FINAL REPORT ON IMPROVEMENT AND INNOVATIONS

DELIVERABLE 3.6

Lead Author: SATWAYS Ltd

Contributors: JRC, LAUREA, ICDS, KEMEA, L3CE

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

D3.6 FINAL REPORT ON IMPROVEMENT AND INNOVATIONS

Deliverable number	**D3.6**	
Version:	**1.0**	
Delivery date:	**30/04/2025**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main author:	**Dr. Souzanna Sofou**	**Satways Ltd**
Contributors:	Julien Theron	JRC, EC
	Aphroditi Gagara	KEMEA
	Marek Kohv	ICDS
	Edmundas Piesarskas	L3CE
	Petteri Partanen, Tiina Haapanen	Laurea
	Michael Meisinger	ZITiS

DOCUMENT CONTROL

Version	Date	Author(s)	Change(s)
0.1	30.01.2025	Souzanna Sofou, SATWAYS	Table of content
0.2	27.04.2025	Souzanna Sofou, SATWAYS	Drafting deliverable, compiling partner contributions
0.3	29.04.2025	Souzanna Sofou, SATWAYS	Added Conclusions and References chapter
0.4	29.04.2025	Isto Mattila, LAUREA	Review
0.5	30.04.2025	Petteri Partainen, LAUREA	Review
0.6	30.04.2025	Souzanna Sofou, SATWAYS	Document editing
1.0	30.04.2025	Tiina Haapanen, LAUREA	Finalization and submission to EC

DISCLAIMER

TABLE OF CONTENTS

TABLES

FIGURES

INTRODUCTION

I. OVERVIEW

The Deliverable D3.6 titled 'Final Report On Improvement And Innovations' summarises the work completed as part of Work Package 3 (WP3) titled 'Surveys to Technology, Research and Innovations' and specifically Task 3.2 'Technology and Innovations Watch', in the frame of the H2020 Project 'Empowering a Pan-European Network to counter Hybrid Threats (EU-HYBNET)'.

In more detail, the present Deliverable provides a list of Innovations and Ideas proposed to counter specific dimensions of Hybrid Threats for specific focus areas. The latter are primarily defined in the Description of Action (DoA) as 'Core Themes', which are studied in detail by WP2 of EU-Hybnet. The Core themes represent the leading multidisciplinary methodological principles of the project, together with the 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.

For every project cycle, different 'Primary Contexts'/ Threats are defined for the Core themes. The Final Evaluation of gaps and needs has been presented in D2.8 by the European Centre of Excellence for Countering Hybrid Threats with the participation of the JRC.

Based on D2.8, this Deliverable presents ideas and innovations for each of the three primary contexts of each of the four Core themes. It should be noted, that as the relevant Deliverable D2.8 is confidential (CO), the present deliverable doesn't directly refer to the identified gaps and needs, but rather to the primary contexts/ Threats these are more relevant to.

The present work also serves to present the most important innovations that have been presented in the previous cycles. The latter have been used in other Tasks of EU-Hybnet for further actions. In more detail:

i) WP3 'Surveys to Technology, Research and Innovations' / T3.1 titled 'Definition of Target Areas for Improvements and Innovations'
T3.1 proceeded with the prioritization and selection of the innovations that can be utilised by pan-European practitioners and other relevant actors to counter hybrid threats.

ii) 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
D3.5 describes for T2.3 what could be the innovations that should be part of the training scenarios and eventually training activities for the most promising innovations to the identified gaps and needs.

The importance of this Deliverable for EU-Hybnet and the interactions with other Tasks is depicted in the Figure below.

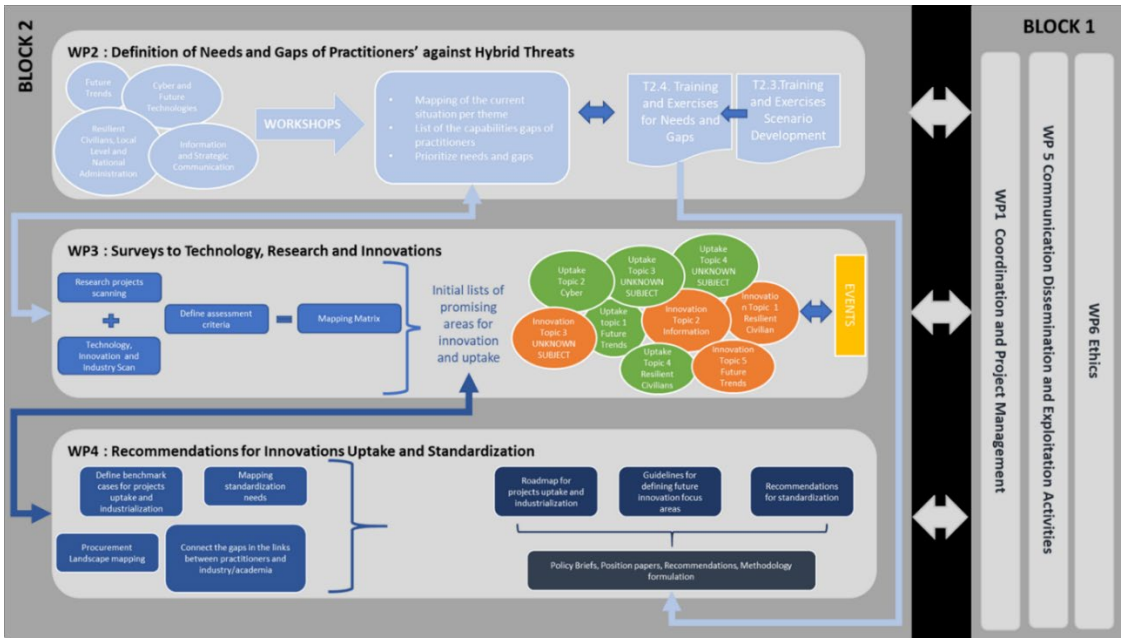

Figure 1 : EU-HYBNET structure of Work Packages and Main Activities

Additionally, D3.6 address the goals of EU-HYBNET project objective (OB) 3 and contributes to reaching its key performance indicators (KPI), as described in EU-HYBNET Description of Action (DoA) document. The OB.3 and KPI3.2 to which D3.5 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, including areas of knowledge /performance	At least 4 reports every 18 months that address technological innovations that are able to fulfil European actors' gaps and needs

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". The EU-HYBNET's definition and approach of Hybrid Threats is in line with the European Commission's "The Landscape of Hybrid Threats. A Conceptual Model" written by the Joint Research Centre and the European Center of Excellence for Countering Hybrid Threats (Nov 2020) [3].

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". [4] 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.

[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] European Commission, Joint Research Centre, The landscape of hybrid threats : a conceptual model : public version, Giannopoulos, G.(editor), Smith, H.(editor), Theocharidou, M.(editor), Publications Office, 2021,
[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

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 second time during the project – first analysis was delivered during the EU-HYBNET 1st project working cycle (M1 – M17/ May 2020 – September 2021) and the second analysis during the second project cycle (M18 – M34/ October 2021 – February 2023). Both analyses 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 needs include the identification of the obstacles to developing, maintaining and improving societal resilience in countering hybrid threats. D3.6 is in line with the Final Evaluation of gaps and needs that has been presented in D2.8.

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

Deliverable D3.6 is the forth deliverable of WP3 Task 3.2 of the EU-Hybnet project. The main actions identified at the beginning of the EU-HYBNET's 3rd project working cycle (starting at M35/March 2023 – M52/ August 2024), included:

1. Careful consideration of the results of the 1st ,2nd and 3rd cycles, including the assessment of the innovations by T3.1
2. Study of D2.8, the long list of defined gaps and needs prepared by the European Centre of Excellence for Countering Hybrid Threats
3. Design and preparation of a table to record, based on the final long list of gaps and needs:
    - The nature of the problem, its origination, immediate outcomes, particular manifestation that needs to be addressed.

- The need to focus on in order to solve security practitioners' and other stakeholders' Gap&Need /Threat
- The expected outcome from the use of a chosen innovation
- The end users of this innovation

SPACE: GOVERNANCE/CIVIC/SERVICES CORE THEME:				
What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who are the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
To fill in one of the options below based on the spaces civic-governance-services I) ministry level (administration): II) local level (cities and regions): III) support functions to ministry and local levels (incl. Europe's third sector):				

4. A List of six scheduled discussions took place during January -February 2025 between the deliverable leader, JRC and T3.2 partners to discuss in detail each threat, the primary contexts and the suggested ideas for countering each threat.
5. Preparation of the presentation for the Final event that took place in Brussels by the Deliverable leader.
6. Thorough analysis of the previous deliverables of this Task and study of the relevance of previous innovations to the final list of gaps and needs.
7. Continuous monitoring of technologies and innovations, and assessment of their suitability to counter the specific dimensions of Hybrid threats.
8. As a result, new innovations have been listed in the present deliverable, along with innovations that have been identified in previous deliverables that have been studied in relevance to the final list of gaps and needs and proved to be still relevant and adequate to counter specific dimensions of hybrid threats.

Additionally, the dedicated template that has been designed by TNO (T3.1 leader) during the first project working cycle (M1 – M17/ May 2020 – September 2021) for presenting innovations and ideas has been updated by TNO, discussed with the Work Package leader and presented by TNO during the programmed T3.2 calls. This template helps present the innovations chosen in a coherent and systematic manner, which also enables T3.1 to proceed with assessments and comparisons of innovations in a later stage. Additionally, the use of the template supports all consortium partners in following the present work more closely and make use of the provided information.

This document suggests potential innovations and solutions to improve pan-European practitioners and other relevant actors' measures to counter hybrid threats, utilising the knowledge collected in the five years of the project.

The main innovations and ideas presented in this work are presented in the following Table per core theme and primary context. The presentation starts with the dedicated Table listed above and continues with the template for presenting innovations.

Table 1 -Ideas and Innovations for Countering Hybrid Threats

CORE THEME		PRIMARY CONTEXT	IDEA/ INNOVATION PROPOSED	Partner proposing the innovation
1. FUTURE TRENDS OF HYBRID THREATS	1.1	Destabilisation due to Instrumentalization of migration	We-Verify, a video plugin to debunk fake videos on social media that spread conspiracy theories	LAUREA
			Media Pluralism Monitor (MPM)	
	1.2	Foreign Interference into domestic politics including elections processes	Establishment of a fully functional intelligence cooperation service at EU level	KEMEA
			Online Collaboration Platform for Foreign Interference	
	1.3	Leveraging lags in foresight and anticipation	Situational awareness tools for cross border and cross organisational operations	STWS
			CONNECTOR CE-CISE	
2. CYBER AND FUTURE TECHNOLOGIES	2.1	Targeting European critical infrastructure and the psychological reliability of digital infrastructures	Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience	STWS
	2.2	Weaponization of Mass Data - massive availability of societal data aggregates & algorithmic computation	Nordlayer or other similar solutions	KEMEA
			Fair Trade Data Program	SATWAYS
	2.3	Leveraging the autonomy and power of digital actors	Tools for protection of personal data and Legislation initiative for the selling of mass data	SATWAYS

3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1	Mainstreaming violence -The growing broadcasting and becoming accustomed to violence weaken democratic politics	Expansion of existing directives and new legislation initiatives	SATWAYS
	3.2	Intimidation of civil society and political engagement	Breach Guard or Any Other Similar Available Solution	SATWAYS
			Network of anti SLAPP financial and legal support	SATWAYS
	3.3	Boosting demand and spread of conspiracy theories, Exploiting Emotions & promoting victimhood in social relations	HYPSTER (as illustration)	L3CE
			Use of Common Frameworks and outcomes of FIMI related EU-Funded projects	L3CE
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1	Reversing priorities from what needs to be broadcasted to what people want to be broadcasted	Journalism Trust Initiative	SATWAYS
	4.2	Advanced forms of AI-enhanced disinformation	BLOCKCHAIN-BASED VERIFICATION	ZITiS
	4.3	Understanding the systemic impacts of disinformation, misinformation, propaganda, and other manipulative activities in the information domain	"Bad News" Prebunking Game platform	KEMEA

The selection of the innovations presented in the current Deliverable was based on continuous monitoring of technology advances and a thorough search in various fields. The different scientific background and complementarity of the T3.2 partners allowed for a deeper understanding of possible applications of various technologies.

Additionally, during the EU-HYBNET 5th Annual Workshop and 5th Future Trends workshop (T3.4) that took place in Brussels, February 13th-14th 2025, the T3.2 partners had the opportunity to discuss with innovation providers and consortia that were invited to participate and present their solutions in these events.

It should be highlighted that, as detailed in the Grant Agreement, the technological innovations presented aim to help European Practitioners counter hybrid threats. This Deliverable also lists societal interventions, which could help European practitioners protect European citizens from offensive populist influences.

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

1.1 Destabilisation due to Instrumentalization of migration

EU-HYBNET responsible partner for this section: **LAUREA**

1.1.1 WE-VERIFY

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
The challenge originates from the increasing use of deepfake videos which spread and feed conspiracy theories. Such media fuels polarization in the societies and resonates within groups where media literacy is low. These groups are susceptible to hybrid influencing. I) ministry level (administration): II) local level (cities and regions): III) support functions to ministry and local levels (incl. Europe's third sector) End-users: Media organizations, journalists, online platforms, data hosts and providers, fact-checkers and researchers working on disinformation.	The outcome is polarization of the societies. More there is groups which feel to be marginalized more those groups are susceptible and resonate with populist news and information. There is also more room for hybrid influencing i.e. mis- and disinformation which serves the aggressors goals. The scope should be on EU level, the influence does not limit to member states only. The spreading of mis- and disinformation can shatter the whole European democratic system and violate shared values.	It provides verification of textual claims, images, and videos (incl. AI-generated fakes); cross modal content verification; content provenance and source trustworthiness via a user-friendly web interface.	Support for media, strategic communication and the development of the media literacy.	Media organizations, journalists, online platforms, data hosts and providers, fact-checkers and researchers working on disinformation.

BOX 1 NAME OF THE IDEA

WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

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

InVID WeVerify is a plugin that allows fact-checkers, journalists and any other interested users to quickly get contextual information about videos posted on Facebook, Twitter and YouTube videos. It can also perform reverse image searches on many platforms and efficiently query them. It can fragment videos, to enhance and explore key frames and images through a magnifying lens, to read video and image metadata, to check media copyright licenses, and to apply forensic filters on still images, all of which are vital tools for anyone trying to check the authenticity and source of the material.

Applicable hybrid threat domains as stated by the gaps/need:

In the first hand cyber, Information and Military /Defense domains could benefit from such solutions. In general, all the domains could benefit, because mis- and disinformation touches every domain.

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

Cyber and Future Technologies, future trends of hybrid threats

BOX 3 TYPE OF SOLUTION

- **Technical**

The innovation proposed is a technical one

- **Social/Human**

- **Organizational/Process**

Whereas the innovation proposed is a technical one, it entails compliance to standards, therefore making the necessity of legal requirements and a legal framework substantial.

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**

In the first hand cyber, Information and Military /Defense domains could benefit from such solutions. In general, all the domains could benefit, because mis- and disinformation touches every domain.

- **Provide the level of practitioners in the same discipline:**

The threat was listed under Services Space in Deliverable D2.7 (Long List of Gaps and Needs)

  - I) ***ministry level*** **(administration):**
  - **II)** ***local level*** **(cities and regions):**
  - **III)** ***support functions to ministry and local levels*** **(incl. Europe's third sector):**

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

Media organizations, journalists, on line platforms, data hosts and providers, fact-checkers and researchers working on disinformation

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Available innovation
- **Expected time to TRL-9.**
  0
- **Expected time to market.**
  0

BOX 6 DESCRIPTION OF USE CASE(S)

It can fragment videos, to enhance and explore key frames and images through a magnifying lens, to read video and image metadata, to check media copyright licenses, and to apply forensic filters on still images, all of which are vital tools for anyone trying to check the authenticity and source of the material.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  It provides verification of textual claims, images, and videos (incl. AI-generated fakes); crossmodal content verification; content provenance and source trustworthiness. Creates a decentralized database of already debunked claims and tampered images and videos, accessible both programmatically (e.g. by search engines or social platforms) and via a user-friendly web interface.

- **Resilience/defensive/offensive**
  The solution can be used in countering hybrid threats in all three manners: to promote resilience, to defend against a threat and also to provide offense against a threat.

BOX 8 ENABLING TECHNOLOGY

Which technologies are critical in fielding the idea?

- Pursue a holistic, cross-disciplinary approach including methods for identifying the key information sources, analysing information cascades and social network actors, and multi-modal and cross-modal content verification techniques (text, images, video).
- The blockchain will ensure that already verified facts are recorded in an incorruptible, decentralized ledger, with no single point of failure. When the contributing verification community grows large enough, the blockchain will be absolutely necessary to ensure that individuals or groups cannot tamper with the database of known fakes to serve their own purposes.
- New modules, released in open source, help verification professionals to identify disinformation ecosystems, the disinformation sources and the way in which disinformation campaigns are exploiting the filter bubbles, echo

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
- No

<table>
<tr><td>chambers, and highly polarized communities for maximum damage</td><td></td></tr>
<tr><td>BOX 10 Implementation effort
- Indication of costs:
Describe the types of efforts and costs needed to implement the idea.
Browser Plugin free of charge</td><td>BOX 11 COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Progress in deep fake creation methodologies
- How durable is the idea (how long is the idea expected to be effective/useful?)
The solution is expected to be useful for a very long time</td></tr>
<tr><td>BOX 12 Preconditions (optional)
- Have all preconditions been met for the idea to be ready for implementation?
No preconditions exist.</td><td>BOX 13 Life cycle maintenance (optional)
- Describe who will operate, maintain, update, and upgrade the described idea.
The solution is designed on a EU funded research project that provides verification systems that can help factcheckers, journalists and human rights activists to debunk and fact-check videos and images online. Many different users are using the deliverables.</td></tr>
<tr><td colspan="2">BOX 14 MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide
Keeping people safe is the number one priority for the European Union and governments across the world, and being able to respond quickly and effectively to the spread of misinformation is key. The InVID WeVerify plugin (https://weverify.eu/), funded through the EU’s Horizon 2020 research and innovation programme (https://cordis.europa.eu/project/id/825297), has already proved to be a vital tool in tackling COVID-19 related disinformation across Europe and beyond. Producing and spreading of mis- and disinformation i.e. influencing is evolving trend which is widely related to different domains and sectors of societies.</td></tr>
</table>

1.1.2 MEDIA PLURALISM MONITOR

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
The challenge originate from the competition environment of the media where rapid media is more profitable than quality media. The rapid low quality media fuels polarization in the societies and resonates within groups where media literacy is low. These groups are susceptible to hybrid influencing. All levels which may be affected and their actions hampered by bad media publicity. In extreme cases the media can transmit mis-/disinformation which may shatter the whole society.	The outcome is polarization of the societies. More there is groups which feel to be marginalized more those groups are susceptible and resonate with populist news and information. When there is more to offer low quality rapid "click" news, there is also more room for hybrid influencing i.e. mis- and disinformation which serves the aggressors goals. The scope should be on EU level, the influence does not limit to member states only. The spreading of mis- and disinformation can shatter the whole European democratic system and violate shared values.	Information and Strategic Communications should be supported and for example the funding of quality and investigative journalism in order to support media pluralism and freedom and that way also inclusiveness	The support for media (see previous box), strategic communication and the development of the media literacy	Crisis Management experts in municipalities and ministries, other experts, strategic communication actors

BOX 1 NAME OF THE IDEA

Media Pluralism Monitor (MPM)

DESCRIPTION OF THE IDEA

Media Pluralism Monitor (MPM) is a tool developed by the Centre for Media Pluralism and Media Freedom (CMPF) of the European University Institute (EUI) to assess the potential weaknesses in national media systems that may hinder media pluralism. Based on 20 indicators, summarizing 200 variables, it covers four areas:

a. Fundamental protection
b. Market plurality
c. Political independence
d. Social inclusiveness.

The news media industry has been severely hit by the COVID-19 pandemic and the accompanying economic crisis. Although the shock was largely foreseeable due to the extraordinary circumstances, its depth and the diverging effect between different countries has to be investigated.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
  The solution can be used to prevent the deprivation of market shares from quality journalistic media by ensuring that sufficient investment in investigative journalism is not sacrificed in the face of journalistic competitiveness, by identifying and sharing best practices for journalistic media economic sustainability
- **Applicable hybrid threat domains as stated by the gaps/need:**
  Information, cyber, culture, social/societal, legal, economy, intelligence domains could benefit from such solutions.
- **Applicable core theme(s) as stated by the gap/need:**
  Information and Strategic Communications, future trends of hybrid threats

BOX 3 TYPE OF SOLUTION

- **Technical**
- **Social/Human**
  The innovation proposed is a Social/Human one
- **Organizational/Process**
  Whereas the innovation proposed is a Social/Human one, it entails compliance to various policies, therefore making the necessity of legal requirements and a legal framework substantial.

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  The threat was listed under Civic Space in Deliverable D2.7 (Long List of Gaps and Needs)
- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level*** **(administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
  Media outlets, journalists, publishers, broadcasters, editors and other related stakeholders are the end-users of the idea

BOX 5 STATE OF THE ART

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

0 years

Expected time to market.

0 years

BOX 6 DESCRIPTION OF USE CASE(S)

Media Pluralism Monitor (MPM) assesses the potential weaknesses in national media systems that may hinder media pluralism and covers the areas of fundamental protection, market plurality, political independence and social inclusiveness.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

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

  The solution can be used to help mitigate the loss of market shares from quality journalistic media (i.e. sufficient investment in investigative journalism), by bridging the gap between true quality journalistic competitiveness (i.e. journalistic integrity), as opposed to competition in terms of which outlet will first transmit the story (i.e. speed of news coverage). The need which arises therefore is the identification and sharing of best practices for journalistic media economic sustainability. A correct and accurate situational snapshot of the ways in which media can be sustained is required, to strengthen the economic model of journalism. Creating a register of good and best practices whereby media outlets have increased their economic viability without compromising content quality and journalistic investigations would therefore be required, across the EU. The solution proposed falls under the information and strategic communications theme.
- **Resilience/defensive/offensive**

  The solution can be used in countering hybrid threats by promoting journalistic economic viability by ensuring its resilience, by defending against threats towards journalistic economic viability.

BOX 8 ENABLING TECHNOLOGY

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

  N/A

BOX 9 Implementation

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

  No.

BOX 10 Implementation effort

- **Indication of costs**:

  Describe the types of efforts and costs needed to implement the idea.

BOX 11 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?)**

  Since media in all its forms will exist indefinitely, the solution is expected to be useful for a very long time.

BOX 12 Preconditions (optional)

- **Have all preconditions been met for the idea to be ready for implementation?**

  No preconditions exist.

BOX 13 Life cycle maintenance (optional)

- **Describe who will operate, maintain, update, and upgrade the described idea.**

BOX 14 MISCELLANEOUS

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

It will be important for future research to evaluate to what extent “active” gamified inoculation is superior to “passive” approaches—including traditional fact-checking and other critical thinking interventions—especially in terms of eliciting a) motivation, b) the ability to help people discern reliable from misinformation, and c) the rate at which the inoculation effect decays over time.

1.2 FOREIGN INTERFERENCE INTO DOMESTIC POLITICS INCLUDING ELECTIONS PROCESSES

EU-HYBNET responsible partner for this section: **KEMEA**

1.2.1 ESTABLISHMENT OF A FULLY FUNCTIONAL INTELLIGENCE COOPERATION SERVICE AT EU LEVEL

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who are the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
The curent EU & global security environment involves a spectrum of hybrid threats wider than ever before. This is increased rapidly because of great power competition and the readiness of various authoritarian states to use violence in order to achieve their goals on political & tactical level. Instrumentalization of migration, use of mercenaries, black operations, use of third party companies etc. is only part of the means that are used. The EU intelligence personnel, LEAs, security forces' personnel with the support of the member states' governments have to be sufficiently equipped, trained, informed and supported to be able to prevent, withstand,	E.g. political instability, societal cohesion destabilzed, territorial loss, widespread disinformation External hostile actors, criminal organizations as well as other third party intelligence agencies might attempt to challenge the credibility, security and status quo of EU. Since hybrid threats include a wide spectrum of possible attacks, in the context of exécuting black operations- the external hostile actor is possible to attack against European security, EU democratic values	The establishment of a fully functional intelligence cooperation service at EU level, will be able to offer excessive amount of information flow, technical means & even human resources when needed in order to handle successfuly and withstand extremely complex and sudden outbursts of emergency situations & attacks. At the same time it is possible to be orgenized in such way that will provide expert specialized training to a large	Enhancing EU security and intelligence cooperation & resilience against possible threats. Establish a register of best practices and best structures.	Member states' intelligence, law enforcement and security forces' personnel.

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who are the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
tackle and preserve the security of the EU countries more than ever. Please fill in one of the options below based on the spaces civic-governance-services **Governance space** i) Ministry level (administration) Coherent governmental and harmonized policies towards better intelligence cooperation. ii) Local level (cities and regions) Sufficiently trained and equipped intelligence and security personnel able to	and autonomy values all at the same time aiming to distabilize a particular EU region, city or country.	amount of EU security practitioners, elevating their capabilities at the highest possible level.		

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who are the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
tackle appropriately any crisis/incident locally. iii) Support functions to ministry and local levels (incl. Europe's third section)				

BOX 1 NAME OF THE IDEA

Short introduction

Establishment of a **fully functional intelligence cooperation service at EU level** which will have the capabilities to tackle the EU urgent strategic and operational needs. Such needs focus more and include countering espionage threats within EU institutions, as well as creating Europe-wide networks of defence against sabotage targeting EU critical infrastructure. Part of the new agency's mission would be to prevent foreign intelligence services from operating inside the EU.

In this context the European Union in order to be able to more effectively prevent and tackle the hybrid threats that geopolitical changes create, should begin to think preventively towards the conventional and unconventional threats to its security.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

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

Operationalizing European responses to hybrid threats.

Overlap and low coherence of government crisis response.

Lack of strategic notice and awareness to interference practices.

Applicable hybrid threat domains as stated by the gaps/need:

Use of mercenaries

The innovation contributes to controlling and preventing the spread of violence and attacks on societal cohesion on a pan- European level. It helps to overcome lack of awareness by state institutions – especially law enforcement and security personnel.

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

Future Trends of Hybrid Threats

BOX 3 TYPE OF SOLUTION

- **Technical**

The first step would be to improve the flow of information & intelligence gathering through existing EU members' security bodies and networks, such as the European Union Intelligence and Situation Centre (EU-IntCEN) and the European Centre for Information Policy and Security (ECIPS) but it will be technologically enhanced in order to be able to handle the large amount of information.

- **Social/Human**

Although it is primarily an organizational solution, the innovation also has strong societal and human dimension, as it requires the cooperation and involvement of a large number of intelligene, law enforcement and security personnel.

- **Organizational/Process**

Primarily an organizational type of solution, since it will require the creation of European agreements and detailed framework to secure the establishment of certain cooperation protocols & procedures between the member states' security services as well as functional plan of cooperation procedures between them.

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**

The main beneficiaries on tactical level are the Intelligence Military/Defence & Infrastructure while focusing more on law enforcement agencies that will have a wide & strong network and flow of information on pan- European level. It will enforce their everyday functions towards fighting external influence and hybrid operations and attacks

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

The Information network that will be created will ensure the information flow for all EU member states' administration enhancing their ability for policy planning and programming future strategic actions also on a political level.

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

Local level authorities and the local police and security forces will be able to use the provided information gathered by the innovation for tackling any relevant threat and event occurring in local level and will be able to get immediate warning in the case of escalation. (informational support in crisis response)

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

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

Intelligence personnel, security forces' personnel, law enforcement agents

BOX 5 STATE OF THE ART

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

TLR 8 : the information & intelligence will be gathered through existing EU members' security bodies and networks, such as the European Union Intelligence and Situation Centre (EU-IntCEN) and the European Centre for Information Policy and Security (ECIPS).

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

The technology to be used for innovation already exists, it will have to be further developed & enhanced in order to cover the requirements of a pan European flow of information.

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

2-3 years

Expected time to market.

Up to 5 years

BOX 6 DESCRIPTION OF USE CASE(S)

The EU has to confront a situation of a 'weaponisation of everything' which has as a consequence the securitisation of everything. The aim of the proposed innovation is European Union to be able to: Anticipate, prevent, withstand and tackle effectively all possible threats & crises in all cross-border areas, as well as inside the European countries' territory.
The European Union will develop agreements between the member states for a fully functional intelligence cooperation service at the EU level that will be able to handle the required operational needs without interrapting at the same time the individual national intelligence agencies' operations, but instead will cooperate with them and even enhance their benefits from this cooperation including providing and exchanging information.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

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

The innovation proposal offers advanced situational awareness between the EU intelligence institutions, its member states' governments (and cities) which could be targeted by hostile hybrid activities and attacks.

- **Resilience/defensive/offensive**

All of the above

BOX 8 ENABLING TECHNOLOGY

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

Highly secured network & platform of exchanging information between intelligence agencies.

BOX 9 Implementation

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

Data and privacy protection regulations must be fully respected and technologically guaranteed.
Legal agreements & protocols are required to be signed between the individual governments and agencies.

<table>
<tr>
<td>BOX 10 Implementation effort
- Indication of costs:
Describe the types of efforts and costs needed to implement the idea.

Depends on technical configurations and agreement conditions.</td>
<td>BOX 11 COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?

Hostile cyber-operations, hostile tactical operations, external attempt of hybrid attack, misinformation, disinformation, propaganda.

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

No limit</td>
</tr>
<tr>
<td>BOX 12 Preconditions (optional)
- Have all preconditions been met for the idea to be ready for implementation?
European agreements between member states and agencies as well as security protocol agreements are required to be signed in order to proceed.</td>
<td>BOX 13 Life cycle maintenance (optional)
- Describe who will operate, maintain, update, and upgrade the described idea.
EU authorities, member states’ authorities, Intelligence Information officers in cooperation with national and regional units.</td>
</tr>
<tr>
<td colspan="2">BOX 14 MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide
https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf</td>
</tr>
</table>

1.2.2 Online Collaboration Platform for Foreign Interference

SPACE : GOVERNANCE/CIVIC/SERVICES CORE THEME :				
What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who are the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
« Intensification of the potential lever for instrumentalizing migrants » Foreign interference in universities Criminal organizations and terrorist networks are trying to infiltrate universities with the aim of radicalizing migrant students themselves or others against them. CIVIC SPACE	Espionage tactics including Infiltration, information leaks, brain-drain of the student and academic community, penetration of sensitive research facilities and projects by foreign powers inside the inner campus life of the university facilities targeting to influnce and radicalize the migrant students. All the above are threatening European Security, Democracy	Young people and students are the next generations that will form society in a few years after entering their productive phase. Securing the academic environment against	Securing universities' facilities and overall campus environment. Ensuring the safety and equal rights of migrant students towards education. Prevention of radicalization of	Local police authorities (LEAs in general) Academic Authorities

Please fill in one of the options below based on the spaces civic-governance-services i) <u>Ministry level (administration)</u> National governmental policy towards a comprehensive culture of security, based on assessments of the topics addressed by the institutions and overall risk assessment. ii) <u>Local level (cities and regions)</u> Municipalities will assist universities along with the cooperation of local police authorities towards tackling the lack of practice of background checks regarding exchange and migrant students. iii) Support functions to ministry and local levels (incl. Europe's third section)	Autonomy and Values at the same time since it means that certain third party criminal interest groups are aiming to pressure and mold academia (against or pro) treatment of particular topics, ending up constraining and/or molding in a desired and specific desired for the way the academic freedom.	external influence is critical.	migrant and other students.	

BOX 1 NAME OF THE IDEA

Short introduction

Creating an **online collaborative interconnected platform** between the national ministry of education, other universities and police authorities that will provide end-users with the capabilities of getting information and recent updates instantly. The purpose of the platform will provide the responsible end-user with the ability to identify and/ or inform the responsible ministry and police authorities of any potential risk factor/ evidence of foreign interference inside the academic facilities and campus. The platform will also include a detailed updated database of cases of foreign interference.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
-
- 1. GAP: TRADITION OF OPENNESS
  Tradition of openness of research cooperation and lack of practice of background checks and resources for it.
- NEED: identifying or creating a database of cases of foreign interference.
-

Applicable hybrid threat domains as stated by the gaps/need:

Societal, cultural, information, political are all applicable and potentially relevant

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

CORE THEME 1: Future Trends of Hybrid Threats

BOX 3 TYPE OF SOLUTION

- **Technical**
  The technical background of creating an inter connected platform between the national ministry of education and all the universities as well as the local police authorities already exists.
- **Social/Human**
  The innovation will combine also strong societal and human dimension, as it requires the cooperation and involvement of the academic authorities, the ministry of education as well as the local law enforcement and security personnel.
- **Organizational/Process**

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  The innovation contributes to controlling and preventing the spread of violence and attacks on societal cohesion on national level and if widely adopted will also have a pan- European applicability.
- **Provide the level of practitioners in the same discipline:**
  - I) ***ministry level*** **(administration):**
    The Ministry of education will have the information required in order to be in direct communication will all university authorities in case it is needed and thus to coordinate and take decisions in case of emergency.
  - **II) *local level* (cities and regions):**
    (Local level authorities if needed), university authorities and the local police including security forces will be able to use the provided information gathered by the innovation for tackling any relevant threat inside the academic facilities & campus when any relevant event occurs and will be able to get immediate warning in the case of escalation. (informational support in crisis response)
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
    -
- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
  Police authorities, university authorities, Ministry of education

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  TLR 8: the technology for the intra connected platform already exists and will need to be adjusted for the purposes of the innovation.
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  The technology that needs to be used for the innovation already exists, it will have to be updated & enhanced in order to be adapted to the requirements of the innovation.
- **Expected time to TRL-9.**
  Depending on the procedure requirements up to one year.
  Expected time to market.
  Up to one year. Similar solutions already exist.

BOX 6 DESCRIPTION OF USE CASE(S)

Over the past years police agencies have implemented a wide range of technological advancements to improve operational efficiency and outcomes in several areas including cross border operations. Such a technological solution is the existence of an online collaborative interconnected platform securing the instant communication and exchange of crucial information between the Ministry of Education, university authorities & the local police authorities.
Criminal organizations and terrorist networks are trying to infiltrate universities with the aim of radicalizing migrant students themselves or others against them. Espionage tactics including Infiltration, information leaks, brain-drain of the student and academic community, penetration of sensitive research facilities and projects by foreign powers inside the inner campus life of the university facilities targeting to influence and radicalize the migrant (but not exclusively) students. The purpose of the platform will provide the responsible end-user with the ability to identify and/ or inform the responsible ministry and police authorities of any potential risk factor/ evidence of foreign interference inside the academic facilities and campus. The platform will also include a detailed updated database of cases of foreign interference.
In case of an emergency event, or evidence of an existing possible case that requires further attention the relevant end-users of the platform will be supplied with the necessary practical means to communicate immediately between each other passing the information and deciding the next steps of action.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  While assisting the fight against spread of violence inside the campus and spread of disinformation in the academic community the innovation also engages the academic authorities and the local police in building resilience against attacks on societal coherence and therefore rises also awareness.
- **Resilience/defensive/offensive**
  The innovation provides universities with the ability to defend themselves in case of an emergency or the potential indication of a risk factor existing inside the campus university. At the same time, it also contributes on building resilience against the risk of external infiltration and/or influence since the database provides constant flow of information and is updated regularly.

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  The technologies needed for/used in the innovation exist and are already similar in use in order to facilitate exchange of information and data between ministries for example.

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  Data and privacy protection regulations must be fully respected and technologically guaranteed.

BOX 10 Implementation effort

- **Indication of costs**:
  Describe the types of efforts and costs needed to implement the idea.
  The innovation will be used while performing on desktop computers or laptops.

BOX 11 COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  The only possible countermeasures would be an online attack to the system, or the use of the

<table>
<tr><td>Exact cost depends on configurations and tender conditions.</td><td>system for malicious purposes from external not authorized personnel.
- How durable is the idea (how long is the idea expected to be effective/useful?)
There is no limit.</td></tr>
<tr><td>BOX 12 Preconditions (optional)
- Have all preconditions been met for the idea to be ready for implementation?
In order to become useful, the innovation needs large amount of end-users updating it regularly and adopting it in their daily tasks.</td><td>BOX 13 Life cycle maintenance (optional)
- Describe who will operate, maintain, update, and upgrade the described idea.
The main beneficiaries of the platform will be the ministry of education, universities and law enforcement. The life cycle maintenance is to be taken care of by public sector.</td></tr>
<tr><td colspan="2">BOX 14 MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

1.3 Leveraging lags in foresight and anticipation

EU-HYBNET responsible partner for this section: **SATWAYS**

1.3.1 SITUATIONAL AWARENESS TOOLS FOR CROSS BORDER AND CROSS ORGANISATIONAL OPERATIONS

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
In cross border incidents and in incidents where different entities are involved in the response, there is no common operational picture among agencies. This is due to the fact that different Member states have different organizational rules, while users may also be reluctant to share their operational information to other involved agencies/actors. All levels which may be affected and their actions hampered by absence of situational awareness.	The lack of a common operational picture creates delays, and causes misuse of resources and inadequate response.	Common situational awareness tool	Better use of resources, minimised time delays, protection of human lives	All response agencies and operational centers.

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, has been tested for the case of a big refinery in order to route information to the responsible public safety agencies (InfraStress H2020 project)
It has 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>

1.3.2 CONNECTOR CE-CISE

The following analysis is based on the proposed CE-CISE currently being developed in the frame of the CONNECTOR project[5]

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
There is a lack of shared risk assessment, management and control system for customs administration in the EU. The challenges phased include high volumes of goods & persons, absence of real time information, absence of expertise, multiple sources of information and inefficient sharing of information. Risk indicators are different, and illegal trade occurs at import, export and intra-EU borders. Overall, there is no consistent approach across the EU.	The limited ability to share intelligence in real time and have common risk indicators leaves no room for common response and ultimate use of resources and intelligence.	The proposed CE-CISE is a fully interoperable technical framework, which expands the scope and capabilities of CISE to Customs domain, ensuring effective management of EU external borders at operational, tactical & strategic level, facilitating the information exchange at interagency and transnational level, to: • Improve the common operational picture and	➔ Near real time, secure information, shared between customs, border guards across the Union ➔ **Information on trends**, smuggling routes and concealments ➔ **Improved targeting** through consistent risk rating application ➔ **Ability to improve and share intelligence reports,** especially for planned operations	Customs and Border Guards will be the end users:

[5] CustOms exteNded iNteroperablE Common informaTiOn shaRing environment , CONNECTOR, (EU-Funded project , Grant Agreement No 101121271)

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
All levels which may be affected by lack of common situational awareness.	Therefore, public authorities do not have the means to act proactively and respond efficiently for hybrid threats, and that may enhance the effect of hybrid threat activity.	enhance situational awareness • Enable the EU cross border joint operations • Support and complement each other's work	➔ **Improved cooperation, efficiencies and deployment of resources** ➔ Improved ability to target cross border criminal gangs, ➔ **Potential capability to target crime at all levels, from source to destination.**	

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

2.1 TARGETING EUROPEAN CRITICAL INFRASTRUCTURE AND THE PSYCHOLOGICAL RELIABILITY OF DIGITAL INFRASTRUCTURES

EU-HYBNET responsible partner for this section: **Satways**

2.1.1 MULTI-STAGE SUPPLY CHAIN DISRUPTION MITIGATION STRATEGIES AND DIGITAL TWINS FOR SUPPLY CHAIN RESILIENCE

NAME OF THE IDEA

Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience

DESCRIPTION OF THE IDEA

In recent years, several authors have studied the supply chain disruption risk, while the pandemic stimulated further research. Indicatively, the idea presented in a paper by Chen et al (2022) [6] studies a supply chain disruption recovery problem in the context of Covid-19 pandemic with supply disruption risk and manufacturer capacity fluctuations in a four-tier supply chain with make-to-order manufacturing.

The authors have developed a mixed-integer linear programming (MILP) model based on emergency procurement and product design change strategies considering the product life cycle with the manufacturer's maximum profit as the goal. Also, they have developed a heuristic for the solution of the MILP model. A few interesting conclusions are also presented in this paper. It has been shown that when the number of disrupted suppliers is high, the manufacturer adopts a combination of emergency procurement and product design changes. The implementation of the idea can support the manufacturers in establishing an optimal recovery strategy whenever the supply chain system experiences supply disruptions, which is especially relevant in times of war.

Besides the mitigation strategy, supply chain disruptions can be avoided with visibility, analysis, and planning[7]. In order to address resilience, leading companies are turning to supply chain specific tools that allow for a new supply chain model – the digital supply chain network (DSN). These new tools can account for problems that can affect a whole supply chain, such as the ripple effect of an exceptional disruption.

A digital twin represents the current state of a supply chain, with the actual transportation, inventory, demand, and capacity data. Then, simulation in the digital twin can help show disruption propagation and quantify its impact. In addition, simulation enables efficient recovery policy testing and the adaptation of contingency plans according to the situation[8]. Stress testing a supply chain with what if scenarios can reinforce any mitigation strategy and strengthen the resiliency of a critical entity.

[6] Chen, J., Wang, H. & Fu, Y. A multi-stage supply chain disruption mitigation strategy considering product life cycle during COVID-19. Environ Sci Pollut Res (2022) Feb 5;1-15.

[7] Wilkinson, G., How To Avoid Supply Chain Disruptions, anyLogistix supply chain management.

[8] Ivanov, D., Managing Risks in Supply Chains with Digital Twins and Simulation, White Paper, Hochschule fuer Wirtschaft und Recht Berlin.

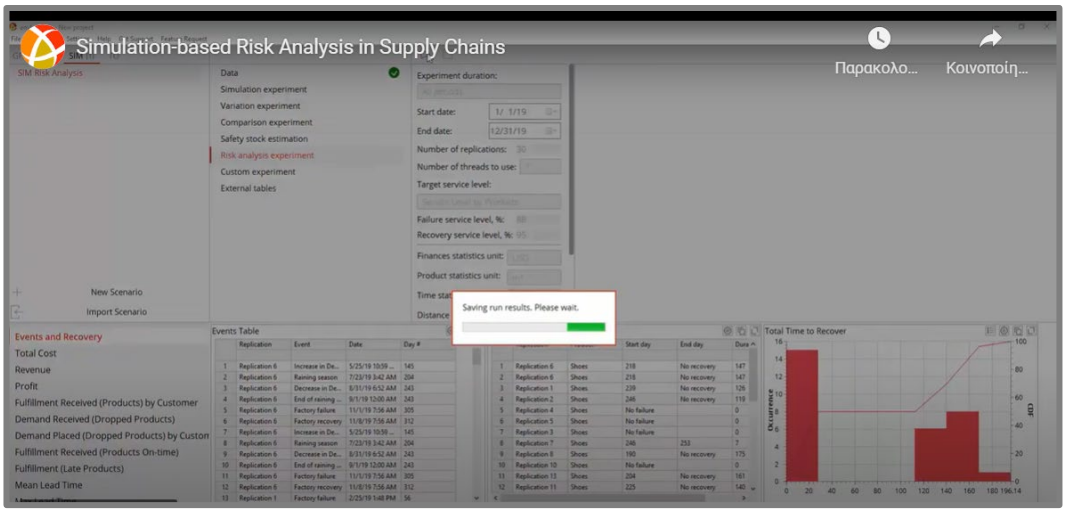

Figure 2: Simulation -based Risk Analysis in Supply Chains, video available in Youtube by anyLogistix supply chain software

Another example is the one of Resilink that offers End-to-End SCRM including resiliency scorecard for suppliers' performance[9].

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- **Describe the use of the solution in reference to the gaps/need** The aim is to help address the problems of Supply disruption on key strategic raw materials and of EU dependence on non-EU strategic supply and value chains. - **Applicable JRC domains as stated by the gaps/needs:** political, economic and infrastructure - **Applicable core theme(s) as stated by the gap/need:** o Future Trends of Hybrid Threats	- **Technical** - **Social/Human** - **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
- political, economic, information and infrastructure domains
  .
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):**
  - **II) *local level* (cities and regions):** Cities and representatives of Critical Infrastructures
  - **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 (manufacturers – CIs)

[9] Resilink, company webpage

STATE OF THE ART

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

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  - Mitigation strategy: research. Simulation software: proven innovation
- **Expected time to TRL-9.** 9
  Expected time to market. Simulation software available in the market

DESCRIPTION OF USE CASE(S)

- A description of the use cases for the software can be found at this **link** and include supply chain optimisation for various companies.
- One of the most interesting use case is the one of the Logistics Institute - Asia Pacific (TLI-AP), a premier research institute in Asia Pacific nurturing logistics excellence in research and education, that was approached by one of the leading humanitarian organizations to address a supply network design challenge for disaster preparedness so as to support the Indonesian National Government.
- Using anyLogistix, the TLI-AP research team designed a comprehensive decision support framework for stockpile prepositioning in the context of humanitarian response. By focusing on network optimization, this work improved the capabilities of the Indonesian national government to cope with disasters by achieving an average transportation time to disasters affected zone of 0.5 days.

IMPACT ON COUNTERING HYBRID THREATS

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

- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  No specific requirements, Software can run in a windows environment

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:
  Not available but expected to be the normal pricing of commercial software
- **Differentiate if possible in development, procurement and exploitation**

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Not applicable
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  This software type is expected to be constantly updated while new methodologies emerge.

MISCELLANEOUS

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

2.2 WEAPONIZATION OF MASS DATA - MASSIVE AVAILABILITY OF SOCIETAL DATA AGGREGATES & ALGORITHMIC COMPUTATION

EU-HYBNET responsible partner for this section:

2.2.1 NORDLAYER OR OTHER SIMILAR SOLUTIONS

Introduction

The leak and trading of personal and medical information from hospitals, for various purposes, such as identity theft, carries societal implications of sufficient scale. This leads to the need to place adequate consideration on the integrity of medical data.

Following the EU medical data security regulations landscape mapping, the outcomes could be tested for readiness in terms of the following aspects, which are the main things the medical community can do to strengthen their systems against a security breach:

1. Analyzing current security risks.
   Providers should conduct an annual security risk analysis for vulnerability detection and policy review, additionally making regular security audits a priority.

2. Having an incident response plan.
   Creating and implementing a response plan will help avoid escalations when a breach or incident occurs. This plan can give clear guidelines for the necessary decisions and follow-up measures.

3. Constantly educating staff.
   Employees should fully understand the consequences of a data breach in healthcare, as well as the different types of data breaches. They should also be aware of measures for both preventing a threat and dealing with one when it occurs.

4. Limiting access to health records
   It is important to identify users, track their activity, and ensure the right procedures for logging in and out of a system. Effective access permissions should be in place, depending on user position, so that only those healthcare specialists who work with medical records can access them.

5. Creating subnetworks
   Dividing a wireless network into separate subnetworks for different user groups, such as patients, visitors, personnel, and medical devices is advised. In other words, provide public wi-fi access to guests which is separate from your secure network where patient data is circulating.

6. Limiting the use of personal devices
   Healthcare professionals often use personal devices for quick remote access, but this creates additional risks, as malware entering the system makes it vulnerable to attacks. If employees are allowed to bring and use their own phones or other electronic devices for work, creation of a strict and clear policy that outlines which devices they can use within and outside the network, how to connect them to the network, and so on is crucial.

7. Avoiding the use of outdated IT infrastructure

The older the equipment, the higher the risks of hackers accessing it. Replacing outdated devices regularly would reduce the risk of medical data breaches.

8. Updating software regularly
   Regular software updates lower the risk of cyberattacks. Having extensive expertise in healthcare software development.

9. Reviewing service-level agreements
   When choosing third-party vendors that will need access to patient data, verifying that they comply with regulations and other applicable laws should be mandatory.

10. Encrypting data
    Encryption technologies help mitigate the consequences of cyberattacks. In the USA, as per HIPAA's Breach Notification Rule, encrypted data is not considered unsecured, and so encrypted data loss does not constitute a breach.
11. Setting and enforcing retention schedules
    A retention schedule should be required. so that electronic health records (EHRs) containing sensitive data don't stay in the digital environment longer than required. This schedule should specify what information to keep, the period, storage type, and destruction methods.

12. Destroying sensitive information properly
    Confidential information should be securely destroyed.

13. Investing more in security
    Along with advanced network security tools, allocating funds to IT and legal teams is important.

Following the above steps could help avoid data privacy breaches in healthcare, but they may not be enough to eliminate the risk of cyberattacks. Understanding more about the foundation of industry security is essential.

Five Pillars of digital healthcare security

Digital healthcare security is made up of five pillars: EHR systems, connected devices, payers, providers, and authorities (Government Regulators).

1. **Electronic Health Record (HER) systems**
2. **Connected medical devices**
3. **Hospitals and other providers**
4. **Health payers**
   Healthcare providers aren't the only ones who deal with personal patient records. Insurance providers, company health plans, and governmental organizations can also be targeted by attackers.
5. **Government regulators (in the USA)**
   The medical industry is one of the highest regulated sectors. The government defines the rules for all organizations operating in the healthcare arena, including those related to the protection of patient privacy and health information:

   - HIPAA is the major legislation in the field that has spurred the need for compliance in healthcare and provides standards and guidelines for handling confidential patient records.

- HITECH has tightened up enforcement of the HIPAA guidelines by implementing regular governmental audits and imposing penalties.

- The Affordable Care Act (ACA) has promoted cooperation among providers to achieve lower costs and better outcomes of care delivery by incentivizing providers who have shifted to a “pay-for-value” model instead of typical “pay-for-service.”

By implementing penalties and incentivizing compliant providers, the government can ensure that patient records are secure.

With so many factors and parties affecting data security and data quality in healthcare, the question is how risk can be mitigated.

Software solutions that help protect patient information follow:

- Cloud-based infrastructure.
- Encryption.
- Secure data standards.
- Backups.

BOX 1 NAME OF THE IDEA

NordLayer or other similar solutions.

DESCRIPTION OF THE IDEA

The specific solution has been selected for exemplary purposes alone, since there are various other solutions which offer similar services.

NordLayer contributes to the protection of hospital patient data from leaking by providing secure remote access, implementing access control, encrypting data, ensuring compliance to standards in Cloud environments, providing multi-factor authentication, as well as activity monitoring and visibility.

Secure Remote Access is crucial, since healthcare organizations need modern security solutions that adapt to the complexities of today's hybrid working environments and to HIPAA rules in the USA or GDPR rules in Europe. Wherever their location, users, devices, apps, and data must have the same advanced level of network access protection.

Implementation of Access Controls is achieved by verifying all user identities before network access permissions are granted. Whoever access is granted to (enterprise users, third-party administrators, or business associates), the experience is efficient, seamless, and safe.

Data Encryption of protected health information or other sensitive data that is being sent between networks is carried out through AES 256-bit encryption, which is the most optimal solution for protecting sensitive data and minimizing cyber risks.

Ensuring Compliance to standards in Cloud Environments when using any communication service provider (CSP) such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, or others, becomes a shared responsibility between the CSP and the hospital (which is the customer). The hospital is, therefore, responsible for configuring and using cloud services in a way that complies with HIPAA or GDPR privacy requirements (USA & EU respectively).

Multi-factor Authentication (MFA) is a powerful defense against the theft of Protected Health Information (PHI) as a fundamental security measure used in many devices. NordLayer offers MFA for accessing gateways that connect hospitals and other customers to valuable resources. By following best practices in Zero Trust Network Access (ZTNA), resource access is strengthened, with the added layer of MFA protection.

Activity Monitoring & Visibility via verifying user access to resources allows businesses / organizations to understand who is inside the enterprise network. In the USA, this is one of the HIPAA requirements.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

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

  The solution can be used to prevent the leak of hospital patient data by bridging the gap of system diversity, the outdatedness of existing systems, the inadequacy of cyber security requirements and practices, as well as the inadequacy in levels of protection and regulation of health operators.

- **Applicable hybrid threat domains as stated by the gaps/need:**

  Cyber, Information and Military /Defense domains could benefit from such solutions.

BOX 3 TYPE OF SOLUTION

- **Technical**

  The innovation proposed is a technical one

- **Social/Human**

- **Organizational/Process**

  Whereas the innovation proposed is a technical one, it entails compliance to standards, therefore making the necessity of legal requirements and a legal framework substantial.

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

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  Cyber, Information and Military /Defense domains could benefit from such solutions.

- **Provide the level of practitioners in the same discipline:**
  The threat was listed under *Services Space* in Deliverable D2.7 (Long List of Gaps and Needs)
  - I) ***ministry level*** **(administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**

- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
  Hospitals, healthcare providers, healthcare facilities, health insurance companies, and ultimately private citizens are the main beneficiaries of these kinds of technologies.

BOX 5 STATE OF THE ART

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

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

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

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

BOX 6 DESCRIPTION OF USE CASE(S)

NordLayer contributes to the protection of hospital patient data from leaking by providing secure remote access, implementing access control, encrypting data, ensuring compliance to standards in Cloud environments, providing multi-factor authentication, as well as activity monitoring and visibility.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
As mentioned above, the solution can be used to prevent the leak of hospital patient data by bridging the gap of system diversity, the outdatedness of existing systems, the inadequacy of cyber security requirements and practices, as well as the inadequacy in levels of protection and regulation of health operators. The need which arises therefore is the in-depth mapping of the landscape of medical data security regulations in the EU, with the expected outcome being an enhanced benchmarking of EU hospital patient data protection actions and improved harmonization amongst EU medical practitioners. The technologies proposed by the solution can help towards compliance to these practices and they fall under the Cyber and Future Technologies theme.

- **Resilience/defensive/offensive**
  The solution can be used in countering hybrid threats in all three manners: to promote resilience, to defend against a threat and also to provide offense against a threat.

<table>
<tr>
<td>

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  A Microsoft Windows, macOS, Linux, Android or iOS environment are required.

</td>
<td>

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No

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

BOX 10 Implementation effort

- **Indication of costs:**
  Describe the types of efforts and costs needed to implement the idea.
  Approximately 100€ per year (or 550€ per year including a dedicated server with a fixed IP)

</td>
<td>

BOX 11 COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution?**
  Cyber-attacks are constantly evolving and becoming more complex. However, cyber security as a science is also constantly developing.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  Since patient data is stored for an unforeseeable amount of time, the solution is expected to be useful for a very long time.

-

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

BOX 12 Preconditions (optional)

- **Have all preconditions been met for the idea to be ready for implementation?**
  No preconditions exist.

</td>
<td>

BOX 13 Life cycle maintenance (optional)

- **Describe who will operate, maintain, update, and upgrade the described idea.**
  The solution is designed mainly for organizations, therefore, the organizations' IT department will be responsible for its operation, maintenance, update, and necessary upgrade.

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

BOX 14 MISCELLANEOUS

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

As mentioned in the Introduction, in the USA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule. The Privacy Rule standards address the use and disclosure of individuals' health information (known as protected health information or PHI) by entities subject to the Privacy Rule. These individuals and organizations are called "covered entities."

GDPR, on the other hand, is a broader legislation that supervises any organization handling personally identifiable information of an EU or UK citizen.

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

2.2.2 FAIR TRADE DATA PROGRAM

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[10], '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[11]
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>

[10] 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

[11] 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

2.3 Leveraging the autonomy and power of digital actors

EU-HYBNET responsible partner for this section: SATWAYS

2.3.1 TOOLS FOR PROTETCION OF PERSONAL DATA

Introduction

Personal identity data is becoming massively available and transparent, therefore allowing, with the help of currently available technologies, the criminal offences of impersonation and taming with billing systems and obligations.

In more detail, according to a recent article[12], there are 4 steps followed, that is, Discovery and investigation, Deception and hook, Attack, and Retreat. Although the tactics have not changed, phishing attacks are becoming more convincing due to the contemporary advances and capabilities of relevant technologies. The rise of deep fakes is also an alarming factor, as deception is one of the 4 stages of the attack.

Using Artificial Intelligence assisted real time fraud detection could be critical in addressing this problem, along with multistage authentication. In online fraud detection and prevention, machine learning is a collection of artificial intelligence (AI) algorithms trained with a user's historical data to suggest risk rules. By implementing the rules, certain actions can be blocked or allowed, including suspicious logins, identity theft, or fraudulent transactions. The benefits of machine learning include[13] faster and more efficient detection, reduced manual review time, better predictions with large datasets and cost-effective solution. According to a recent article[14], AI-powered fraud detection can also uncover complex and subtle patterns, thus reducing false negatives. Additionally, AI systems can adapt and evolve alongside ever-evolving fraud techniques, staying ahead of fraudsters and minimising false positives.

Another important step in online fraud detection is combining AI with biometric authentication, such as fingerprint or facial recognition. However, it should be highlighted that ethical concerns are raised by the use of AI technology in fraud detection, and these regard privacy, consent and transparency, and they should be taken into consideration.

It may also be interesting to note that AI is not only used in fraud detection but also in fraud prediction and prevention[15]. Modern collaboration platforms are using AI for that reason to stay ahead of fraudsters.

In order to support a holistic solution, relative initiatives or research consortia should be identified that would collaborate with communication experts in order to communicate to the public the risks of social engineering.

Additionally, a legislation initiative is proposed on an EU level for the selling of mass data, to help reduce the growth of power of social media platforms. This initiative should take under consideration the power concentrated with the concentration, maintenance and selling of mass data, as well as its dynamics, in light of AI possibilities and future adaptations of quantum technology.

[12] Shivananghan, M., Modern Engineering Explained -10 Types of Social Engineering Cyberattacks, FreeCodeCamp, March 21st, 2023.
[13] Tanant, F., Fraud Detection with Machine Learning & AI, Seon company online article, accessed September 2023
[14] The Rise of AI-powered Fraud Detection in Payments: Securing your transactions, Sweep, May 24th, 2023.
[15] AI improves fraud detection, prediction and prevention, IBM Watson Studio, online article assessed July 2023

BOX 1 Shield, Watson Studio, Or Any Other Similar Available Solution

IBM Watson Studio, formerly Data Science Experience or DSX, is IBM's software platform for data science, consisting of a workspace that includes multiple collaboration and open-source tools for use in data science. In Watson Studio, a data scientist can create a project with a group of collaborators, all having access to various analytics models and using various languages (R/Python/Scala). The user can choose the tools needed to visualize or cleanse and shape data or ingest streaming data, or, most importantly to create and train machine learning models.

IBM Security QRadar Suite is a threat detection and response solution with AI capabilities, that can be used by analysts to automatically contextualise and prioritize threats. The tool can accelerate response time using advanced AI and automation and an open platform for connecting with existing legacy tools.

SHIELD comprises of three solutions.

Device Intelligence detects and stops fraud in real time with machine learning. It provides customers with knowledge regarding which users, devices and accounts are trustworthy.

AdShield blocks invalid traffic (IVT) which damages every marketing campaign and therefore revenue, and is the result of intentional and unintentional bot traffic on a website[16], whether paid or organic, data or content driven, direct or affiliate.

Compliance AI is the enterprise-grade fraud prevention comprehensive solution for the protection of the entire ecosystem. It leverages the power of device, network and artificial intelligence to profile every user, device, and account at every step of the user journey. The Hybrid AI Engine combines neural networks with symbolic AI to detect coordinated fraud attacks that other solutions miss. The user can identify suspicious patterns in real time.

Figure 3 : Shield Compliance AI, end to end solution for fraud management and compliance

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
  The solutions can be used to protect citizen's data and prevent fraud actions against them, therefore filling the gap of insufficiencies in personal data protection.
- **Applicable hybrid threat domains as stated by the gaps/need:**
- **Applicable core theme(s) as stated by the gap/need:**
- **Cyber and Future Technologies**

BOX 3 TYPE OF SOLUTION

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

[16] Invalid Traffic – What Is It and How to Prevent It?, SETTUPAD blog, June 2022

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  Economy, Cyber, Societal
- **Provide the level of practitioners in the same discipline:**
- **The threat has been listed under *Services Space* in the D2.17 Deliverable (long list of gaps and needs)**
  - I) ***ministry level* (administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
- **Private companies**

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index):**
  9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  The suggested products are currently being sold.
- **Expected time to TRL-9.**
  0 years
- **Expected time to market.**
  0 years

BOX 6 DESCRIPTION OF USE CASE(S)

The SHIELD company webpage mentions various use cases, including truemoney (financial technology brand, providing e-payment services in Southeast Asia), inDrive (international ride-hailing service, passenger transport, operating in 48 countries), MPL (gameplay experiences)

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

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

  Utilising available technologies, such as online banking and online communication, are choices of many citizens and in some cases these choices help boost the economy and social cohesion, respectively. On the contrary, the vast amount of personal data available on the internet and the ignorance with respect to risks can threaten both individuals and private companies, and jeopartise the society's well being and trust in the democratic system. It is imperative that citizens are protected and at the same time alerted of possible risks.

- **Resilience/defensive/offensive**
-

<table>
<tr><td>BOX 8 ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Typical computer operating systems</td><td>BOX 9 Implementation
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
No, there are no restrictions, the solution will be used to prevent fraud attacks.</td></tr>
<tr><td>BOX 10 Implementation effort
- Indication of costs:
Describe the types of efforts and costs needed to implement the idea.
Customised prising is offered for SHIELD based on the company characteristics. Details can be found here</td><td>BOX 11 COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
The threat itself is constantly evolving to overpass such technologies, but so is the solution itself.
- How durable is the idea (how long is the idea expected to be effective/useful?)
These technologies are constantly updated</td></tr>
<tr><td>BOX 12 Preconditions (optional)
- Have all preconditions been met for the idea to be ready for implementation?
- There are no preconditions for these solutions.</td><td>BOX 13 Life cycle maintenance (optional)
- Describe who will operate, maintain, update, and upgrade the described idea.
The company risk analysts and data scientists will be the responsible for the solution usage and maintenance</td></tr>
<tr><td colspan="2">BOX 14 MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide
Other Fraud detection software exist that include for example Ravelin. The presented solutions are given as examples, and not as preferences.
Further to the solutions identified, communication experts can drive the alerting of society about the risks of social engineering enabled by massive data availability and transparency. This can only ne accomplished with the help and guidance of the Academia.
It is important also to highlight the role of legislation in order to minimize harmful threats to individuals, especially the less privileged ones.</td></tr>
</table>

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

3.1 MAINSTREAMING VIOLENCE -THE GROWING BROADCASTING AND BECOMING ACCUSTOMED TO VIOLENCE WEAKEN DEMOCRATIC POLITICS

EU-HYBNET responsible partner for this section: SATWAYS

3.1.1 EXPANSION OF EXISTING DIRECTIVES-NEW LEGISLATION INITIATIVES

Introduction

Violent modes of expression, whether in speech or act, have become more accepted and mainstreamed in public discussion.

The amount of violence broadcasted by national and private television, the film industry and the social media channels has severely increased during the last years throughout Europe and the rest of the world.

The North American public's concern over the potentially harmful effects of violent television programming dates back to at least 1952[17]. Several actions have been taken ever since from the Canadian Radio-Television and telecommunications Commission[18], including the CRTC Policy on Television Violence[19].

Within the EU, audiovisual media services (including broadcasting and on-demand services) are to a broad extent regulated under the Audiovisual Media Services Directive 2010/13/EC (the AVMS Directive). In February 2014, the European Regulators Group for Audiovisual Media Services was established, which is responsible for advising on the implementation of the AVMS Directive. The AVMS Directive in particular aimed to harmonise national rules on: regulation of television broadcasts, including satellite broadcasts, under the 'country of origin', including the right for EU member states to restrict the retransmission of unsuitable broadcast content from another EU member state; promotion, production and distribution of television programmes within the EU, including quotas for European-produced content and content made by independent producers; access by the public to major (sports) events; television advertising, product placement and programme sponsorship; **protection of minors from unsuitable content**; and right of reply (of any natural or legal person whose legitimate interest has been damaged by an assertion in a television programme).

Expansion of 2010/13/EC (the AVMS Directive) with stricter rules on protection of minors from unsuitable content would probably be a solution in the value-added direction.

Additionally, in light of the extreme amount of violence broadcasted in television and social media, new legislation initiatives should be initiated for the protection of the phycological health of the citizens, both minors and seniors, as well as the minimisation of violence spread.

[17] Alter, S., Violence on television, Law and Government Division, publications of the Government of Canada
[18] Canadian Radio-Television and Telecommunications Commission, Government of Canada
[19] CRTC Policy on Violence in Television Programming, 1996-36

3.2 Intimidation of civil society and political engagement

EU-HYBNET responsible partner for this section: SATWAYS

3.2.1 BREACH GUARD OR ANY OTHER SIMILAR AVAILABLE SOLUTION

Introduction

During the last years, the exposure and tolerance to violence in the social media has unfortunately dramatically increased. As a form of online harassment, doxxing (also spelled "doxing") is a form of online harassment that means publicly exposing someone's real name, address, job, or other identifying info without a victim's consent. The aim of doxxing is to humiliate, bully, harass, or otherwise harm a victim.

This kind of attack was known for several years. An interesting article published in 2014 as a blog reveals numerous easy ways that are available to achieve this goal, in order to help internet users being more careful[20].

Recently, governments around the world have begun to pass or propose anti-doxxing laws. In the US, the state of Kentucky passed an anti-doxxing law in 2021, and Hong Kong passed an anti-doxxing law the same year[21]. Disclosing personal data without consent, with an intent to cause psychological harm, is now a criminal offence in Hong Kong that can be punishable by up to a HK$1 million fine and five years in jail[4]. Furthermore, doxing itself can escalate to very serious crimes, sometimes also considered doxing, such as identity theft and swatting.

Activists that work for Civil Society Organisations are often victims of such attacks and their personal and family safety is endangered. Protecting them from such attacks in a prompt and efficient way is therefore imperative.

Besides the legal framework that needs to be established, available solutions like Avast One act can help protect against doxing attacks.

Additionally, this kind of solution can help prevent stealing employee data in all kinds of organisations, including politically exposed institutions. In more detail, these solutions prevent data loss, leaks, breaches and collection by third parties, which in the case of political institutions is a critical matter, as the recipients of these data are violent groups that aim to harm the individuals working in such institutions/organisations.

[20] Blechschmidt, B., Guide to doxing: Tracking identities across the web, Blog Article, November 2014.
[21] 'What Is Doxxing, Is Doxxing Illegal, and How Do You Prevent or Report It?', Avast, Academy, online article, accessed June 2023.

BOX 1 NAME OF THE IDEA

BREACH GUARD Or Any Other Similar Available Solution

Solutions like the Avast BreachGuard help protect personal information against data loss, data leaks, data breaches and collection by third parties, even on the dark web, and offer personal assistance by their experts whenever needed.
The solution offers monitoring for data breaches on a 24/7 basis, and protection from hackers. It automatically scans the dark web for personal information that may have been part of a data leak or data breach and helps protect the user's personal information and avoid identity theft.
Also, the solution allows reclaiming personal info from data brokers. The latter are companies that build a profile based on a user's online activity, including address, health, and financial information. Then, they can then sell this information to third parties, which can seriously impact a user's credit rating, insurance rates, and loan eligibility. Solutions like BreachGuard stops these companies from collecting or selling this kind of information by removing it from their databases.
Strengthening the privacy setting of online accounts is also one of the solutions' capabilities, with the goal of reducing the amount of personal info companies have on the user, as well as stopying the spying on social media.
Such solutions may also be useful for cases of identity thefts, which are common in North America.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
  The solution can be used to prevent doxing and automatically scans the web for personal information that may have been part of a leak or data breach (see description above).
- **Applicable hybrid threat domains as stated by the gaps/need:**
  Cyber, Information and Military /Defence could benefit from such solutions.
- **Applicable core theme(s) as stated by the gap/need:**
- **Cyber and Future Technologies**

BOX 3 TYPE OF SOLUTION

- **Technical**
- **Social/Human**
- **Organizational/Process**
  The innovation is of technical nature, but a legal framework would also be necessary in countering the problem and its routes.

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  Cyber, Information and Military /Defence could benefit from such solutions.
-
- **Provide the level of practitioners in the same discipline:**
- **The threat has been listed under *Civic Space* in the D2.17 Deliverable (long list of gaps and needs)**
  - I) ***ministry level*** **(administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
- **Private citizens are the main beneficiaries of these kinds of technologies.**

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index):**
  9
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  This is a market ready product.
- **Expected time to TRL-9.**
  0 years
- **Expected time to market.**
  0 years

BOX 6 DESCRIPTION OF USE CASE(S)

As explained in the description, the solution can be especially useful in cases. Individuals working in journalism would especially find these technologies very useful in maintaining their anonymity.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

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

  As mentioned above, these technologies can help all individuals that may be working as fact checkers and in that sense it can help socieatal resilience. Most importantly, activists that work for Civil Society Organisations are often victims of such attacks and their personal and family safety is endangered.

- **Resilience/defensive/offensive**
- **The idea can be used in a defensive way to counter hybrid threats.**

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  A Windows environment is necessary. It is not known if VPN is offered, but it is also useful.

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No

BOX 10 Implementation effort

- **Indication of costs:**
  Describe the types of efforts and costs needed to implement the idea.
  In the order of 60$/year

BOX 11 COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution?**
  Cyber-attacks are constantly evolving and becoming more complex. However, cyber security as a science is also constantly developing.
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  The solution is expected to be useful for a very long time, as nothing is ever really erased from the internet, and so personal data can be stolen at any time.

BOX 12 Preconditions (optional)

- **Have all preconditions been met for the idea to be ready for implementation?**
  No preconditions are needed.

BOX 13 Life cycle maintenance (optional)

- **Describe who will operate, maintain, update, and upgrade the described idea.**
  The solution is designed mainly for Individuals. in the case where it is used by companies, the company IT department can be responsible for its maintenance.

BOX 14 MISCELLANEOUS

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

Identity theft is a crime mainly committed in North America, but it could be also committed in Europe. Such solutions can help prevent such criminal actions.

3.2.2 NETWORK OF ANTI SLAPP FINANCIAL AND LEGAL SUPPORT

Introduction

During the last years, SLAPP attacks (Strategic Lawsuits against Public Participation) have become more intense, thereby threatening democratic values and rights. According to the Commission,[22] SLAPPs are manifestly unfounded or abusive court proceedings. They are a particular form of harassment increasingly used against journalists, human rights defenders and others engaged in public participation in a matter of public interest and upholding democratic values and fundamental rights.

The Expert Group Against SLAPP (E03746, JUST- DG Justice and Consumers) was founded in March 2021, with the mission of advising the Commission on any matter relating to the fight against SLAPP or the support to their victims.

Among their members are A) individual experts, appointed in his/her own personal capacity, B) or as representative of a common interest, C) organizations like the Council of Bars and Law Societies in Europe (CCBE), who have also written a policy paper CCBE Position on abusive litigations targeting journalists and right defenders, the European Federation of Journalists (EFJ), who claimed that the Commission adopted a watered-down position on anti-SLAPP directive, the News Media Europe (NME), who also published a position paper on the proposed EU Directive anti SLAPPs , and other public entities.

It is interesting to highlight that one of the topics discussed in the agenda of one the Expert Group meetings [23] (21-11-2022) was the funding opportunities to buttress organizations that provide guidance and support for such targets. In particular, the CERV Programme (Citizens, Equality, Rights and Values) has been mentioned[1], which aims to promote rights and EU values by providing financial support and capacity building for civil society organisations, including those active in anti-SLAPP practices. In fact, protection from SLAPP falls under the EU Charter of fundamental rights call.

Additionally, the Creative Europe Program aims, among other objectives, to provide legal and practical support (sheltering program and financial support) to journalists and other media practitioners in need, including targets of SLAPP.

Besides the legislative initiatives that the Commission is leading, it is important to ensure that an ongoing investigation will not be stopped because of a lawsuit. A potential countermeasure would be to identify or create a consortium of journalists that would support and enable each other's investigations when some of them would be silenced by strategic lawsuits and abusive litigation.

[22] European Commission, The 2023 CHAR-LITI Call for proposals under the CERV, January 26th 2023
[23] European Commission Expert Group against SLAPP, Meeting of 21 November 2022 – Minutes

BOX 1 NAME OF THE IDEA

NETWORK OF ANTI-SLAPP FINANCIAL AND LEGAL SUPPORT

DESCRIPTION OF THE IDEA

The European Anti-SLAPP Conference (third edition to take place in London and online on November 27th-28th 2023) will focus on tracking implementations of SLAPP solutions. It is organized by The Foreign Policy Centre (FPC, an outward-looking, non-partisan international affairs think tank based in the UK), the Justice for Journalists Foundation (JFJ, a London-based charity whose mission is to fight impunity for attacks against media) and the International Bar Association's Human Rights Institute (IBAHRI, which works with the global legal community to promote and protect human rights and the independence of the legal profession worldwide). The conference wass also supported by a list of other organisations.
The conference web page also presents resources, that is, a list of initiatives to address SLAPP as well as ways to acquire practical and legal support.
Firstly, a dedicated tool (offered in 5 languages) helps journalists understand if they are facing SLAPP.

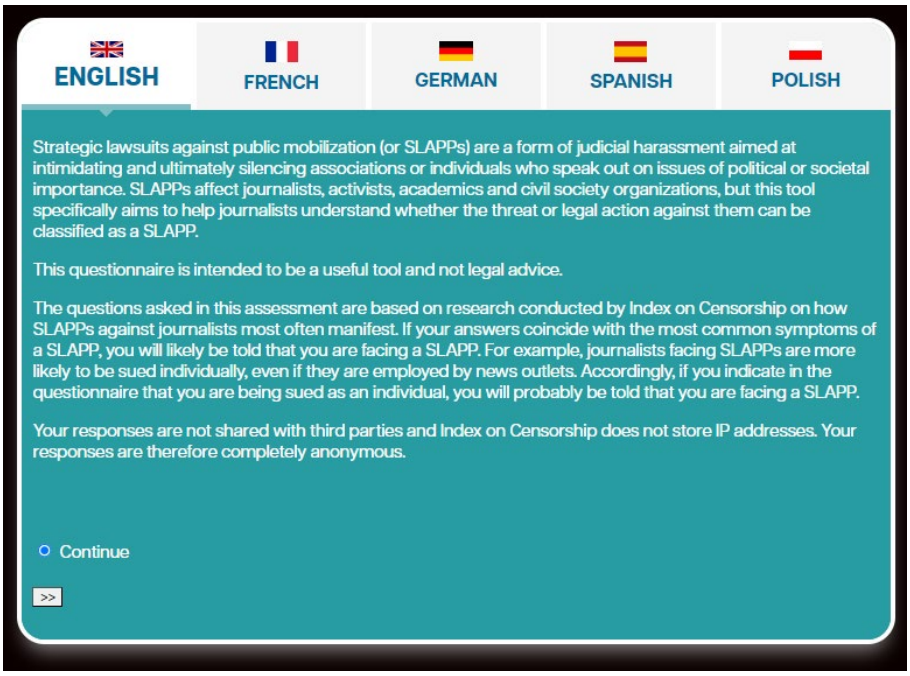

Figure 4 : Screenshot of a tool offered by Index on Censorship for helping journalists understand wheather the threat or legal action against them can be classified as a SLAPP

Then, means to acquire legal support are presented, and these include:
the European Centre for Press and Media Freedom (ECPMF), that proffers and coordinates legal support on matters related to free speech for individuals and organisations working in countries located geographically in Europe. Depending on ECPMF assessment, such support may consist of Financial support to cover lawyer's fees, General guidance, Access to expertise in policy and law making, Engagement in national or international litigation Provision of independent analysis, observation or advocacy around a case.
Furthermore, the Coalition against SLAPPs in Europe (CASE) provides a map based directory of law firms providing pro-bono legal support across Europe.

Finally, there are options for reporting the case, and these include CASE and if the particular case pertains to the UK, the UK anti-SLAPP coalition.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED	BOX 3 TYPE OF SOLUTION
- Describe the use of the solution in reference to the gaps/need **The solution is meant to be used as a response to the vulnerable situation of journalists in light of SLAPP.** - Applicable hybrid threat domains as stated by the gaps/need: - Applicable core theme(s) as stated by the gap/need: **Resilient Civilians, local level ad administration**	- Technical - **Social/Human** - Organizational/Process.

BOX 4 PRACTITIONERS

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

BOX 5 STATE OF THE ART

- Indication of current Technology Readiness Level (TRL 1-9 index):
  9
- In which stage is the solution (research, technology, available innovation, proven innovation):
  the network is available and active
- Expected time to TRL-9.
  N/A
- Expected time to market.
  0 years

BOX 6 DESCRIPTION OF USE CASE(S)

Use cases can be found via the relative webpages

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

- Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
  The network can be used to stop the intimidation of journalists which forces them to spend an enormous amount of money and energy and prevents them from doing their service to democracy, which has a profound impact on media freedom.
- Resilience/**defensive**/offensive

BOX 8 ENABLING TECHNOLOGY	BOX 9 Implementation
- Which technologies are critical in fielding the idea? **No technologies needed other to safe access to the internet**	- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.? **No**
BOX 10 Implementation effort	**BOX 11 COUNTERMEASURES**
- Indication of costs: Describe the types of efforts and costs needed to implement the idea. **There are no costs , the solution is meant to support the journalists legally and financially**.	- 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 idea has a great potential to stay effective; in fact, the network is only expected to grow and become stronger**
BOX 12 Preconditions (optional)	**BOX 13 Life cycle maintenance (optional)**
- Have all preconditions been met for the idea to be ready for implementation? **No preconditions in this case**	- Describe who will operate, maintain, update, and upgrade the described idea. **The organisations listed above regulate their operation**
BOX 14 MISCELLANEOUS Any additional remarks/disclaimers/comments/information you might want to provide	

3.3 BOOSTING DEMAND AND SPREAD OF CONSPIRACY THEORIES, EXPLOITING EMOTIONS & PROMOTING VICTIMHOOD IN SOCIAL RELATIONS

EU-HYBNET responsible partner for this section: L3CE

In all 3 full scope cycles of project implementation attention been given for phenomena of disinformation, misinformation, propaganda, and other information manipulative activities. At least 7-8 innovative solutions, related to the subject, in each cycle were identified and described in respective deliverables. The final document on Gaps and needs highlights the need to understand the systemic effects of information manipulation and particular attention is given for conspiracy theories.

While looking at the innovative solutions proposed in three previous cycles, they can be considered still relevant. All cycles suggested solutions related to debunking, fact checking or identification of fakes. Looking from todays perspective, those not proved to be most effective, but in certain circumstances they still remain relevant. Another area, especially in the early stages of project implementation, was different education, critical thinking or similar solutions for making society more resilient. Other, usually more specific solutions, were related to wider involvement of society, information sharing, verification systems, vulnerable individuals and soft solutions (e.g.: Code of practice). Throughout the project implementation proposed solutions were getting more focused and targeted to a certain aspect of the phenomenon. As an example, is STARLIGHT project Disinformation-Misinformation toolset, providing very specific tools for LEA's.

Needs and gaps identified and solutions proposed were mainly focused on fighting different components of information manipulation. The final cycle shifts focus on understanding the systemic effects, including conspiracy theories, to counter them in a comprehensive way. Such shift also propose that countering hybrid threats also needs more complex process, methodologies and tooling, extending focus from stand alone events to complex actions from identification to effects mitigation.

Different solutions proposed during the project remain relevant to a different degree. The gap on understanding and comprehensive handling of hybrid threats is more important. Automation, attribution, integration of different functionalities and other changes are making different tools more precise and support faster reactions. Thus, in this section we describe one of solutions as an example in a complex journey of information components of hybrid warfare.

3.3.1 HIPSTER INITIATIVE (AS ILLUSTRATION)

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
Tension with different countries outside (and inside to some extend) EU are growing. This is not only about the traditional adversary countries, but also close allays. At the same time distinction between facts, interpretation, contextualization becomes very blur. Political leaders and other authorities do not avoid own interpretations more and more. Understanding of information manipulation effects, fragmentation of society by attitudes towards different phenomena becomes more and more essential. This understanding is not aiming at construction of ultimate truth, but on building resilience and integrity of societies. Following the evolution of suggested solutions, they tend to be more complex and tailored specifically to a certain aspect (conspiracy theories, fifth column, migration, etc.)	Deliberately constructed manipulative information results in two main outcomes: - Fragmentation of society followed by different tensions and isolation; - Distrust in democratic institutions and values. Thus, this directly impacts different common European structures, staring from value system, believe in democracy and institution, up to readiness to defend them, or event to activities to disturb common systems.	Mainly comprehensive understanding of how information manipulation works in short and long term would help to master counter measures. The current approach, mainly focused on identification and short term measures is not enough. Such understanding is relevant for variety of stakeholders working in hybrid threats area.	There is no single solution available. The approach proposed is more an example of how narrowed issues, related to the information weaponisation can be tackled. Comprehensive solution should not be limited to technical deployments, it requires significant organisational, process, involvement and other soft components.	There is variety of potential users of the approach. Decision makers – understanding the effects and considering mitigation actions. Academia – researching effects and understanding construction and impacts. LEA's – monitoring and safeguarding the information environment. Hybrid treat specialists – comprehensive understanding, monitoring and supporting decision making.
IV) ministry level (administration): decision makers strategic communication units				

V) VI)	local level (cities and regions): decision makers strategic communication units support functions to ministry and local levels (incl. Europe's third sector) influencing authorities				

Further the example of HYPSTER initiative is described to illustrate the optional patrial implementation of the approach and to demonstrate how similar solutions evolve. There might be different vectors for other solutions, while the presented one goes for a deeper specialisation on certain threats.

BOX 1 NAME OF THE IDEA

HIPSTer initiative (as illustration)

The HIPSTer project aims to develop a Hybrid Information Psychological Societal Threats Handling System that applying recent developments in OSINT, SocMINT, NLP, and AI to automatically detect, attribute, and counter or prevent prioritized threats. Currently, there is no widely accepted framework for identifying and attributing hybrid threats. The HIPSTer project aims to advance the SOTA in this area by developing new models for threat detection and attribution that can handle the complex nature of hybrid threats. Advancements are expected in different areas, e.g.: replace rule-based OSINT data processing with real-time automated and/or semi-automated modules, NLP in threat detection and attribution, etc. The project's focus on 24x7 operations and the ability to deploy new technologically-based TTPs for emerging and changing phenomena processing represents a significant area of innovation.

By staying at the forefront of these developments, the HIPSTer project aims to provide a comprehensive solution for handling hybrid threats in the public security domain and minimize latency from early threatful activity detection till counter action.

One of differentiating aspects of the initiative is that it is pre-formulated to focus on some priorities. In case of Lithuania, it is shaped to monitor and attribute information manipulations in areas of:

- Conspiracy theories
- 5th colon
- Radicalization
- Ideology aspects

Based on predefined areas, the solution composes functionalities, that are needed for given tasks.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
- **Applicable hybrid threat domains as** stated by the gaps/need:
- Information domain, described as Understanding the systemic effects of disinformation, misinformation, propaganda, and other manipulative activities in the information domain and Boosting demand and spread of conspiracy theories.

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

- Solution can be relevant for two core themes: Information and strategic communication and resilient civilians, local level and national administration.

BOX 3 TYPE OF SOLUTION

- **Technical –** OSINT type solution
- **Social/Human**
- **Organizational/Process**

BOX 4 PRACTITIONERS

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

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 6
- **In which stage is the solution (research, technology, available innovation, proven innovation):** technology development
- **Expected time to TRL-9.** 2-3 years
  Expected time to market. 2028

BOX 6 DESCRIPTION OF USE CASE(S)

The solution can be used as any other OSINT solution, the difference is mainly in application of technologies that provide automation and pre-described functionalities that are relevant for end-users of that solution.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  As in it was described in all cycles, different aspects of information manipulation are important part of hybrid threats. So, OSINT type tools remain relevant for countering variety of components of hybrid threats.
- **Resilience/defensive/offensive –** can be both, defensive and supporting resilience.

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
- Detection of communication metadata
- Identification and analysis of language and phrasing, symbols and images, narratives and storytelling
- Detection of behaviour patterns etc.

There are different technologies that allow comprehensive detection, analysis, attribution of aforementioned aspects of information manipulations.

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
- Restrictions and limitations of application depends on the institution, national legislation and particular application case.

BOX 10 Implementation effort

- **Indication of costs**:
  Describe the types of efforts and costs needed to implement the idea.
  The is no estimation provided. Costs of such solutions might reach 1 – 2 mln eur.

BOX 11 COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
- Fast evolution of technology.
- Appearance of new manipulation techniques.
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
- Depending on evolution of threats and maintenance / update efforts it might remain relevant for 10+ years.

BOX 12 Preconditions (optional)	BOX 13 Life cycle maintenance (optional)
- Have all preconditions been met for the idea to be ready for implementation? - .	- Describe who will operate, maintain, update, and upgrade the described idea.
BOX 14 MISCELLANEOUS Any additional remarks/disclaimers/comments/information you might want to provide	

3.3.2Use of Common Frameworks and outcomes of FIMI related EU-Funded projects

Different aspects of information manipulations, spread of disinformation, fakes and trust were in scope of all cycles throughout the implementation od the project. Different innovative solutions or concepts were suggested by WP3 for further review. Thos included guides, debunking, fact checking, verifications and other innovative initiatives. 4 – 6 solutions were proposed in each cycle that can be related to FIMI. During the initial part of the project gaps and need, folllowed by respective propositions of solutions were not directly linked to the current FIMI concept. They ežwere more generic, even understanding that information manipulation can be originated from hostile countries.

Considering that FIMI phenomena is similar to other information manipulations to some extend, beeng better planned, organised, long term oriented and sometomes more subtile, all innovative solutions mentioned are still relevant. As some activities presented in the previous cycles were implemented or experimented inn different formats and extend they can be assessed. For example simple debunking appeared to be be less efectve than expected, different trust mechanisms seems not to be working ets. Despite that, understang FIMI, antisipating naratives and contradicting some long standing naratives remais very relevant. It might become even more important due to growing polarisation in European societies and increasing variety of actors interested to construct their ouwn interpretations.

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
Efforts to create different perception of environment are gaining speed. Countries like Russa, Chaina and others, including some of democratic countries, are putting significant efforts to reconstruct European understanding of democracy, shared value systems and interpretation of behavioral norms. From one side this is not a new phenomenon and there are	The FIMI impact or targets from adversary point of view on the high level are well known. This is analysed and described in many different projects deliverables, documents of different institutions and academia articles. Impacts include polarization of societies, growing violence, uncertainty, separation,	Few needs can be listed: - Complex ecosystem development as separate components are available; - More resolute response; - Understanding and response to FIMI as a war action. There are instruments getting available. The DISARM framework is among the significant steps. The six EU-funded projects ATHENA, SAUFEX, RESONANT, DE CONSPIRATOR, ADAC.IO and ARM projects	As no particular innovation is presented in this section, there are still some insights: - Use of common frameworks (DISARM at current stage); - Outcomes of FIMI related EU-funded projects.	There is a wide range of different end-users that are or should be involved in FIMI related countermeasures. Issue of FIMI and other hybrid attacks is a subject of national security and should be handled at respective level. Wile today

What is the problem and where does it originate from? What are the parameters contributing to its escalation? Who is the pan-European security practitioners whose Gap &Need /Threat we are referring to?	What are the problem's immediate outcomes? What is the particular manifestation that we want to address? How is it threatening European Security, Democracy/ Autonomy/ Values?	What is the need to focus on in order to solve security practitioners' and other stakeholders' Gap & Need/Threat?	What is the expected outcome from the use of a chosen innovation?	Who will be the end users of this innovation? (Optional question)
many initiatives to counter misinformation and manipulation activities, on the other side, this is heavily increasing, gaining wider coverage and better coordinated. Thus, securing current law based democracy systems, FIMI is one of the main challenge. More predictable, better prepared responses, resolute differentiation from free speach and other measures are essential.	protectionism and others. Adversary authoritarian regimes, especially Russia, is escalating different aspects in EU, making it very complex issue. On the other hand EU and MS have no capabilities for adequate response. It is difficult of evaluate all FIMI targets, but at the end point is national security and democracy. Direct target of FIMI is cognitive dissonance, leading to doubts about the current EU values and governance practice.	are under implementation. Development and outcomes of them might make a significant contribution to countering FIMI efforts.		countering hybrid threats, FIMI including is still left fragmented (e.g.: disinformation is left for journalists, spread of fakes for media platforms, etc.)

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

4.1 Reversing priorities from what needs to be broadcasted to what people want to be broadcasted

EU-HYBNET responsible partner for this section: SATWAYS

Although the Media Pluralism Monitor that has already been mentioned can be utilised in this section as well, it is important to also highlight the Jounralism Trust Initiative that has been presented in a previous deliverable.

4.1.1 JOUNRALISM TRUST INITIATIVE

<table>
<tr><td colspan="2">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.</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
- 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:
- 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>
<tr><td colspan="2">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.</td></tr>
</table>

<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.
Increases societal resilience to fake news

- Resilience/defensive/offensive</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Machine learning and AI</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
No, it is free of charge and available to the public</td></tr>
<tr><td>COSTS
- Indication of costs:
Free of Charge
- Differentiate if possible, in development, procurement and exploitation</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Not possible as the stakeholders are involved
- How durable is the idea (how long is the idea expected to be effective/useful?)</td></tr>
<tr><td colspan="2">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.</td></tr>
</table>

4.2 ADVANCED FORMS OF AI-ENHANCED DISINFORMATION

EU-HYBNET responsible partner for this section:

4.2.1 BLOCKCHAIN BASED VERIFICATION

The increased use of visual illusions can have a number of negative consequences. Fake videos, deep fakes, and manipulative images that are quick to spread false information can mislead the public and skew their opinions. People's trust in the media, institutions and even each other is decreasing because they are constantly exposed to visual misinformation. Because of this loss of trust, people find it difficult to differentiate between authentic and manipulated media, contributing to an overall loss of trust.

Visual misinformation can be used as a tool to polarize society, exacerbate existing divisions, and manipulate public opinion. It is easier to manipulate people's beliefs and influence their perceptions by deliberately disseminating misleading images that support certain narratives or ideologies. Using visual misinformation can also seriously damage the reputations of people, businesses, and even entire communities. Altered images and videos can be used to falsely accuse people of damaging a company's reputation or creating public scandals. Even if the misinformation is later debunked, the damage to reputation can be lasting.

The impact of increasing levels of visual misinformation not only affects a person's reputation, but also changes the social and political climate. It undermines democratic processes, distorts elections and fuels social unrest. False or manipulated images can incite violence, trigger outrage and provoke conflict by exploiting people's emotions.

The spread of visual misinformation also poses challenges for media companies and technology platforms responsible for moderating content. In order to detect and combat the proliferation of misleading images, efficient mechanisms and algorithms must be created, which can be difficult and time-consuming.

Prioritizing media literacy, critical thinking, fact checking, and responsible use of visual content is critical to preventing these potential consequences. By developing these skills, people can navigate the world of visual information more successfully. Fully addressing the challenges associated with visual misinformation will also require collaboration between technology companies, policymakers and society at large.

BOX 1 BLOCKCHAIN-BASED VERIFICATION

Blockchain technology can play a crucial role in the fight against the increasing use of visual misinformation. By leveraging the inherent security and transparency of blockchain, a robust system can be established to verify the authenticity of images and videos. Blockchain allows us to timestamp visual content at the time of creation. Each medium is linked to a unique cryptographic hash and recorded on the blockchain, creating an immutable record of its provenance. This timestamp ensures that the authenticity of the content can be easily verified, thus helping to identify real footage and distinguish it from manipulated images.
In addition, the blockchain can store tamper-proof metadata about the content, such as information about the author, location and any editing history, further strengthening the credibility of the information from the visual media.
Decentralized content sharing platforms are built on blockchain technology, which ensures that content is verified before being widely distributed. Mobile apps and browser plug-ins to be developed, will enable users to use blockchain-based verification. Such tools allow people to easily examine the blockchain records of visual content they reach online.
Fact-checking organizations are integrating this blockchain technology into their processes by recording their findings and conclusions on the blockchain. This creates an immutable record of verified information, increasing confidence in their reviews. Collaborating with content creators is essential. Encouraging professionals and journalists represents a sign of trustworthiness to certify the authenticity of their work on the blockchain. This also increases trustworthiness in a time plagued by misinformation. Public blockchain visual content verification databases managed by a consortium of organizations can further improve transparency and accountability. Furthermore recognizing blockchain as evidence in court cases related to misinformation is an incentive to use this technology to verify content.

It is important to note that while blockchain can improve the trustworthiness of visual content, it is not a panacea. It has its limitations and its effectiveness depends on widespread acceptance and proper implementation. Additionally, blockchain should be used in conjunction with other strategies such as media literacy and fact-checking to create a comprehensive approach to combating visual misinformation.

BOX 2 REFERENCE TO CAPABILITY GAPs/NEED

- **Describe the use of the solution in reference to the gaps/need**
  The solution can be used to improve the trust in correctness of news and helps against spreading of fake news.
- **Applicable hybrid threat domains as stated by the gaps/need:**
  Civic space, governance space, services space could benefit from such solutions.

Applicable core theme(s) as stated by the gap/need:
Information and strategic communications

BOX 3 TYPE OF SOLUTION

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

The innovation is of technical nature combined with Social/Human theme. A legal framework would also be necessary in countering the problem and its routes as well as the civilians needs to be anxious to use these methods

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  Civic space, governance space, services space could benefit from such solutions.

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

Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):
Private citizens and governance space are the main beneficiaries of these kinds of technologies.

BOX 5 STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index):**
  6
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  The most important tasks have to be done in the parts research ,technology and bring to market.
- **Expected time to TRL-9.**
  2-4 years, an end of improvements will never be reached
- **Expected time to market.**
  2-4 years with an important work for advertising for using the functionality

BOX 6 DESCRIPTION OF USE CASE(S)

This technology and tools can be used in every situation of the whole everyday life in every situations of all men who consuming information and news in all formats, e.g. Text, audio or video.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
As mentioned above, these technologies can help all individuals and it can help societal resilience.

- **Resilience/defensive/offensive**
  The idea can be used in a defensive and offensive way to counter hybrid threats.

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  The databases which are used for the proven facts needs to be verified all the time and needs to be certified.
  Faked browser plugins could be produced and offered which doing false verification checks.

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No

<table>
<tr>
<td>

BOX 10 Implementation effort

- **Indication of costs:**
  Describe the types of efforts and costs needed to implement the idea.
  1-2 Mio €/a until the base system is ready after some regular costs for maintenance and improvement

</td>
<td>

BOX 11 COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution?**
  Wrong verified information stored in the database lead to false positive checked news.

- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  The solution is expected to be useful for a very long time, with a steady maintenance and efforts for monitoring the

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

BOX 12 Preconditions (optional)

- **Have all preconditions been met for the idea to be ready for implementation?**
  No preconditions are needed.
  Current browsers are supporting all necessary techniques for this.

</td>
<td>

BOX 13 Life cycle maintenance (optional)

- **Describe who will operate, maintain, update, and upgrade the described idea.**
  The services shall be offered by more than one operator. Maybe founded installations and/or commercial instances from e.g. news agencies who are interested in the correctness of their reports, pictures/videos or audio streams.

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

BOX 14 MISCELLANEOUS

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

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

4.3 UNDERSTANDING THE SYSTEMIC IMPACTS OF DISINFORMATION, MISINFORMATION, PROPAGANDA, AND OTHER MANIPULATIVE ACTIVITIES IN THE INFORMATION DOMAIN

EU-HYBNET responsible partner for this section:

4.3.1 BAD NEWS Prebunking Game platform

BOX 1 "BAD NEWS" Prebunking Game platform **Active prebunking interventions require the individual to take action, making choices that help them retain information and engage more deeply with the content they see. The primary active approach researched to date is games[24]. While games are more immersive and allow individuals to be inoculated against multiple manipulation techniques commonly used in misinformation, they require a larger investment from the viewer in terms of time and focus, which may reduce the number of people engaging with it. They are also a larger investment to produce, though some high-impact games have been implemented on a large-scale. The inoculation metaphor relies on a medical analogy: by pre-emptively exposing people to weakened doses of misinformation cognitive immunity can be conferred. An example is the Bad News game, an online fake news game in which players learn about six common misinformation techniques. (https://www.getbadnews.com/books/english/ offered in 23 languages)**	
BOX 2 REFERENCE TO CAPABILITY GAPs/NEED - **Describe the use of the solution in reference to the gaps/need** - **This was the first-ever prebunking game. It is a choice-based browser game created by DROG and the University of Cambridge in which players take on the role of a fake news producer and learn to identify and mimic six misinformation techniques (e.g. trolling, conspiratorial reasoning, impersonation) over six levels. Since then, several other games with similar premises have been designed.** - **Applicable hybrid threat domains as stated by the gaps/need:** **Cyber, Information and Military /Defense domains could benefit from such solutions.** - **Applicable core theme(s) as stated by the gap/need:** **Cyber and Future Technologies**	**BOX 3 TYPE OF SOLUTION** - **Technical** **The innovation proposed is a technical one.** - **Social/Human** **Broadly speaking, the longer and more engaged the person is with the prebunk, the greater the size and duration of the prebunking effect.** - **Organizational/Process**

[24] Melisa Basol, Jon Roozenbeek, and Sander Van der Linden, "Good News About Bad News: Gamified Inoculation Boosts Confidence and Cognitive Immunity Against Fake News," Journal of Cognition 3, no. 1 (January 10, 2020): 2

BOX 4 PRACTITIONERS

- **Provide the applicable hybrid threat domains for which the idea is valuable:**
  Cyber, Information and Military /Defense domains could benefit from such solutions.

- **Provide the level of practitioners in the same discipline:**
  The threat was listed under *Services Space* in Deliverable D2.7 (Long List of Gaps and Needs)
  - I) ***ministry level*** **(administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**

- **Provide the end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments):**
  Citizens, users, news consumers, audiences in general

BOX 5 STATE OF THE ART

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

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

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

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

BOX 6 DESCRIPTION OF USE CASE(S)

It can fragment videos, to enhance and explore key frames and images through a magnifying lens, to read video and image metadata, to check media copyright licenses, and to apply forensic filters on still images, all of which are vital tools for anyone trying to check the authenticity and source of the material.

BOX 7 IMPACT ON COUNTERING HYBRID THREATS

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

- **Playing Bad News significantly improves people's ability to spot misinformation techniques compared to a gamified control group, and crucially, also increases people's level of confidence in their own judgments. Importantly, this confidence boost only occurred for those who updated their reliability assessments in the correct direction. This offers further evidence for the effectiveness of psychological inoculation against not only specific instances of fake news, but the very strategies used in its production. Implications are supported for inoculation theory and cognitive science research on fake news.**
- **Resilience/defensive/offensive**
  The solution can be used in countering hybrid threats in all three manners: to promote resilience, to defend against a threat and also to provide offense against a threat.

BOX 8 ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  The purpose of the game is to produce and disseminate disinformation in a controlled environment whilst gaining an online following and maintaining credibility. Players

BOX 9 Implementation

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No

start out as an anonymous netizen and eventually rise to manage their own fake news empire. The theoretical motivation for the inclusion of these six strategies are explained in detail in Roozenbeek and van der Linden (2019)[25] and cover many common disinformation scenarios including false amplification and echo chambers. Moreover, although the game scenarios themselves are fictional they are modelled after real-world events. In short, the gamified inoculation treatment incorporates an active and experiential component to resistance-building.	
BOX 10 Implementation effort - **Indication of costs:** **Describe the types of efforts and costs needed to implement the idea.** **The solution is free of charge**	**BOX 11 COUNTERMEASURES** - **Are there any potential countermeasures that could degrade the effectiveness of the solution?** **Progress in disinformation methodologies** - **How durable is the idea (how long is the idea expected to be effective/useful?)** **The solution is expected to be useful for a very long time.** -
BOX 12 Preconditions (optional) - **Have all preconditions been met for the idea to be ready for implementation?** **No preconditions exist.**	**BOX 13 Life cycle maintenance (optional)** - **Describe who will operate, maintain, update, and upgrade the described idea.** **Exclusive licensing of this game for purposes of scientific research has been granted to researchers at the Cambridge Social Decision-Making Lab at Cambridge University. This website and its contents may only be used with the permission of TILT and the Cambridge Social Decision-Making Lab. Tilt is a company that aims at increasing people's information resilience and arming them against the harmful influences of disinformation and online manipulation. This game was designed and developed by GUSMANSON, a design studio creating serious games.**
BOX 14 MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** **It will be important for future research to evaluate to what extent "active" gamified inoculation is superior to "passive" approaches—including traditional fact-checking and other critical thinking interventions—especially in terms of eliciting a) motivation, b) the ability to help people discern reliable from fake news, and c) the rate at which the inoculation effect decays over time.**	

[25] Roozenbeek, J., & van der Linden, S., Fake News Game confers Psychological Resistance against online Misinformation, Nature Palgrave Communications, 5(65), 2019

5. CONCLUSIONS

5.1 SUMMARY

This Deliverable presents the main outcomes of the work completed during the 4th cycle of the EU-Hybnet H2020 project, and more specifically under Task 3.2 titled 'Technology and Innovations Watch'. This Deliverable has served to provide ideas and innovations for countering different dimensions of Hybrid Threats.

For the **first Core Theme, Future Trends of Hybrid Threats**, and more specifically the *primary context relevant to destabilization due to the instrumentalization of migration*, the idea presented is a video plugin to debunk fake videos on social media that spread conspiracy theories, aiming to help respond quickly and effectively to the spread of misinformation. Additionally, the Media Pluralism Monitor developed by EUI is proposed, to assess the potential weaknesses in national media systems that may hinder media pluralism.

For the primary context of *Foreign Interference into domestic politics including elections processes*, the new idea presented is the Establishment of a fully functional intelligence cooperation service at EU level, complemented by an online collaboration platform for Foreign Interference. The Information network that will be created will ensure the information flow for all EU member states' administration enhancing their ability for policy planning and programming future strategic actions also on a political level.

For the primary context of *Leveraging Lags in Foresight and anticipation,* the Smart message routing and notification service is proposed for sharing the operational picture to every agency involved in the response at every level of coordination. This tool can be utilised for cross border and cross organizational operations and has have been tested in various cases to enable the sharing of information among involved actors at every level of coordination, thus enabling collaborative response and the proper alerting of personnel/practitioners/stakeholders. Additionally, in light of the European Integrated Border Management concept and the EU Customs Action Plan, the tools developed in EU-funded projects like CONNECTOR can be considered. The proposed CE-CISE is a fully interoperable technical framework, which expands the scope and capabilities of CISE to Customs domain, ensuring effective management of EU external borders at operational, tactical & strategic level, facilitating the information exchange at interagency and transnational level. This can help improve the common operational picture and enhance situational awareness, enable the EU cross border joint operations and support and complement the different agencies work.

With respect to the **second Core Theme, Cyber and Future Technologies,** for the primary context of *Targeting European critical infrastructure and the psychological reliability of digital infrastructures*, *Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience are* proposed. Thus, stress testing a supply chain with 'what if' scenarios can reinforce any mitigation strategy and strengthen the resiliency of a critical entity.

For the primary context of *Weaponization of Mass Data - massive availability of societal data aggregates & algorithmic computation,* the Nordlayer (only named for exemplary purposes) or other similar solutions are proposed that can be used to prevent the leak of hospital patient data.

Regarding the primary context of *Leveraging the autonomy and power of digital actors*, tools for the protection of personal data are proposed to be used. Additionally, a legislation initiative is proposed on a EU level for the selling of mass data, which has been a crucial question since the appearance of social media. Such legislation can help reduce the growth of power of companies owning social platforms.

It is also important to recall an innovation presented in a previous deliverable, named 'Fair Trade Data Program', as 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

With respect to the **third Core Theme, Resilient Civilians, Local level and administration**, and the first primary context *Mainstreaming violence -The growing broadcasting and becoming accustomed to violence weaken democratic politics,* it is proposed that existing directives are expanded and new legislation initiatives are put forward, for the protection of the phycological health of the citizens, both minors and seniors, as well as the minimisation of violence spread

Regarding the second primary context *Intimidation of civil society and political engagement,* the BREACH GUARD or any other similar available solution is proposed against doxxing , which involves publicly exposing someone's real name, address, job, or other identifying info without a victim's consent, aiming to humiliate, bully, harass, or otherwise harm a victim. Commercially available software can help protect personal information against data loss, leaks, breaches and collection by third parties. Furthermore, the software automatically scans the dark web for personal information that may have been part of a data leak or data breach and helps protect the user's personal information and avoid identity theft. Besides individuals, these solutions can help fact checkers and activists of Civil Society Organisations that are often victims of such attacks.

For online political harassment and SLAPP, a network of financial and legal support is proposed, as in the case of the Foreign Policy Centre, the Justice for Journalists Foundation and the International Bar Association's Human Rights Institute, that jointly organized the European Anti-SLAPP conference. Such a network can be used to stop the intimidation of journalists which forces them to spend an enormous amount of resources and energy and prevents them from offering their service to democracy, which has a profound impact on media freedom.

For the third primary context of *Boosting Demand and Spread of Conspiracy Theories, Exploiting Emotions & Promoting Victimhood In Social Relations*, the Hypster project initiative is proposed, that aims to develop a Hybrid Information Psychological Societal Threats Handling System that applies recent developments in OSINT, SocMINT, NLP, and AI to automatically detect, attribute, and counter or prevent prioritized threats. Additionally, the use of common frameworks and outcomes of FIMI related EU Funded projects is proposed to be studied, to fight the continuous effort to create different perception of environment, and to ultimately help maintain our European Values.

The first primary context of the **forth core theme, Information and Strategic Communications**, named *Reversing priorities from what needs to be broadcasted to what people want to be broadcasted*, is also relevant to creating a different perception of reality.

The Media Pluralism Monitor (MPM) developed by the European University Institute can also be utilized in this case, but it is also important to recall the Journalism Trust Initiative (JTI) that was presented in the 1st cycle. 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 process focused tool that evaluates how information is produced and disseminated.

For the second *primary context, Advanced Forms of AI enhanced Disinformation,* blockchain based verification is proposed, to help establish a robust system to verify the authenticity of images and videos. It should be noted that blockchain should be used in conjunction with other strategies such as media literacy and fact-checking to create a comprehensive approach to combating visual misinformation.

Finally, for the third primary context *Understanding the Systemic Impacts of Disinformation, Misinformation, Propaganda, And Other Manipulative Activities in the Information Domain*, the bad news Prebunking Game platform is proposed, that was created by DROG and the University of Cambridge. This game can help users learn about six common misinformation techniques. This gamified inoculation treatment incorporates an active and experiential component to resistance-building.

5.2 FUTURE WORK

This deliverable has summarised the results of Task 3.2 “Technology and Innovations Watch” of the H2020 funded EU-HYBNET project for the project’s fourth cycle.

As detailed in the previous cycles’ work, a hybrid threat is considered to be multidimensional and time-dependent (dynamic). Therefore, in order to produce one holistic solution, specific patterns would be needed, to timely attribute hybrid threats across all domains.

Teaching computers how to respond to a multidimensional and time dependent situation is not yet easy to implement, as hybrid threat patterns are not ready to be described. In the future, Artificial Intelligence tools and quantum technology could be used to help identify and respond to such threats in a timely manner. Additionally, besides advanced technologies, interdepartmental and international cooperation and alignment would be required.

5.3 ACKNOWLEDGEMENTS

This Deliverable has presented, besides new innovations, solutions that were discussed and presented in previous cycles of the EU Hybnet project. It includes a summary of work conducted during the five years of the project that remains relevant to current gaps and needs of hybrid threats. We are grateful to all authors of previous Deliverables of Task 3.2 for their work and our interesting discussions. The complete list of authors for (D3.3, D3.4, D3.5, D3.6) is as follows:

S. Sofou (SATWAYS) Julien Theron, (JRC, EC), Michelle Stebner (ZITiS) Maria Kampa, Mirela Rosgova, Panagiota Benekou, Alex Koniaris, Athanasios Kosmopoulos, Athanasios Grigoriadis, Vanessa Papakosta, Aphrodite Gagara (KEMEA) Ramon Loik, Ivo Juurvee (ICDS), Evaldas Bruze, Edmundas Piesarskas, Rimantas Zylius (L3CE), Pham Son (COMTESSA) Rick Meessen, Okke Lucassen (TNO) Päivi Mattila, Isto Mattila, Petteri Partanen (Laurea) and Daniel Fritz (EEAS).

.

ANNEX I. GLOSSARY AND ACRONYMS

Table 2 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats
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. [26]
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.[27]
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
DDS-Alpha	DDS-alpha is the Disinformation Data Space, a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan
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

[26] De Mauro, A., Greco, M., and Grimaldi, M., "A formal definition of Big Data based on its essential features" *Library Review* 65(3), 2016.

[27] Kok, J. N., Boers, E. J. W., Kosters, W.A, van der Putten, P., and Poel, M., "Artificial Intelligence: Definition, Trends, Techniques, and Cases." *Artificial intelligence* Volume 1, 1-20, 2009.

Satways	Satways Ltd
ZITiS	Central Office for Information Technology in the Security Sector
KEMEA	Center for Security Studies
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 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] European Commission, Joint Research Centre, The landscape of hybrid threats : a conceptual model : public version, Giannopoulos, G.(editor), Smith, H.(editor), Theocharidou, M.(editor), Publications Office, 2021.

[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] CustOms exteNded iNteroperablE Common informaTiOn shaRing environment , CONNECTOR, (EU-Funded project , Grant Agreement No 101121271)

[6] Chen, J., Wang, H. & Fu, Y. A multi-stage supply chain disruption mitigation strategy considering product life cycle during COVID-19. Environ Sci Pollut Res (2022) Feb 5;1-15.

[7] Wilkinson, G., How To Avoid Supply Chain Disruptions, anyLogistix supply chain management

[8] Ivanov, D., Managing Risks in Supply Chains with Digital Twins and Simulation, White Paper, Hochschule fuer Wirtschaft und Recht Berlin.

[9] Resilink, company webpage

[10] 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.

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

[12] Shivananghan, M., Modern Engineering Explained -10 Types of Social Engineering Cyberattacks, FreeCodeCamp, March 21st, 2023.

[13] Tanant, F., Fraud Detection with Machine Learning & AI, Seon company online article, accessed September 2023.

[14] The Rise of AI-powered Fraud Detection in Payments: Securing your transactions, Sweep, May 24th, 2023.

[15] AI improves fraud detection, prediction and prevention, IBM Watson Studio, online article assessed July 2023.

[16] Invalid Traffic – What Is It and How to Prevent It?, SETTUPAD blog, June 2022.

[17] Alter, S., Violence on television, Law and Government Division, publications of the Government of Canada, October 1997.

[18] Canadian Radio-Television and Telecommunications Commission, Government of Canada, assessed July 2023.

[19] CRTC Policy on Violence in Television Programming, 1996-36, Canadian Radio-Television and Telecommunications Commission webpage, assessed July 2023.

[20] Blechschmidt, B., Guide to doxing: Tracking identities across the web, Blog Article, November 2014.

[21] What Is Doxxing, Is Doxxing Illegal, and How Do You Prevent or Report It?', Avast, Academy, online article, accessed June 2023.

[22] European Commission, The 2023 CHAR-LITI Call for proposals under the CERV, January 26th 2023.

[23] European Commission Expert Group against SLAPP, Minutes of Meeting, 21 November 2022.

[24] Basol, M., Roozenbeek, J., and Van der Linden, S., "Good News About Bad News: Gamified Inoculation Boosts Confidence and Cognitive Immunity Against Fake News," Journal of Cognition 3, no. 1, 2020.

[25] Roozenbeek, J., & van der Linden, S., Fake News Game confers Psychological Resistance against online Misinformation, Nature Palgrave Communications, 5(65), 2019.

[26] De Mauro, A., Greco, M., and Grimaldi, M., "A formal definition of Big Data based on its essential features" *Library Review* 65(3), 2016.

[27] Kok, J. N., Boers, E. J. W., Kosters, W.A, van der Putten, P., and Poel, M., "Artificial Intelligence: Definition, Trends, Techniques, and Cases." *Artificial intelligence* Volume 1, 1-20, 2009.