Contributors:	Michelle Stebner	ZITiS
	Maria Kampa, Mirela Rosgova	KEMEA
	Ramon Loik, Ivo Juurvee	ICDS
	Evaldas Bruze Edmundas Piesarskas	L3CE
	Pham Son	COMTESSA
	Rick Meessen, Okke Lucassen	TNO
	Päivi Mattila, Isto Mattila	Laurea

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	12/11/2020	Souzanna Sofou (STWS)	Table of Contents
0.2	13/11/2020	>>	Added allocation of work (as a comment)
			Updated with the slightly modified template for providing solutions
0.3	16/11/2020	>>	Added overview and definitions §1.1,1.2 Added innovations for the Primary Context 'Reliance on Critical Services and Technological Systems'
0.4	20/11/2020	Souzanna Sofou (STWS) Michelle Stebner (ZITiS) Rick Meessen, Okke Lucassen (TNO)	Added ZITiS context description and innovations on the contexts 'Trend: Official strategic communication losing power', 'Big data as a new power source' Added TNO's input for the context 'Trend: Official strategic communication losing power' Added comments from the 20-11-2020 telco Changed order of core themes to match the GA
0.5	24/11/2020	Souzanna Sofou (STWS)	Added context description and innovations for the primary contexts 'Globalization vs. localisation' and 'Going Viral'
0.6	24/11/2020	Souzanna Sofou (STWS)	Added context description for primary context 'Trend; increasing strategic dependency of critical services'
0.7	27/11/2020	Maria Kampa, Mirela Rosgova (KEMEA)	Added KEMEA context description and innovations for primary contexts 'hyper connectivity as an impact multiplier of cyber' and 'the individual as a digital entity'
		Ramon Loik (ICDS)	Added ICDS introduction and innovation provided for primary context 'Distrust and Stress in political decision making'

0.8		Isto Mattila (LAUREA)	First review comments
		Souzanna Sofou	Added context description and innovations for primary context 'digital monopoly and massification of data'. Added statistics and comments requested from first review
			Added responses to IM review, added more input from KEMEA
		Pham Son (COMTESSA)	Added innovation provided from COMTESSA on primary context 'Increasing Strategic Dependency of Critical Services'
		Evaldas Bruze (L3CE) Edmundas Piesarskas (L3CE)	Added description and innovations provided from L3CE for the primary context 'Game changers: Quantum as a disruptive technology' and 'Going Viral'
		Michelle Stebner (ZITiS	Some changes on 'Trend: Official strategic communication losing power', 'Big data as a new power source'
0.9	11/12/2020	Souzanna Sofou (STWS)	Added structure of the document with short description of the core themes. Added Table of proposed innovations
		Michelle Stebner (ZITiS)	Added short descriptions of 'Big data', 'Artificial intelligence' and 'Machine learning' to Glossary
		Souzanna Sofou (STWS)	Added Context description for 'Deterioration for the quality of content'
0.9b		Ivo Juurvee (ICDS)	Added Context description and innovation for 'Deterioration for the quality of content'
		Souzanna Sofou (STWS)	Updated Table of proposed Innovations
0.9c	11/12/2020	Evaldas Bruze (L3CE) Edmundas Piesarskas (L3CE)	Additions in the introduction of the primary context 'Game Changers: Quantum as a disruptive technology'
		Pham Son (COMTESSA)	Additions in the definitions
		Michelle Stebner (ZITiS)	Additions in the cost structure
0,96d	15/12/2020	Ivo Juurvee (ICDS)	Added innovation for 'Deterioration for the quality of content'
		Maria Kampa (KEMEA)	Small additions in 'The individual as a digital identity' context
		Souzanna Sofou (Satways)	Small changes and additions in the deliverable, more information on proposed innovations for the 'Reliance on critical services and technological systems' context, methodology, references, conclusions and future work. Submitted for review.
	16/12/2020	Okke Lucassen (TNO)	Review and remarks for finalization
	16/12/2020	Päivi Mattila, Isto Mattila (Laurea)	Review and text editing
1.0	17/12/2020	Souzanna Sofou (Satways)	Final text editing
1.1	18/12/2020	Päivi Mattila (Laurea)	Final review and document submission

DISCLAIMER

TABLE OF CONTENTS

TABLES

INTRODUCTION

I. OVERVIEW

Empowering a Pan-European Network to counter Hybrid Threats (EU-HYBNET) project deliverable (D) 3.3 titled "First report on Improvement and innovations" aims to present the work carried out in the frame of the project Task T3.2 "Technology and Innovations Watch".

The EU-HYBNET deliverable D3.3 is part of and Work Package (WP) 3 "Surveys to Technology, Research and Innovations"/ Task 3.2 "Technology and Innovations Watch" and D3.3 has the important role of feeding information to T3.1 "Definition of Target Areas for Improvements and Innovations" and WP2 "Gaps and Needs of European Actors against Hybrid Threats"/ T2.3 "Training and Exercises Scenario Development" and T2.4 "Training and Exercises for Needs and Gaps". In short, D3.3 will deliver material for T3.1 to further analyze what could be the most sound innovations to identified EU-HYBNET gaps and needs of pan-European practitioners and other relevant actors to counter hybrid threats. In addition, D3.3 describes for T2.3 what could be the innovations that should be part of the training scenarios and eventually training activities where to the test the most promising innovation to the identified gaps and needs. The link and importance of WP3 T3.2 and its deliverable 3.3. for the EU-HYBNET project content is highlighted in the project WP interdependency picture below:

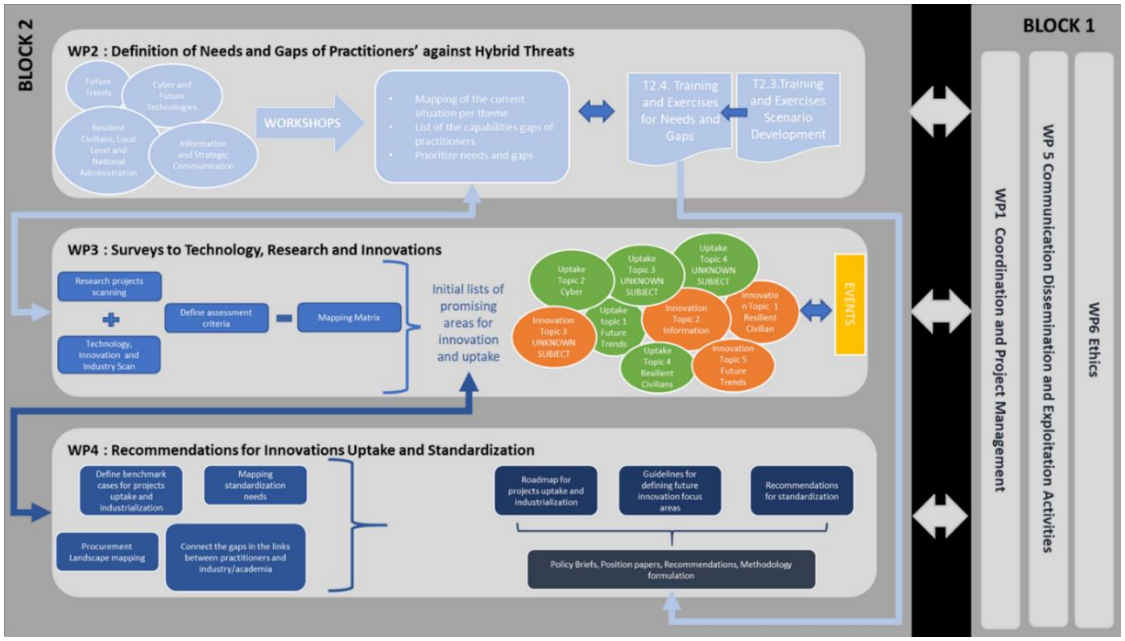


Figure 1 : EU-HYBNET structure of Work Packages and Main Activities

The D3.3 is also important in that it serves to address the goals of EU-HYBNET project objective (OB) 3 and contribute in reaching its key performance indicators (KPI), as described in EU-HYBNET Description of Action (DoA) document. The OB.3 and KPI3.2 to which D3.3 delivers results are the following:

OB3: To monitor developments in research and innovation activities as applied to hybrid threats			
Goal		**KPI description**	**KPI target value**
3.2	To monitor significant developments in technology that will lead to recommending solutions for European actors' gaps and needs	Monitor existing innovations addressing gaps and needs; incl. areas of knowledge/performance	At least 4 reports every 18 months that address technological innovations that are able to fulfill European actors' gaps and needs

In more detail, following the relevant work (EU-HYBNET Deliverable 2.1 "Long list of defined gaps and needs") conducted by the European Centre of Excellence for Countering Hybrid Threats with respect to identifying gaps and needs in countering hybrid threats, a deeper analysis and a short list of gaps and needs was prepared by JRC and presented in D2.9.

Based on the deeper analysis presented in D2.9, this deliverable, D3.3, presents technologies and innovations for each of the EU-HYBNET project four 'core themes'. The four core themes are mentioned in the Description of Action (DoA) and they represent the leading multidisciplinary methodological principles of the project together with Conceptual Model approach developed by the Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). The EU-HYBNET project four core themes are following: 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication.

The project core themes provide a lens through which to analyse how hybrid threats manifest themselves across the 13 hybrid threat domains defined in the Conceptual Model of Hybrid Threats, and how such threats interact across the various domains. This analytical lens enables the project to deliver coherent results in relation to the Conceptual Model countering hybrid threats.

Additionally, for each of the EU-HYBNET project four core themes, three primary contexts are studied– the primary contexts are deriving from EU-HYBNET D2.9 "Deeper analysis, delivery of short list of gaps and needs". This deliverable presents one to three innovations that may be feasible in countering hybrid threats, for each of the primary contexts and gaps and needs, for each of the core themes.

It should be noted, that as the relevant Deliverable D2.9 is confidential (CO), the present deliverable doesn't directly refer to the identified gaps and needs, but rather to the primary contexts these are more relevant to.

II. DEFINITIONS

Hybrid Threats

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties. [1] Hybrid threats can be characterised as a coordinated and synchronised action that deliberately targets democratic vulnerabilities of states and institutions through a wide range of means. The aim is to influence different forms of decision making at institutional, local, regional and state levels to favour and/or achieve strategic goals while undermining and/or hurting the target. To effectively respond to hybrid threats, improvements in information exchange, along with breakthroughs in relevant research, and promotion of intelligence-sharing across sectors, and between the EU and its MS and partners, are crucial[2].

According to the Joint Framework on Countering Hybrid Threats[1], "while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the Framework's conceptualisation aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives, while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats".

Practitioners at different levels

The EU-HYBNET project follows the European Commission (EC) definition of practitioners in the security domain 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". [3] In addition[2], 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.

Practitioners operate at different levels of governance. Therefore, 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 its primary focus is on civilian security issues.

Gaps and Needs

The EU-HYBNET project has already delivered in the frame of project Work Package (WP) 2 "Gaps and Needs of European Actors against Hybrid Threats" in Task (T) 2.1 and T2.2 an analysis of the pan-European practitioners and other relevant actors' gaps and needs to counter hybrid threats. The analysis aimed to identify, record, and understand the nature of practitioners and other relevant European actors' gaps and needs and vulnerabilities in countering hybrid threats. These gaps and

[1] Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats, European Commission (2016)
[2] EU-Hybnet Description of Action, Coordination and Support Action, Grant Agreement No 883054
[3] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq;keywords=/3156

needs include the identification of the obstacles to developing, maintaining and improving societal resilience in countering hybrid threats.

III. STRUCTURE OF THE DELIVERABLE

The document includes four main sections, each listing ideas and innovations proposed for the primary contexts of each EU-HYBNET project four core theme. More specifically,

Section 1 addresses the first Core Theme named 'Future trends of Hybrid Threats'.

Section 2 introduces innovations for the second Core Theme named 'Cyber and Future Technologies'

Section 3 presents ideas and innovations for the third Core Theme named 'Resilient Civilients, Local Level and Administration'.

Section 4 describes the ideas proposed for the forth Core Theme, named 'Information and Strategic Communications.

Section 5 provides the conclusions on the work performed, highlighting main focus areas and outcomes, as well as future work.

IV. METHODOLOGY

The present deliverable is the first deliverable in WP3 Task (T) 3.2 of the EU-HYBNET project.

The main actions identified in the planning of this Deliverable included analysing the gaps and needs findings of WP2 and the requirements defined by WP T3.1 "Definition of Target Areas for Improvements and Innovations" to map the innovations provided by T3.2 on the gaps and needs. In addition, the relative technology innovations developed from the private sector in Europe and abroad have been assessed.

With respect to the presentation of the ideas for each primary context, a special template was designed by TNO (T3.1 leader) and was thoroughly discussed. The main idea behind this template is to characterise the innovations in a coherent and systematic manner, thereby enabling T3.1 to proceed with assessments and comparisons of innovations in a later stage. Additionally, the use of templates will also support all consortium members to acquire a clear understanding of the identified innovations and to eventually comment on the innovations. For this purpose, the Innovation Arena platform, developed by Laurea to the project consortium and EU-HYBNET network members, will be used throughout the entire project.

In the next chapters, ideas and innovations will be presented according to the TNO template format. For some innovations some information is currently lacking on the cost. By using the Innovation Arena Platform and by continuing the search for innovations in the next four project years, we aim to enrich the portfolio of solutions proposed for countering hybrid threats.

It should be mentioned that the Innovation Arena (IA) is a platform where project partners and those who will join via the project to the European Network against hybrid threats may announce their needs for new innovations. In addition, in the IA, those network members who may provide possible solutions to announced innovation needs may present their solutions and what is reasonably expected, and according to which timetable. The project will use this information in WP3 and WP2 and eventually in WP4 to deliver the recommendations of the most promising innovations uptake (including industrialisation).

This document suggests potential innovations and solutions to improve pan-European practitioners and other relevant actors' measures to counter hybrid threats through the analytical lens of the EU-HYBNET project four core themes. As mentioned in the EU-HYBNET Grant Agreement (GA), each of the four project core themes has a vision that encompasses the variety of challenges that the European Union (EU) Member States (MS) may face when countering hybrid threats in targeted domains, and interfaces with other domains. For each of the project core themes, 3 Primary Contexts are studied, and innovations and solutions are suggested for each of these 12 cases.

I. Section 1: CORE THEME: FUTURE TRENDS OF HYBRID THREATS
   Hybrid Threats are difficult to detect due to their nature (see paragraph 1.2.1), as they also manifest a constantly changing character. To reflect this inherent quality, the proposed potential innovations and solutions presented in this report are multidisciplinary and multidimensional in their descriptions.
   The three primary contexts in this core theme are: I) the loss of power of official strategic communication II) big data as a new power source; and III) the increasing strategic dependency of critical services.
II. Section 2: CORE THEME: CYBER AND FUTURE TECHNOLOGIES
   Recent advancements and breakthroughs in the fields of cyber and future technologies have provided numerous benefits to society. At the same time, sophisticated tools based on these technologies can also be used by adversaries to harm the society. It is therefore imperative that a thorough study is conducted on the manner in which recently developed technologies, their advancements or a combination of these can form a basis for societal defences.
   The three primary contexts in this core theme are: I) quantum as a disruptive technology; II) hyper connectivity as an impact multiplier of cyber; and III) the individual as a digital entity.
III. Section 3: CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION
   In order for a society to become and remain resilient, a thorough understanding of its time-dependant and invariant vulnerabilities is needed. Then, attention should be focused on embracing diversities and their unique capabilities, utilizing the variety of perspectives therefore offered and then applying the technology advancements to support the community as a whole.
   The three primary contexts in this core theme are: I) distrust and stress in political decision making; II) reliance on critical services and technological systems; and III) globalisation versus localisation.
IV. Section 4: CORE THEME: INFORMATION AND STRATEGIC COMMUNICATIONS
   Disinformation and propaganda are the most known dimension of Hybrid Threats. AI-generated fake audio and visual material have proved to be a serious threat to democracy and to the trust to institutions, truth and processes. Effective strategies, counter technologies and

a sound understanding of the communication process and power can protect the societies from a number of hostile activities.

The three primary contexts in this core theme are: I) false information going viral; II) digital monopolies and massification of data; and III) the deterioration of the quality of content.

The main innovations and ideas presented in this work are presented in the following Table per core theme and primary context.

Table 1 -Ideas and Innovations for Countering Hybrid Threats

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

4. INFORMATION AND STRATEGIC COMMUNICATIONS		Debunking of Fake News
		Non-partisan native-language news channels for most interdependent abroad regions
	4.2 DIGITAL MONOPOLIES AND MASSIFICATION OF DATA	Fair Trade Data Program
	4.3 DETERIORATION OF THE QUALITY OF CONTENT	Training application for media literacy
		Automated fact-checker

1. INNOVATIONS FOR COUNTERING HYBRID THREATS:
CORE THEME: FUTURE TRENDS OF HYBRID THREATS

1.1 PRIMARY CONTEXT NO.1: TREND: OFFICIAL STRATEGIC COMMUNICATION LOSING POWER - HOW TODAY'S INFORMATION ENVIRONMENT EFFECTS KNOWLEDGE?

Introduction to the primary context

The process of decision-making is influenced by the information that is relevant for the resulting decision. The challenge here is to decide which information can be trusted and should be considered by relying on data, expertise and algorithmic calculations. Especially in stressful situations, like when decisions need to be made quickly, the evaluation of the information's validity is difficult. Therefore, the resulting deficit in knowledge or wrong information sources can lead to non-optimal decisions. This applies to both, the personal decision-making as well as government and public authorities' decision-making. The main problem of today's information environment is that in this globalized and interconnected world knowledge changes fast and can create contradicting messages. Combined with disinformation spread by individuals it can be hard to find simple and clear facts that are needed for the decision, what leads to increasing distrust in official communications.

The main need here is to increase the media literacy of citizens, so governmental decisions are more comprehensible and citizens more rely on statements given by trustful sources. As the influence by (social) media increases, also new methods and channels of communication should be considered.

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- Technical
○ n/a
- <u>Social/Human</u>
○ Guides/ guidelines
- Organizational/Process
○ n/a</td></tr>
</table>

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)**:
- **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.
  Expected time to market.

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.

<table>
<tr><td>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.</td><td>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.</td></tr>
<tr><td>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.</td><td>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).
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.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

.

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.

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	RESTRICTIONS FOR USE
- **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.	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc?.** If using classified scenario's, then some restrictions apply for the online use (internet). However, it is possible to use it in a controlled IT environment.
COSTS	**COUNTERMEASURES**
- **Indication of costs** **Differentiate if possible in development, procurement and exploitation** Indication of procurement costs is assessed as low Exploitation costs are also assessed as low; normally the production of the content (scenario, dilemmas, advices etc.) can be done in 100 hours, provided that the people working on it have sufficient knowledge about the envisaged scenario.	- **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. - **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.

1.2 PRIMARY CONTEXT NO.2: TREND: BIG DATA AS A NEW POWER SOURCE

Introduction to the primary context

Because of the intensive use of technology, big data provides the optimal conditions to develop statistics based on the behaviour of citizens. This enables the use of machine learning (ML) as well as artificial intelligence (AI). The big challenge is to extract as much information as possible from the collected data but in a limited scope so that it is possible to compute the information in a foreseeable time and identify correlation between the given attributes.

There is massive amounts of personal data that is widely accessible for digital actors, which can use it to personalize messages/advertisements on all channels of communication. Therefore, a combination of past behaviour as well as the present surrounding and circumstances is taken into account and results into a micro-targeting. Together with developments in online surveillance and behaviour tracking, artificial intelligence (AI) and machine learning (ML), a so-called hyper-personalized influence targeting (HPIT) can be performed to achieve political, economic, military and geopolitical objectives.

The collection and evaluation of data offers a strong potential to better tailor information given by governmental or trustful organisations to the current needs of citizens. Therefore, it is important to identify opinions and react with appropriate measures to stabilize the trust in reliable sources and society itself.

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- Technical
software
- Social/Human
Personalized adverts based on interests
- Organizational/Process</td></tr>
</table>

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)**:
- **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.**
  Expected time to market.

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 Language Processing is used. Based on statistic evaluations a heat	- **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 influence elections or manipulate other authorities. Regarding to the General Data Protection Regulation GDPR there are already conditions

map on popular questions/topics can be created and predictions can be derived.	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.
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. - **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.	

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:**
  It is related to all domains including detection of opinions and disinformation, because the concept can be applied to various thematic.
- **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**
  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.

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Semantic analysis
Machine learning
Sentiment analysis
Artificial intelligence</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
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.
- 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.</td></tr>
<tr><td>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</td><td>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</td></tr>
</table>

	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**	

1.3 PRIMARY CONTEXT NO.3: TREND: INCREASING STRATEGIC DEPENDENCY OF CRITICAL SERVICES

Introduction to the primary context

Growing concerns have been raised the past years regarding certain foreign investors' efforts seeking to acquire control of or influence in European firms whose activities have repercussions on critical technologies, infrastructure, inputs or sensitive information, putting security or public order at risk. The new Regulation includes an indicative list of factors that Member States and the Commission may take into account when assessing whether a foreign direct investment (FDI)[4] The cooperation mechanism established under the EU framework on FDI screening applies from 11 October 2020.

As stated in a working paper on the Global FDI network by the International Monetary Fund[5], in order to describe a globalized world, where national borders are less relevant, economic statistics also need to adapt: information on the "national economy" needs to be supplemented with information on global interconnectedness.

<table>
<tr><td colspan="2">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" [6].
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 information; this information can be partly anonymized. The investment transactions in the system should be verified based on the blockchain technology. Each member of the system has two main tasks: sharing the information and verifying the investments based on the system's information. Only verified investments are allowed then to be executed. Verification can be done by government /EU officials. The system's information should always be updated and visualized/monitored so that the member of the network can easily access important information.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- 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</td><td>TYPE OF SOLUTION
- Technical
Blockchain technology
Information management and monitoring tool
- Social/Human
Verify the investments
- Organizational/Process
Sharing information</td></tr>
</table>

[4] European Commission, MEMO - Frequently asked questions on Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, 09 October 2020
[5] IMF, WP/17/258, The Global FDI Network: Searching for Ultimate Investors, 2017
[6] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187. Chicago

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

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[7].

In another effort to expand its use, Francisco and Swanson suggest serious ethical concerns and serious human rights violations in several companies that are implementing supply chain implementations in all areas (Francisco & Swanson, 2018) [8]. 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.

[7] 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.

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

<table>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Blockchain
Real Information processing and visualization</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
Security
Anonymity
Legal</td></tr>
<tr><td>COSTS
- Indication of costs:
high cost for tool development, for getting enough members for the system and high operation cost
- Differentiate if possible in development, procurement and exploitation</td><td>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
- How durable is the idea (how long is the idea expected to be effective/useful?)
very durable</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

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 special 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 which can decide on approval of foreign direct investment and should therefore be the main 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

- **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 information is highly unstructured and in many different formats 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[9].The genetic and ant algorithms were combined to improve the performance of the focused crawler.

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 against the fake news.

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY

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

Natural language processing
Computer vision
Information retrieval

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:
  medium
- **Differentiate if possible in development, procurement and exploitation**

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  no
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  very durable

MISCELLANEOUS

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

[9] 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

2. INNOVATIONS FOR COUNTERING HYBRID THREATS: CORE THEME: CYBER AND FUTURE TECHNOLOGIES

2.1 PRIMARY CONTEXT NO.1: GAME CHANGERS: QUANTUM AS A DISRUPTIVE TECHNOLOGY

Introduction to the primary context.

Many people have heard of quantum computing, know that it's coming and are aware that it will bring an almost unimaginable speed-up in the ability of computers to perform many kinds of calculations. This will allow wonderful advances in, for example, our ability to discover new materials and design new life-saving drugs. Unfortunately, powerful quantum computers will also enable the hacking of today's "unbreakable" encryption in minutes.

As things stand, the encryption that underpins the security of society's critical infrastructure is at serious risk of being undermined by quantum computers within the next eight to 15 years. This is the "quantum threat" (The Quantum Threat to Cyber Security, Michele Mosca Bill Munson, 2020).

In addition, there are many aspects of daily life, that are heavily dependent fundamentally on the security of the underlying cryptographic algorithms. Online banking, e-commerce, telemedicine, mobile communication, cloud computing and more can be mentioned. Public-key algorithms are particularly crucial since they provide digital signatures and establish secure communication without requiring in-person meetings.

All current encryption systems can become vulnerable as soon as large quantum computers are built. Society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. As predicted, a large-scale quantum computer becomes a reality within the next 15 years, existing public-key algorithms will be open to attack. In parallel, quantum safe algorithms are being developed. They target to solve critical infrastructure protection issue. However, next to it stands legacy infrastructure security, that have been under the development and deployment for last 50 years and never been designed for core architecture upgrade. If that would become a target – we can easily loose trust in all technologically enabled environments that surrounds us. It is so massive, that is hardly imaginable to be replaced and therefore is one of top priority targets for security, resilience, defence innovations development.

Long-term confidential documents such as patient health-care records and state secrets, systems used by critical infrastructure, must guarantee security for many years. Abilities to access them and use for malicious purposes is one of the considerations, going beyond technological aspects of the subject.

Access to stockpiled confidential or sensitive information, attacks on private computers or systems used by critical infrastructures or other intrusion vectors are mainly of cyber nature and to be left to the field of cybersecurity. But use of leaked information, construction of fake or partly fake information bring new challenges in the light of hybrid treats. Massive targeted or even micro targeted attacks on certain groups of citizens can also be a one of components within a larger scale event. Thus, it is important to understand the overall vulnerability scope, initiate and have intense dialog with cybersecurity community. Preparing community to understand the challenge, get ready for wide scope of emerged vulnerabilities, is the task more relevant to institutions dealing with hybrid threats than pure cybersecurity exercise.

Despite the fact, that most of activities of in the field are concentrated around technological aspects of quantum computing and post quantum security, there is a need to understand and prepare institutions and society for the appearance of the game changer in the digital world.

In the context of hybrid threats, there are few ongoing projects presented, that despite their technical nature, can provide insights on scope and prospect targets of appearing vulnerabilities. At this stage all scanned developments are technology focused and can be used as a kick-starters for further understanding of how technology can be exploited in light of hybrid treats, define the scope of vulnerabilities.

<table>
<tr><td colspan="2">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</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- <u>Technical:</u> <u>the testbed itself is a technical solution</u>
- 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.</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">STATE OF THE ART
- Indication of Technology Readiness Level (TRL 1-9 index):
TBD, probably low
- In which stage is the solution (research, technology, available innovation, proven innovation):
Research
- Expected time to TRL-9.
N/A
- Expected time to market.
N/A</td></tr>
</table>

<table>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td>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</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
TBD</td></tr>
<tr><td>COSTS
- Indication of costs:
N/A
- Differentiate if possible in development, procurement and exploitation
N/A</td><td>COUNTERMEASURES
- Are there any 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</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

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 standardised 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

- **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: T**PM based solutions including cryptographic tools/algorithms
- **Social/Human**
- **Organizational/Process**

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.**
  N/A

Expected time to market.

- N/A

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**	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the solution?** QR crypto and Trusted Platform Module (TPM) developers	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** TBD
COSTS - **Indication of costs**: N/A - **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.

2.2 PRIMARY CONTEXT NO.2: HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER

Introduction to the primary context.

Cyber-attacks have increased in frequency and sophistication, presenting significant challenges for organizations that must defend their data and systems from capable threat actors. These actors range from individual, autonomous attackers to well-resourced groups operating in a coordinated manner as part of a criminal enterprise or on behalf of a nation-state. Threat actors can be persistent, motivated, and agile, and they use a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, and expose or steal intellectual property and other sensitive information. Given the risks these threats present, it is increasingly important that organizations share cyber threat information and use it to improve their security posture especially regarding indicators of zero-day vulnerabilities and attacks.

By exchanging cyber threat information within a sharing community through hyper connectivity networks, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.

Three ideas are presented below that can also complement one another.

<table>
<tr><td colspan="2">NAME OF THE IDEA
Efficient cyber threat information sharing through Hyper Connectivity networks

DESCRIPTION OF THE IDEA
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>REFERENCE TO CAPABILITY GAP/NEED
- Describe the use of the solution about the gap/need
Use hyper connectivity as a multiplier of cyber security and cyber defense against common and zero-day vulnerabilities, through sharing.
- 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:
o CT2: Cyber and Future Technologies
o CT3: Information and Strategic Communications
o CT4: Future Trends of hybrid threats</td><td>TYPE OF SOLUTION
- Technical
o Information Sharing Platforms
- Social/Human
o Information Security Collaboration programs
- Organizational/Process
o Security Operation Centers
o CSIRTS
o Information Sharing and Analysis Centers (ISACs)
o Financial Services Information Sharing and Analysis Center (FS-ISAC)
o Electricity Sector Information Sharing and Analysis Center (ES-ISAC)</td></tr>
</table>

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, 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.

- **Resilience/defensive/offensive**

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

<table>
<tr><td colspan="2">

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).

</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
o Open IOC,
o STIX,
o IODEF
o TAXII model</td><td>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.</td></tr>
<tr><td>COSTS
- Indication of costs:
N/A
- Differentiate if possible, in development, procurement and exploitation
- N/A</td><td>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?)
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.</td></tr>
<tr><td colspan="2">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</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 defense 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**

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, 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**): 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.**

Through hyper connectivity networks 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.?**

Not really

COSTS

- **Indication of costs**:
  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

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. 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

are available, participation costs act as a barrier - **Differentiate if possible, in development, procurement and exploitation** N/A	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**	

NAME OF THE IDEA

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

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 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.

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**

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.

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.

- **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

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**

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.

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

N/A	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**	

2.3 PRIMARY CONTEXT NO.3: THE INDIVIDUAL AS A DIGITAL ENTITY

Introduction to the primary context.

In the age of internet connectivity, more and more people are using social media platforms such as Facebook, Whatsapp, and Twitter, which together, have about 4 billion users worldwide (Statista, 2019). Checking notifications, sending, and receiving content and information have become part of our daily routine, changing the way news are published and consumed.

A result of this new way of getting informed is the increased range and volume of data, which result eventually in the increased spread of false news. This makes checking the truth of the facts a difficult task (Ciampaglia et al., 2015) and therefore represents an important current problem of our society. In this regard, several attempts have been made to detect when something out of place happens, in order to let the right people know. Both technology and industry will be important facilitators in this attempt. To determine the reliability of an article, machine learning algorithms can be used to detect sensitive content. AI-powered analytics tools can be used to include stance classification to determine whether a headline agreed with the article body, text processing to analyze the author's writing style, and image forensics to detect Photoshop use. Finally, individuals can also assist in this direction given the growing number of fake news throughout the world. By creating factcheckers communities, the society as a whole can provide a scalable solution to the problem.

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- Technical
software
- Social/Human
n/a
- Organizational/Process
n/a</td></tr>
<tr><td colspan="2">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:</td></tr>
</table>

- 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.?**
  Not really. Probably the only caveat might be that justified information could accidentally be categorized as fake news, which could lead to legal issues and claims

COSTS

- **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 inbedding it in governmental organisations.

COUNTERMEASURES

- **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.
- **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.

MISCELLANEOUS

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

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	**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** - **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

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
- **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 simialar 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

3. INNOVATIONS FOR COUNTERING HYBRID THREATS: CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

3.1 PRIMARY CONTEXT NO.1: DISTRUST AND STRESS IN POLITICAL DECISION-MAKING

Introduction to the primary context.

The recent communication on the *EU Security Union Strategy* (COM2020/605 final) binds the security, civil resilience-building and protection of democracy together by emphasizing that security is not only the basis for personal safety, but also protects fundamental rights and provides the foundation for confidence in economy, society and democracy. The strategy sees that the EU can ensure that security policy remains grounded in common values – respecting and upholding the rule of law, equality and fundamental rights, guaranteeing transparency, accountability and democratic control – to give policies the right foundation of trust.

The EU Security Union Strategy makes also a point of direct inter-relationship between the protection of important infrastructures and resilience of democracy by addressing that[10]: "Individuals rely on key infrastructures in their daily lives, to travel, to work, to benefit from essential public services such as hospitals, transport, energy supplies, or to exercise their democratic rights. If these infrastructures are not sufficiently protected and resilient, attacks can cause huge disruption – whether physical or digital – both in individual Member States and potentially across the entire EU."

Hence, early warning, coherent communication and timely response to the crises are key to effectively tackling emerging security challenges. In other words, protecting society's critical infrastructure — with governments as important enablers and facilitators — while minimising the risk of excessive foreign interference and erosion of democratic authority. The measures should include developing legal frameworks, establishing institutional processes and technical cooperation arrangements between public authorities, civil society, and private sector entities. Extending the protection to non-governmental sectors is also an important matter of creating a public-private cooperation framework enabling the key stakeholders that are most vulnerable to draw upon and complement the existing public and private sector capabilities and resources.

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 state(s) – to resist and (quickly) recover from crises. The resilience is multi-

[10] European Commission, Communication on the EU Security Security Union Strategy, July 2020

level and should comprehensively binding together all societal resources available to withstand and recover from large-scale shocks.

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- **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	- **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 platform should contain:

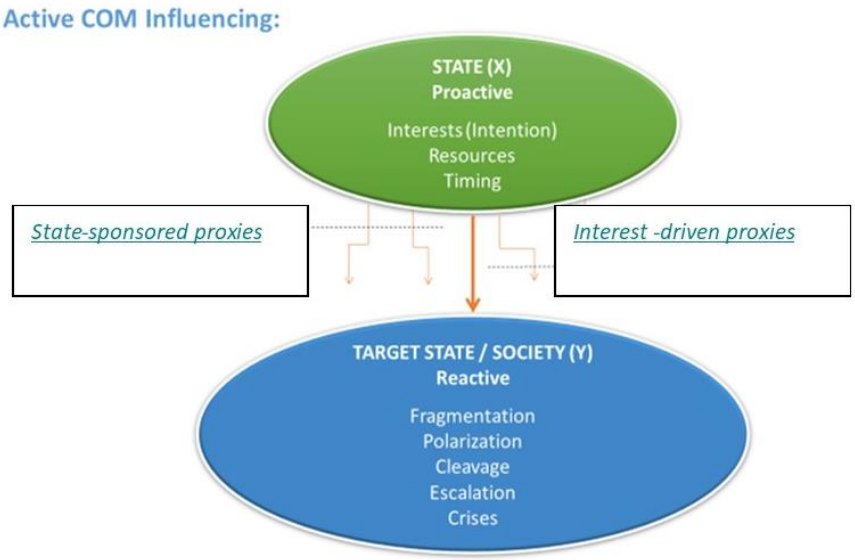
- Official announcements *all-in-one-place online* to the public by the governmental agencies and local authorities.
- Expert advise on how to behave in different emergency and crises situations, incl. what to do in the event of pandemic, a power outage, how to provide first aid, information about fire 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 disinformation 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

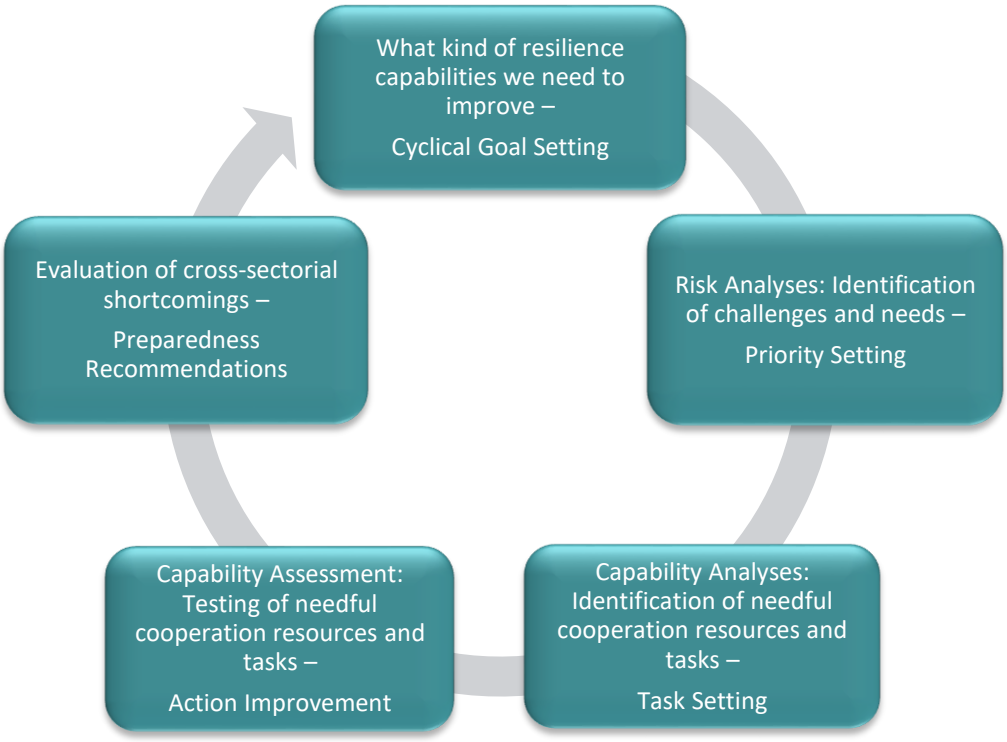
- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**

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.

- **Resilience/defensive/offensive**



ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the solution?** Highly secured IT standards and CERT services.	- **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	**COUNTERMEASURES**
- **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.	- **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	

3.2 PRIMARY CONTEXT NO.2: RELIANCE ON CRITICAL SERVICES AND TECHNOLOGICAL SYSTEMS

Introduction to the primary context

Advances in technology have undoubtedly elaborated the automation in production units and the supply chain, thus reducing the involvement of human resources. As a result, reliance on digital means can potentially decrease the resilience of the production units and the supply chain, as the digital world offers an attractive context for hybrid threats.

The vital need for an uninterrupted operation of critical infrastructures and supply chains was also brought to the surface during the pandemic outbreak. This need became evident due to the disruption of the global supply chain and the shortage in supplies as a result of closed borders and travel limitations.

Besides the legal and economic framework that will support public private partnerships, 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 practitioners to take appropriate actions and initiate strategically planned processes.

<table>
<tr><td colspan="2">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.</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- <u>Technical</u>
- 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</td></tr>
</table>

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.**

- **<u>Resilience</u>/defensive/offensive**

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  GIS and Computational Probabilistic techniques.

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Not applicable

COSTS

- **Indication of costs**:
  Depending on the magnitude of the deployment

- **Differentiate if possible, in development, procurement and exploitation**
  Development is an important part of the cost

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Incomplete representation of the structural details of the CI

  Low resolution input data

  Inaccurate estimation of hazards can degrade the solution

	- **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

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.

<table>
<tr><td colspan="2">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</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Distributed event streaming technology</td><td>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</td></tr>
<tr><td>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</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Users may be reluctant to share their operational information to other involved agencies/actors
- 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</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

3.3 PRIMARY CONTEXT NO.3: GLOBALIZATION VS. LOCALISATION

Introduction to the primary context

Globalisation is often defined and studied in three dimensions: Political, Social/Cultural and Economic. Political globalization refers to the growth of the worldwide political system, in terms of size and complexity. Cultural Globalisation refers to the transmission of ideas, meanings, and values around the world in such a way as to extend and intensify social relations. Last but not least, Economic globalization refers to the widespread international movement of goods, capital, services, technology and information. The society is now experiencing the fourth wave of globalisation, driven by the digital revolution and characterised by cyber physical systems.

Some of the outcomes of the three dimensions of globalisation that makes the latter debatable are: the declining importance of the nation-state and the rise of other actors on the political scene, social inequality and discrimination, as well as worker exploitation in the quest for bigger profits and changes in the power balance between developed and developing countries. Under these circumstances, for societies to remain resilient to hybrid threats, besides proper legislation, it is vital that education both to children and adults focuses on democratic values to overcome social inequality and injustice. Several other strategies and tools have been proposed[11] for inclusion and impact, that include ensuring community buy-in through targeted information sessions and outreach strategies. For this measure, it is also important to grasp the citizen's response to the outreach strategies in order to capture responses and evaluate the success of the communication campaign.

<table>
<tr><td colspan="2">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</td></tr>
<tr><td>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:
Resilient civilians, local level and administration</td><td>TYPE OF SOLUTION
- Technical
Organisational
Probably the central government could be involved to facilitate the implementation on local level</td></tr>
</table>

[11] Successful Strategies Facilitating the Inclusion of Marginalized Groups in Customary and Democratic Governance: Lessons from the Field, International Institute for Democracy and Electoral Assistance, Nepal (2012)

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	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?**	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - To be discussed
COSTS	**COUNTERMEASURES**
- **Indication of costs**: Not known to the author - **Differentiate if possible, in development, procurement and exploitation**	- **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 - **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[12], 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.

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

4. INNOVATIONS FOR COUNTERING HYBRID THREATS: CORE THEME: INFORMATION AND STRATEGIC COMMUNICATIONS

4.1 PRIMARY CONTEXT NO.1: GOING VIRAL

Introduction to the primary context

It is widely acknowledged that disinformation is a rising global issue. According to 2018 data, 85% of surveyed EU citizens consider disinformation to be a threat to democracy .

The scale of the issue is also apparent when looking at the number of attempts to spread false information. Disinformation includes all forms of false, inaccurate, or misleading information which is designed, presented and promoted to intentionally cause public harm or to gain profit. Those can vary from misinformation to actually harmful propaganda.

False information can influence and shape the public opinion on certain issues using written, visual and audio tools which can be spread through various channels. Disinformation techniques include conspiracy theories, fabrication, band-wagoning, clickbait, whataboutism and others. By using those techniques, hostile actors manipulate and distort the truth.

Following the exponential scale of content production, misinformation campaigns have succeeded in dividing the public on crucial matters where societies need to put up a united front. A recent example would be the pandemic outbreak, where spreading of fake news has caused irreversible damage. Increasing social resilience against fake news can be achieved through normative, technological and educational means.

An effort to combine normative and technological means are tools that serve to authenticate journalists and publishers, as for example the Certified Content Coalition, an initiative to encourage standards among online media publishers and certify publishers who meet such standards. Publishers who are certified will receive and display a digital certificate

Regarding educational tools, Fakey for example is a web-based interactive educational tool designed to improve media literacy. It presents news stories that incorporate characteristics of clickbait, fake news, conspiracy theories, etc. Users are then asked to choose to share, hide, or fact-check that information. The goal is to provide users with experience identifying true v. false information.

Among the most important normative efforts is the Journalism Trust Initiative that promotes trust in journalism through the development of standards. It will do so through its Workshop Agreement of the European Centre of Standardization and the participation of media outlets, press councils, and other stakeholders.

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	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Machine learning and AI	- **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	**COUNTERMEASURES**
- **Indication of costs**: Free of Charge - **Differentiate if possible, in development, procurement and exploitation**	- **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.	

Yet, another important effort is to provide operational and near real time fact checking on news in order to establish basis for fact-based identification of fake news. Most reasonable initiatives are built around debunking by combining AI technologies, crowdsourced experts' engagement in analysis and verification. Debunk EU is a good example launched recently in Lithuania, Latvia, and Estonia to fight fake news and propaganda cases coming from East neighbourhood region.

<table>
<tr><td colspan="2">NAME OF THE IDEA
Debunking of Fake News
DESCRIPTION OF THE IDEA
"Debunk EU" is 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 the crowdsourced local experts involvement spots and identifies disinformation within 2 minutes from real time.</td></tr>
<tr><td>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:
Information
Social/Societal
Cyber
- Applicable core theme(s) as stated by the gap/need:
Information and Strategic Communications</td><td>TYPE OF SOLUTION
- Technical
- Organizational/Process</td></tr>
<tr><td colspan="2">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):
- 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</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

DESCRIPTION OF USE CASE(S)

This tool is focused on establishing a point of truth for various news feed via AI empowered platform that spots and identifies disinformation within 2 minutes from real time, civil society of elves and journalists who verify claims and competing newsrooms that seek for maximum outreach. The platform engage community and unites professionals from different fields, including but not limited to experts in foreign affairs, security, IT, cyber, environmental, economic and other affairs. Depending on the specific situation, experts may act both proactively or reactively.

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 improves societal resilience to fake news and propaganda, provide categorization of media and news flow

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** Machine learning and AI	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** Free of charge in Baltic MS and available for individual deployment upon request
COSTS	**COUNTERMEASURES**
- **Indication of costs**: Free of Charge - **Differentiate if possible, in development, procurement and exploitation**	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Not identified for today - **How durable is the idea (how long is the idea expected to be effective/useful?)** As long as the platform will be supported by community

MISCELLANEOUS

Any additional remarks/disclaimers/comments/information you might want to provide
https://debunk.eu/about-debunk/

Information war in which it has become increasingly difficult to differentiate between genuinely objective news reporting and slanted propaganda. The media play a fundamental role in this struggle to influence public opinion while seeking to maintain a position of trust as an unbiased observer of events and current affairs. General public in some regions are highly limited in selecting information source at it is spoken language limited.

Moscow has pumped substantial funds into expanding its international media services, broadcasting news in 30 languages under its Sputnik brand.

At the same time, debates and some developments have begun in the European Union concerning the possible creation of a non-partisan Russian-language TV channel to offer Russian-speaking communities in the EU an independent news source as an alternative to Moscow's officially approved news broadcasts. Same solution should follow Arabic and Chinese (Mandarin) speaking regions.

<table>
<tr><td colspan="2">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</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- Technical
- Organizational/Process</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

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	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** Multilingual news and media content	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - **N/A**
COSTS	**COUNTERMEASURES**
- **Indication of costs**: **TBD** - **Differentiate if possible, in development, procurement and exploitation**	- **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 station**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
NA

4.2 PRIMARY CONTEXT NO.2: DIGITAL MONOPOLIES AND MASSIFICATION OF DATA

Introduction to the primary context.

Several years ago, the lack of digital education and of a proper legal framework has led to the voluntary submission of data from millions of users to online platforms and social media applications. The exact intended use of the data was not clearly communicated to the user at that time and, despite recent advancements in legislation and citizen protection initiatives, citizen data is still a tradable commodity. As correctly pointed out in a recent research paper[13], 'the digital monopoly's profit and social surplus always increase as privacy decreases'. The opportunity for targeted, dynamically changing information offered to the citizens carries the inherent danger of manipulation. In that sense, the value of data has to be re-examined by both governments and citizens, especially with respect to lurking threats for democracy.

<table>
<tr><td colspan="2">NAME OF THE IDEA
Fair Trade Data Program[14]
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.</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- <u>Technical</u>
- Social/Human
- Organizational/Process</td></tr>
</table>

[13] Loertscher, S. and Marx, L.M., Digital Monopolies: Privacy protection or price regulation?, International Journal of Industrial Organisation, doi: 10.1016/j.ijindorg.2020.102623, May 2020

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

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)**

- **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

4.3 PRIMARY CONTEXT NO.3: DETERIORATION OF THE QUALITY OF CONTENT

Introduction to the primary context.

Social media, have, in some ways, democratised news in the sense that they have allowed every citizen to create content and publish it. At the same time, they have provided the means for the public to be deceived by fake news[15].

Another important and negative impact is the fact that the quality of the articles has significantly reduced, and, in that sense, a label for quality journalistic content could be developed. Quality journalistic content could also be labelled as 'Critical Commodity'; this would require a new set of rules and regulations on an international level.

The Journalism trust initiative presented in the previous primary context of the same core theme could be utilised to advance the quality of the articles produced. Other approaches include the ones mentioned in an article of the American Press Institute[16].

Attention should also be paid to the monopolization of digital platforms which is contrary to the principal of fair economic competition. On December 9th, 2020, The Federal Trade Commission of the United States and more than 40 states accused a well-known social media platform of buying up its rivals to illegally squash competition[17].

<table>
<tr><td colspan="2">NAME OF THE IDEA
<u>Training application for media literacy</u>
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)</td></tr>
<tr><td>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</td><td>TYPE OF SOLUTION
- <u>Technical</u>
- <u>Social/Human</u>
- Organizational/Process</td></tr>
</table>

[15] Liu, Z., et al., 'The Impact of Labelling Journalistic Content on Readership', 12th Networked & Electronic Media Summit Conference, June 2020.
[16] The American Press Institute, Helping readers tell the difference between news and opinion: 7 good questions with Duke Reporters' Lab's Rebecca Iannucci ,
[17] The New York Times Morning Briefing, U.S. and States Say Facebook Illegally Crushed Competition, December 9th, 2020.

CT3: Information and Strategic Communications CT4: Future Trends of Hybrid Threats	

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:**
  The officials are not the main target audience, however, it would be advisable for them to use the application as well. 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 and first responder

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 rather primitive solutions are already operational.

- **Expected time to TRL-9.** Three years.

- **Expected time to market.**
  Some rather primitive solutions are already operational.

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.**

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

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** IT only.	- **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	**COUNTERMEASURES**
- **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.	- **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. - **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.

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.

<table>
<tr>
<td>

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

</td>
<td>

TYPE OF SOLUTION
Technical
Social/Human
Organizational/Process

</td>
</tr>
<tr>
<td colspan="2">

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):**

</td>
</tr>
<tr>
<td colspan="2">

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.

</td>
</tr>
<tr>
<td colspan="2">

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.

</td>
</tr>
<tr>
<td colspan="2">

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.

</td>
</tr>
<tr>
<td>

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.

</td>
<td>

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.

</td>
</tr>
</table>

<table>
<tr><th>COSTS</th><th>COUNTERMEASURES</th></tr>
<tr><td>- Indication of costs:
Estimated EUR 2.3 Million (highly dependent on the advances in quantum technologies and translation software)

- 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 foreseen constant feedback to users by system handlers), although this all depends on how the content will be upgraded in the future.</td><td>- 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, 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 and disinformation/misinformation are distinguishable from true information -it just takes too much time.

- 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. 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">MISCELLANEOUS
Any additional remarks//disclaimers/comments/information you might want to provide
There has been some theoretical work conducted in the field, see e.g.
https://www.aclweb.org/anthology/C18-1283.pdf</td></tr>
</table>

5. CONCLUSIONS

5.1 SUMMARY

This report presents potential innovations and solutions to EU-HYBNET project's identified pan-European practitioners and other relevant actors' gaps and needs to counter hybrid threats. The gaps and needs, and innovations mapped to them, are presented according to the EU-HYBNET project four core themes – the project four core themes are: the future trends of hybrid threats; cyber and future technologies; resilient civilians, local level and administration; and information and strategic communications. For each of the project core theme, three primary contexts were studied, and potential innovations and solutions were suggested for each of the twelve cases. The main outcomes derived from the study are summarised below.

With respect to the **future trends of hybrid threats**, the first primary context studied is the loss of power of official strategic communication. The main need is to increase the media literacy of citizens in order to increase trust in official communication, and it is suggested that an online analysis of suspicious objects is offered to the public, along with hybrid online dilemma games, that can improve the awareness and understanding of the complexity and cross-sectoral impact of hybrid threats. A better understanding of the hybrid threats and its associated risks for national security can enhance trust in government communication and decision-making.

The second primary context studied is big data as a new power source. The main need is to fight microtargeting of citizens and disinformation by and the solution presented is to raise the attention for the correct information from a trustworthy source. Therefore, it is suggested that the same data that is used by digital actors to achieve political, economic, military and geopolitical objectives, is now used to stabilise the trust in reliable sources and the society itself. Additionally, automatic detection of hate speech in social media is proposed to intervene earlier against disinformation, distrust and destabilization.

With respect to the increasing strategic dependency that governments have on critical services, an alarming fact is that certain foreign investors are seeking to acquire control of or influence in European firms operating in the areas of critical infrastructures, technologies or sensitive information. For that, a blockchain-based real-time information management and monitoring system is proposed to verify the origin of the investment. Additionally, a special crawler and a real-time search engine is proposed to be developed, only for the investors' information; this can provide a quick overview of the investor to be evaluated better and can also help in the development of a database of investors and in the detection of connections between investors.

The quantum disruptive technology is the primary context for the core theme of **cyber and future technologies**. It is believed that, in the near future, it will enable the hacking of critical encryptions in minutes. The open European Quantum Key distribution Testbed is proposed, that will develop an innovation ecosystem and training ground to understand the vulnerabilities and the scope of potential impact. A quantum resistant trusted platform module is also proposed that will include several use cases and will allow long-term security, privacy and operational assurance for future ICT systems and services.

Regarding the increase of hyper connectivity, efficient cyber threat information through these networks is proposed in order to improve cyber defence against zero-day vulnerabilities. Additionally, cross sector cyber threat information sharing is proposed to account for the cases where specific jurisdictions might be absent from information-sharing groups. Furthermore, Public-private information-sharing groups are proposed to develop collaborative investigations and proceed to collective action.

The individual as a digital entity is also a primary context for this core theme and the need for exposing and countering disinformation and increasing societal resilience is profound. A variety of tools is presented, while research is now focusing on automating the whole procedure by solutions that mainly focus on the source of the news. Nonprofessional factcheckers communities are proposed, a solution that would also facilitate the training of the civil society on how to identify fake news; this could be an important step towards winning the war on misinformation.

Resilient civilians, local level and administration is the third core theme studied. The European Union Security Strategy sees a direct interrelationship between the protection of the Union's critical infrastructures and the resilience of democracy. For the distrust and stress in political decision making, the first primary context of this core theme, a resilient democracy Infrastructure platform is a future vision proposed that could drive a value-added approach in solving the issue.

Regarding the reliance on critical services and technological systems, it is suggested that, besides the legal and economic framework that will support public private partnerships, 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 practitioners to take appropriate actions and initiate strategically planned processes. An Early or Rapid Damage Assessment System is proposed that provides 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 the catastrophic event. In addition, it is suggested that a smart message routing and notification service is used for sharing the operational picture to every agency involved in the response at every level of coordination.

With respect to the primary context of globalisation versus localisation, and the negative outcomes of globalisation, it is highlighted that, for the society to remain resilient to hybrid threats, besides proper legislation, it is vital that school and adult education focuses on democratic values to overcome social inequality and injustice. It is also important to grasp the citizen's response to the outreach strategies in order to capture responses and evaluate the success of the communication campaign. For that reason, a tool that monitors and detects the population's response to the information being published and is able to identify the dominant emotion occurring in social networks is proposed.

Information and Strategic Communications is the last core theme studied. The 'viral' dimension in communicating news has reinforced misinformation campaigns that have succeeded in dividing the public on crucial matters where society needs to put up a united front. For this primary context, the Journalism Trust Initiative has been proposed to tackle this matter. This initiative is a collaborative standard setting process according to the guidelines of CEN, the European Committee for Standardization. Additionally, Debunk EU, a digital platform and independent crowdsourced analytical centre can be utilised, as its main task is to research disinformation in the public space and execute educational media literacy campaigns. Non-partisan native language news channels can also offer an independent news source to governmentally approved and biased broadcasting.

Digital monopolies and massification of data are by far the most vivid illustration of a hidden hybrid threat. The California Consumer Privacy Act of 2018 should be thoroughly studied, especially with respect to the right that is given to consumers to opt-out of the sale of personal information. The value of personal data can also be communicated to the public by a 'fair trade data program'. The name was used by Killi company, marking 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 deterioration of the quality of data was probably inevitable as the society was first introduced with social media content creation capabilities. Short time frames are offered to all of us for critical thinking and a training application for media literacy could possibly cover this need, provided that it is appealing enough to the majority of the public. Automated fact-checkers using Artificial intelligence could help humans in that sense, as computers can be faster in producing outcomes following explicit commands for cross checking. Advances in automatic translation could also assist in that direction.

This deliverable has served to identify solutions for different dimensions of hybrid threats. It should be highlighted that a hybrid threat is multidimensional and time dependent. Therefore, in order to produce one holistic solution, we should be able to identify and then teach a computer how to respond to a multidimensional and time dependent situation. This is not yet easy to implement as patterns are not ready to be described. In the future, Artificial Intelligence tools and quantum technology could be used to identify and respond to such threats in a timely manner.

5.2 FUTURE WORK

This deliverable has served to identify solutions for different dimensions of hybrid threats. It should be highlighted that a hybrid threat is multidimensional, part of a larger hybrid campaign and targets vulnerabilities, sometimes by occasion and opportunity. Therefore, in order to produce one holistic solution, we should be able to detect and attribute hybrid threats timely across all domains in order to effectively respond. This is not yet easy to achieve. It requires interdepartmental and international cooperation and alignment and also advanced technologies and tools. Some promising technologies were presented in this deliverable. Mapping of innovations to pan-European practitioners and other relevant actors gaps and needs will continue in EU-HYBNET project Task (T)3.2 also in the forthcoming four years.

In addition, the work performed in this deliverable will be next used in EU-HYBNET T3.1 "Definition of Target Areas for Improvements and Innovations" and Workpackage2 "Gaps and Needs of European Actors against Hybrid Threats"/ T2.3 "Training and Exercises Scenario Development" and T2.4 "Training and Exercises for Needs and Gaps". T3.1 will further analyze what could be the most sound innovations to identified EU-HYBNET gaps and needs of pan-European practitioners and other relevant actors to counter hybrid threats. The information in this deliverable will be used by T2.3 to plan the training scenarios for EU-HYBNET trainings and exercises (T2.4) where the most promising innovations to the identified gaps and needs will be tested and evaluated. This eventually support EU-HYBNET WP4 "Recommendations for Innovations Uptake and Standardization" to proceed in their work: mapping on the EU procurement landscape, creation of strategy for innovation uptake and industrialization, and compiling recommendations for standardization.

ANNEX I. GLOSSARY AND ACRONYMS

Table 2 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	
Big Data	Big data is the term used for large amounts of data collected from areas such as the Internet, mobile communications, the financial industry and healthcare, that are stored, processed and evaluated using special solutions. Therefore, usually a program is used to detect rules or anomalies within the data. [18]
Artificial Intelligence (AI)	The exact definition of artificial intelligence (AI) can vary depending on the applied area. In general, AI describes systems that are able to think or act like a human being. Some of the main skills for a system to be considered as intelligent are machine learning, natural language processing, knowledge representation and automated reasoning. An artificial intelligence learns from input data and applies the extracted rules to similar situations. By receiving feedback, it improves itself.[19]
Machine Learning (ML)	The core of most training algorithms is machine learning: based on the training data the program extracts rules that it applies to similar data in order to classify it or to react with a fitting output. Depending on the received feedback, it adjusts the rules and improves its results.[16]
Blockchain	A blockchain consists of data sets which are composed of a chain of data packages (blocks) where a block comprises multiple transactions (Nofer et al, 2017)
CEN	The European Committee for Standardization
EU	European Union
EC	European Commission
EU MS	European Union Member States
H2020	Horizon 2020
GA	Grant Agreement
DoA	Description of Action
WP	Work Package
T	Task
OB	Objective
KPI	Key Performance Indicator
IA	Innovation Arena
Satways	Satways Ltd
ZITiS	Central Office for Information Technology in the Security Sector
KEMEA	Center for Security Studies

[18] De Mauro, Andrea, Marco Greco, and Michele Grimaldi. "A formal definition of Big Data based on its essential features." *Library Review* (2016).

[19] Kok, Joost N., et al. "Artificial intelligence: definition, trends, techniques, and cases." *Artificial intelligence* 1 (2009): 1-20.

COMTESSA	UNIVERSITAET DER BUNDESWEHR MUENCHEN
ICDS	International Centre for Defence and Security
L3CE	Lithuanian Cybercrime Center of Excellence for Training Research & Education
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk Onderzoek
LAUREA	Laurea University of Applied Sciences Ltd
HYBRID CoE	European Centre of Excellence for Countering Hybrid Threats
JRC	Joint Research Centre-European Commission

ANNEX II. REFERENCES

[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] European Commission, MEMO - Frequently asked questions on Regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union, 09 October 2020

[4] IMF, WP/17/258, The Global FDI Network: Searching for Ultimate Investors, 2017

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

[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.

[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

[9] Successful Strategies Facilitating the Inclusion of Marginalized Groups in Customary and Democratic Governance: Lessons from the Field, International Institute for Democracy and Electoral Assistance, Nepal (2012)

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

[11] Loertscher, S. and Marx, L.M., Digital Monopolies: Privacy protection or price regulation?, International Journal of Industrial Organisation, doi: 10.1016/j.ijindorg.2020.102623, May 2020

[12] Fair Trade Data Program**,** company webpage of 'Killi' link

[13] Liu, Z., et al., 'The Impact of Labelling Journalistic Content on Readership', 12th Networked & Electronic Media Summit Conference, June 2020.

[14] The American Press Institute, Helping readers tell the difference between news and opinion: 7 good questions with Duke Reporters' Lab's Rebecca Iannucci ,

[15] The New York Times Morning Briefing, U.S. and States Say Facebook Illegally Crushed Competition, December 9th, 2020.

[16] De Mauro, Andrea, Marco Greco, and Michele Grimaldi. "A formal definition of Big Data based on its essential features." Library Review (2016).

[17] Kok, Joost N., et al. "Artificial intelligence: definition, trends, techniques, and cases." Artificial intelligence 1 (2009): 1-20.

[18] European Commission Decision C (2014)4995 of 22 July 2014.

[19] Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.

[20] European Commission, Communication on the EU Security Security Union strategy, July 2020

[21] Certified Content Coalition, Rand Corporation, Fighting Disinformation page, accessed December 2020 link

[22] Fakey , web-based interactive educational tool designed to improve media literacy, link to application , accessed December 2020

[23] Journalism Trust Initiative , developing indicators for trustworthiness of journalism, link