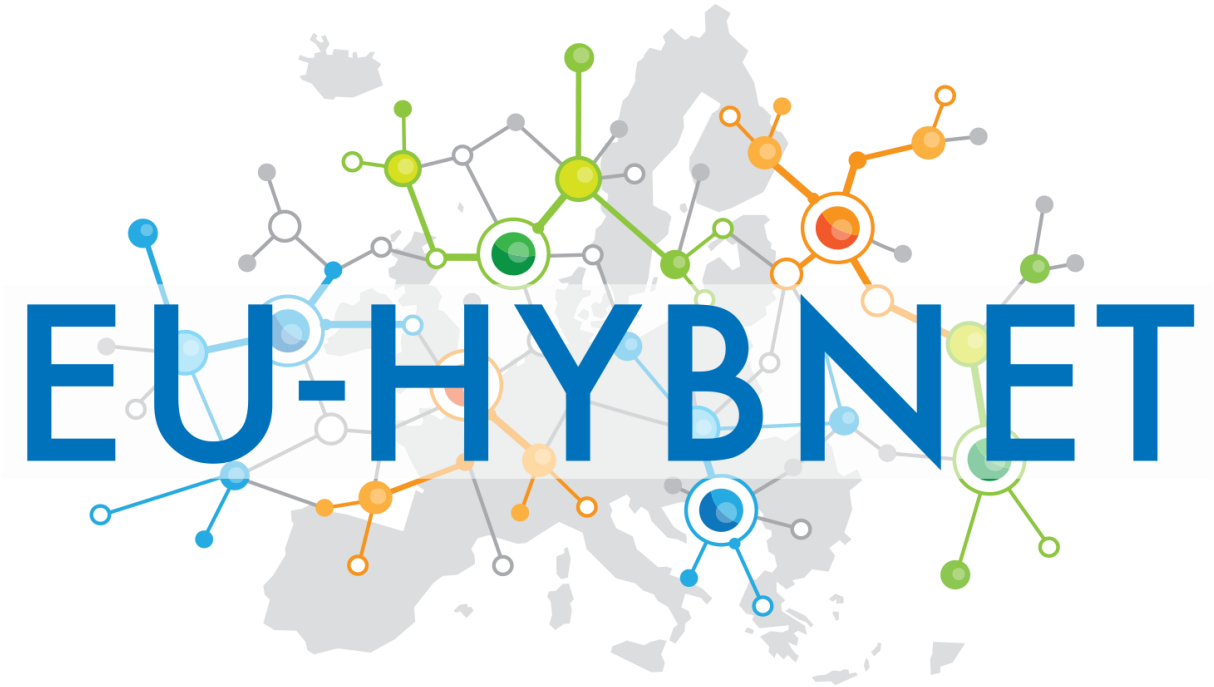

FIRST MID-TERM REPORT ON IMPROVEMENT AND INNOVATIONS

DELIVERABLE 3.4

Lead Author: SATWAYS Ltd

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

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

D3.4 FIRST MID TERM REPORT ON IMPROVEMENT AND INNOVATIONS

Deliverable number	**D3.4**	
Version:	**1.6**	
Delivery date:	**09/06/2022**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Final Version after Internal Review**	
Nature:	**Report**	
Main author:	**Dr. Souzanna Sofou**	**Satways Ltd**
Contributors:	Michael Meisinger	ZITiS
	Panagiota Benekou, Alex Koniaris, Athanasios Kosmopoulos, Athanasios Grigoriadis	KEMEA
	Ramon Loik, Ivo Juurvee	ICDS
	Evaldas Bruze	L3CE
	Pham Son	COMTESSA
	Daniel Fritz	EEAS
	Päivi Mattila	Laurea

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	10/03/2022	Souzanna Sofou (STWS)	Table of Contents
0.2	11/03/2022	>>	Added context description in §1.1 and context description and Innovation in §3.2
0.3	14/03/2022	Panagiota Benekou, Alex Koniaris, Athanasios Grigoriadis (KEMEA)	Added context description and innovations for context §2.2
0.4	18/03/2022	Panagiota Benekou, Alex Koniaris, Athanasios Grigoriadis (KEMEA)	Improvements in § 2.2
		Souzanna Sofou (STWS)	Additions in §1.1, §2.1, §3.2
		Michael Meisinger (ZITiS)	Added Innovation for §1.2
0.5	21/03/22	Souzanna Sofou (STWS)	Added second innovation in §2.1
	22/03/22	Souzanna Sofou (STWS)	Added innovation in §4.1
0.6	24/03/22	Athanasios Kosmopoulos (KEMEA)	Added innovations in §2.3
0.7	31/03/2022 07/04/2022	Michael Meisinger (ZITiS) Edmundas Piesarskas (L3CE)	Added innovations in §1.3 Added innovations in §4.1, §4.3
0.8	13/04/2022	Michael Meisinger (ZITiS)	Added innovations in §1.3, §1.2
0.9	14/04/2022	Edmundas Piesarskas (L3CE)	Added and Updated innovations in §4.1, §4.3
	18/04/2022		ToC Update
0.9b	20/04/2022	Ramon Loik (ICDS)	Added innovations in §3.1, §4.2
0.9c	27/04/2022	Souzanna Sofou (STWS)	Added innovation in §3.2
0.9d	04/05/2022	Souzanna Sofou (STWS)	Added context description and innovation in §3.3
0.9e	10/05/2022	Souzanna Sofou (STWS) Daniel FRITZ (EEAS)	Additions in §4.1.3
0.9f	11/05/2022	Souzanna Sofou (STWS)	Addition in §1.1

0.9g	16/05/2022	Ramon Loik (ICDS) Souzanna Sofou (STWS)	Additions in §3.1.1., §3.1.2., §4.2.1. §4.2.2. Added comments from Comptessa (of v0.9e)
0.9k	16/5/2022	Souzanna Sofou	changes and additions in §3.2.1, §1.1
0.9l	18/05/2022	Michael Meisinger (ZITiS)	Additions in §1.2.1.
0.9m	18/05/2022	Souzanna Sofou (STWS)	Additions in §1.1, §3.2.1,
0.9n	19/05/2022	Souzanna Sofou (STWS)	Conclusions, Final changes in the text Additions in §2.1.2. provided by Risk Technologies
1.0	19/05/2022	Souzanna Sofou (STWS)	Final changes in the text, introduction to §1.2, Introduction, methodology, references
1.0b	30/05/2022	Päivi Mattila (Laurea)	Initial review comments
1.1	01/06/2022	Souzanna Sofou (STWS)	Respond to Laurea comments- short additions to methodology, added use case in §1.1.2., relevancy for European Security Practitioners in §1.1.1 Added response to comment by Ath. Grigoriadis
1.2	05/06/2022	Päivi Mattila (Laurea)	Comments for editing
1.3	03/06/2022	Souzanna Sofou (STWS)	Respond to comments and editing
1.4	03/06/2022	Päivi Mattila (Laurea)	Review and comments for editing
1.5	05/06/2022	Souzanna Sofou (STWS)	Editing
1.6	09/06/2022	Päivi Mattila (Laurea)	Final review and submission of the document to the EC

DISCLAIMER

TABLE OF CONTENTS

TABLES

INTRODUCTION

I. OVERVIEW

The Deliverable D3.4 First Mid-Term Report On Improvement And Innovations presents the work completed in the frame of the H2020 Project 'Empowering a Pan-European Network to counter Hybrid Threats (EU-HYBNET)'. In more detail, this work is part of Work Package 3 (WP3) titled 'Surveys to Technology, Research and Innovations' and specifically Task 3.2 'Technology and Innovations Watch'.

The present Deliverable provides a list of Innovations and Ideas proposed to counter specific dimensions of Hybrid Threats. The focus areas, defined as 'Core Themes' and 'Primary Contexts' are defined by the Description of Action (DoA) and the WP2 of EU-Hybnet, respectivelly.

In more detail, the Long list of defined gaps and needs has been presented in D2.6 by the European Centre of Excellence for Countering Hybrid Threats, while in D2.10, JRC presented a Deeper Analysis, the short list of gaps and needs.

Based on D2.10, this Delivearble presentes ideas and innovations for each of the three primary contexts of each of the four Core themes. The latter are mentioned in the Description of Action (DoA) and they 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.

It should be noted, that as the relevant Deliverable D2.10 is confidential (CO), the present deliverable doesn't directly refer to the identified gaps and needs, but rather to the primary contexts these are more relevant to.

The outcomes of the present work is then provided to 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 will proceed 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
D3.4 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.

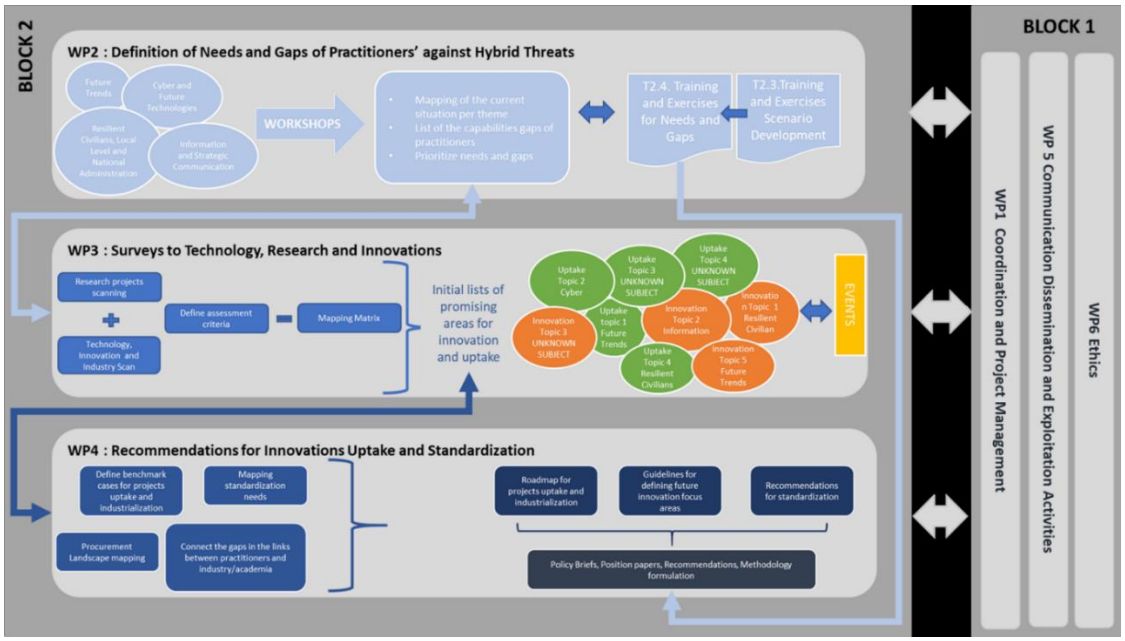

Figure 1 : EU-HYBNET structure of Work Packages and Main Activities

Additionally, D3.4 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 D3.3 delivers results are the following:

OB3: To monitor developments in research and innovation activities as applied to hybrid threats			
Goal		**KPI description**	**KPI target value**
3.2	To monitor significant developments in technology that will lead to recommending solutions for European actors' gaps and needs	Monitor existing innovations addressing gaps and needs, 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.

Gaps and Needs

[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

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 of the analysis aimed to identify, record, and understand the nature of practitioners and other relevant European actors' gaps and needs and vulnerabilities in countering hybrid threats. These gaps and needs include the identification of the obstacles to developing, maintaining and improving societal resilience in countering hybrid threats. The D3.4 is in line with the second cycle gaps and needs analysis and focus areas.

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 D3.4 is the second deliverable of WP3 Task 3.2 of the EU-Hybnet project. The main actions identified at the beginning of the EU-HYBNET's 2nd project working cycle (M18 – M34/ October 2021 – February 2023), included:

- careful consideration of the results of the 1st cycle, including the assessment of the innovations by T3.1
- study of D.6, the long list of defined gaps and needs prepared by the European Centre of Excellence for Countering Hybrid Threats,
- thorough analysis of the D2.10, where JRC presented a deeper analysis, the short list of gaps and needs.
- Continuous monitoring of technologies and innovations, and assessment of their suitability to counter the specific dimensions of Hybrid threats

As in the first project working cycle (M1 – M17/ May 2020 – September 2021), a special template for presenting innovations and ideas is being used, that has been designed by TNO, T3.1 leader. The main idea behind this template is to characterise the innovations in a coherent and systematic manner. This 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. The Innovation Arena platform, developed by Laurea for the project consortium and EU-HYBNET network members, is being used throughout the entire project for this purpose.

This document suggests potential innovations and solutions to improve pan-European practitioners and other relevant actors' measures to counter hybrid threats through the analytical lens of the EU-HYBNET project four core themes.

The main innovations and ideas presented in this work are presented in the following Table per core theme and primary context. An introduction to the primary context is provided at the beginning of each subchapter.

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	Geopolitical heavyweight of domestic policy	End To End Supply Chain Visibility Labels	STWS
			Multi-stage supply chain disruption mitigation strategy and Digital Twins for Supply Chain Resilience	
	1.2	Digital escalation and AI-based exploitation	Digital connected security in response to hybrid tactics	ZITiS
			Commitment to Validating and Verifying AI	
	1.3	Rise of populism	Establishment and reinforcement of political education of democratic values	ZITiS
			Installation of rules for mandatory declarations	
2. CYBER AND FUTURE TECHNOLOGIES	2.1	Space interference and counterspace weapons	7SHIELD: a holistic framework for European Ground Segment facilities	STWS
	2.2	Offensive cyber capabilities	The Development of a Proactive Defensive Framework based on ML and cloud	KEMEA
			A fully automated incident response solution based on CT Intelligence	
	2.3	Disruptive innovation	The Development of a Deepfake Detection System	KEMEA
			Counter-Unmanned Aircraft Systems	

3. RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION	3.1	Exploitation of existing political cleavages	Detection of Disinformation Delivery Proxy Actors	ICDS
			Development of Real-time Rapid Alert System on Disinformation	
	3.2	Exploitation of critical infrastructure weaknesses and economic dependencies	Impact and Risk assessment of critical infrastructures in a complex interdependentscenario	STWS
			ResilienceTool (incl. RiskRadar)	
	3.3	Exploitation or investment in companies by foreign actors	A crawler for correlation of screened FDI with suspicious financial activity	STWS
4. INFORMATION AND STRATEGIC COMMUNICATIONS	4.1	Information manipulation with the aim of destabilization	Increasing capabilities to systematically assess information validity throughout the lifecycle	L3CE
			Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications	
			DDS-alpha (EEAS)	STWS
	4.2	Foreign interference in key information institutions	Integrated Monitoring System Against Malware-Based Cyber Operations	ICDS
			Integrated Monitoring System Against Cyber-enabled Information Operations	
	4.3	Promoted ideological extremism and violence	Collection and sentiment analysis of targeted communication	L3CE
			Identify and safeguarding vulnerable individuals	

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. All ideas and innovations were discussed in T3.2 teleconferences that took place on a weekly basis after the submission of D2.10, from the beginning of March 2022 until the end of May 2022.

Additionally, during the EU-HYBNET 2nd Annual Workshop (T5.3) and 2nd Future Trends workshop (T3.4) that took place in Rome, April 5th-6th 2022, the T3.2 partners had the opportunity to discuss with innovation providers-companies and consortia that were invited to participate and present their solutions in these events. Some of them were also contacted after the event in order to provide more information on the innovations they presented.

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. The interventions include the establishment and reinforcement of political education of democratic values and the installation of rules for mandatory declarations. The latter could provide the audience the opportunity to evaluate the manner in which the line of argument is structured.

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

1.1 GEOPOLITICAL HEAVYWEIGHT OF DOMESTIC POLICY

EU-HYBNET responsible partner for this section: STWS, L3CE, Laurea

Introduction to the primary context

The growing economy of third countries has inevitably led to a series of investments to support the change of geopolitical balance. Therefore, competition policies are in constant need of being updated as well as adjusted to a mosaic of local conditions in the Member States. At the same time, climate change paves the way for new trade routes to be developed, while technology advancements can, in the future, alter the digital market. The support of European Industry in such conditions is therefore imperative, and actions like the new Global Connectivity Strategy[5] will certainly benefit the European Industry in the long run, creating synergies that will be based on the European values and will develop sustainable and high quality digital, climate, energy and transport infrastructures and strengthen health, education and research systems across the world, taking into account their needs and the EU's own interests.

Additionally, the supply chain disruption has proven to be a crucial issue recently, due to the pandemic, but also the recent war. This, in turn has had cascading effects to other infrastructures. The recent global chips shortage has disrupted supply chains, caused product shortages, and even forced factories to close. The European Chips Act, adopted by the Commission on 8 February 2022, seeks to strengthen the semiconductor ecosystem and develop a resilient supply chain, while setting measures to prepare, anticipate and respond to future supply chain disruptions[6]. It is composed of a Communication, which spells out the European Strategy and rationale behind the Chips Act, a proposal for a Regulation, and a Recommendation to Member States[7]. The Regulation[8] establishes a framework of measures for strengthening Europe's semiconductor ecosystem.

The approach of increasing resilience through good governance should also be considered in the effort to maintain the competitiveness of European companies. The European Label of Governance Excellence (ELoGE)[9] has already succeeded in promoting the 12 Principles of Good Democratic Governance, while the Centre of Expertise for Good Governance is supporting the implementation of ELoGE by providing guidance, advice and training. Organisations like the Council of European Municipalities and Regions (CEMR) can be utilised in that direction. Accordingly, they can contribute to influencing European policy and legislation, and by providing a Forum for debate between local and

[5] European Commission, Press Corner, 'Global Gateway: up to €300 billion for the European Union's strategy to boost sustainable links around the world' December 1st, 2021

[6] European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation, Shaping Europe's digital future, European Commission

[7] European Chips Act, Shaping Europe's Digital Future, European Commission

[8] Proposal for a Regulation Of The European Parliament And Of The Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), European Commission, 2022/0032 (COD)

[9] The European Label of Governance Excellence (ELoGE), Council of Europe

regional governments. Most importantly, they can help create synergies between European cities in order to boost the competitiveness of the European firms.

Domestic Policy Forums can be organised for that reason, emphasizing on the participative nature of the initiative and the ability to rapidly influence decisions: Citizens normally provide feedback to municipalities and they in turn inform the governments. The latter meet and take decisions, which they then communicate back to the citizens. The C.L.E.A.R. tool[10] can also be used as a self-assessment tool for citizen participation at the local level.

1.1.1 END TO END SUPPLY CHAIN VISIBILITY LABELS

NAME OF THE IDEA

End To End Supply Chain Visibility Labels

DESCRIPTION OF THE IDEA

The idea is based on the observation that current labels for manufactured products (excluding food) fail to reveal to the customer every country where a manufacturing step was concluded, therefore not providing the consumer with an opportunity to make an informed choice based on various parameters.

With respect to Labels and Markings for products[11], there are Mandatory and Voluntary Labelling Requirements for various product categories. Mandatory Labels include the following: *CE marking* is only obligatory for products for which EU specifications exist and require the affixing of CE marking. *Energy Labels* rank appliances on a scale from A to G according to how much energy they consume. The *WEEE label* indicates that the product should not be discarded as unsorted waste. Most footwear items sold in the EU must bear a label that informs the potential buyers on what they are made of. Clothes and other textile products sold in the EU are required to carry a label with information on the *textile fibre composition*. There are also Voluntary Labels, the EU Ecolabel and the e-mark.

Regarding food products, the labelling rules in the European Union enable the citizens to get comprehensive information about the content and composition of food products in order to make an informed choice when purchasing their foodstuffs. In fact, the Food Labelling Information System (FLIS) provides a user-friendly IT solution which enables its users to select the food and automatically retrieve the mandatory EU labelling indications in 23 EU languages. The system also provides links to the relevant legal provisions and existing guidance documents.[12] In the Unites States, the country-of-Origin Labelling (COOL) is a consumer labelling law that requires retailers (most grocery stores and supermarkets) to identify the country of origin on certain foods referred to as "covered commodities'[13]

With respect to origin of the products, the 'made in EU' label is a protected designation of origin proposed by the European Commission that indicates the product is *mainly* made in the EU. This would give value to European Products and could stimulate growth in the European Union.

However, consumers need to be in a position to make an informed decision based on various parameters. For example, the Made in Europe manufacturing partnership of Horizon Europe[14] states that European society demands minimal environmental impact of industry and European industrial companies need to re-evaluate their resource efficiency and the carbon intensity of their entire supply chains. Zero Defect Manufacturing and the European Green Deal are also considered, and these could also be parameters for product choice by European consumers in the future.

The various parameters that help European consumers make an informed decision can be addressed with an End-to-End Supply Chain Visibility Label. This could be in the form of a QR code or printed label, and the information shown would include information like:

Country where every step of the production took place, for example:

i) Design: Country A ii) Raw materials: Country B iii) Assembly: Countries C, D iv) Packaging: Country E

[10] European Committee On Local And Regional Democracy (Cdlr), Council of Europe

[11] Labels and Markings, Product Requirements, Your Europe, European Union

[12] European Commission, Food Labelling, Food Labelling Information System (FLIS)

[13] US Department of Agriculture, Agricultural marketing service, USDA

[14] Made in Europe, Manufacturing Partnership in Horizon Europe, European Commission, European Factories of the Future Research Association

This would serve to reveal the real supply chain and provide valid information about where the product was actually produced. This, in turn, would allow citizens to support products that are actually made in Europe, in order to increase European competitiveness and support legal, ethical, sustainable and transparent commerce of safe products.
This is especially relevant for pan-European security practitioners as well, as they need to be in a position to offer to European citizens information about the products' origin, so the latter can support EU initiatives, EU policies, EU alliances, and most importantly, EU companies.
End to End supply chain visibility is an important topic in the business world as well, as one can simply not measure or improve what is not known[15]. Additionally, it can promote market competitiveness[16] .
The technology that could support such an idea is supply chain visibility software, that tracks raw materials, parts, components, and finished goods from suppliers to manufacturers, retailers, or distributors, and to the customer. Companies use supply chain visibility solutions to optimize inventory levels and transportation activities, which translates into increased profitability[17].

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 consumers support European Companies, to help Europe create autonomy **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):** The implementation of the idea would require actions at the ministry level
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
- The idea could be used by private companies and private citizens

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: Multiple software solutions exist in the market for that purpose. QR codes are also very advanced.
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Available innovation
- **Expected time to TRL-9.** Not known

[15] The Growing Emphasis on End-to-End Supply Chain Visibility, Logmore
[16] Verwijmeren, M., What Is End-to-End Supply Chain Visibility? Supply Chain News 24/7, March 2022.
[17] Supply Chain Visibility Software, Supply Chain Management Software, G2 webpage, accessed May 2022.

- **Expected time to market.** The implementation of the idea could be challenging as not many infrastructures have such software.

DESCRIPTION OF USE CASE(S)

- The idea could be first implemented for critical products, including for example medical supplies. The shortage on face masks during the pandemic brough this problem to the surface.

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 End To End Supply Chain Visibility Labels and relevant software to support its implementation would improve transparency in complex supply chain networks. It would help European consumers make informed decisions. Most importantly, it would provide the citizens the opportunity to support European products and support Europe's autonomy.
-
- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** End to End supply chain visibility software, QR codes	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - . There are no restrictions but adding this label in the Mandatory and Voluntary Labelling Requirements would require legislative actions by the Commission
COSTS	**COUNTERMEASURES**
- **Indication of costs**: - **Differentiate if possible in development, procurement and exploitation** Development and legal costs for the labelling requirements	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? The usual risk is cyber-attacks; however most firms have proper software for that purpose. - **How durable is the idea (how long is the idea expected to be effective/useful?)** The are no time limits for the implementation of the idea; it is expected to be very useful and effective during all political and financial circumstances

MISCELLANEOUS

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

1.1.2 Multi-Stage Supply Chain Disruption Mitigation Strategy 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) [18] 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[19]. 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[20]. Stress testing a supply chain with what if scenarios can reinforce any mitigation strategy and strengthen the resiliency of a critical entity.

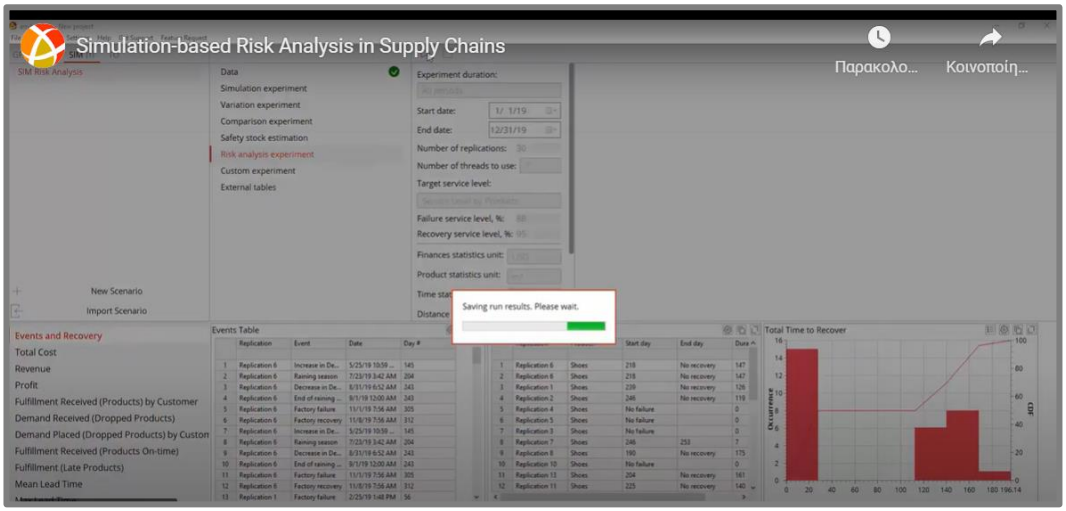

Figure 2: Simulation -based Risk Analysis in Supply Chains, video available in Youtube by anyLogistix supply chain software

Another example is the one of Resilink that offers End-to-End SCRM including resiliency scorecard for suppliers' performance[21].

[18] 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.

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

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

[21] Resilink, company webpage

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)

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.

<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.

- <u>Resilience</u>/defensive/offensive</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
No specific requirements, Software can run in a windows environment</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
- Not specific restrictions, CIs</td></tr>
<tr><td>COSTS
- Indication of costs:
Not available but expected to be the normal pricing of commercial software
- 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 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.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

1.2 DIGITAL ESCALATION AND AI-BASED EXPLOITATION

EU-HYBNET responsible partner for this section: ZITiS. Introduction: STWS

Introduction to the primary context

Following the recent advantages of Artificial Intelligence (AI), driving the Fourth Industrial Revolution, and their numerous application areas, hidden hybrid threats have been recognised, while AI is also expected to increase the complexity of warfare[22]. Additionally, the network power and AI power cannot presently be considered separately, since it is precisely their synergy that determine the present strategic and tactical momentum of hybrid operations[23] .

Actions need to be taken towards an agreement on a common approach by the Member States, taking under consideration the criticality of the decisions taken by AI and their performance in the tasks. Humans should be kept in-the-loop and that should be the guiding ethical principle.

A comprehensive network approach is proposed in this section, along with commitment to validating and verifying AI.

1.2.1 Digital Connected Security In Response To Hybrid Tactics

NAME OF THE IDEA

Digital connected security in response to hybrid tactics

DESCRIPTION OF THE IDEA

Complex security policy challenges can be addressed through a comprehensive network approach. So, the idea of "cybersecurity" is the answer to hybrid threats. The aim is to identify messages and reports that present themselves as false or misleading. This could prevent national or even international conflicts of a political or economic nature, or at least solve them more quickly. This also contributes to national security. A news tool based on a service that automatically identifies, rates, and sorts fake news can help identify the accuracy of a new news story. Pictures, voice messages and texts should be included.

In order to achieve such security, it is imperative that the content of messages or reports is searched and checked as a whole, as well as in sections or parts, with an AI-based machine-learning scan landscape. It is also necessary to check for statements or reports that have been taken out of context, since those with changed images may convey completely different content or misleading information. Sometimes texts can only be given a different meaning by rearranging, adding or omitting words. This type of manipulation must also be recognized and evaluated. An adaptive and scalable system is absolutely necessary here, since the number of elements to be searched is constantly increasing. The learning process is carried out by the users, who constantly provide feedback regarding the automatic machine evaluation and thus (must!) contribute to a constant improvement of the AI. Mechanisms such as signing could be used to determine the authenticity of a message. In order to determine the complete authenticity of a discussion, for example, means such as blockchain- based messages could be used. Messages that are transmitted end-to-end encrypted cannot be considered in this environment, since there is no access to them and in most cases they are not intended for the general public, but are to be seen in a private context.

[22] Thiele, R. Artificial Intelligence –A key enabler of hybrid warfare, Hybrid CoE Working paper 6

[23] Gonçalves, Carlos Pedro, Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats, Cyberspace, 2019.

<table>
<tr>
<td>

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  Defining clear areas of application

- **Applicable JRC domains as stated by the gaps/needs:**
  Cyber, political, military/defence; also information, culture, social, intelligence

- **Applicable core theme(s) as stated by the gap/need:**
  - Future Trends Of Hybrid Threads. Also links to “Information and Strategic Communication”.

</td>
<td>

TYPE OF SOLUTION

- **Technical**
  Software
  - News- /Message groups

- **Social/Human**

- **Organizational/Process**
  - building interest groups

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

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Strategic decisions are required as to whether, when and to what extent governmental (local, national and EU) and non-governmental (industry, media and business) security connections can be established. This also involves the development of criteria that enable measurability and evaluation. Transparency of both governmental and non-governmental methods is essential.

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

- **Provide the expected end-users of the idea (such as NGO’s, private citizens, private companies, media outlets, police, firefighting departments**
  Police, intelligence services, (security) authorities, governments

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  Idk – probably not very high

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
- To build up a national and/or a EU-wide messaging network, where multiple persons of interest getting automatically informed.

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

- **Expected time to market.**

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

DESCRIPTION OF USE CASE(S)

-

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

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
- Rapid distribution of messages, which have already been pre-evaluated by an AI, are checked by a 'community'. Necessary feedback to the AI model helps to improve the automatic pre-evaluation algorithms.

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

<table>
<tr><td colspan="2">- Resilience/defensive/offensive
Such a tool can significantly accelerate the speed at which messages can be examined and classified automatically and with human knowledge.</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
- Depending on the tool, the critical field can vary. The use of a closed system with state-of-the-art IT security shall be used in that context</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
- n/a</td></tr>
<tr><td>COSTS
- Indication of costs:

- Differentiate if possible in development, procurement and exploitation
Depending on if an already available tool getting used or a complete new development shall be used the costs vary in a high range. Administrative and editorial effort may very high.

5M+</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
- As long as these options are used responsibly, there should not be any major disadvantages.

- How durable is the idea (how long is the idea expected to be effective/useful?)
- After a run-up phase and depending on the technology used, the benefit can be felt relatively quickly.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

1.2.2 Commitment to Validating and Verifying Ai

NAME OF THE IDEA

Commitment to Validating and Verifying AI

DESCRIPTION OF THE IDEA

AI systems are becoming ubiquitous in modern life in more and more areas, ranging from medical diagnostic systems to financial trading algorithms, driverless cars, customer loyalty systems and myriad other areas. Sometimes the performance of the AI is critical, in the sense that a patient could die, an accident could happen, or a company could collapse if wrong decisions were made. An AI can also be used in critical environments, e.g. early warning systems that react to special external parameters. So key questions are: Can you trust your AI?
Does it do what you want and how do you know is doing it correctly? Possible questions that definitely need to be asked are:

- Is the task formulated sufficiently and correctly?
- What is the probability of software errors?
- How reliable is the training data of the AI, is it representative?
- Is the AI system stable and robust enough to handle variability and cope with the inevitable data glitches will?

Certification of artificial intelligence (AI) or self-learning systems is a possible key requirement to promote the use of AI systems in various areas of the economy and life or to regard them as safe. Certification should be necessary for AI systems and should help to exploit the potential for social benefit safely and in a way that is oriented towards the common good. Certification of AI systems according to defined guidelines and processes enables important social and economic principles, such as legal certainty, interoperability, IT security or data protection, to be fulfilled. In addition, it can create trust among citizens, lead to better products and influence national and international market dynamics or safety. However, to ensure that certification procedures do not prove to be an obstacle to innovation, it is necessary to guarantee certain standards of AI systems, to avoid over-regulation, to enable innovation and, ideally, to be able to trigger new developments for a European way of using AI. Experts from the Platform for Learning Systems have systematized the area of tension between potentials and challenges in the certification of AI systems.

A certification should be a temporary confirmation that specified standards, norms or guidelines are being observed. This assessment must be carried out by independent certification bodies. The basis are different nationally or internationally recognized and valid industry-specific standards and guidelines. Products and services as well as systems, processes and people can be certified. Most of the time there is a certification on a voluntary basis to demonstrate the quality of the certified item. In order to be able to carry out a certification, reliable standards and norms must be defined in order to form the basis of a certification.

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gaps/need** Set up AI-based modules robustly against attacks and ward off conscious, or more or less controlled, use with wrong information that leads to desired wrong results or (AI) decisions. - **Applicable JRC domains as stated by the gaps/needs:** cyber, military/defence, political; also information, culture, social, intelligence - **Applicable core theme(s) as stated by the gap/need:** o Future Trends to Hybrid Threats. Also links to “Cyber and future	- **Technical** o Software o Framework definitions o Requirements - **Social/Human** - **Organizational/Process**

Technologies" and "Information and Strategic Communication".	

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Strategic decisions are required as to whether, when and to what extent governmental (local, national and EU) and non-governmental (industry, media and business) security connections can be established. This also involves the development of criteria that enable measurability and evaluation. Transparency of both governmental and non-governmental methods is essential.

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

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
  Police, intelligence services, (security) authorities, governments, private companies.

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  Probably not very high: 1-2

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  To build up a national and/or a EU-wide framework with requirements and rules how a AI-System shall be checked and certified.

- **Expected time to TRL-9.**
  > 5 years

- **Expected time to market.**

DESCRIPTION OF USE CASE(S)

-

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  AI systems are more robust against extreme situations, which are also described with conflicting information and mutually exclusive data.

- **Resilience/defensive/offensive**
  Evaluation of news, political or financial events can be assessed more stably or classified as non-evaluable by the model.

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Depending on the implementation, the critical field can vary.	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - n/a

COSTS	COUNTERMEASURES
- **Indication of costs**: - **Differentiate, if possible, in development, procurement and exploitation** Difficult to specify. Since it is a more or less completely new technology and area could be very high. 5M+	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? As long as these options are used responsibly, there should not be any major disadvantages. - **How durable is the idea (how long is the idea expected to be effective/useful?)** But an ongoing process for new kinds of models, algorithms shall be implemented to stay at the level of state-of-the-art technology.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** **The reader can also see the interesting work of the SAFAIR program, also known as SPARTA WP7. The program seeks to address two major contemporary problems caused by the proliferation of artificial intelligence (AI). The first objective is to ensure the security of AI solutions, the second objective deals with the issue of trustworthiness and fairness of AI.**	

1.3 RISE OF POPULISM

EU-HYBNET responsible partner for this section: ZITiS

Introduction to the primary context

Populism is on the rise with the current trend towards post-democracy. The dark side of populism is particularly evident in Europe today when one looks at its scapegoat tendencies, which come in various forms. At the same time, radical and democratic advocates emphasize the importance of equality and popular sovereignty as a source for populists to revitalize democracy. This ambivalence of populism relates both to the rule of law and to political culture as a prerequisite for humanitarian democracy. In terms of political culture, nonviolence and fraternity are highlighted as important political virtues.

1.3.1 Establishment And Reinforcement Of Political Education Of Democratic Values

<table>
<tr><td colspan="2">NAME OF THE IDEA
Establishment and reinforcement of political education of democratic values

DESCRIPTION OF THE IDEA
In the long term, the best measure against being seduced by populists is probably to educate the population, but above all children and young people, so that they recognize the value of democracy as a form of government that enables them to have a say and protects them from arbitrariness, at least better than any other previously known form of government such as the absolutist monarchy or the dictatorship, in which there is no separation of powers and the power is exercised unlimited and uncontrolled by only one person or a few persons. Furthermore, it must be made plausible to them that all human beings are essentially equal in terms of their basic needs, rights and duties and can therefore also claim equal respect. Direct contact with people who do not belong to your own group, at work or in your free time, can help to get a realistic picture of members of other groups. In addition, children and young people should be able to think and make independent judgments based on sufficient and reliable information, to plan and act long-term, well-considered, beyond their own lifetime, to listen and to be willing to compromise, to be peaceful, to have appropriate self-confidence on the basis of sufficient Knowledge of one's own strengths and weaknesses, awareness of one's own prejudices and possible fears, as well as cooperative behaviour not only with regard to one's own group but also with regard to strangers.
Relevant technological innovations that are needed are the ones that support media literacy skills (See for example §4.3 of EU-Hybnet Deliverable 3.3, Training application for media literacy.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED

- Describe the use of the solution in reference to the gaps/need
Improving society's resilience to populist influences

- Applicable JRC domains as stated by the gaps/needs:
Political, social, information

- Applicable core theme(s) as stated by the gap/need:
o Future Trends of Hybrid Threats.</td><td>TYPE OF SOLUTION

- Technical
n/a

- <u>Social/Human</u>
o Education system
o Increase cognitive thinking mechanisms

- <u>Organizational/Process</u>
o Changes in the education processes
o More support in ‘how to’ learn than what to learn.</td></tr>
</table>

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Supporting the free and democratic order in governments and the general population.
  Although this task is an absolutely difficult task, current governments must face the task openly.

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

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
  Private citizens, or more absolutely everybody.

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  TRL 2
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  education, teaching
- **Expected time to TRL-9.**
  1 – 3 years, but with an ongoing process of improvement and change
- **Expected time to market.**
  1-3 years

DESCRIPTION OF USE CASE(S)

In almost all situations that occur in everyday life. In dealing with crises or stressful situations of the population, be it national or international.
".

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to general education; everyone is empowered and encouraged not simply to believe information, but to question it and also to look for and weigh up counter-arguments.

- **Resilience/defensive/offensive**
  Such establishment of procedures for new information improves societal resilience to offensive cyber capabilities and is thus a defensive capability against hybrid state actors employing particular rhetoric, policies and technologies.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  It is a new concept of education mechanisms.

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:

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

  5M € +

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  As long as these options are used responsibly, there should not be any major disadvantages.

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

	As long as an ongoing process of continuous improvement and adjustment mechanisms with sufficient controls is used, this is an idea that can run indefinitely.

MISCELLANEOUS

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

Note from the lead author:

As discussed in a recent EU-Hybnet workshop in Rome, it is of crucial importance to understand the main dimensions of populism and the typical cases of citizens (or groups of citizens) that are being exploited. Even though populism provides the unique opportunity to expose and understand the society's main social weaknesses, technology and social interventions can prevent the exploitation of citizens.

Populism -based exploitation usually relies on growing distrust and disappointment, offering to 'give voice' to the ones that haven't one. Also, exploitation is based on the victimhood narrative on how badly citizens are treated by governments and projects identities (gender, religion). However, exploitation works as a way to diverge from the real problem, and therefore all innovations proposed to counter disinformation are also relevant in this section.

1.3.2 Installation of Rules For Mandatory Declarations

NAME OF THE IDEA

Installation of rules for mandatory declarations

DESCRIPTION OF THE IDEA

Reports, speeches, etc. must have an opinion-forming character with references to backgrounds, historical developments, sources of arguments, and much more should be provided. This gives the audience the opportunity to see how the line of argument is structured or whether there are any contradictions. In future approaches, a machine could (at least) check the validity of the specified links. Further expansion stages could be provided with an AI, which could already make an assessment of the information to be examined. A network of bodies that share their information and results should also be helpful. Notifying each other, even between different countries, can significantly increase the speed and accuracy of the assessment, since different training data are probably used.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  Defining clear areas of application
- **Applicable JRC domains as stated by the gaps/needs:**
  Political, social, information.
- **Applicable core theme(s) as stated by the gap/need:**
  - Future Trends Of Hybrid Threats. Also links to: “Information and Strategic Communication” and “Resilient Civilians, local level and administration”

TYPE OF SOLUTION

- **Technical**
- **Social/Human**
  - commitment to self-information
- **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Strategic decisions are required as to whether, when and to what extent governmental (local, national and EU) and non-governmental (industry, media and business) security connections can be established. This also involves the development of criteria that enable measurability and evaluation. Transparency of both governmental and non-governmental methods is essential.
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe’s third sector):**
- **Provide the expected end-users of the idea (such as NGO’s, private citizens, private companies, media outlets, police, firefighting departments**
  Intelligence services, (security) authorities, governments, private citizens and companies

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  Probably not very high
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
- **Expected time to TRL-9.**
  2 to 5 years, since many discussions in the parliaments will be necessary

<table>
<tr><td colspan="2">- Expected time to market.</td></tr>
<tr><td colspan="2">DESCRIPTION OF USE CASE(S)
-</td></tr>
<tr><td colspan="2">IMPACT ON COUNTERING HYBRID THREATS
- Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
Rapid distribution of checked messages and give everybody sources for checking the validity.

- Resilience/defensive/offensive</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
- n/a</td></tr>
<tr><td>COSTS
- Indication of costs:

- Differentiate if possible in development, procurement and exploitation

5M+</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Everybody is responsible for his activity with checking the facts.

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

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

2.1 SPACE INTERFERENCE AND COUNTERSPACE WEAPONS

EU-HYBNET responsible partner for this section: STWS

Introduction to the primary context.

Space based services (e.g. Positioning, Navigation and Timing (PNT)) are value-added, operational services delivered to a final user and enabled by space-based systems. In the generation of data and delivery of services, space-based systems can be complemented by ground-based and/or airborne systems. These space-based services have become a utility and many critical infrastructures are relying on them. Indicative of the importance of the matter in light of global security, the European Commission recently proposed two new flagship initiatives to boost satellite-based secure connectivity and Space Traffic Management[24]: The EU space-based secure connectivity system and the Space Traffic Management. At the same time, the need for a holistic approach in crisis management of space ground segments, that can address preparedness, detection, response, mitigation and recovery is profound.

2.1.1 7SHIELD: A Holistic Framework for European Ground Segment Facilities

NAME OF THE IDEA
7SHIELD: a holistic framework for European Ground Segment facilities that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely pre-crisis, crisis and post-crises phases[25].
DESCRIPTION OF THE IDEA
Ground segments appear to be potential new targets for complex physical/cyber threats as they receive massive amounts of satellite data. In more detail, the ability to disrupt, inspect, modify or re-route traffic provides an opportunity to conduct cyber/physical attack. Such an attack could have a dramatic impact on the security of European citizens and can initiate cascading effects to other Critical Infrastructures. The 7Shield framework is being developed to be able to confront complex cyber and physical threats by covering all the macrostages of crisis management, namely the pre-crisis, crisis and post-crises phases. The integrated framework is flexible and adaptable enabling the deployment of innovative services for cyber-physical protection of ground segments. The framework will integrate advanced technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection. *Pre-crisis* phase: An early warning mechanism is being used to estimate the level of risk before the occurrence of the attack. *Crisis* phase: During the attack, detection and response is effective and efficient, considering also budgetary constraints. A mitigation plan is designed and automatically updated to offer a quick recovery after an intentional attack or a system failure. Business continuity scenarios are also supporting the security and resilience of private installations.

[24] EU Space Programme, Defence Industry and Space, European Commision

[25] 7Shield H2020 Project Webpage

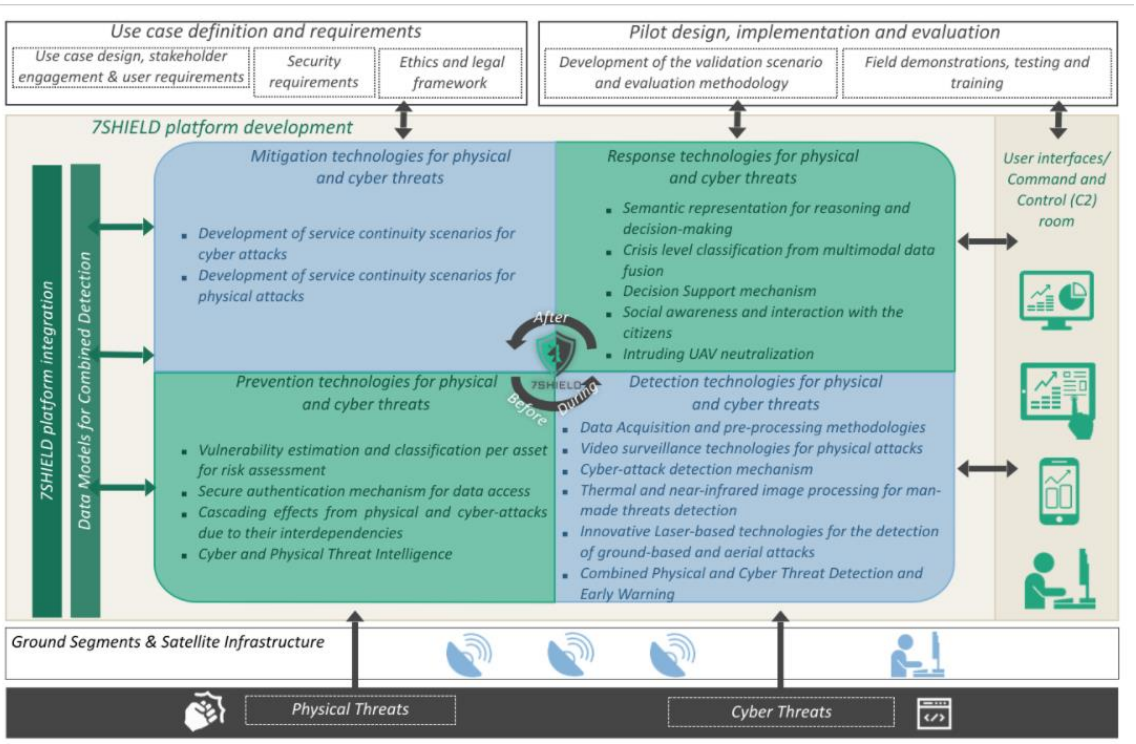

Figure 3 : Schematic Concept of the 7Shield

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  The solution can be used to protect ground segments from cyberattacks that can exploit military advantages in space
- **Applicable JRC domains as stated by the gaps/needs:**
  space, cyber and military/defence domains
- **Applicable core theme(s) as stated by the gap/need:**
  - CYBER AND FUTURE TECHNOLOGIES

TYPE OF SOLUTION

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

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:** space, cyber and military/defence domains
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):**
  - **II) *local level* (cities and regions):** The cities and regions can utilise the solution to showcase vulnerabilities and suggest protective actions
  - **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**
- Owners and security Managers of Ground Segments, police, firefighting departments

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: Possibly 6-7
- **In which stage is the solution (research, technology, available innovation, proven innovation):**

Research

- **Expected time to TRL-9.**
  Maybe different for the different components
- **Expected time to market.**

DESCRIPTION OF USE CASE(S)

The framework and its technology bricks will be tested in five Pilot Use cases, consisting of several scenarios involving physical, cyber or combined cyber/physical attacks. The platform will be tested in training grounds owned by the Finnish Meteorological Institute, the National Observatory of Athens, Deimos Space, Space Applications Services and Serco italia

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  An attack on ground segments could have a dramatic impact on the security of European citizens and can initiate cascading effects to other Critical Infrastructures.
- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** There are several technologies used in 7Shield: advanced technologies for data integration, processing, and analytics, machine learning and recommendation systems, data visualization and dashboards, data security and cyber threat protection	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - .
COSTS	**COUNTERMEASURES**
- **Indication of costs**: Not known yet - **Differentiate if possible in development, procurement and exploitation** The development cost is the most important. Maintenance cost should also be considered.	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? - **How durable is the idea (how long is the idea expected to be effective/useful?)**

MISCELLANEOUS

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

2.2 OFFENSIVE CYBER CAPABILITIES

EU-HYBNET responsible partner for this section: KEMEA

Introduction to the primary context [4-6].

Offensive cyberattacks are a major problem for society and range, for instance, from eavesdropping, intercepting, and hijacking private computers or cell phones, to large-scale theft of corporate secrets or blackmailing companies through malware and ransomware, to sabotaging democratic elections or critical infrastructure through targeted cyber operations. The introduction and proliferation of AI in all areas of life, but especially in the business and infrastructure sector, has greatly increased the vulnerabilities for innovative AI-enabled attacks or the hacking of AI-controlled systems.

References used for this section[26,27,28].

2.2.1 The Development of A Proactive Defensive Framework Based on Ml And Cloud

NAME OF THE IDEA

The Development of a Proactive Defensive Framework based on ML and cloud

DESCRIPTION OF THE IDEA

Offensive cyber capabilities run the gamut from sophisticated, long-term disruptions of physical infrastructure to malware used to target human rights journalists. As these capabilities continue to proliferate with increasing complexity and to new types of actors, the imperative to slow and counter their spread only strengthens. Innovation is critical to improving society and is key to the cyber domain. The rapid growth of the internet has meant that tools for operating in cyberspace have constantly evolved. It has often been said, however, that the only innovation taking place in cyber warfare is in offensive operations. So where is the innovation for the defense?
The development of a defensive framework for proactive situational awareness using Machine Learning technology and Cloud Computing, to better understand one's network and system can be a way to quickly identify and defend against cyberattacks and emerged types of offensive cyber capabilities.
Faced with a constant stream of threats from cybercriminals, hackers, and other malicious actors, it is almost impossible for anyone to keep up with any form of automation or artificial intelligence, so self-learning cyber-defense products that use artificial intelligence to detect and even respond to emerging attacks are required.

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gaps/need** - Improve societal resilience against cyber attacks. **Applicable JRC domains as stated by the gaps/needs:** It can be related to helping countering	- **Technical** o software - **Social/Human** o n/a - **Organizational/Process** n/a

[26] Wong, Ernest & Hutton, Katherine & Gagnon, Ryan. (2018). Thinking Outside-the-Box for Cyber Defense: Introducing an Innovation Framework for the 21st Century.

[27] ENISA, Foresight Challenges

[28] Best Starup, TOP ISRAELI STARTUPS & COMPANIES

disinformation across all 13 domains. Main focus: cyber, infrastructure. - **Applicable core theme(s) as stated by the gap/need:** ○ Cyber and Future Technologies. Also links to "Information and Strategic Communications" and "Resilient Civilians, Local Level and National Administration"	

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  A framework like this can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry) organizations as well as citizens. However, the primary focus seems to be directed to governmental organizations and critical infrastructures.
  The governmental focus is applicable to all 13 JRC domains, esp. cyber, infrastructure.

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

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 9
  Today, a CERT / CSIRT provides alerts and avoidance guidance for cybersecurity incidents as a security sustaining tool. In the offensive domain of many platforms / software / tools are already in use providing situational awareness as part of proactive services. The important integrient is to implement ML and AI in these tools and combined capabilities by leveraging and expanding upon current disruptive innovation in the cyber doman that is focused on increasing basic cyber education for users, developing partnerships for better information sharing, automated intelligence exchange, and harnessing the potential of the cloud computing architecture.

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Available innovation, however, it seems that governments / industry is not widely using it in an operational environment.

- **Expected time to TRL-9.** 1-3 years
- **Expected time to market.** 1-3 years

DESCRIPTION OF USE CASE(S)

Improving proactive situational awareness by better understanding one's network and system can be a way to quickly identify and defend against offensive capabilities and cyberattacks.
Cloud Computing and Machine Learning, which includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Security as a Service (SECaaS), is an emerging market that creates a breeding ground for disruptive innovations. By developing software programs compatible with cloud computing architecture implemented with AI and ML technology,

entrepreneurs can better sense and defend to emerged type of attacks. These cyber services originated as complex and customized in-house solutions for security and storage to large banks, industrial corporations, technology companies, and sensitive government agencies.

Today several Cybersecurity Companies like DarkTrace, manufactures defense systems that replicate human antibodies to automatically detect and neutralize cyber threats without human intervention. By applying learning models to the network, AI systems can be trained to test various defense strategies to minimize or stop the spread of malware during a cyber-attack by controlling the infection and eliminating the root cause.

IMPACT ON COUNTERING HYBRID THREATS

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

Resilience/defensive/offensive

- Such a tool is improving societal resilience against offensive cyber capabilities and is also a defensive capability against hybrid state actors using new technologies.

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Machine learning is a critical technology.	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - Not really
COSTS	**COUNTERMEASURES**
- **Indication of costs**: - **Differentiate if possible in development, procurement and exploitation**	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? - **How durable is the idea (how long is the idea expected to be effective/useful?)** Certainly for the next 5 years.

MISCELLANEOUS

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

Not applicable.

2.2.2 A Fully Automated Incident Response Solution Based on CT Intelligence

NAME OF THE IDEA

A fully automated incident response solution based on CT Intelligence

DESCRIPTION OF THE IDEA

Offensive cyber capabilities and Cyber-attacks have become a common phenomenon. These attacks and breaches happen daily, and can affect large corporations, causing damage that can sum up to hundreds of millions of dollars. Over the past five years, cyber security breaches have increased by 67%, and ransomware attacks now occur every 14 seconds.
A fully automated incident response solution based on Cyber Threat Intelligence feed, that enables organizations to investigate every cyber-alert they receive and close out incidents in minutes, even seconds. This Automated Incident Response Solution maximizes an enterprise's ability to investigate all cyber-alerts, uncover hidden threats and remediate the full extent of a breach to increase the organization's productivity, reduce ongoing costs, and strengthen the organization's overall security.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  - Improve societal resilience against cyber attacks
- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all 13 domains. Special focus: Cyber, Infrastructure.
- **Applicable core theme(s) as stated by the gap/need:**
  - Cyber and Future Technologies. Also links to "Information and Strategic Communications" and "Resilient Civilians, Local Level and National Administration"

TYPE OF SOLUTION

- **Technical**
  - software
- **Social/Human**
  - n/a
- **Organizational/Process**
  n/a

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  A solution like this can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry) organizations as well as citizens.
  However, the primary focus seems to be directed to governmental organizations and critical infrastructures.
- The governmental focus is applicable to all 13 JRC domains.
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):**
  - **II) *local level* (cities and regions):**
  - **III) *support functions to ministry and local levels* (incl. Europe's third sector):**
- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: TRL9
- A comprehensive security operations platform that combines security orchestration from CTI feeds, incident management, machine learning from analyst activities, and interactive investigation from threat hunting labs.
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
- Available innovation, however, it seems that governments / industry is not widely using it in an operational environment.
- **Expected time to TRL-9.** 1-2 years
- **Expected time to market.** 1-2 years

DESCRIPTION OF USE CASE(S)

- An innovative solution, such as a preemptive incident-response platform, which is designed to help security teams cut incident response time to minutes, manage attacks immediately without affecting business continuity, and bolster company / organizations defenses against future attacks. The solution will combine historical, threat-level endpoint visibility and threat hunting lab-based outcomes to automatically investigate any alert and trace the forensic timeline and attack-chain back to the root cause. This process provides full context, including entities involved, behaviors, infected hosts, damage assessment and more.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to the need for exposing and countering disinformation.
-
- **Resilience/defensive/offensive**
- Such a tool is improving societal resilience against offensive cyber capabilities and is also a defensive capability against hybrid state actors using new technologies.

ENABLING TECHNOLOGY

Which technologies are critical in fielding the idea?

i) Machine learning is a critical technology.

- ii) AI

RESTRICTIONS FOR USE

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

COSTS

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

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  Certainly for the next 5 years.

MISCELLANEOUS

Any additional remarks/disclaimers/comments/information you might want to provide
Not applicable.

2.3 DISRUPTIVE INNOVATION

EU-HYBNET responsible partner for this section: KEMEA

Introduction to the primary context.

While digital challenges are already introducing monumental changes on politics and society, business as well as the Army, the avantgarde of innovation is already setting course for a post-digital era. Disruptive and radically enhanced innovations can change information flow, networks of sensors, video analytics, big data analysis, AI processing, to immensely accelerate the cycle of information dissemination, decision-making and action. Eventually they'll seriously change the security landscape once more.

References used for this section[29,30,31,32,33]

2.3.1 The Development of A Deepfake Detection System

NAME OF THE IDEA **The Development of a Deepfake Detection System** **DESCRIPTION OF THE IDEA** Photo and video manipulation is crucial to the spreading of typically quite convincing disinformation on social media and cyberspace generally. Computer-generated photos of people's faces, conversely, have already become common hallmarks of subtle foreign interference campaigns, aiming to build faux accounts. In this respect deepfakes seem to be more authentic. One issue is of course very important, to find a lot of ways to identify media that has been manipulated or modified within the fight against on-line disinformation. The repercussions of such deepfakes are dangerous with compromised videos of public figures in circulation that threaten their name. Worse, it's anticipated that deepfakes might even play an outsized role in swaying elections of nations. Notably, Facebook, Twitter, and TikTok have already prohibited such deepfake content on their platform. In order to tackle this problem a reliable Deepfake detection system is needed while techniques for making deepfakes keep developing and advancing. The tools and techniques shall deliver complete accuracy and effectiveness.	
REFERENCE TO CAPABILITY GAP/NEED - **Describe the use of the solution in reference to the gaps/need** - Improve preparedness to counter the strategic disadvantages and vulnerabilities that could result from disruptive innovations **Applicable JRC domains as stated by the gaps/needs:** It can be related to helping countering disinformation across all 13 domains. Special focus to political, social, military/defence -	**TYPE OF SOLUTION** - **Technical** o software - **Social/Human** o n/a - **Organizational/Process** o n/a

[29] Burt,T., New Steps to Combat Disinformation, Microsoft on the Issues, 2020

[30] Using AI to Detect Seemingly Perfect Deep-Fake Videos, Human-Centered Artificial Intelligence, Stanford University

[31] Counter Unmanned Aerial Systems (C-UAS) , Northrop Grumman

[32] Counter-Unmanned Aerial Systems (UAS), General Dynamics Mission Systems

[33] Counter Unmanned Aircraft Systems: EagleShield, Thales

- **Applicable core theme(s) as stated by the gap/need:** o Cyber and Future Technologies. Also links to "Information and Strategic Communications" and "Resilient Civilians, Local Level and National Administration"	

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  A framework like this can potentially be used by both governmental (local, national and institutional like EU) and non-governmental (media, industry) organizations as well as citizens.
  However, the primary focus seems to be directed to governmental institutions and media professionals.

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

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 6-7.
  Today, with such major consequences of deepfakes, there have been several efforts to create tools, albeit with varying degrees of success, which can help detect them.

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Techniques for creating deepfakes keeps developing and advancing. The tools and techniques to identify them do not present complete accuracy and effectiveness. However, they are making strides in the right direction for a battle that is much bigger.

- **Expected time to TRL-9.** 1-3 years

- **Expected time to market.** 1-3 years

DESCRIPTION OF USE CASE(S)

- A video authenticator tool is created by Microsoft. It can analyze a still photo or video to provide a confidence score to detect whether or not the media is manipulated. It detects the blending boundary of the deepfake and subtle grayscale elements that are undetectable to the human eye. It also provides this confidence score in real-time. The tool has been created with a public dataset from Face Forensics++ and has been tested using the Deepfake Detection Challenge Dataset. Both these datasets are leading technologies for training and testing deepfake detection technologies.
- -Researchers from Binghamton University and Intel created a tool that goes beyond just deepfake detection and recognises the deepfake model behind the compromised video. This tool looks for unique biological and generative noise signals 'deepfake heartbeats' left by deepfake model videos. These signals are detected from 32 different spots in a person's face, called the Photoplethysmography (PPG) cells.
- - A model is invented by researchers from Stanford University and the University of California. This technique exploits the fact that visemes, which denote the dynamics of the mouth shape, are sometimes different or inconsistent with the spoken phoneme. For example, for saying words such as mama, baba, and papa, there might be a phoneme-viseme mismatch, which can be used in detecting even spatially small and temporally localised manipulations in deepfake videos. The team used lipsync

deep fakes created using three synthesis techniques – Audio-to-Video (A2V), Text-to-Video for short utterances (T2V-S), and Text-to-Video for longer utterances (T2V-L).

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  This contributes to the need for exposing and countering disinformation.
-
- **Resilience/defensive/offensive**
- Such a tool is improving societal resilience against disinformation hybrid campaigns by state/non state actors and is also a defensive capability against them.
-

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Image processing via AI / Machine learning assisted by neural network implementations.	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - No
COSTS	**COUNTERMEASURES**
- **Indication of costs**: - **Differentiate if possible in development, procurement and exploitation**	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? - Advance in hybrid actors' methods - **How durable is the idea (how long is the idea expected to be effective/useful?)** Certainly for the next 5 years.

MISCELLANEOUS

Any additional remarks/disclaimers/comments/information you might want to provide
Not applicable.

2.3.2 Counter-Unmanned Aircraft Systems

NAME OF THE IDEA

Counter-Unmanned Aircraft Systems

DESCRIPTION OF THE IDEA

The rapid increase in the availability and sophistication of UAS represents a significant challenge, as their capabilities progress faster than the ability to assess and mitigate the threat posed by lawless small UAS.
Most technological advances include a vast number of positives. And yet, at the same time, we can also be affected by the negative side of the same technology.
In recent years, the drone market has had a significant expansion, with applications in various fields (surveillance, rescue operations, intelligent logistics, environmental monitoring, precision agriculture, inspection and measuring in the construction industry). Given their increasing use, the issues related to safety, security and privacy must be taken into consideration.
Their use could cause damage to the community due to failures and improper or criminal use. A significant increase has been observed in the number of accidents involving drones or unmanned aerial systems (UAS). For example, improper use in the vicinity of an airport can represent a serious threat to public safety and a source of discomfort, as evidenced by the hundreds of flights canceled at London Gatwick airport in a few months of 2018.
For this reason, the development of technologies for the detection, identification and mitigation of malicious drones has become of primary importance. A countermeasure system, also called a counter-UAS (C-UAS) or counter-UAS system (CUS), can identify and neutralize an intruder drone classified as a threat.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
- Improve critical infrastructure protection ad overall security.

Applicable JRC domains as stated by the gaps/needs:

It can be related to Infrastructure, Military / Defense, Administration, Social/ societal, Political domains.

-
- **Applicable core theme(s) as stated by the gap/need:**
  - Cyber and Future Technologies. Also links to “Future Trends to Hybrid Threats” and “Resilient Civilians, Local Level and National Administration”

TYPE OF SOLUTION

- **Technical**
  - Hardware / software
- **Social/Human**
  - Training
- **Organizational/Process**

Coordination

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Applicable JRC domains are mentioned here above.
- **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):**

  A solution like this can potentially be used by governmental (local, national) organizations as well as civil protection, armed forces and critical infra practitioners.
- **Provide the expected end-users of the idea (such as NGO’s, private citizens, private companies, media outlets, police, firefighting departments**

End users could be first responders, Law enforcement agencies, armed forces etc.

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 8

The development of technologies for the detection, identification and mitigation of malicious drones has become of primary importance. A countermeasure system, also called a counter-UAS (C-UAS) , can identify and neutralize an intruder drone classified as a threat.
From an architectural point of view, an anti-drone system generally consists of the following fundamental sub-systems:

- Sensing system;
- Mitigation system;
- Command and control (C2) system.

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

Available innovation in several forms and prototypes, not widely using it in an operational environment.

- **Expected time to TRL-9.** 1-2 years
  Expected time to market. 1-2 years

DESCRIPTION OF USE CASE(S)

Many different companies have developed C-UAS systems. Regarding the research area there is ongoing a PESCO project as well at the EU level.
These systems must be reliable at both an urban environment as well as on battlefield conditions.

- The majority of solutions are offered for use only by law enforcement entities since their use in the majority of countries remains illegal.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
- This contributes to the need for protecting critical infrastructure on a civilian landscape while supporting military ops.
-

Resilience/defensive/offensive

- Such a system is improving critical infra resilience against offensive capabilities and is also a defensive capability against hybrid state actors using disruptive new technologies.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  many different technologies are involved mainly Information and Communication technologies, Network and aviation technologies and several others.

RESTRICTIONS FOR USE

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

COSTS

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

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
- Certainly for the next 5 years.

MISCELLANEOUS

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

The reader may also be interested in drone detection systems, see for example AARTOS DDS website link

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

3.1 EXPLOITATION OF EXISTING POLITICAL CLEAVAGES

EU-HYBNET responsible partner for this section: ICDS

Introduction to the primary context.

Foreign interference itself is not new phenomena, but the 'toolbox' of information manipulations has grown rapidly in the past 10-15 years, especially as different digital and social media platforms spread. After several cases – as interference in the 2016 US presidential elections, the suspected role of Russian interference before the Brexit referendum, the 'Lisa Case' in Germany and the 'Macron Leaks' in France – for governments under attack from disinformation, it became clear that hostile information operations pose a real threat to proper democratic processes.

By today, the EU has clearly recognised that polarizing and radicalizing disinformation seriously endangers public safety, and democratic values, as enshrined in the Charter of Fundamental Rights of the European Union. Some key areas of EU initiatives to strengthen the information security environment are the European Endowment for Democracy (EED), which looks to empower civil society and grassroots movements along EU borders and beyond. Second, the European Regulators Group for Audiovisual Media Services (ERGA), as a model for improving inter-governmental cooperation between EU member states as national regulators. And third, the EUvsDisinfo counter-disinformation platform[34], which should be further developed and empowered by integrative efforts in enhanced cooperation between EU institutions, national governments, civil society, media, and private sector.

3.1.1 Detection of Disinformation Delivery Proxy Actors

NAME OF THE IDEA
Detection of Disinformation Delivery Proxy Actors

DESCRIPTION OF THE IDEA

Authoritarian regimes are increasingly attempting to undermine the shared democratic values of the EU and its member states and polarise societies for their own strategic purposes using various types of hybrid activities, including information manipulation and lawfare. Hence, the protection of democracy infrastructure against exploitation of political cleavages and foreign interference needs more comprehensive attention.

For that purpose, the EU vs Disinfo analytical capabilities should be further advanced and inter-connected with relevant media monitoring assets to detect and identify harmful disinformation delivery by proxy actors whose connections with their hostile 'employers' may be obscured or denied but could be better identified by integrating the most capable Media Monitoring Software assets with EU vs Disinfo database.

The main outcome of the innovation proposal could be better situational awareness, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels

[34] Loik, R. and Madeira, V. (2021). European Union Strategy and Capabilities to Counter Hostile Influence Operations. In: H. Mölder; V. Sazonov; A. Chochia; T. Kerikmäe (Ed.). The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood. Switzerland: Springer Nature. (Contributions to International Relations CIR), pp. 247–264.

to avoid hostile exploitation of existing political cleavages such as polarization, radicalization and undervalue of democratic institutions as we've seen during the Covid-19 pandemic crises.

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- **Describe the use of the solution in reference to the gaps/need** Improving EU and member states' capabilities to tackle hostile information manipulations in more coordinated manner and strengthen the protection of democracy infrastructure against exploitation of political cleavages and foreign interference. - **Applicable JRC domains as stated by the gaps/needs:** Political, Social, administration, Information - **Applicable core theme(s) as stated by the gap/need:** ○ Resilient Civilians, Local Level, National Administration. Links to protection of democratic infrastructure and socio-political stability to strengthen the information security environment.	- **Technical** - **Social/Human** - **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Political, Social, Informational

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

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

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):**
  Average

- **Expected time to TRL-9.**
  1-2 years

- **Expected time to market.**
  2-3 years

<table>
<tr><td colspan="2">DESCRIPTION OF USE CASE(S)
- Different NGO’s, governmental institutions, private bodies, media outlets and academia could use such integrated database to examine the background of particular (proxy) actor and its possible engagement of (previous) disinformation activities as an optional ‘trust-measure’ before accepting and delivering its messages, expertise, etc. information and publicity (re-)production.</td></tr>
<tr><td colspan="2">IMPACT ON COUNTERING HYBRID THREATS
- Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.
Improve cross-border media initiatives and integrated digital tools employed for news verification and cross-verification, open-source investigations to detect, locate and document the proxy actors of information manipulations.

- Resilience/defensive/offensive
Resilience, defensive.</td></tr>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
Integrated Media Monitoring Software with high data protection standards.</td><td>RESTRICTIONS FOR USE
- 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.</td></tr>
<tr><td>COSTS
- Indication of costs:
Depends on technical configurations and tender conditions.

- Differentiate, if possible, in development, procurement and exploitation
Should be EU (EEAS) coordinated procurement.</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Different hostile cyber-operations.

- How durable is the idea (how long is the idea expected to be effective/useful?)
3-5 years</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

3.1.2 Development Of Real-Time Rapid Alert System On Disinformation

NAME OF THE IDEA

Development of Real-time Rapid Alert System on Disinformation

DESCRIPTION OF THE IDEA

The idea is not unique itself. European Commission's Action Plan against Disinformation[35] states (p. 6) that 'a Rapid Alert System will be set up to provide alerts on disinformation campaigns in real-time through a dedicated technological infrastructure'. As James Pamment (2020: 14) emphasizes,[36] that 'while the Rapid Alert System was used to share reporting among EU member states, an alert related to the pandemic has not been triggered.' So, this attempt seems like a missed opportunity, which needs to be carefully assessed and further developed to be real-time, rapid and really alerting.

Thus, the Rapid Alert System on Disinformation should link the national SITCEN-s with EU INTCEN via 24/7 operational information exchange platform in cause of time-criticality, especially in times of large-scale crises as pandemics, irregular immigration flows, etc. The platform should also be securely integrated with EU vs Disinfo database to enable hit-based and advanced searches for identifications of (original) sources and spread (possible impact) projections of disinformation.

The main outcome of the innovation proposal could be better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups.

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- **Describe the use of the solution in reference to the gaps/need** Improving EU and its Member States', including municipalities` capabilities to tackle hostile information manipulations in more rapid, alert-based and coordinated manner and strengthen the protection of democracy infrastructure against exploitation of political cleavages and foreign interference, especially in times of large-scale crises. - **Applicable JRC domains as stated by the gaps/needs:** Political, social, administration, information - **Applicable core theme(s) as stated by the gap/need:** o Resilient Civilians, Local Level, National Administration. Also links to better preparedness of member states` governments and municipalities to respond *fake-news* and other disinformation, which could harm the societal resilience in times of large-scale crises.	- **Technical** - **Social/Human** - **Organizational/Process**

[35] JOIN(2018) 36 final. Brussels 5.12.2018.

[36] Pamment, J. (2020). The EU's Role in Fighting Disinformation: Taking Back the Initiative. Washington, D.C: Carnegie Endowment for International Peace.

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Political, social, administration, information

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

- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments:**
  Member States' governments, municipalities, civil society

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):**
  Average

- **Expected time to TRL-9.**
  1-2 years

- **Expected time to market.**
  2-3 years

DESCRIPTION OF USE CASE(S)

- The Rapid Alert System on Disinformation should link the national SITCEN-s with EU INTCEN via 24/7 operational information exchange platform in cause of time-criticality, especially in times of large-scale crises such as pandemics, irregular immigration flows, etc. The platform should be securely integrated with *EUvsDisinfo* database to enable both hit-based and advanced searches for identifications of (original) sources and spread (possible impact) projections of disinformation (in-)between the member states, regions, municipalities and different societal target-groups.

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 institutions, its Member States' governments and municipalities, empowered analytical capabilities and swiftly coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups, which could be targeted by hybrid activities.

- **Resilience/defensive/offensive**
  Resilience, defensive

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  The existing information exchange platform(s) between the authorities could be the existing vases for further advancements.

RESTRICTIONS FOR USE

- **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.

COSTS	COUNTERMEASURES
- **Indication of costs**: Depends on technical configurations and tender conditions. - **Differentiate, if possible, in development, procurement and exploitation:** Should be EU INTCEN (EEAS) coordinated procurement.	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Different hostile cyber-operations. - **How durable is the idea (how long is the idea expected to be effective/useful?)** 3-5 years
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide**	

3.2 EXPLOITATION OF CRITICAL INFRASTRUCTURE WEAKNESSES AND ECONOMIC DEPENDENCIES

EU-HYBNET responsible partner for this section: STWS

Introduction to the primary context

The cascading effects that can be caused after an attack on a critical infrastructure have raised the concern about the interdependencies of critical infrastructures. However, the strategic dependencies have not been clarified, let alone the aggregated risk and impact implications.

3.2.1 Impact and Risk assessment of critical infrastructures in a complex interdependent scenario

NAME OF THE IDEA

Impact and Risk assessment of critical infrastructures in a complex interdependent scenario

DESCRIPTION OF THE IDEA

This idea is based on a paper by Weilan et al, 2019[37] and on the Critical Infrastructure Resilience Platform (CIRP)[38] developed by Satways Ltd.

The paper by Weilan et al (2019) discusses a decision support approach for CI risk assessment with a holistic consideration of complexity, dual interdependency, vulnerability, and uncertainty. In this study, **A)** CI interdependency can be classified into three types, namely, geographic, functional, and stochastic. **B)** CIs can be regarded as system-of-systems to model the interdependent network structure and each CI can be viewed as a collection of components, where facilities are regarded as nodes and pipelines are treated as undirected edges that link facilities. **C)** Coupling effects are used to represent the influence of CI interdependency on the aggregated risk, and they are classified into complementary, redundancy, and zero.

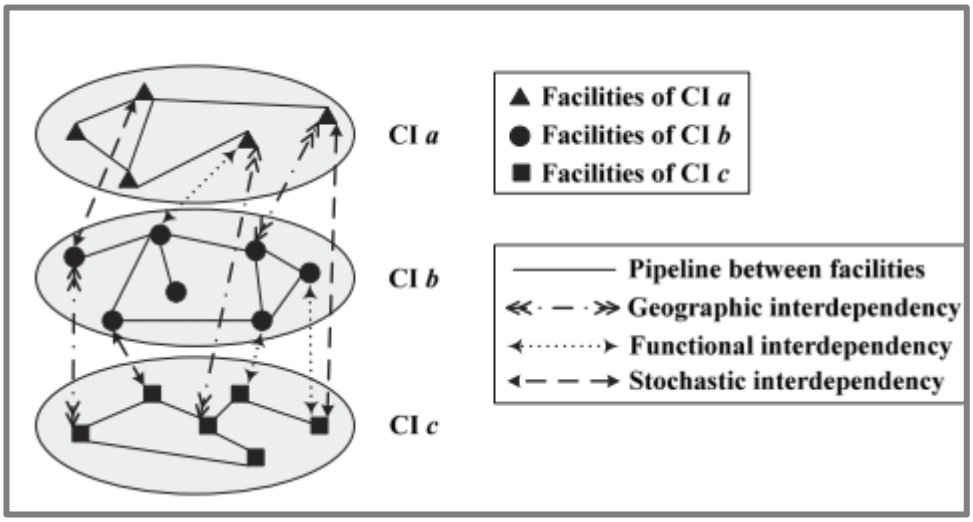

Figure 4 : Representation of the interdependent network structure of CIs (Weilan et al, 2019)

[37] Weilan Suoa, Jin Zhangb, Xiaolei Suna, Risk assessment of critical infrastructures in a complex interdependent scenario: A four-stage hybrid decision support approach, Safety Science, 120, 692-705 (2019).
[38] Kostaridis, A., et al, CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures, 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment

The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment. The essential elements for impact assessment are hazards, assets and the assets' fragility. Hazard is considered as the descriptive parameter quantifying the possible phenomenon within a region of interest. The assets in a region exposed to hazards are defined by an inventory. Finally, fragility is the sensitivity of certain assets of an inventory when subjected to a given hazard.

The implementation of such an algorithm in the CIRP Platform would include the following steps:

a. Development of the asset taxonomy (including for example buildings, departments, infrastructure, servers)
b. Definition of interdependencies of the CIs (including geographic, functional, and stochastic)
c. Calculation of the vulnerability of all assets according to the fragilities defined
d. Selection of a threat scenario that can affect one or more assets
e. Execution of the threat scenario
f. Visualisation of the scenario results

REFERENCE TO CAPABILITY GAP/NEED	**TYPE OF SOLUTION**
- **Describe the use of the solution in reference to the gaps/need** Understanding dependencies will help identify measures to reduce their impact, including diversifying production and supply chains, ensuring strategic stockpiling and promoting production and investment in the EU. - **Applicable JRC domains as stated by the gaps/needs:** Economy, Infrastructure, Cyber, Administration - **Applicable core theme(s) as stated by the gap/need:** Resilient civilians, local level, national administration	- **Technical** - **Social/Human** - **Organizational/Process**

PRACTITIONERS

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

Infrastructure, Administration

- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):** The Ministry of Civil Protection could be informed for interdependencies and their impact for strategic planning in cases of hybrid attack
  - **II) *local level* (cities and regions):** The municipalities should also be involved in this for safety reasons
  - **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**
- Crisis Management experts in municipalities, ministries and critical infrastructures

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 5
- **In which stage is the solution (research, technology, available innovation, proven innovation):** Research
- **Expected time to TRL-9.** Not known

- **Expected time to market.** Not known

DESCRIPTION OF USE CASE(S)

- The CIPR platform has been successfully used in the EU-CIRCLE H2020, the InfraStress H2020 project and currently at the 7Shield H2020 project for modelling, among others, the modelling the impact of climate change to Cis.

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?**
  The platform's backend infrastructure is developed upon the Web Services architectural style, using the Java EE Framework
- A Web client to access the Web Application Graphical User Interface is needed for the user.
- Depending on the size of input data, a server infrastructure with respective processing capabilities is needed.

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:
  Depending on the size and complexity of the infrastructure and interdependencies with other CIs
- **Differentiate if possible in development, procurement and exploitation**
  Development is the most important part of the cost

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Inaccurate modelling of CIs (including asstes' vulnerability and interdependencies can possibly degrade the solution
- **How durable is the idea (how long is the idea expected to be effective/useful?)**

MISCELLANEOUS

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

What-if scenarios can be used for impact and risk assessment that will be used by the practitioners for preparedness, that is identifying measures to reduce the impact of the existing interdependencies.
The Critical Infrastructure Resilience Platform (CIRP) is a collaborative software environment that creates new capabilities for CI policy-makers, decision makers, and scientists by allowing them to use different and diverse modelling and risk assessment solutions, to develop risk reduction strategies and implement mitigation actions that help minimise the impact of climate change on CIs.

3.2.2. Resiliencetool (Incl. Riskradar) Steinbeis Eu-Vri

NAME OF THE IDEA

ResilienceTool (incl. RiskRadar)

Steinbeis EU-VRi (European Risk & Resilience Institute)

DESCRIPTION OF THE IDEA

The ResilienceTool is a web application for performing indicator-based resilience and functionality assessment for critical entities using a tested methodology based on composite indicators organized as a multi-level hierarchical checklist, known as dynamic checklists (DCLs). DCLs allow a dynamic combination of indicators recommended (for a particular sector/industry e.g., standards of IT systems in the transportation sector), and user-specific (e.g., policies applicable to a company or enterprise) indicators for monitoring, stress-testing and reporting of risk-resilience of cyber-physical systems. Further, the tool supports before/after analysis, assessment of existing interdependencies between infrastructures, as well as a multi-criteria decision method (MCDM) based tool for appraisal of resilience enhancing investment options.

The key concept of the methodology involves the "resilience" of an infrastructure which describes its ability to cope with potential adverse scenarios or events that can lead to significant disruptions in its operation or functionality.

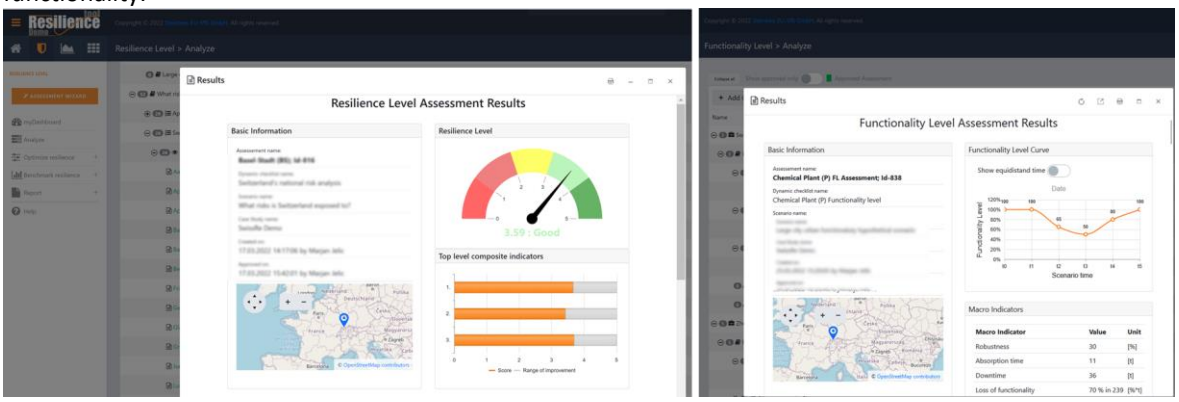

Figure 5 : Screenshots of the Resilience Tool

The RiskRadar tool allows continuous and automated horizon scanning of "emerging risks" related to certain threats including hybrid threats that can potentially result in an "actual" risk in the medium to long term. The tool uses a natural language processing (NLP) algorithm to identify, locate and assess emerging risks by considering risks posed by threats based on factors including Environmental, Socio-political, Economic/Financial, Regulatory/Legal and Technological. It can extract textual data from a wide range of openly accessible documents from sources such as News media, Social media, Scientific publications, and Regulatory and Government agencies. It has been effectively used for the identification and location of different types of perceived and real emerging risks/threats.

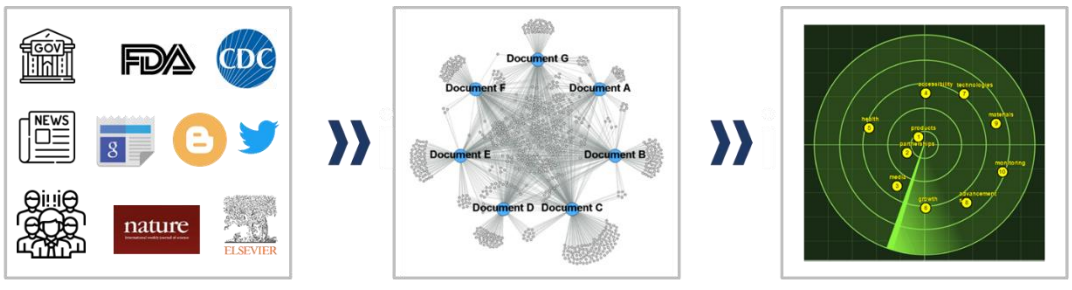

Figure 6 : Illustration of the RiskRadar tool

REFERENCE TO CAPABILITY GAP/NEED	TYPE OF SOLUTION
- **Describe the use of the solution in reference to the gaps/need** Hybrid threats seek to exploit the vulnerabilities of a system or organization using a mix of measures (i.e. diplomatic, military, economic, technological)	- **Technical** The ResilienceTool and the RiskRadar tool are technical solutions developed as web applications. - **Social/Human**

while remaining below the threshold of formal warfare. ResilienceTool including the RiskRadar allows indicator-based assessment of the resilience of infrastructures, cities, communities, states and even countries to plan, prepare and absorb, recover and learn from going through such hybrid (or unknown "x" threats). The tools allow tracking and analyzing emerging risk to all the way it becomes a full-fledged risk thus enhancing resilience by detecting, preventing and responding to hybrid threats. - **Applicable JRC domains as stated by the gaps/needs:** Space, Cyber and Military/defence domains - **Applicable core theme(s) as stated by the gap/need:** o Cyber and Future Technologies	- **Organizational/Process**

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Infrastructure (e.g. space-based services, energy, water, hospitals etc.), Cyber, Information, Social/Societal Economy/Financial, Military/Defence

- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):**
  - **II) *local level* (cities and regions):** to identify gaps within current systems, plans to improve resilience
  - **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**
  From Infrastructure owners, First responders within Tactical (low level), to disaster management agencies, policymakers and governmental bodies at strategic (high level). For industry (to monitor resilience, understand and prepare for threat scenarios and identify gaps within current systems, plan and implement investment options to improve resilience), for policymakers (to have situational awareness, data-driven insights and take relevant and impactful policy decisions).

STATE OF THE ART

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

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Available innovation
- **Expected time to TRL-9.**
  0-2 years

- **Expected time to market.**
  0 (already available)

DESCRIPTION OF USE CASE(S)

- **Use case #1**: Horizon scanning of emerging cyber threats in the energy sector using the RiskRadar tool.
  Actor: Chemical industrial plant security (CPS) manager
  Scenario: The CPS manager uses the RiskRadar to assess the emerging risk environment in the chemical industry, especially focussing on the risks to their plant and surrounding environment from cyber and space interference threats.
  The CPS manager defines their search query in the RiskRadar tool as "(cyber OR space) AND (risk OR threat) AND chemical plant AND Finland", followed by selecting the data source from a list including public/openly accessible webpages from Government agencies, Scientific journals as well as News and

social media. The search includes information generated over the last six months with future searches automatically scheduled to recur every month.
The Risk Radar tool extracts the textual data from web-based sources followed by pre-processing and analysing the textual data using natural language processing (NLP) techniques to calculate indices (e.g. Document centrality etc.). The results in the form of keywords identified as related to emerging risks/threats are ranked based on their criticality (prevalence) with time.
The CPS manager uses the results from the quantitative score of emerging risks to define a specific cyber threat scenario of a Denial-of-service (DDoS) attack on the plant Supervisory control and data acquisition (SCADA) system, which acts as an input for the Functionality level analysis of the chemical plant in ResilienceTool (Use case #2).

- **Use case #2**: Functionality level (FL) analysis of the chemical plant when operations are disrupted due to a DDoS attack to shut down the plant. Furthermore, understand the cascading impact of the scenario on related critical infrastructures.
  Actor: Chemical industrial plant risk (CPR) manager
  Scenario: The CPR manager uses the ResilienceTool and starts a new Case study defining Assets/Vulnerabilities within and outside of the chemical plant and identifying the interdependent infrastructures (see the example in Figure 7 and Figure 8). This is followed by defining a timeline of the threat event from t_1-t_7 and its impact on defined interdependent Assets/Vulnerabilities (the example shown here graphically in Figure 9). This is followed by the FL assessments performed by the CPR manager of all defined Assets/Vulnerabilities. The example of resulting FL curves for the Assets/Vulnerabilities are shown in Figure 10.
  The results from the FL analysis provide insights into the performance of the Assets/Vulnerabilities relative to a predefined theoretical Acceptance limit which is used to identify and improve the response of critical system components to prepare for an actual threat event.

Figure 7 – Defining critical infrastructure Assets/Vulnerabilities (top), followed by identifying interdependencies within them

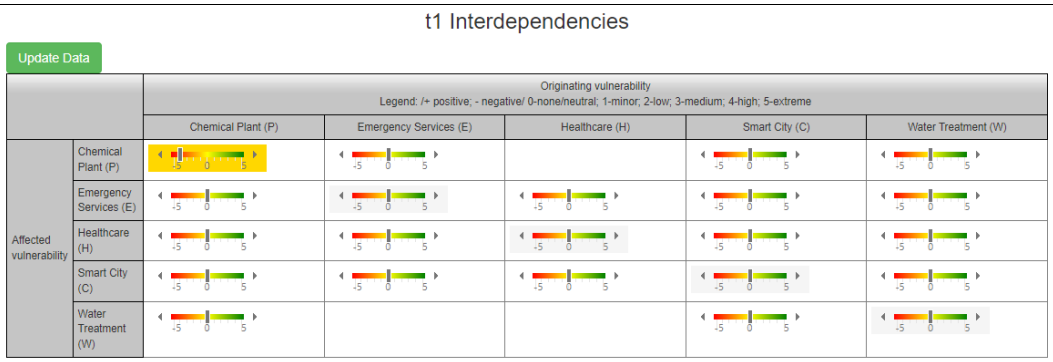

Figure 8 – Defining Impact on interdependent Assets/Vulnerabilities with event-driven time points (figure shows the impacts for time point t_1)

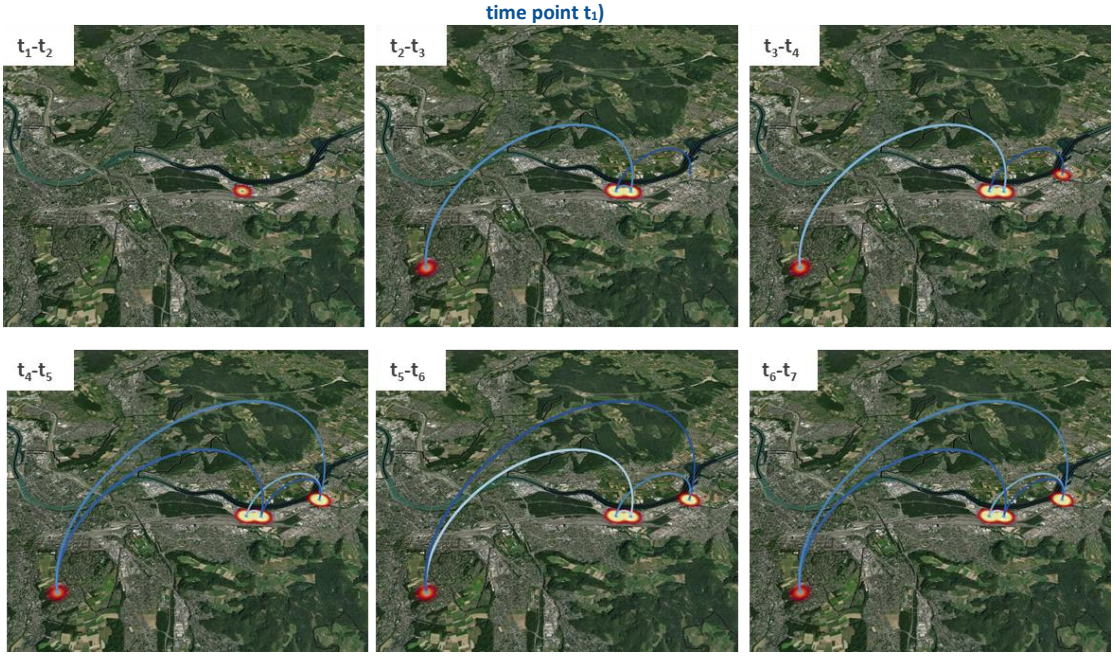

Figure 9 – Visualization of the defined Impacts on Assets/Vulnerabilities for the event-driven time points $t_1 – t_7$

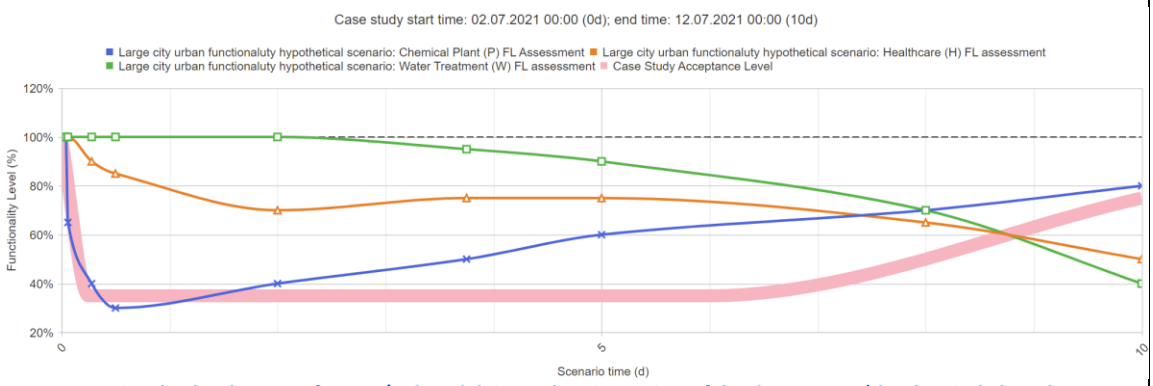

Figure 10 – Functionality level curves of Assets/Vulnerabilities within time points of the threat event (the chemical plant shown in blue) with a theoretical Acceptance level defined (bold pink line)

IMPACT ON COUNTERING HYBRID THREATS

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

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

<table>
<tr><td>ENABLING TECHNOLOGY
- Which technologies are critical in fielding the idea?
- The ResilienceTool: Big data, Digital twin technology
- The RiskRadar tool: Natural language processing (NLP), a subfield of linguistics, computer science, and artificial intelligence (AI)</td><td>RESTRICTIONS FOR USE
- Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
<u>None.</u></td></tr>
<tr><td>COSTS
- Indication of costs (for the entire tool and IT infrastructure):
- 1M-2M€
o Research and Development: 1M-2M€
o Exploitation: 200k-500k€
o Procurement: 100-200k€</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
Cyberattack. However, our systems and processes are compliant with the latest quality and risk management standards.

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

The need for Resilience assessment and horizon scanning is expected to increase with the increase in the number and type of threats and risks in the future.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide
Added Value of the Innovation
The solution offered by the ResilienceTool is big data-oriented, customizable and dynamic in nature that can enable monitoring of operations and provide situational awareness, and adaptable to various threat-vulnerability combinations and anchored in national and international standards (ISO 31050, DIN SPEC 91461). Additionally, the multi-criteria decision making (MCDM) module within the tool allows appraisal of investment options to optimize Resilience (risk analysis, preparedness, absorption, recovery, adaptation) of critical infrastructures exposed to multiple cyber-physical and/or hybrid threats and adverse events.
The RiskRadar tool can be used to identify and prioritize emerging risks related to a wide range of threats including hybrid threats assessed according to their criticality. The criticality is based on two aspects, the first one is how active the topic is currently and how fast the trend in the topic is growing. The tool delivers emerging risk foresight with regular reports with trend analysis of potential risks over time flagging specific risks that communities and policymakers can proactively use for pre-resilience analysis. The tool and regular results will allow identifying, and prioritizing difficult to detect threats (e.g., high impact, low probabilities “black swan” events COVID-19 like pandemic or Russia-Ukraine war) enabling users to plan and prepare to ensure the right mitigations are in place.
Note from the lead author: The innovation is also applicable for §2.1 Space Interference and counterspace weapons</td></tr>
</table>

3.3 EXPLOITATION OR INVESTMENT IN COMPANIES BY FOREIGN ACTORS

EU-HYBNET responsible partner for this section: STWS

Introduction to the primary context

The recent case of Alpi Aviation has brought the attention of the public to the efforts of the European Union to screen foreign investments. Screening is defined in the Regulation (EU) 2019/452 of the European Parliament and of The Council[39] as a procedure allowing to assess, investigate, authorise, condition, prohibit or unwind foreign direct investments.

Awareness of the problem itself has initiated relative discussions in the Member States (MS), as not all MS have national screening mechanisms, which could be a precondition for a successful alignment[40]. Both the exploitation and the investment in companies by foreign actors require a common approach by all MS. In Australia, for example, the Foreign Investment Review Board (FIRB) reviews foreign investment proposals on a case-by-case basis. This is to ensure the investment is not contrary to the national interest or national security[41]. In Canada, the Investment Canada Act and the National Security Review of Investments Regulations address investments injurious to National Security[42].
Such actions naturally require international cooperation. As part of the U.S.-E.U. Trade and Technology Council (TTC), the Investment Screening Working Group focuses on exchanging information on *investment trends impacting security*, including strategic trends with respect to industries concerned, origin of investments and types of transactions. Also, it is engaging with stakeholders to gain perspectives and input from the business community, thought leaders, law firms, academia, and others to help inform the working group's efforts. The European Commission's DG Trade, U.S. Department of Treasury (Treasury) and U.S. Department of State (State) virtually co-hosted the first outreach event on December 2, 2021. The Futurium platform is being used for that purpose.

Regarding the protection of data, it should be mentioned that the Member States and the Commission have concluded a Joint Controllership Arrangement (JCA) -which entered into force on 28 April 2022- in line with data protection rules, notably the GDPR (Article 26), the EDPR (Article 28) and the EU FDI Screening Regulation (Article 14) and the underlying Commission Decision. The JCA is basically an agreement between MS and the Commission on the processing of personal data, and it sets out the allocation of the respective roles, responsibilities and practical arrangements between MS and the Commission: both being joint controllers of these data[43].

The areas set out in the EU for screening by MS authorities include critical infrastructures, critical technologies and dual use areas, supply of critical inputs, access to or the ability to control sensitive information, as well as freedom and pluralism of the media[44]. However, the triggers for screening

[39] Regulation (Eu) 2019/452 Of The European Parliament And Of The Council, Official Journal of the European Union, L79 I/1, 21.03.2019
[40] Ghiretti, F., How To Protect Europe From Risky Foreign Direct Investment, Texas National Security Review, January 2022.
[41] Official website of the Australian Government, Approval for Foreign Investment
[42] Official website of the Government of Canada, Justice Laws Website
[43] European Commission, Enforcement and Protection, Investment Screening, official website
[44] Modrall, J., Foreign Investment Screening: European Union, Norton Rose Fulbright, online article, November 2021.

mechanisms in all countries include[45] (i) the value of a proposed investment (ii) sectors in which an investment is planned to be made (iii) the characteristics of an investment (iv) the type of asset being acquired (v) the extent of ownership/control over the enterprise, and (vi) the share of a product/service market that would be controlled by the enterprise.

A dedicated unit in the Commission with multilingual skills has been proposed to facilitate the identification of cases that could be accidentally remain unnoticed[46]. Additionally, homogenous screening mechanisms by the Member States would facilitate better and clearer picture of existing and emerging acquisitions in the region (Ghiretti, 2022). Mutual recognition of regulatory regimes will allow countries to fast-track foreign investments in their respective jurisdictions[47].

Based on the above, correlation of FDI under screening with any criminal activity would be a common ground for a fast-track screening and universal acceptance of the screening result. The proposed solution builds on the two solutions that were proposed in D3.3, namely a blockchain-based real-time information management and monitoring system and a crawler and real-time search engine for investors.

3.3.1 A Crawler For Correlation Of Screened FDI With Suspicious Financial Activity

<table>
<tr><td colspan="2">NAME OF THE IDEA
A crawler for correlation of screened FDI with suspicious financial activity
DESCRIPTION OF THE IDEA
The main goal of this idea is to have strict procedures for the investigation of screened FDI, and at the same time exchange information with practitioners active in preventing criminal activity. The rational for this approach is based on the fact that such hybrid attacks would require some logistical infrastructure (such as illegal residencies) as well as anonymous bank accounts to fund relevant actions. Therefore, the ability to link screened FDI with various types of suspicious financial activity would provide evidence for rejecting such investments. The cooperation of the FDI screening practitioners with the practitioners active in preventing criminal activity could be enabled by a crawler that would automatically search for investors' information relative to suspicious financial activity and detect hidden connections with other investors, but also with entities that are engaged in illegal or criminal activities.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- Describe the use of the solution in reference to the gaps/need
In that way, the Member States can 'take into account whether the investor has been involved in activities affecting security or public order or whether there is a serious risk of the investor being engaged in illegal or criminal activities ' and perform the assessment on a case-by-case basis.

- Applicable JRC domains as stated by the gaps/needs:</td><td>TYPE OF SOLUTION
- <u>Technical</u>
Crawling, Search Engine
- Social/Human
- <u>Organizational/Process</u></td></tr>
</table>

[45] Stormy-Annika Mildner. Claudia Schmucker, Policy Brief, 'Investment Screening: Protectionism and Industrial Policy? Or Justified Policy Tool to Protect National Security?'

[46] Ghiretti, F., Screening foreign investment in the EU – the first year, Merics Mercator Institute for China Studies, October 2021

[47] Vasuki Shastry, How countries can regulate investment screening, Chatham House, April 2022

- Economy, Political, Intelligence, Administration, Diplomacy
-
- **Applicable core theme(s) as stated by the gap/need:**
  Resilient civilians, local level, national administration.

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
- **Economy, Political, Intelligence**

- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):** The Ministry that is responsible for screening FDI
  - **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**
  Ministry that is responsible for screening FDI , Police, Organised Crime Units

STATE OF THE ART

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

- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  The solution still needs to overcome the problem that the information that can be found in the internet is in various formats
- **Expected time to TRL-9.** 3 years

- **Expected time to market.** 4-5 years

DESCRIPTION OF USE CASE(S)

- Google and Bing search engines use web crawlers

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 Idea supports the Member States in applying Regulation (EU) 2019/452 of the European Parliament and of The Council. Therefore, it supports the protection of the Union from foreign actors trying to influence or take control of European firms.
- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Computer Vision, Information retrieval

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
- Legal: the Member States and the Commission have concluded a Joint Controllership Arrangement (JCA) - entered into force on 28 April 2022- in line with data protection rules, notably the GDPR (Article 26), the EDPR (Article 28) and the EU FDI Screening Regulation (Article 14)
-

COSTS	COUNTERMEASURES
- **Indication of costs**: - **Differentiate if possible in development, procurement and exploitation**	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? no - **How durable is the idea (how long is the idea expected to be effective/useful?)** It is expected to be effective for as long as the foreign actors use such methods.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide**	

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

4.1 INFORMATION MANIPULATION WITH THE AIM OF DESTABILIZATION

EU-HYBNET responsible partner for this section: L3CE.

Introduction to the primary context

Information manipulation is widely used instrument by different actors. It might serve different purpose, varying from very situational, aiming at short term responses, to long term, aiming to construct wanted perception of certain phenome or construct attitudes of some target group(s) in the society. Different tools can be used for information manipulation, from traditional social media platforms to more difficult to access encrypted message services. In the context of hybrid threats information manipulation can be treated as a standalone threat, or integral component of complex adversarial campaign. This chapter considers specific aspect of information manipulation used to destabilisation.

An outcome of information manipulation aiming at destabilisation are actions. Those actions can be considered as a result of attitudes of certain groups of society. Construction (changing, reinforcing, etc.) of attitudes is usually made applying some narratives (a way of presenting or understanding a situation or series of events that reflects and promotes a particular point of view or set of values[48]).

Identification of those attempts is the first step in countering disinformation. Further counter measures should be taken, including analysis of disinformation sharing, understanding and describing the disinformation attempts, share those descriptions, plan and implement short term and long-term actions. All this process requires relevant tooling and methodologies.

4.1.1 Increasing Capabilities to Systematically Assess Information Validity Throughout The Lifecycle

NAME OF THE IDEA
Increasing capabilities to systematically assess information validity throughout the lifecycle
DESCRIPTION OF THE IDEA
There are different initiatives aiming to identification and debunking of disinformation. Some of them are crowdsource base, some relay or media practitioners. Majority of such initiatives are focused on the detection of fake information at a given point in time. Outcome of debunking or fact checking activities are usually “story-to-story” type (a new, rational, fact-based story, denying fake one, usually based on emotions, rather than facts. is developed) and tailored as a response to be used by media to users, possessing critical thinking that can empower citizens and journalists to avoid falling pray to online disinformation. Attitudes are constructed over long period of time, thus separate disinformation events (Information attacks) could be linked to the narratives (or vectors), as a long term targets. Understanding that identification is only the first step, effective countering of disinformation requires more complex solutions that integrates set of tools that allow to trace sources of identified fakes, make analysis of spreading of such information identifying involved bots and artificial accounts. Description of the disinformation, by providing structured information on narrative, targets and other components is also to be included in the information validity verification workflow. Such description should be made available for interested stakeholders.

[48] Narrative Definition & Meaning - Merriam-Webster

To make a significant impact, such platform should be widely used and recognised by different stakeholders and cover complete information validation verification workflow. It should also be linked with LEA's to be applicable for criminalization if needed.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  Improving tools to tackle information manipulation and further measures to counteract information manipulation.
- **Applicable JRC domains as stated by the gaps/needs:**
  It can be related to helping countering disinformation across all 13 domains, especially political, economy
- **Applicable core theme(s) as stated by the gap/need:**
  - Information and Strategic Communications. Also links to Resilient Civilians, Local Level and National Administration

TYPE OF SOLUTION

- **Technical**
  - software tooling
  - Information sharing environment
- **Social/Human**
  - Multidisciplinary engagement
- **Organizational/Process**
  - Methodological solutions
  - Co-creation capabilities
  - Utilisation of national / business initiatives

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  All domains, especially political and economy.
- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):** High level planning of narrative supporting
  - **II) *local level* (cities and regions):** Managing disinformation outcomes
  - **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**
  Wide spectrum of end-users can be identified for the idea provided. First of all, those are policy makers and strategic communication specialists at different levels. Media outlets, education institutions are also to be named as end-users.

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  Current solutions, covering debunking and fact checking scope in different countries (e.g.: Debunk EU in Lithuania, Maldita in Spain, etc.) or internationally are TRL 9 level.
  Technologies enabling social media monitoring to identify disinformation sources, sharing patterns, clustering are also available at TRL 9.
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Despite availability of separate technological and methodological solutions, there is no methodological solution, supported by technological means, to cover the full workflow.
  European Digital Media Observatory can be considered as similar initiative. No reasonable evaluation of EDMO TRL level can be provided at this time.
- **Expected time to TRL-9.**
  Can be developed within 3-5 years if based on current initiatives.
- **Expected time to market.**
  Same estimation is applicable.

DESCRIPTION OF USE CASE(S)

As it was mentioned, there are some separate solutions, that can be listed as prospect components of the full workflow concept. Few to be mentioned:

- In VID and WeVerify projects some relevant tooling – Verification Plugin and Truly Media Workbench (Tools - WeVerify) (Description - InVID project (invid-project.eu) was developed. Those can be an examples how separate components can be developed. Project also provides the concept of complete content verification workflow that can be developed further for the EU wide implementation.
- FANDANGO project (fandango-project.eu) can be another example. Project aims to break data interoperability barriers providing unified techniques and an integrated big data platform to support traditional media industries to face the new "data" news economy with a better transparency to the citizens under a Responsible, Research and Innovation prism. Some relevant tools are collected within the scope of the project (Tools | FANDANGO (fandango-project.eu)).
- Project defalsif-AI is another good example of employing AI aiming to media content for credibility and/or authenticity. Project also plans to link content analysis to legal and ethical perspective (defalsif-AI - AIT Austrian Institute of Technology).
- Project AI4media focus on AI technologies to improve support tools used by journalists and fact-checking experts for digital content verification and disinformation detection. New AI-based features will be made available within two existing journalism tools: Truly Media (a web-based platform for collaborative verification) and TruthNest (a Twitter analytics and bot detection tool). (AI4media project)
- European Digital Media Observatory (EDMO's Vision And Mission – EDMO) is an initiative of a different nature, being not a technical initiative, but more oriented towards methodological and involvement aspects. EDMO brings together experts and organizations from digital media fields in the widest sense, including fact-checkers, academic researchers, media professionals, media literacy experts to better understand and analyse online disinformation. The EDMO BELUX's (Belgium-Luxembourg Digital Media and Disinformation Observatory) provides information about basic facts-checking techniques (Fact-Checking Toolkit – EDMO Belux).
- DESARM Framework (Framework (disarm.foundation)) can be explored as potential tool to connect all technical components through the complete workflow.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Better structured identification, analysis, description and sharing of disinformation can contribute by countering it in long term perspective, building new narratives and identify actors, involved in destabilisation activities.

- **Resilience/defensive/offensive**
  Effective management of evolving narratives make significant impact on resilience. Clear understanding adversary narratives can lead to more effective offensive actions as well.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
- Platform covering whole workflow
- Information sharing capabilities
- Visualization functionality

RESTRICTIONS FOR USE

- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?**
  No restrictions, just concerns:
  - Ethical application of AI
  - Trusted and secure information exchange

COSTS	COUNTERMEASURES
- **Indication of costs**: Not possible to estimate now. - **Differentiate, if possible, in development, procurement and exploitation** NA	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Can be compromised by fake actors involved. Can lose credibility due to security issues, bias propositions etc. - **How durable is the idea (how long is the idea expected to be effective/useful?)** Can lose importance with changing social media technologies, becoming difficult to access, niche solutions.
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide** Comprehensive platform can and should be build using current EU initiatives.	

4.1.2 Crowdsourced Verification Systems Of Fake News To Counter Disinformation In Encrypted Messaging Applications

NAME OF THE IDEA

Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications

DESCRIPTION OF THE IDEA

In recent years we are facing a strong grow of disinformation spread through the social media platforms such as Facebook, Twitter, YouTube. Some of them might be focused on intention to increase their social media marketing and visibility, gain more followers, make business, or create a distraction. Nevertheless, the mainstream platforms invested a great deal of work and resources to understand and combat disinformation by implementing a variety of tools to prevent false content appearing.

In response to the changing environment, actors who have been pushed off mainstream platforms started active migration to unregulated spaces that are more secretive and specialized, such as Telegram, WhatsApp. Platforms based on encrypting messaging services act as places for groups to create large followers, communities and broadcast messages in their own, unregulated, news feeds that can be accessed by anyone[49].

Important to note, that encrypted messages application (EMAs) gaining more popularity between different groups of society, and the reason behind users seeks for more privacy and security for their digital lives. Telegram, WhatsApp recently became a perfect place in which propaganda thrives and spreads online with limited means of detection, monitoring and prevention. The key objective of these platforms, for both users and for those seeking to manipulate them, is the ability to create relationally close-knit information silos. These more secure digital spaces are populated by anywhere from two to several hundred people who have a broader shared identity. Encrypted spaces are uniquely vulnerable because they require the development of specialized strategies to counter disinformation without compromising the security of a given platform[50].

In the advent of growing cyber threats, the attempts to combat spread of disinformation are focused on the innovative technologies that automatically can detect fake news and fact-checkers and verify the statements contained in news or opinion articles. However, fact-checkers can access very small part of online information and their attempts not always achieve desired effect with the risk of non-detecting and preventing disinformation at the early stage of dissemination. Thus, the crowdsourcing could be an effective tool to make fact-checking more scalable and more protective from allegations of bias.

However, due to the limited access to encrypted messages academia has very limited possibilities to initiate new research on disinformation spread through encrypted messaging platforms.

Considering the barriers described above, the key attention of research could be focused on the deeper analysis of mass public broadcasts offered by EMAs in addition to the private messaging services. There are a few state-of -the-art technology solutions available in the market, however due to the legal and privacy issues and limited access to the data, next generation tools that would bring drastically changes to fighting online disinformation in the closed social platforms are still at an early stage of development.

[49] Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. Terrorism and Political Violence, 31(6), 1242-1254. https://doi.org/10.1080/09546553.2017.1339695 ↩

[50] Reis, J., Melo, P. D. F., Garimella, K., & Benevenuto, F. (2020). Detecting Misinformation on WhatsApp without Breaking Encryption. arXiv preprint arXiv:2006.02471. ↩

REFERENCE TO CAPABILITY GAP/NEED

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

Improving tools to tackle information manipulation in EMA's and further measures to counteract information manipulation

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

It can be related to helping countering disinformation across all 13 domains, special focus to information and cyber

- **Applicable core theme(s) as stated by the gap/need:**
  - Information and Strategic Communications. also links to "Resilient Civilians, Local Level and National Administration"

TYPE OF SOLUTION

- **Technical**
  - Software tooling
  - Information sharing environment
- **Social/Human**
  - Multidisciplinary engagement
- **Organizational/Process**
  - Methodological solutions
  - Co-creation capabilities
  - Utilisation of national / business initiatives

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  All domains, especially information and cyber.

- **Provide the level of practitioners in the same discipline:**
  - **I) *ministry level* (administration):** New policy and legislative measures for encrypted messaging service providers, however the freedom of expression must be considered.
  - **II) *local level* (cities and regions):** managing disinformation outcomes
  - **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):**

  Wide spectrum of end-users can be identified for the idea provided. First of all, those are policy makers and strategic communication specialists at different levels. Media outlets, education institutions, law enforcement agencies, Stratcoms are also to be named as end-users.

STATE OF THE ART

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

Current technology solutions for investigating content in encrypted messaging app.

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

Solution is in the status of available innovation

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

Can be developed within 3-5 years if based on current initiatives.

- **Expected time to market.**

Same estimation is applicable.

DESCRIPTION OF USE CASE(S)

As it was mentioned, there are some separate solutions, that can be listed as prospect solutions:

- **FACTS system (**Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Compliant Tally Systems) (https://arxiv.org/abs/2109.04559).

  FACTS system tracks user complaints on messages obliviously, only revealing the message's contents and originator once sufficiently many complaints have been lodged. FACTS system is:

  - private, meaning it does not reveal anything about the senders or contents of messages which have received few or no complaints
  - secure, meaning there is no way for a malicious user to evade the system or gain an outsized impact over the complaint system
  - scalable, as we demonstrate excellent practical efficiency for up to millions of complaints per day.

  FACTS main technical contribution is a new *collaborative counting Bloom filter*, a simple construction with difficult probabilistic analysis, which may have independent interest as a privacy-preserving randomized count sketch data structure.

- **PHEME project** (https://www.pheme.eu). The project combines big data analytics with advanced linguistic and visual methods. The results are suitable for direct application in medical IS and digital journalism. Set of tools aimed to empower users and journalist to tackle disinformation developed and tested in real world conditions:
  - Graph visualization- flexible graph visualization library to investigate the evolution of online dialogues
  - Social media thread processing- the conversation collection script allows the user to collect the set of tweets replying to a specific tweet, forming a conversation or a thread
  - Rumour categorization- Tracking the spread of rumours online detecting if a message support denies, or queries the claim.
  - Multilingual pre-processing- social media processing in English, Bulgarian.
  - Datasets - rumour analyses-journalism use case and medical use case.
  - Temporal models of events- code for Hawkes Process models of the intensity of event discussion over time
  - Entity recognition- a generic entity recognition tool extended to other tasks such as event annotation and timely recognition
  - Capturing- collects social media from various sources, feed in it forward for processing.

IMPACT ON COUNTERING HYBRID THREATS

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

Better structured disinformation detection, analysis process automation, description and sharing of disinformation can contribute to the more effective ways of countering it in long term perspective, identify actors, involved in destabilisation activities and building response means.

- **Resilience/defensive/offensive**

Next generation tools based on AI technologies in combination with new investigation methods and techniques can close the gaps needed for effective response actions to disinformation campaigns and improve intelligence capabilities on serious criminal developments in closed communication environments.

<table>
<tr><td>ENABLING TECHNOLOGY
• Which technologies are critical in fielding the idea?
Automated fact- checking and verification tools for tackling disinformation in Encrypted Messaging applications</td><td>RESTRICTIONS FOR USE
• Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?
Might be ethical and legal implications on technology solutions used for encrypted platforms</td></tr>
<tr><td>COSTS
• Indication of costs:
Not possible to estimate now.

• Differentiate, if possible, in development, procurement and exploitation
NA</td><td>COUNTERMEASURES
• Are there any potential countermeasures that could degrade the effectiveness of the solution?
Can be compromised by fake actors involved. Can lose credibility due to security issues, bias propositions etc.

• How durable is the idea (how long is the idea expected to be effective/useful?)
Can lose importance with changing social media technologies, becoming difficult to access, niche solutions.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide</td></tr>
</table>

4.1.3 DDS-ALPHA (EEAS)

Responsible partner for this section: STWS

Introduction

Steering conflicts has been an old and successful strategy in all kinds of warfare, and this includes disinformation. Fast and efficient communication between stakeholders is therefore imperative in order to prevent or mitigate the effects of such actions.

<table>
<tr><td colspan="2">NAME OF THE IDEA
DDS-alpha (EEAS)

DESCRIPTION OF THE IDEA
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. We introduce an inclusive set of open tools, frameworks and standards, adapted from the cybersecurity sector and best-case practices on information manipulation and interference (IMI) analysis to provide the most comprehensive database on informational threats. DDS-alpha allows for all stakeholders with information on IMI activities in government, international organisations, civil society, the private sector and academia to pool, extract and recombine those insights to enable a wide range of countermeasures and products, depending on the stakeholders' needs and capabilities. It will also offer new insights on the threat, enabling new and faster means to achieve situational awareness or build new products.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- Describe the use of the solution in reference to the gaps/need
EU-HYBNET Policy Brief No3 noted that IMI activities and campaigns and the mitigation of their effects, affect and involve a large number of stakeholders on domestic, EU and international level which all need to exchange information. According to the brief, effective sharing of relevant threat-related information between these stakeholders is limited by three factors: 1) the lack of a commonly accepted and jointly used taxonomy for IMI and TTPs (Tactics, Techniques and Procedures), 2) the confidentiality of some of the information and 3) the inaccessibility and non-machine-readable format information is currently shared. To achieve common situational awareness within reasonable delays, EEAS proposes a set of mutually reinforcing elements from standards to tools which will overcome this information exchange problem and pave the way for an evidence-based development and application of solutions as well as facilitating new innovation.

- Applicable JRC domains as stated by the gaps/needs:
Information, cyber

- Applicable core theme(s) as stated by the gap/need:
o Information and Strategic Communications</td><td>TYPE OF SOLUTION
- <u>Technical</u>

- Social/Human

- <u>Organizational/Process</u></td></tr>
</table>

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Information, cyber.

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

  Primarily tactical
- **Provide the expected end-users of the idea (such as NGO's, private citizens, private companies, media outlets, police, firefighting departments**
- The solution will serve the governmental and security sector which requires in-time and complete information on the security situation to enable fast reaction. Private sector companies (particularly online platforms) will benefit from a systematic inflow of threats observed and flagged to them for interventions. Academia may be the biggest benefactor as for the first time structured data on IMI and hybrid threats will be made available for research.

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: TRL5-7

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

- **Expected time to TRL-9.** End of 2023

- **Expected time to market.** End of 2022

DESCRIPTION OF USE CASE(S)

- Consolidation of available information on IMI in a queryable dataset for government purposes to identify developing trends, provide focused support and recommendations to stakeholders
- Facilitate information exchange on a more granular basis between stakeholders, in particular NGOs to platforms communication and vice versa. Civil society can efficiently flag signals to platforms and receive enriched information within the same data standard back from platforms.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
- Hybrid threats only reveal themselves after they have been exploited. If the exploits remain unidentified or the scope of the exploitation remains unknown, no or wrong countermeasures may be taken. The innovation described above leverages a diverse network of stakeholders to collectively highlight the biggest current and emerging threats and thus help to act in a targeted way, focusing resources and attention. Only by aggregating individual stakeholders' insights, can the complete picture of the threat landscape be made visible. Necessary components of data standards and common taxonomy to enable aggregation are part of the innovation.
-
- **Resilience/defensive/offensive**

ENABLING TECHNOLOGY	**RESTRICTIONS FOR USE**
- **Which technologies are critical in fielding the idea?** - STIX (data standard), TAXII (data exchange protocol) , Graph databases, Open Source development: React, GraphQL, ElasticSearch, Redis, MinIO	- **Are there any restrictions with respect to using the solutions, e.g.: legal, ethical, security, etc.?** - Some information is sensitive and would fall under confidentiality. The granularity of the data and settings to determine user rights addresses this restriction

<table>
<tr><td></td><td>- Making all data available for all stakeholders may have GDPR considerations which require vetting, training and standardising which information can be stored in the system for various stakeholders.</td></tr>
<tr><td>COSTS
Indication of costs:
The system runs on open source solutions on consume for a small NGO or individual researchers the cost of running a small scale server (<100€ per year). Professional setup, hosting and maintenance accounts for 100.000€ mostly for HR. Larger options for large enterprises and commercial use would go beyond that.

-
- Differentiate if possible in development, procurement and exploitation
- Exploitation will hold the highest part in the costs as development is carried out by an Open Source community for users that do not require custom solutions</td><td>COUNTERMEASURES
- Are there any potential countermeasures that could degrade the effectiveness of the solution?
- If not enough stakeholders adopt the solution its setup and maintenance costs may be too high.
- Low quality standards when inputting data into the network will lead to low quality outcome and requires training and a shared methodology.

- How durable is the idea (how long is the idea expected to be effective/useful?)
- The idea remains useful as long as counter hybrid activities are a network activity. Lessons from cybersecurity show that the solutions remains relevant while the threat continues to exist.</td></tr>
<tr><td colspan="2">MISCELLANEOUS
Any additional remarks/disclaimers/comments/information you might want to provide
Added Value: There are currently no available solutions addressing the challenge of making up-to-date, complete and machine-readable data on IMI activities available to all stakeholders to inform products and countermeasures. We want to replace a multitude of incompatible and incomplete bilateral, text-based information exchange means with a common approach accessible and usable for all stakeholders.</td></tr>
</table>

4.2 FOREIGN INTERFERENCE IN KEY INFORMATION INSTITUTIONS

EU-HYBNET responsible partner for this section: ICDS

Introduction to the primary context.

Recently adopted EU Strategic Compass for Security and Defence (7371/22, 21 March 2022) emphasize that cyberspace has become a field for strategic competition, at a time of growing dependence on digital technologies and that the EU and its member states increasingly facing more sophisticated cyberattacks (p. 12). Furthermore, the armed aggression against Ukraine is showing the readiness to use the highest level of military force, combined with hybrid tactics, cyberattacks, foreign information manipulation and interference (p. 7). Thus, the EU Cyber Defence Policy is needed to be better prepared for and respond to cyberattacks (p. 6), increasing cyber resilience of transport infrastructure and its support systems (p. 20), enhance the protection of most critical processes, assets, and information, and ensure that it can rely on robust and trustworthy information and adequate European communication systems (p. 21).

4.2.1 Integrated Monitoring System Against Malware-Based Cyber Operations

<table>
<tr><td colspan="2">NAME OF THE IDEA
Integrated Monitoring System Against Malware-Based Cyber Operations

DESCRIPTION OF THE IDEA
Several cyber operations use wiper malwares exploiting supply chain weaknesses, which cause cascading- and ‘spill-over’ side-effects for inter-connected customers. Some examples cover Viasat Outage against Ukraine, which harmed tens of thousands of systems in Europe, including German energy company Enercon or HermeticWiper (known also as ‘FoxBlade’), which ‘spilled-over’ several European countries in parallel with attacking hundreds of Ukrainian IT-systems.

Integrated Monitoring System against malware-based cyber operations should enable more rapid Alert-exchanges between N-CERT-s, CERT-EU, mil CERT and private companies, especially those who provide vital services, vital services related-services, critical infrastructure protection and/or important informational services to increase the speed of early warning and EU-wide coordinated action.</td></tr>
<tr><td>REFERENCE TO CAPABILITY GAP/NEED
- Describe the use of the solution in reference to the gaps/need
Improve rapid Alert-exchanges between N-CERT-s, CERT-EU, mil CERT and private companies, especially those who provide vital services, including critical infrastructure protection and important informational services to increase the speed of early warning and EU-wide coordinated action.

- Applicable JRC domains as stated by the gaps/needs:
Political, culture. Also links to cyber, economy, infrastructure</td><td>TYPE OF SOLUTION
- <u>Technical</u>

- Social/Human

- <u>Organizational/Process</u></td></tr>
</table>

- **Applicable core theme(s) as stated by the gap/need:** ○ Resilient information- and protected cyber environment.	

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Political, culture, cyber, economy, infrastructure

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

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**: 5

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

- **Expected time to TRL-9.**
  1-2 years

- **Expected time to market.**
  2-3 years

DESCRIPTION OF USE CASE(S)

- Increased EU capability quickly respond to cyberattacks, including state-sponsored malicious cyber activities targeting vital services, critical infrastructure, malware- and ransomware attacks in a swiftly coordinated manner. Improved interoperability and information exchange, strengthened cybersecurity and capacity to counter cyber-enabled information operations.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Pro-active mitigation of cyber- and cyber-enabled interference threats to the EU's vital services and critical infrastructure-, including information institutions.

- **Resilience/defensive/offensive**
  Defensive, resilience

ENABLING TECHNOLOGY	RESTRICTIONS FOR USE
- **Which technologies are critical in fielding the idea?** Very highly secured data-exchange systems.	- **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.
COSTS	**COUNTERMEASURES**
- **Indication of costs**: Depends on technical configurations and tender conditions. - **Differentiate, if possible, in development, procurement and exploitation** Should be initiated, coordinated, and procured by CERT-EU and mil CERT.	- **Are there any potential countermeasures that could degrade the effectiveness of the solution**? Misfit of (very) different IT platforms and vulnerabilities to new types of cyber-attacks. - **How durable is the idea (how long is the idea expected to be effective/useful?)** 3-5 years
MISCELLANEOUS **Any additional remarks/disclaimers/comments/information you might want to provide**	

4.2.2 Integrated Monitoring System Against Cyber-Enabled Information Operations

NAME OF THE IDEA

Integrated Monitoring System Against Cyber-enabled Information Operations

DESCRIPTION OF THE IDEA

In addition to different cyber operations, the hostile actors use various cyber-enabled information operations in their targeted hybrid activities. The cyber-enabled information operations combine different cyber-attacks with hostile informational interference to deceive or discredit the targeted subject(s) such as *Hack & Release* -type of operations, including active *phishing*; *Site Capture* and 'make it faceless' -type of operations; *Cloned Websites* and exploitation and/or special types of forgeries, including *Deepfake* operations.

The idea is aimed to enable more rapid identification and Alert-exchanges about cyber-enabled information operations between N-CERT-s, CERT-EU, mil CERT, various national and local authorities and private companies for time-critical responses and cooperative counter-efforts to mitigate the risks and damages of such types of hostile operations.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need:**
  Improve rapid Alert-exchanges between N-CERT-s, CERT-EU, mil CERT, various national and local authorities and private companies for time-critical responses and cooperative counter-efforts to mitigate the risks and damages of such types of hostile operations.
- **Applicable JRC domains as stated by the gaps/needs:**
  Political, culture. Also links to cyber-informational, society, economy, infrastructure
- **Applicable core theme(s) as stated by the gap/need:**
  - Resilient information- and protected cyber environment.

TYPE OF SOLUTION

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

PRACTITIONERS

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

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):**
  Average
- **Expected time to TRL-9.**
  1-2 years
- **Expected time to market.**
  2-3 years

DESCRIPTION OF USE CASE(S)

The cyber-enabled information operations such as *Hack & Release* -type of operations, including active *phishing*; *Site Capture* and 'make it faceless' -type of operations; *Cloned Websites* and exploitation and/or special types of forgeries, including *Deepfake* operations can cause remarkable damage to legal authorities, democratic leadership, and societies, having different cascading effects and misbehaviour, especially in times of crises.

The idea is aimed to enable more rapid identification and Alert-exchanges about cyber-enabled information operations between N-CERT-s, CERT-EU, mil CERT, various national and local authorities and private companies for time-critical responses and cooperative counter-efforts to mitigate the risks and damages of such types of 'threat multiplying' hostile operations.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Pro-active mitigation of cyber- and cyber-enabled interference threats to the societies, vital services and critical/important infrastructure-, including information institutions.
- **Resilience/defensive/offensive**
  Resilience, defensive

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  Very highly secured data-exchange systems.

RESTRICTIONS FOR USE

- **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.

COSTS

- **Indication of costs**:
  Depends on technical configurations and tender conditions.
- **Differentiate, if possible, in development, procurement and exploitation:**
  Should be initiated, coordinated, and procured by CERT-EU in cooperation with EEAS and N-CERT-s.

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Misfit of (very) different IT platforms and vulnerabilities to new types of cyber-attacks.
- **How durable is the idea (how long is the idea expected to be effective/useful?)**
  3-5 years

MISCELLANEOUS

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

4.3 PROMOTED IDEOLOGICAL EXTREMISM AND VIOLENCE

EU-HYBNET responsible partner for this section: L3CE

Introduction to the primary context

Promotion of extremism and violence in different communication channels can be considered as primary the legal issue – how and at which point expressions can be criminalised. But it also can be considered as an area of continuous intensity level monitoring. Most of violent actions do not appear accidentally, attitudes of individuals or groups are intensified emotionally and this lead to action. Promotion of ideological extremism and violence is very much related to the information manipulation and can be linked to innovative ideas described in chapter "4.1 INFORMATION MANIPULATION WITH THE AIM OF DESTABILIZATION". Thus, targeted monitoring of intensity of expression can provide insights on possible evolution scenario.

Social media providers themselves demonstrated attempts to avoid accountability for the spread of misinformation, violent extremist content and incitements to terror on their platforms during the observed period. Even though it is more and more evident, that social platforms provide new possibilities for spread of extremism and violence. Interesting facts can be found in Facebook internal report [51]on the impact of the algorithms.

The Bergen Plan of Action[52], being the recent relevant document, proposes that an independent body of moderators should be used across all tech companies to better enable transparency and accountability surrounding moderation. Moderators would also be supported with counselling and mental-health resources since the nature of the content they're exposed to can be immensely distressing.

> „Ultimately, a multi-stakeholder solution — including governments, tech platforms and civil society — that can be meaningfully adopted by each sector is an ambitious but vital task to prevent future events like the Capitol Hill insurrection and radical-right terrorist attacks like the 2011 tragedy in Norway.[53]"

This chapter focuses on ideas, that can help monitor and measure expressions in different communication platforms. For that reason, relevant promotion should be identified and horizontal (widening) and vertical (intensity) should be monitored.

[51] Facebook did not act on own evidence of algorithm-driven extremism | E&T Magazine (theiet.org)
[52] The Bergen Plan of Action (squarespace.com)
[53] Is Big Tech Ready to Tackle Extremism? The Bergen Plan of Action - VOX - Pol (voxpol.eu)

4.3.1 Collection and Sentiment Analysis of Targeted Communication

NAME OF THE IDEA

Collection and sentiment analysis of targeted communication

DESCRIPTION OF THE IDEA

Even though extremism and violence content is criminalised in EU, it still available through online sources. Identification, collection and evaluation of hate content and radicalization on the web remains a significant challenge which pose a threat to democracy.

There are several components to be considered while handling harmful content. First it should be detected, properly collected for forensic purposes. At the same time, it should be monitored, as semantic indicators, analysed as sentiments, can provide understanding of intensity and help predict violence events. Content should be also classified according to legal paragraphs from a criminal law perspective.

At the core of idea is the continuous platform to handle targeted extremism and violence communication and sharing from identification to sentiments monitoring and to criminalization.

Currently there are many initiatives providing capabilities to handle harmful content in different stages, but there is no unified platform, covering most important aspects together.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  It will limit widening of extremism and violence involvement in online environment. Provide insights to prevent violent events.

- **Applicable JRC domains as stated by the gaps/needs:**
  Legal, cyber, culture, social, legal, intelligence, information.

- **Applicable core theme(s) as stated by the gap/need:**
  - Information and Strategic Communications. Links also to "Resilient Civilians, Local Level and National Administration"

TYPE OF SOLUTION

- **Technical**
  - software tooling
  - Integration
- **Social/Human**
  - Sentiment analysis
- **Organizational/Process**
  - Methodological solutions

PRACTITIONERS

- **Provide applicable JRC domains for which the idea is valuable:**
  Cyber, culture, social, legal intelligence, information.

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

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  There are initial solutions at high TRL level (8-9).
- **In which stage is the solution (research, technology, available innovation, proven innovation):**
  Some separate solutions are available, integration and additional developments are needed.
- **Expected time to TRL-9.**
  Difficult to identify.
- **Expected time to market.**

Difficult to identify.

DESCRIPTION OF USE CASE(S)

There are some separate initiatives, that can be listed as prospects for wide adoption and improvement:

- Platforms like HENSOLDT (Sensor Solutions | HENSOLDT) should be considered for the adaption for the Treat identified.

- Another example can be RAIDAR project. (RAIDAR - Rapid Artificial Intelligence based Detection of Aggressive or Radical content on the Web | KIRAS Sicherheitsforschung). The innovations of RAIDAR include the development and definition of metrics, measures and methods for quantitative and qualitative evaluation of online hate and radicalization.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Restrains diffusion of extremism and violence content and increase predictive capabilities.

- **Resilience/defensive/offensive**
  Increase resilience to violence.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
  - Multilingual sentiment analytics
  - Integration

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:
  Not possible to estimate now.

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

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Extremism and violence move to new safer platforms, making it difficult to interfere.
  Use of niche tools for spread of harmful content.

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

MISCELLANEOUS

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

Provided Use-cases selected from EU-HYBNET project database.

4.3.2 Identify And Safeguarding Vulnerable Individuals

NAME OF THE IDEA

Identify and safeguarding vulnerable individuals

DESCRIPTION OF THE IDEA

Promotion of extremism and violence in different communication channels has variety of purposes. One of them is recruiting and incorporation of new followers. Widening of extremism minded community is mainly made targeting vulnerable individuals. There were significant efforts made to identify and analyse the underlying drivers to violent extremism offline. Online environment provided new possibilities for such activities and experience from kinetic environment were not utilised, so extremist propagandists and recruiters continue to hunt for vulnerable individuals. Vulnerability is considered as lack of individual resilience to be involved or recruited into violent extremism. Lack of resilience can be related to distrust on society / institutions approaches or actions in respect to certain phenome. Such distrust can be reinforced by other vulnerable groups, despite the phenomena in target. Groups of distrusted individuals are formed, leading to further segregation, making resilience weaker.

The idea would be to have different methodological / technological solutions (e.g.: algorithms, redirections to less harmful content, etc.) that would put additional thresholds for people accessing content supporting extremism and violence.

REFERENCE TO CAPABILITY GAP/NEED

- **Describe the use of the solution in reference to the gaps/need**
  It will limit widening of extremism and violence involvement in online environment.
- **Applicable JRC domains as stated by the gaps/needs:**
  Cyber, culture, social, legal, intelligence, information.
- **Applicable core theme(s) as stated by the gap/need:**
  - Information and Strategic Communications. Links also to "Resilient Civilians, Local Level and National Administration"

TYPE OF SOLUTION

- **Technical**
  - Software tooling
  - Algorithms
- **Social/Human**
  - Content support
- **Organizational/Process**
  - Methodological solutions

PRACTITIONERS

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

STATE OF THE ART

- **Indication of current Technology Readiness Level (TRL 1-9 index)**:
  There are initial solutions at high TRL level (8-9).
- **In which stage is the solution (research, technology, available innovation, proven innovation):**

Some solutions are available, still actions to identify vulnerable individuals and harmful content, better understanding of algorithms, alternative content needs to be developed further.

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

- **Expected time to market.**
  Difficult to identify.

DESCRIPTION OF USE CASE(S)

There are some separate initiatives, that can be listed as prospects for wide adoption and improvement:

- The Redirect Method (The Redirect Method - Moonshot (moonshotteam.com)) is an open-source methodology that uses targeted advertising to connect people searching online for harmful content with constructive alternative messages. Piloted by Jigsaw and Moonshot in 2016 and subsequently deployed internationally by Moonshot in partnership with tech companies, governments and grassroots organizations, it uses pre-existing content made by communities across the globe, including content not created for the explicit purpose of countering harm, to challenge narratives which support violent extremism, violent misogyny, disinformation and other online harms.

IMPACT ON COUNTERING HYBRID THREATS

- **Describe how the idea contributes to countering hybrid threats; relate this to one or more capability gaps and needs.**
  Restrains diffusion of extremism and violence content and reduce involvement of vulnerable individuals.

- **Resilience/defensive/offensive**
  Increase resilience to violence.

ENABLING TECHNOLOGY

- **Which technologies are critical in fielding the idea?**
- Algorithms
- Content monitoring

RESTRICTIONS FOR USE

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

COSTS

- **Indication of costs**:
  Not possible to estimate now.

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

COUNTERMEASURES

- **Are there any potential countermeasures that could degrade the effectiveness of the solution**?
  Extremism and violence move to new safer platforms, making it difficult to interfere.
  Use of niche tools for spread of harmful content.

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

MISCELLANEOUS

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

5. CONCLUSIONS

5.1 SUMMARY

This Deliverable has served to provide ideas and innovations for countering different dimensions of Hybrid Threats.

This Deliverable has served to provide ideas and innovations for countering different dimensions of Hybrid Threats.

With respect to the first Core Theme studied, the **future trends of hybrid threats**, the first primary context studied is the Geopolitical heavyweight of domestic policy. In order to support the competitiveness of the European Companies, End to End Supply Chain Visibility Labels are proposed to improve transparency in complex supply chain networks, that will, in turn, help consumers make informative decisions. Additionally, Multi-Stage Supply Chain Disruption Mitigation Strategies and Digital Twins for Supply Chain Resilience are proposed. These will help address the problems of Supply disruption on key strategic raw materials and of EU dependence on non-EU strategic supply and value chains. The ideas presented can be especially relevant for pan-European security practitioners, as they need to be in a position to offer to European citizens information about the products' origin, so the latter can support EU initiatives, EU policies, EU alliances, and most importantly, EU companies.

For the Digital Escalation and Ai-Based Exploitation, actions need to be taken towards an agreement on a common approach by the Member States, taking under consideration the criticality of the decisions taken by AI and their performance in the tasks. Digital connected security is proposed in response to hybrid tactics, in order to significantly accelerate the speed at which messages can be examined and classified automatically and with human knowledge. In addition, validation and verification of Artificial Intelligence or self-learning systems is proposed for protection against hybrid attackers, who are able to corrupt the data used for AI-assisted decision-making, hacking outcomes to their advantage.

The Rise of Populism is the last primary context studied in this core theme. The establishment and reinforcement of political education of democratic values is proposed to improve society's resilience to offensive populist influences. Also, installation of rules for mandatory declarations is proposed to provide the audience the opportunity to evaluate the manner in which the line of argument is structured. These will serve to improve the society's resilience to populist influences, as well as to support European practitioners, especially the ones having a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats.

Cyber and Future Technologies is the second core theme studied. For Space Interference and Counterspace Weapons, a holistic framework for European Ground Segment facilities is proposed that is able to confront complex cyber and physical threats by covering all the macrostages of crisis management. Protecting Ground segments can help European practitioners protect Europe from the exploitation of military advantages in space.

The Development of a Proactive Defensive Framework based on ML and cloud is proposed to increase societal resilience against Offensive Cyber Capabilities; this also serves as a defensive capability against hybrid state actors using new technologies. A fully automated incident response solution based on CT

Intelligence is also proposed to maximize an entity's ability to investigate all cyber-alerts and uncover hidden threats.

For the primary context of Disruptive Innovations, Deepfake detection systems are proposed to improve preparedness and are expected to improve societal resilience against disinformation hybrid campaigns by countering strategic disadvantages and vulnerabilities. Additionally, Counter-Unmanned Aircraft systems are proposed for protecting critical infrastructure on a civilian landscape, but also for supporting military operations.

For the core theme of **Resilient Civilians, Local level and administration** and the primary context of Exploitation of Political Cleavages, detection of Disinformation Delivery Proxy Actors is proposed in order to improve EU and Member States' capabilities to tackle hostile information manipulations in a more coordinated manner, and to strengthen the protection of democracy infrastructure against exploitation of political cleavages and foreign interference. Furthermore, the development of a real time Rapid Alert System on Disinformation is proposed for better situational awareness among the EU and the Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels.
Regarding the Exploitation of Critical Infrastructure Weaknesses and Economic Dependencies, a methodology and software for assessment of impact and risk of critical infrastructures in a complex interdependent scenario is proposed. Understanding dependencies of Critical Infrastructures will help identify measures to reduce their impact, including diversifying production and supply chains, ensuring strategic stockpiling and promoting production and investment in the EU. In addition, the Resilience Tool is proposed, that allows indicator-based assessment of the resilience of infrastructures, cities, communities, states and even countries to plan, prepare and absorb, recover and learn from going through such hybrid attacks.

For the Exploitation or Investment in Companies by foreign actors a Crawler for Correlation of Screened FDI with Suspicious Financial Activity is proposed. In that way, the Member States can 'take into account whether the investor has been involved in activities affecting security or public order or whether there is a serious risk of the investor being engaged in illegal or criminal activities ' and perform the assessment on a case-by-case basis.

For the last core theme, **Information and Strategic Communications** and the primary context of Information Manipulation with the aim of destabilization, increasing capabilities to systematically assess information validity throughout the lifecycle are proposed. These include a set of tools, while structured information on narrative, targets and other components of the disinformation are also to be included in the information validity verification workflow. Furthermore, Crowdsourced verification systems of fake news to counter disinformation in encrypted messaging applications are also proposed. This can contribute to counter the problem in a long term perspective, and identify actors that are involved in destabilisation activities and building response means. The DDS-Alpha tool of EEAS is also proposed, a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan. To achieve common situational awareness within reasonable delays, EEAS proposes a set of mutually reinforcing elements from standards to tools, which will overcome this information exchange problem and pave the way for an evidence-based development and application of solutions.

To counter Foreign Interference in key Information Institutions, an Integrated Monitoring System Against Malware-Based Cyber Operations is proposed to enable more rapid Alert-exchanges between N-CERT-s, CERT-EU, mil CERT and private companies, especially those who provide vital services, critical infrastructure protection and/or important informational services to increase the speed of early warning and EU-wide coordinated action. Also, an Integrated Monitoring System Against Cyber-enabled Information Operations is proposed, with the aim of enabling more rapid identification and Alert-exchanges about cyber-enabled information operations.

For the primary context of Promoted Ideological Extremism and Violence, Collection and sentiment analysis of targeted communication is proposed to limit widening of extremism and violence involvement in the online environment. Identifying and safeguarding vulnerable individuals and relative initiatives are also proposed.

5.2 FUTURE WORK

This work summarises the results of H2020 EU-HYBNET Task 3.2 "Technology and Innovations Watch" for the project's second cycle and serves to identify innovations and ideas for countering different dimensions of hybrid threats. As in the previous cycle 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 attribute hybrid threats timely across all domains. This solution would also require advanced technologies and tools, and some promising innovations have been included in this deliverable. Most importantly, interdepartmental and international cooperation and alignment would be a precondition.

The present work will be used by EU-HYBNET T3.1 "Definition of Target Areas for Improvements and Innovations" and Workpackage2 "Gaps and Needs of European Actors against Hybrid Threats"/ T2.3 "Training and Exercises Scenario Development" and T2.4 "Training and Exercises for Needs and Gap. Also, it will support the work of WP4 "Recommendations for Innovations Uptake and Standardization" on mapping on the EU procurement landscape, creation of strategy for innovation uptake and industrialization, and compiling recommendations for standardization.

The mapping of innovations to specific gaps and needs of pan-European practitioners and other relevant actors will continue for the next three years. The Border security dimension of hybrid threats is expected to be more emphasized in the next cycle.

ANNEX I. GLOSSARY AND ACRONYMS

Table 2 Glossary and Acronyms

Term	Definition / Description
EU-HYBNET	
Big Data	Big data is the term used for large amounts of data collected from areas such as the Internet, mobile communications, the financial industry and healthcare, that are stored, processed and evaluated using special solutions. Therefore, usually a program is used to detect rules or anomalies within the data. [54]
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.[55]
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
Satways	Satways Ltd

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

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

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 Framework on Countering Hybrid Threats, Join (2016) 18 Final, European Commission

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

[3] European Commission, 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] European Commission, Press Corner, 'Global Gateway: up to €300 billion for the European Union's strategy to boost sustainable links around the world' December 1st, 2021

[6] European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation, Shaping Europe's digital future, European Commission

[7] European Chips Act, Shaping Europe's Digital Future, European Commission

[8] Proposal for a Regulation Of The European Parliament And Of The Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), European Commission, 2022/0032 (COD)

[9] The European Label of Governance Excellence (ELoGE), Council of Europe

[10] European Committee On Local And Regional Democracy (Cdlr), Council of Europe

[11] Labels and Markings, Product Requirements, Your Europe, European Union

[12] European Commission, Food Labelling, Food Labelling Information System (FLIS)

[13] US Department of Agriculture, Agricultural marketing service, USDA

[14] Made in Europe, Manufacturing Partnership in Horizon Europe, European Commission, European Factories of the Future Reserach Association

[15] The Growing Emphasis on End-to-End Supply Chain Visibility, Logmore

[16] Verwijmeren, M., What Is End-to-End Supply Chain Visibility? Supply Chain News 24/7, March 2022.

[17] Supply Chain Visibility Software, Supply Chain Management Software, G2 webpage, accessed May 2022.

[18] 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.

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

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

[21] Resilink, company webpage

[22] Thiele, R. Artificial Intelligence –A key enabler of hybrid warfare, Hybrid CoE Working paper 6

[23] Gonçalves, Carlos Pedro, Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats, Cyberspace, 2019.

[24] EU Space Programme, Defence Industry and Space, European Commision

[25] 7Shield H2020 Project Webpage

[26] Wong, Ernest & Hutton, Katherine & Gagnon, Ryan. (2018). Thinking Outside-the-Box for Cyber Defense: Introducing an Innovation Framework for the 21st Century.

[27] ENISA, Foresight Challenges

[28] Best Starup, TOP ISRAELI STARTUPS & COMPANIES

[29] Burt,T., New Steps to Combat Disinformation, Microsoft on the Issues, 2020

[30] Using AI to Detect Seemingly Perfect Deep-Fake Videos, Human-Centered Artificial Intelligence, Stanford University

[31] Counter Unmanned Aerial Systems (C-UAS) , Northrop Grumman

[32] Counter-Unmanned Aerial Systems (UAS), General Dynamics Mission Systems

[33] Counter Unmanned Aircraft Systems: EagleShield, Thales

[34] Loik, R. and Madeira, V. (2021). European Union Strategy and Capabilities to Counter Hostile Influence Operations. In: H. Mölder; V. Sazonov; A. Chochia; T. Kerikmäe (Ed.). The Russian Federation in Global Knowledge Warfare. Influence Operations in Europe and Its Neighbourhood. Switzerland: Springer Nature. (Contributions to International Relations CIR), pp. 247–264.

[35] JOIN(2018) 36 final. Brussels 5.12.2018.

[36] Pamment, J. (2020). The EU's Role in Fighting Disinformation: Taking Back the Initiative. Washington, D.C: Carnegie Endowment for International Peace

[37] Weilan Suoa, Jin Zhangb, Xiaolei Suna, Risk assessment of critical infrastructures in a complex interdependent

scenario: A four-stage hybrid decision support approach, Safety Science, 120, 692-705 (2019).

[38] Kostaridis, A., et al, CIRP: A Multi-Hazard Impact Assessment Software for Critical Infrastructures, 2nd International workshop on Modelling of Physical, Economic and Social Systems for Resilience Assessment

[39] Regulation (Eu) 2019/452 Of The European Parliament And Of The Council, Official Journal of the European Union, L79 I/1, 21.03.2019

[40] Ghiretti, F., How To Protect Europe From Risky Foreign Direct Investment, Texas National Security Review, January 2022

[41] Official website of the Australian Government, Approval for Foreign Investment

[42] Official website of the Government of Canada, Justice Laws Website

[43] European Commission, Enforcement and Protection, Investment Screening, official website

[44] Modrall, J., Foreign Investment Screening: European Union, Norton Rose Fulbright, online article, November 2021.

[45] Stormy-Annika Mildner. Claudia Schmucker, Policy Brief, 'Investment Screening: Protectionism and Industrial Policy? Or Justified Policy Tool to Protect National Security?'

[46] Ghiretti, F., Screening foreign investment in the EU – the first year, Merics Mercator Institute for China Studies, October 2021

[47] Vasuki Shastry, How countries can regulate investment screening, Chatham House, April 2022

[48] Narrative Definition & Meaning - Merriam-Webster

[49] Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. Terrorism and Political Violence, 31(6), 1242-1254. https://doi.org/10.1080/09546553.2017.1339695 ↩

[50] Reis, J., Melo, P. D. F., Garimella, K., & Benevenuto, F. (2020). Detecting Misinformation on WhatsApp without Breaking Encryption. arXiv preprint arXiv:2006.02471. ↩

[51] Facebook did not act on own evidence of algorithm-driven extremism | E&T Magazine (theiet.org)

[52] The Bergen Plan of Action (squarespace.com)

[53] Is Big Tech Ready to Tackle Extremism? The Bergen Plan of Action - VOX - Pol (voxpol.eu)